Cyber Security Landscape in India

IN New Delhi
<table>
<thead>
<tr>
<th>Section</th>
<th>Slide Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>4</td>
</tr>
<tr>
<td>Research Methodology</td>
<td>8</td>
</tr>
<tr>
<td>Trends in India</td>
<td>10</td>
</tr>
<tr>
<td>Areas of vulnerability</td>
<td>18</td>
</tr>
<tr>
<td>Regulations in India</td>
<td>22</td>
</tr>
<tr>
<td>Mega trends</td>
<td>35</td>
</tr>
<tr>
<td>The ecosystem</td>
<td>42</td>
</tr>
<tr>
<td>Emerging players</td>
<td>47</td>
</tr>
<tr>
<td>Market opportunity</td>
<td>56</td>
</tr>
<tr>
<td>Section</td>
<td>Slide Number</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Network Security</td>
<td>65</td>
</tr>
<tr>
<td>Endpoint Security</td>
<td>76</td>
</tr>
<tr>
<td>Data Security</td>
<td>87</td>
</tr>
<tr>
<td>Managed Security Services</td>
<td>97</td>
</tr>
<tr>
<td>Advanced Threat Protection</td>
<td>107</td>
</tr>
<tr>
<td>Threats in verticals</td>
<td>114</td>
</tr>
<tr>
<td>Maturity in India</td>
<td>122</td>
</tr>
<tr>
<td>Key elements to market entry</td>
<td>125</td>
</tr>
<tr>
<td>The Indian Landscape</td>
<td>131</td>
</tr>
</tbody>
</table>
Executive Summary
The Indian cyber security market is valued at US $717.18 Million as on 2015 and is likely to be US $1,333.65 million by the end of 2020, growing at a CAGR of 13.21%.

With India experiencing 64% rise in cybercrime registration from 2010-2014 and ranking 5th in the world in terms of DNS hijacks, efforts are on from the Government’s end and enterprises in combating the threat.

Much aware of the ill effects of the massive “Digital India Initiative”, the Government needs to be well prepared to fight cybercrime with robust regulations, legal frameworks, and implementable laws.

Banking and financial services, IT/ ITes drive the Indian cyber security market. Fintech innovation in conjunction with digital business disrupts the traditional security approach for the financial sector.

Managed security services grow at a faster pace as compared to security appliances growth, as enterprises have realized that having the best-of-breed security products is not enough, rather it needs continuous monitoring and assessment of threats, prepared to contain the security attack.

The anti-virus market looks to shrink whereas network and endpoint security is expected to have a healthy growth among enterprises.

Skill development remains an agenda, both for the Government and private enterprises, which aim to have 5,00,000 Cybersecurity experts in India within the next five years.
Executive Summary (1/2)

• Over the last few years with the advancement of technology, the growth of cyber-attacks has escalated multiple folds. Be it the attack on Sony Pictures, Target Corporation or eBay, both companies and customers were at the receiving end. While, the customers lost their personal information to the outer world, the companies had to compromise on their reputation.

• This scene is no different in the Indian context. Rather few could rightly argue that cyber-crime in India is far higher than the global average. A research conducted by University of Maryland points out, India along with China, Russia, Saudi Arabia and South Korea is among the most vulnerable to cyber-attacks. This could easily be validated from the fact that several Indian companies and Government entities were under the constant threat of cyber miscreants with financial motives. The Indira Gandhi International Airport, New Delhi website was hacked which resulted in check-in counters being non-operational for several hours. In addition to this, websites of ONGC Corporation, BSNL and TRAI were also attacked few years back.

• We all should agree that constant efforts are being made collectively by the Indian Government, the product & service companies and the regulating bodies. The Central Government has been working hard to improve on the existing cyber regulations however, face challenges in formalising them into laws. Currently, there is limited cyber security policy for the critical infrastructure like Defence, Space, Energy and Telecom.

• Co-ordination between the security regulatory bodies like National Technical Research Organization (NTRO) and the Ministry of Communications and Information Technology is less. These need to be better addressed to make Prime Minister Narendra Modi’s vision of “Digital India” a success by scale and means.
Executive Summary (2/2)

• However, in spite of a poor legal cyber security infrastructure, there remains a bigger scope for the Security companies to benefit from the vibrant Indian market. Currently, standing at USD 717.18 million, the cyber security market in India is expected to value at USD 1333.65 million by the end of 2020. Managed Security Services (MSS) would expect CAGR 18%+ till 2020 while Network and End-point Security would hover around CAGR 11%. This offers enough scope of growth for Security product and service companies to better align their revenue streams. The overall Indian cyber security space is being dominated by the foreign players, the Indian companies partner as System Integrators (SIs), Managed Security Service Providers or Distributers.

• From the demand perspective, certainly the awareness has been high, especially among CISOs. Companies intend to increase their security budgets (71% in 2015), with end-users looking to use advanced security suites. Security Analytics and Identity & Access Management (IAM) is currently the most popular cloud based tool. Customers tend to understand that continuous monitoring and assessment of threats is of large importance, thereby pushing for the need of MSS.

• The cyber security community in India remains highly optimistic and expects high growth. Start-ups along with the enterprise companies have started to make a mark in the security space boosted by the Government’s “Start-up India” initiative. The Government has been trying hard to improve on the “Ease of Doing Business” in the country through constructive reforms. This as a whole would certainly improve on positioning India as Cyber Security Destination.
Research Methodology
Research Framework: Market Assessment

Approach

Supply Side Analysis: Key interviews with all major players and channel ecosystem.

- Industry Players
- Influencers
- Domain Experts

Demand Side Analysis: Interviews conducted across the enterprise ecosystem to map the need, if required.

- Actual Users
- Influencers
- Customers

Economic / Market
Identify the key economic and market variables likely to influence the Cyber Security industry in India.

Technological
Identify the key technology variables likely to influence the market, including disruptive technologies.

Regulatory
Identify the key regulatory issues that are likely to influence the industry.

Ecosystem
Understand the overall industry ecosystem, key influencers, and the business value chain.

Research
Understand competitive positioning, strategies, market shares, cost structure, and future plans.

Focused Verticals:
BFSI, Healthcare, Government, Telecom, Oil & Gas, Media
Trends in India
Cyber Security in India: Facts and Measures

**Facts**

- **64%** Cyber crimes registration increased at a CAGR of 64% from 2010 to 2014 under the IT Act.
- **54,483** Number of Cyber Security incidents reported in 2015.
- **5th** India ranks 5th in terms of a country with the largest number of DNS hijacks.
- **China** Chinese hackers remain a potential challenge to India’s cyber security world.
- **Mobile** Mobile Devices remain the most sought-after medium for security incidents.

**Measures**

- **Building a 500,000 skilled workforce in cyber security in the next five years**.
- **Start-ups expected in the next few years** 1,000.
- **Microsoft (MSFT)** opened the India Cyber Security Engagement Centre in collaboration with the Indian Government for a better security focus.
- **CAGR increase in information security budgets over the last five years** 25%.

Rise of Connected Devices in India
There will be 4 Billion connected devices by 2025

<table>
<thead>
<tr>
<th>Devices</th>
<th>Data</th>
<th>Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 Billion connected devices by 2025</td>
<td>10 exabytes monthly traffic by 2020</td>
<td>500 Million mobile broadband connections by 2025</td>
</tr>
<tr>
<td>2.5 Billion mobile devices by 2025</td>
<td>38 exabytes a month mobile data traffic by 2020</td>
<td>1.36 Billion cellular connections by 2025</td>
</tr>
<tr>
<td>3 connected devices for every user by 2025</td>
<td>18 mbps average Internet speed by 2020</td>
<td>310 Million 3G broadband connections by 2025</td>
</tr>
</tbody>
</table>

Source: IDC–EMC Study; Ericsson; Cisco; Frost & Sullivan
Cyber security in India has evolved in the past few years and has gained huge impetus due to the Digital India initiative, e-Commerce, and mobile payments. Prime Minister Narendra Modi has identified cyber security as one of the major development areas.

India has been known to report the third highest Ransomware in Asia. Statistics say, Indian enterprises, on an average, are attacked seven times in an hour.

### Impact of cyber security breaches in an enterprise

<table>
<thead>
<tr>
<th>Impact</th>
<th>Impact Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Losses</td>
<td>Very High</td>
</tr>
<tr>
<td>Theft of intellectual property / sensitive information</td>
<td>High</td>
</tr>
<tr>
<td>Brand / reputation tarnished</td>
<td>Low</td>
</tr>
</tbody>
</table>

Unsettle business processes        
Non compliance to regulations and laws       
Loss of customers
Cyber Security is a Vital Factor in the Connected World

The connected world, today, faces the challenges of increasingly complex and evolving cyber security issues in the form of unauthorized network access, phishing emails or malicious cyber attacks. Securing the cyber space is the need of the hour for all – Government, enterprises, and individuals.
Global Enterprises are Investing in their Security Infrastructure

| Global enterprises are investing in security to better safeguard their networks against evolving threats |
| Have deployed an overall information security architecture to combat emerging threats |
| Invests in information security training and awareness programs for their employees, third-party vendors, and customers |
| Periodically conduct threat assessments and plan risk mitigation actions |
| Invested and deployed cyber security baselines and standards for third-party vendors |
| Have a dedicated security officer; Chief Information Security Officer (CISO), and personnel in charge of cyber security |
| Conduct active monitoring and analysis using security intelligence |

Key Global Trends in Cyber Security

- Internet of Things (IoT) is here but enterprises are yet to address the security associated
- Increased deployment of cloud, mobile, and social solutions makes security important for enterprises
- Cyber security is a C-level priority
- There is lack of skilled security professionals
- Ransomware, Point of Sales (POS) attacks are on the rise
India Showcasing Better Preparedness toward Cyber Security

India observing a CAGR of 25% in security budgets across organizations in India over the last five years

Security Budgets increased by 71% in 2015

Increased R&D Focus
FireEye plans to invest US $50 Million on its India R&D center until 2018

The Indian Market Trend
• Security Analytics and Identity and Access Management (IAM) are considered the most popular cloud-based tools.
• Organizations are deploying Big Data Analytics to manage insider threats. One of the surveys conducted on cyber security reveals that more than a quarter of the security executives plan to employ Big Data Analytics to improve security in the next 12 months.
• A vast majority of organizations have adopted a security framework, or at most cases an amalgam of frameworks to protect their organizational security. These, in a nutshell, help these organizations identify, detect, and migrate security incidents, thereby gauging the maturity of their cyber security practice and communicate better; both internally and externally.

India-UAE Cyber Security Deal
• Deal Signed in March, 2016
• Objective: Combat cybercrime through a handshake coordination and exchange of information in relation with cybercrime and training during cyber investigation

Setting up a Cyber Monitoring Center in Bangalore
Has opened a cyber center in Bangalore to tackle complex security challenges
# A Robust Regulatory Framework is Required to Address Cyber Security

<table>
<thead>
<tr>
<th>Synergizing Government agencies and private players</th>
<th>The Government collaborates with various vendors to implement various aspects of Digital India and Smart City. In order to ensure successful implementation, risks need to be understood, monitored, and mitigated. Stakeholders should jointly explore avenues to defend cyber risks.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrating security from planning to implementation</td>
<td>Digital India and Smart City initiatives will enhance the levels of digitization, whereby the Government will engage with its citizens through online portals, mobile devices, apps, and social media. This will create an ecosystem involving various technologies and devices to communicate with each. To secure such an environment, the entire ecosystem needs to rise to the concerns right from the planning phase to the actual implementation phase.</td>
</tr>
<tr>
<td>Developing a regulatory framework</td>
<td>Cyber security should be addressed holistically by the way of developing robust regulatory framework and governance. The policy should articulate to provide privacy protection, data protection, cyber law, e-Governance, e-Commerce regulations, and IT disaster recovery.</td>
</tr>
<tr>
<td>Conducting security awareness programs</td>
<td>Public-private partnership is vital in creating security awareness initiatives. This should include best practices in cyber security, adoption of advanced data privacy technologies etc. Also, professionally trained workforce will have an edge over the cyber threat groups.</td>
</tr>
<tr>
<td>Detecting and monitoring real-time breaches</td>
<td>Adopting security analytics will enable the ecosystem to mature from risk identification to risk analysis and finally risk intelligence. Analytics-driven security monitoring will ensure real-time monitoring of the network traffic, consolidating, and coordinating incidents from applications and network logs.</td>
</tr>
<tr>
<td>Role of CISOs</td>
<td>IT leaders play a pivotal role in advising the Government on various aspects of cyber security and also in developing the regulatory framework. Their expertise will enable in developing the right skills and a unified security framework across the country.</td>
</tr>
</tbody>
</table>
Areas of Vulnerability
Personnel in the organization that are prone to cyber attacks

Users are the weakest link in the cyber defense system within an organization; India is no different. Negligence and ignorance of these personnel enable cyber criminals to leverage social engineering to extract critical and sensitive information. The key elements of ignorance are:

- Inadequately secured digital devices
- Sharing / insecurely storing access credentials
- Willingness to share personal data with strangers

Systems that are prone to cyber attacks

Intruders target diverse systems within an organization to achieve their objective of implanting potent malware in vulnerable organization systems. The diverse range of systems that are being attacked increasingly are:

- Email and communication systems
- Social media
- Mobile phones
- POS systems at retail outlets.
- ATMs in banks
- Programmed assembly lines in a factory production system

People and IT Systems are Equally Prone to Cyber Threats
Cyber Criminals Target Diverse Systems to Implant Potent Malware (1/2)

1. Connected devices

With the IoT movement taking a positive move in India, there is tremendous increase in the wearables and other connected devices. Such a dense device-populated environment is paradise for cyber criminals. Once these devices connect with smartphones (in case of wearable) or a unprotected network (at home) enables hackers to access sensitive personal information for malicious purposes.

2. Employee systems

Payment system cyber attackers focus on theft and sale of usernames and passwords required for online transactions. These cyber criminals target the consumers directly, who are the owners of the required credentials as well as the weakest link in the online payment process. The former leverage both traditional theft methods (phishing attacks) as well innovative methods to steal debit and credit card credentials.

3. Online payment systems

Number of attacks continue to grow in an employee-owned system or a company-owned system in an insecure network, such as a hotel, airport or coffee shop. Organizations are in a continuous process to improve their security technologies, create effective policies, and remain vigilant to ensure that corporate network is not breached.

4. Cloud services

The high level of confidential company data shared on various cloud platforms and services attracts cybercriminals, competitors, and nations, who are willing to steal these sensitive information. These cloud-based organizations have to rely on the security architecture and controls of the hosting company.
Malware targeting hardware or firmware has reduced over time. These attacks are mostly from advanced nations and defense agencies, utilizing organized cyber crime syndicates. Hardware in a virtual machines environment could be targeted with various malware.

Application developers and customers in India face the continuous challenge of application vulnerabilities. Adobe Flash, Internet Explorer are the frequently attacked applications. Attacks on OS turns out to be very dangerous in an enterprise computing environment.

With the rise of connected car technology hitting India, automobile hardware systems are prone to cyber attacks. Smart highways, driverless cars would need a highly secured network to protect drivers and passengers from losing their lives. Software and hardware in a connected car should be able to connect to the external systems (such as traffic signals) in a secured way to prevent from any disaster.

Critical infrastructure attacks are more appealing to adversary nations rather than individual cyber criminals. Successful attacks on the critical infrastructure will impair the society and the nation as a whole. These attacks are selective and lesser in number as compared to others, and is more of a strategic act.
Regulations in India
Key Cyber Security Regulations in India

The Cyber Security Laws and e-Security as formulated by the Department of Electronics and Information Communication (DeitY), Ministry of Communications and IT, Government of India

A policy framework by the Department of Electronics and Information Technology (DeitY) with a purpose to protect public and private infrastructure from cyber attacks.

The 12th Five-year Plan looks to address six focus areas / initiatives: enabling legal framework; security policy, compliance, and assurance; security Research and Development (R&D), Security Incident: Early Warning and Response; Security Awareness, Skill Development, and Collaboration.

The IT (Amendment) Act, 2008 is a substantial addition to the existing India’s Information Technology Act, 2000. The amendment was created to address issues that the earlier IT Act, 2000 failed to cover.
# Objectives

1. To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT systems and transactions in cyberspace, and thereby enhance adoption of IT in all sectors of the economy.

2. To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology, and people).

3. To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem.

4. To enhance and create National and Sectoral level, 24x7 mechanisms for obtaining strategic information regarding threats to Information and Communications Technology (ICT) infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective, response, and recovery actions.

5. To enhance the protection and resilience of the nation’s critical information infrastructure by operating a 24x7 National Critical Information Infrastructure Protection Center (NCIIPC) and mandating security practices related to the design, acquisition, development, use, and operation of information resources.

6. To develop suitable indigenous security technologies through frontier technology research, solution-oriented research, proof of concept, pilot development, transition, diffusion, and commercialization leading to widespread deployment of secure ICT products/processes in general; specifically, for addressing National Security requirements.

7. To improve visibility of the integrity of ICT products and services by establishing infrastructure for testing and validation of security of such products.
<table>
<thead>
<tr>
<th></th>
<th>Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>To create a workforce of 500,000 professionals skilled in cyber security in the next five years through capacity building, skill development, and training.</td>
</tr>
<tr>
<td>9</td>
<td>To provide fiscal benefits to businesses for adoption of standard security practices and processes.</td>
</tr>
<tr>
<td>10</td>
<td>To enable protection of information while in process, handling, storage, and transit so as to safeguard the privacy of citizens’ data and for reducing economic losses due to cyber crime or data theft.</td>
</tr>
<tr>
<td>11</td>
<td>To enable effective prevention, investigation, and prosecution of cybercrime and enhancement of law enforcement capabilities through appropriate legislative intervention.</td>
</tr>
<tr>
<td>12</td>
<td>To create a culture of cyber security and privacy enabling responsible user behavior and actions through an effective communication and promotion strategy.</td>
</tr>
<tr>
<td>13</td>
<td>To develop effective public-private partnerships and collaborative engagements through technical and operational cooperation and contribution for enhancing the security of cyberspace.</td>
</tr>
<tr>
<td>14</td>
<td>To enhance global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace.</td>
</tr>
</tbody>
</table>
## Key Priorities for each of the “12th Five-year Plan” focus areas

<table>
<thead>
<tr>
<th></th>
<th>Enabling Legal Framework: Upgrade / development of a robust and dynamic legal framework to enable cyber security and address newer cybercrimes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Security Policy, Compliance, and Assurance: Focus on creating an enabling mechanism for achieving conformance with provisions of the IT Act, statutes, and other policy initiatives of the Government and regulatory bodies.</td>
</tr>
<tr>
<td>3</td>
<td>Cyber Security Research and Development: Carry out innovative R&amp;D with focus on basic research, technology development, and demonstration, setting up test-beds, transition, diffusion, and commercialization leading to widespread deployment.</td>
</tr>
<tr>
<td>4</td>
<td>Security Incident — Early Warning and Response: Strengthening National Cyber Alert System for rapid identification and response to security incidents and information exchange to all desired elements that are critical for cyber security, to reduce the risk of cyber threat and resultant effects.</td>
</tr>
<tr>
<td>5</td>
<td>Security Awareness, Skill Development, and Training: Establish cyber security capacity building and training mechanisms for developing a strong and dynamic cyber security skilled work force and a cyber-vigilant society.</td>
</tr>
<tr>
<td>6</td>
<td>Collaboration: Promote shared understanding and leverage relationships for furthering the cause of security of cyber space.</td>
</tr>
</tbody>
</table>
The IT (Amendment) Act, 2008 is a substantial addition to the India’s existing IT Act, 2000 that was passed by the Indian Parliament in October 2008 and came into action the following year. The IT Act, 2000 is an Act of the Indian Parliament and is the primary law in India, which deals with cybercrime and electronic commerce.

Mentioned below are the additions that were made to the existing Information Technology Act, 2000:

1. **Electronic signatures introduced:** With the passage of the IT (Amendment) Act, 2008, India grew to become technologically neutral toward the adoption of electronic signatures as a legally valid mode of executing signatures. The introduction of digital signatures as one of the modes of signatures and other new forms of electronic signatures covers biometrics. This is a positive change as India consists of different segments of people and all may not be technologically adept to understand and use digital signatures. Hence, allowing forms of authentication that are simple to use (like retina scanning) could be useful in the effective implementation of the Act.

2. **Critique on amended section 43 of IT Act:** The amended Act provides the distinction between “contravention” and “offence” by the introduction of the element of mens rea for an offence (section 43 for contraventions and section 66 of the Act for offences). It is pertinent to note that no ceiling limit for compensation is prescribed under section 43 of the Amended Act, 2008, which was INR 1 Crore in the IT Act. The removal of the ceiling limit can be misused or abused, particularly seen in instances where a company files frivolous claims against its ex-employees who may have joined a competitor firm without breaching its employment contract.
<table>
<thead>
<tr>
<th></th>
<th>Additions to the Act</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td><strong>Corporate responsibility introduced in Section 43A:</strong> The corporate responsibility that is associated with data protection were incorporated in Section 43A in the amended Act, 2000 whereby corporate bodies handling sensitive data in a computer resource are under an obligation to ensure adoption of “reasonable security practices” to maintain its secrecy, failing which they may be liable to pay for the damages.</td>
</tr>
<tr>
<td>4</td>
<td><strong>Important Definitions Added:</strong> Two important definitions were added to the IT Act through IT Amendment Act, 2008 — Communication Device and Intermediary</td>
</tr>
<tr>
<td>5</td>
<td><strong>Legal validity of electronic documents re-emphasized:</strong> The two new sections Section 7A and 10A in the amended Act reinforce the equivalence of paper-based documents to electronic documents.</td>
</tr>
<tr>
<td>6</td>
<td><strong>Critique on Power of Controller under the amended Act:</strong> Section 28 of the Act provides that the Controller or any authorized officer shall investigate “any contravention of the provisions of this Act, rules or regulations made thereunder”.</td>
</tr>
<tr>
<td>7</td>
<td><strong>The Role of Adjudicating officers under the amended Act:</strong> The Adjudicating officer “power under the amended Act in Section 46 (1A) is limited to decide claims where claim for injury or damage does not exceed INR 5 Crore. Beyond INR 5 Crore, the jurisdiction shall now vest with competent court.</td>
</tr>
<tr>
<td>8</td>
<td><strong>Composition of Cyber Appellate Tribunal (CAT):</strong> The amended Act has changed the composition of the Cyber Appellate Tribunal. The presiding officer alone would earlier constitute the CAT, which provision has now been amended.</td>
</tr>
</tbody>
</table>
### Additions to the Act

<table>
<thead>
<tr>
<th>9</th>
<th><strong>New cybercrimes as offences under amended Act:</strong> Many cybercrimes for which no express provisions existed in the IT Act, 2000 now stand included by the IT (Amendment) Act, 2008.</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td><strong>Section 67C to play a significant role in cyber crime prosecution:</strong> The Section 67C brings a significant change in the IT Act, 2000. This section suggests that intermediaries shall be bound to preserve and retain such information as may be prescribed by the Central Government and for such duration and format as it may prescribe.</td>
</tr>
<tr>
<td>11</td>
<td><strong>Section 69-Power of the controller to intercept amended:</strong> Section 69 that deals with power of Controller to intercept information being transmitted through a computer resource is amended. In fact, the power vests now with the Government that empowers it to appoint for reasons in writing, any agency to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource.</td>
</tr>
<tr>
<td>12</td>
<td><strong>Power to block unlawful websites should be exercised with caution:</strong> The Section 69A in the IT Amended Act gives power to the Central Government or any authorized officer to direct any agency or intermediary to block websites in special circumstances as applicable in Section 69.</td>
</tr>
<tr>
<td>13</td>
<td><strong>Section 69B added to confer Power to collect, monitor traffic data:</strong> This amendment confers on the Central Government the power to appoint any agency to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource in order to enhance its cyber security and for identification, analysis, and prevention of intrusion or spread of computer contaminant in the country.</td>
</tr>
<tr>
<td>14</td>
<td><strong>Significance of the term “Critical Information Infrastructure”:</strong> In explanation to Section 70 of the Act, defines what actually is “Critical Information Infrastructure”.</td>
</tr>
</tbody>
</table>
## Additions to the Act

<table>
<thead>
<tr>
<th></th>
<th><strong>Important clarifications on the Act’s application and effect:</strong> By virtue of Section 77 in the Amended Act, a clarification was made that awarding of compensation, penalty imposed or confiscation made under this Act shall not prevent the award of compensation, or imposition of any other penalty or punishment under any law for the time being in force.</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td><strong>The combined effect of Section 77 and 77B:</strong> The combined effect of Section 77 and 77B suggests that once a cybercriminal is arrested by the police, in most cases, he has to be released on bail as a matter of right, by the police.</td>
</tr>
<tr>
<td>16</td>
<td><strong>Combined effect of Section 78 &amp; 80:</strong> The Section 78 of the Amended Act refers to conferring power to investigate offences under the Act from the DSP to Inspector level. The Section 80 has been amended and power to enter and search in a public place is now vested in any police officer not below the rank of the inspector or any authorized officer of central or state government.</td>
</tr>
<tr>
<td>17</td>
<td><strong>Liability of Intermediary amended:</strong> The Amended IT Act of Section 79 suggests that the intermediary shall not be liable for any third party information if it is only providing access to a communication system.</td>
</tr>
<tr>
<td>18</td>
<td><strong>Examiner of Electronic Evidence created:</strong> With amendments in 2008, Section 79A is added that empowers the Central Government to appoint any department or agency of Central or State Government as examiner of electronic evidence.</td>
</tr>
</tbody>
</table>
## Cyber Security Regulatory Bodies in India

<table>
<thead>
<tr>
<th>Bodies</th>
<th>Who they are and What role in play in securing the Indian Cyber world</th>
</tr>
</thead>
</table>
| **Data Security Council of India** | **About:** Data Security Council of India (DSCI) is an industry body on data protection in India, setup by NASSCOM (National Association for Software & Services Companies) committed to making the cyberspace safe, secure, and trusted by establishing best practices, standards, and initiatives in cyber security and privacy.  
**Objectives:**  
- Engage with governments, regulations, industry associations, and think tanks on policy matters through Public Advocacy and, thereby, establish though leadership.  
- Engage with stakeholders through various outreach initiatives.  
- Develop and maintain assurance ecosystem for validation of privacy and security practices implemented by organizations.  
- Increase India’s share in the global security product and services market.  
- Aim at developing Alternate Dispute Resolution. |
| **Cyber Appellate Tribunal** | **About:** Earlier known as the Cyber Regulations Appellate Tribunal (CRAT), the Tribunal started functioning in accordance with the provisions contained under Section 48(1) of the IT Act, 2000.  
**Objectives:**  
- Discharge its functions under the IT Act.  
- Regulate its own procedure including the place at which it has its sittings. |
## Cyber Security Regulatory Bodies in India

<table>
<thead>
<tr>
<th>Bodies</th>
<th>Who they are and What role in play in securing the Indian Cyber world</th>
</tr>
</thead>
</table>
| **Indian Computer Emergency Response Team** | About: CERT-In is the national nodal agency for responding to computer security incidents as and when they occur.  
Objectives:  
• Raise Security Awareness among Indian Cyber Community and to provide technical assistance and advise them to help them recover from computer security incidents.  
• Provides technical advice to System Administrators and users to respond to computer security incidents.  
• Enlightens its constituents about the security awareness and best practices for various systems, networks by publishing advisories, guidelines, and other technical documents. |
| **Controller of Certifying Authorities** | About: The IT Act provides for the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities and also to ensure that none of the provisions of the Act are violated.  
Objectives:  
• Provides the required legal sanctity to the digital signatures based on asymmetric cryptosystems.  
• Has the authority to license and regulate the working of Certifying Authorities.  
• Issues digital signature certificates for electronic authentication users.  
• Aims to promote the growth of e-Commerce and e-Governance through the use of digital signatures. |
# Cyber Security Regulatory Bodies in India

<table>
<thead>
<tr>
<th>Bodies</th>
<th>Who they are and What role in play in securing the Indian Cyber world</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>STQC</strong>&lt;br&gt;Government of India&lt;br&gt;Department of Electronics &amp; Information Technology&lt;br&gt;Standardisation Testing and Quality Certification Directorate&lt;br&gt;Standardisation Testing and Quality Certification (STQC)**</td>
<td><strong>About:</strong> STQC is an associated office of the DeitY, Government of India that provides quality assurance services in the area of Electronics and IT through countrywide network of laboratories and centers. It plays a major role in securing the IT infrastructure in India.&lt;br&gt;&lt;br&gt;<strong>Objectives:</strong>&lt;br&gt;• Ensure the security of IT infrastructure and software in India.&lt;br&gt;• Responsible for auditing and certifying public-private organizations involved in the area of Electronics, IT hardware, and software.</td>
</tr>
<tr>
<td><strong>National Critical Information Infrastructure Protection Centre (NCIIPC)</strong></td>
<td><strong>About:</strong> The National Critical Information Infrastructure Protection Centre (NCIIPC) roll out counter measures in cooperation with other security agencies and private corporate entities to protect the critical sectors.&lt;br&gt;&lt;br&gt;<strong>Objectives:</strong>&lt;br&gt;• Prevent cyber attacks against critical infrastructures (energy, transport, banking and finance, telecom, defence, space, etc.).&lt;br&gt;• Minimizing vulnerabilities to cyber-attacks.&lt;br&gt;• Minimize damage and recovery time from successful cyber-attacks.</td>
</tr>
</tbody>
</table>
### Analysis of Indian Cyber Security Regulations

#### The Background
- With the Government of India pushing for the successful implementation of the Digital India project, it is betting on higher use of mobile commerce, Internet banking, and online applications.
- This big initiative would surface the need for advanced cyber security laws and robust legal framework.

#### The Drawbacks
- Limited cyber security policy for the critical infrastructure like Defense and Aerospace.
- Policy lacks privacy provisions, civil liberties, and cyber security breach disclosure.
- Lacks cooperation between National Technical Research Organization (NTRO) and Ministry of Communications and Information Technology.
- Divergence between Defence and Intelligence Agency’s cyber security measures from the National Cyber Security Policy, 2013.

#### The Measures
- Better coordination and cooperation among regulatory bodies, thereby securing a tightened security framework.
- An improved electronic authentication policy in India.
- Formulating and passing the Electronic Delivery of services (EDS) Bill in the Indian parliament.
- Focusing and strengthening the Encryption Laws in India specially in the mobile industry segment.

Source: Frost & Sullivan
Mega Trends
The Smart City initiative by the Government is going to provide an impetus to Enterprise Telecom solutions.

The Digital India initiative would look up to adoption of telecom solutions to provide government services to the citizens electronically.

The ‘Make in India’ campaign by the Government is expected to create more jobs and opportunities in the manufacturing sector, in particular. Large organizations, which will set up R&D offices and production plants in India, are very likely to Telecom solutions.

This would provide a boost to connected living and has already started to make waves in the wearables market in the healthcare industry.

The Start-up India initiative would be a powerful force for budding Start-up eco-system, especially in the e-Commerce segment.

Mega Trends in India
Organizations are virtualizing their datacenters. Virtualization also supports the hosted Managed Security Services (MSS) model. Acceptance of this technology is expected to increase during the short to medium term. Vendors in partnership with Telecom Service Providers (TSP) are provisioning security services such as firewalls on a virtual basis, and the revenue is being accounted as part of the managed security service portfolio.

Organizations, particularly those with a young workforce, are opting for the Bring-Your-Own-Device (BYOD) culture. This trend presents many security and legal challenges which enterprises cannot ignore.

The increase in public and private cloud deployments has presented prime opportunities for security vendors to partner with other managed security service providers, particularly Conferencing Service Providers (CSP) and data center services providers who can add cloud security, to increase the level of market reach.

Big Data approaches are being used to create Advanced Persistent Threat (APT) detection and defense. For example, Cisco has recently entered the market with a Hadoop-based platform. Such services are complex and require specialized staffing, which fits well into the security as a service model. Additionally, the Big Data analytics model provides higher margins than legacy businesses.
### Overview
- The Indian banking system consists of 26 public sector banks, 20 private sector banks, 43 foreign banks, 56 regional rural banks, 1,589 urban cooperative banks, and 93,550 rural cooperative banks.
- RBI is considering to give more licenses to private players.
- Total credit went up to US $1,089 Billion by FY-15.
- ATMs are increasing at CAGR of 29.6% as on October 2015.

### Initiatives / Mandates
- The Reserve Bank of India (RBI) has relaxed its branch licensing policy, thereby allowing banks (which meet certain financial parameters) to set up new branches in Tier-2 to Tier-6 centers.
- The Reserve Bank of India (RBI) has granted in-principle licenses to 10 applicants to open small finance banks.
- To facilitate an easy access to finance by Micro and Small Enterprises (MSEs); the Government has launched MUDRA Yojana.
- The RBI has given in-principle approval to 11 applicants to establish payment banks.
- The US-based non-profit organization Rockefeller Foundation plans to invest up to US $15 Million in two proposed small finance banks in India.

### Key Takeaways
- BFSI and IT/ITeS are key contributors to the growth of the country and since these verticals are primed for growth in the forecast period with significant initiatives and mandates driven by government policy. More private sector participation in banking is a key area for revenue growth in BFSI, small finance is also an area to be explored in terms of new account acquisition.
- The Start up ecosystem needs a specific Go-To-Market (GTM) by service providers in the IT/ITeS ecosystem and incubating start-ups needs to be looked at as an investment for future customer acquisitions.

---

**Source:** Frost & Sullivan, IBEF, DIPP
# Mega trends impacting various verticals

## Overview

<table>
<thead>
<tr>
<th>Manufacturing</th>
<th>Telecom</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overview</strong></td>
<td></td>
</tr>
<tr>
<td>• India has become one of the most attractive destinations for investments in the manufacturing sector due to the Make in India campaign.</td>
<td>• India is currently the world’s second-largest telecommunications market and has registered strong growth in the past decade and half.</td>
</tr>
<tr>
<td>• The GoI has received investment proposals of over US $3.05 Billion till end of August 2015 from various companies.</td>
<td>• The total mobile services market revenue in India is expected to touch US $37 Billion in 2017 at a CAGR of 5.2%.</td>
</tr>
<tr>
<td>• The Manufacturing sector currently contributes 16% to the GDP.</td>
<td>• The Indian telecom sector is expected to generate four million direct and indirect jobs over the next five years.</td>
</tr>
</tbody>
</table>

## Initiatives / Mandates

<table>
<thead>
<tr>
<th>Manufacturing</th>
<th>Telecom</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initiatives / Mandates</strong></td>
<td><strong>Initiatives / Mandates</strong></td>
</tr>
<tr>
<td>• The Prime Minister has launched the ‘Make in India’ initiative to place India on the world map as a manufacturing hub.</td>
<td>• The Central Government’s several initiatives to promote manufacturing in the country such as ‘Make in India’ appears to have had a positive impact on mobile handsets manufacturing in the country.</td>
</tr>
<tr>
<td>• The Government held the “Make in India Week” in February 2016 in Mumbai to showcase the potential of design, innovation, and sustainability across India’s manufacturing sector over the next decade.</td>
<td>• The GoI plans to roll out free high-speed Wi-fi in 2,500 cities and towns across the country over the next three years.</td>
</tr>
<tr>
<td>• The Government has asked New Delhi’s envoys in over 160 countries to focus on economic diplomacy to help attract investments and make the ‘Make in India’ campaign a success.</td>
<td>• Bharti Airtel has planned to invest INR 60,000 Crore (US $9.02 Billion) over a period of three years with a view to boost its telecom network capacity thereby improving the quality of voice and data services to its customers.</td>
</tr>
<tr>
<td>• Entrepreneurs of small-scale businesses in India will soon be able to avail loans under Pradhan Mantri MUDRA Yojana (PMMY).</td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td><strong>Low</strong></td>
<td><strong>Medium</strong></td>
</tr>
</tbody>
</table>

## Key Takeaways

<table>
<thead>
<tr>
<th>Manufacturing</th>
<th>Telecom</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key Takeaways</strong></td>
<td><strong>Key Takeaways</strong></td>
</tr>
<tr>
<td>• The Manufacturing vertical has received gathering interest from the international community and with the Government pushing for diplomacy around this area, vendors should target global manufacturing MNCs who want to set up in India and strategically focus on acquiring them as customers.</td>
<td><strong>Source:</strong> Frost &amp; Sullivan, IBEF, DIPP</td>
</tr>
<tr>
<td>• With FDI pipeline expanding, the manufacturing vertical will be on course to expand factories and develop IP through products, as more skill sharing and global expertise will come to India through this avenue.</td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td><strong>Low</strong></td>
<td><strong>Medium</strong></td>
</tr>
</tbody>
</table>
## Mega Trends Impacting Various Verticals

### Overview
- In 2015, the overall Media and Entertainment industry grew 11.7% over 2014.
- The Foreign Direct Investment (FDI) inflows in the information and broadcasting (I&B) sector (including print media) in the period April 2000-September 2015 stood at US $4.28 Billion.
- The services sector contributed US $783 Billion to the 2014-15 GDP growing at a CAGR of 9%.
- The Indian services sector has attracted the highest amount of FDI equity inflows amounting to about US $45.38 Billion, which is about 17% of the total foreign inflows.

### Initiatives / Mandates
- Digitizing the cable distribution sector to attract greater institutional funding.
- Increasing FDI limit from 74% to 100% in cable and DTH satellite platforms.
- The Indian and Canadian governments have signed an audio-visual co-production deal that would help producers from both countries to exchange of culture and art among them.
- The Center has given the go-ahead for licenses to 45 new news and entertainment channels in India.
- Mobvista International Technology Ltd, a global mobile advertising and game publishing company, plans to increase its investment in India by US $100 Million.
- By December 2016, the GoI plans to take mobile network to nearly 10% of Indian villages.
- Amazon, the world’s largest online retailer, plans to invest INR 31,700 Crore (US $4.76 Billion) in India in addition to the US $2 Billion investment it had committed earlier.
- The private security services industry in India is expected to register a growth of over 20% over the next few years.
- The GoI has awarded a contract worth INR 1,370 Crore (US $210 Million) to Ricoh India Ltd and Telecommunications Consultants India Ltd (TCIL) to modernize 129,000 post offices through automation.
- The e-Commerce services sector is expecting a major push.

### Key Takeaways
- The Media vertical is set to undergo significant transformation with the FDI limit being raised and more license being granted. This sector is set to go on the path of digital transformation.
- e-Commerce is set to experience a further renaissance with large Global retailers like Amazon expanding their footprint in India.
- Also, local e-Commerce start-up is an exciting opportunity to tap into in the mid segment as their growth and scale can be exponential.

Source: Frost & Sullivan, IBEF,DIPP
# Mega Trends Impacting Various Verticals

## Overview
- The overall healthcare market is valued at US $100 Billion and is growing at a CAGR of 22.9% (2015-2020).
- The sector attracted FDI worth US $3.41 Billion between April 2000-December 2015 for hospitals and diagnostic centers.
- Kerala aims to become India’s healthcare hub in next five years.
- The Indian oil and gas (O&G) industry was worth US $139.8 Billion in 2015.
- India is the fifth-largest LNG importer and accounts for 5.5% of the total global trade.
- The Government has allowed 100% FDI and the sector had attracted FDI of worth US $6.64 during April 2000-December 2015.

## Initiatives / Mandates
### Healthcare
- The Government of West Bengal has introduced G1 Digital Dispensary to provide primary healthcare services to the rural population.
- The e-Health initiative aims at providing effective and economical healthcare services to all citizens. The program aims to make use of technology and portals to facilitate people maintain health records and book online appointments with various departments of different hospitals using e-KYC data of Aadhaar number.
- India is collaborating with Sweden to provide quality healthcare service by filling gaps in the healthcare research.
- Under the National Health Assurance Mission, the Government would provide all citizens with free drugs and diagnostic treatment, as well as insurance cover to treat serious ailments.

### Oil and Gas
- Dhanwati Petrochem Limited in West Bengal and Thailand’s Indorama Ventures Public Company Limited have agreed to enter into an equal joint venture to manufacture and sell Poly Ethylene Terephthalate (PET) resins for the Indian market.
- The Government has introduced initiatives like Hydrocarbon Exploration Licensing Policy (HELP), Marketing and Pricing freedom for new gas production, grant of extension to the Production Sharing Contracts.
- The Government has entered into bilateral discussion with Norway to extend cooperation between the two countries in the field of oil and natural gas and hydrocarbon exploration.
- To incentivize exploration and production in Northeast India, 40% subsidy on gas price has been extended to private companies operating in the region, along with ONGC and OIL.

## Key Takeaways
- The rise in the demand for quality healthcare facilities among the rapidly expanding tech-savvy middle-class and affluent population increases the adoption of HCIT solutions among hospitals and diagnostic centers.
- The healthcare industry will see deployment of tools, such as, telemedicine, HIS/HMIS, online or electronic medical records to improve accessibility and overcome the challenge of manpower shortage.

Source: Frost & Sullivan, IBEF, DIPP
The Ecosystem
Deep Understanding of the Cyber Ecosystem would Determine Effectiveness of the Cyber Defense Mechanisms

A thorough understanding of the multi-tiered cyber ecosystem would determine the effectiveness of cyber security and defense solutions, designed by cyber defenders, security architects, and researchers.

<table>
<thead>
<tr>
<th>Category</th>
<th>Examples</th>
<th>Security Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government</td>
<td>Cyber Laws, Regulations, Policies, Frameworks, Judiciary, etc.</td>
<td>Government Security</td>
</tr>
<tr>
<td>Organization</td>
<td>Cyber Policies, Procedures, Information Security Protocols, etc.</td>
<td>Organizational Security</td>
</tr>
<tr>
<td>Cyber</td>
<td>User IDs, Emails, Passwords, Phone Numbers</td>
<td>Identification and Authentication</td>
</tr>
<tr>
<td>Cyber</td>
<td>Enterprise Applications, Browsers, Office Products</td>
<td>Application Security</td>
</tr>
<tr>
<td>Cyber</td>
<td>Operating Systems (iOS, Windows, Android)</td>
<td>Host Security</td>
</tr>
<tr>
<td>Cyber</td>
<td>Codes</td>
<td>Host Security</td>
</tr>
<tr>
<td>Cyber</td>
<td>OSI Layer</td>
<td>Network Security</td>
</tr>
<tr>
<td>Physical Infrastructure</td>
<td>Hardware, Cables (fiber, copper), etc.</td>
<td>Infrastructure Security</td>
</tr>
</tbody>
</table>
Ecosystem Players Add Value to Enterprises’ Cyber Security Requirements

Source: Frost & Sullivan analysis
Each of the Three Major Ecosystem Participants Play a Role of their Own, Contributing to the Entire Security Value Chain

<table>
<thead>
<tr>
<th>Original Equipment Manufacturer (OEM)</th>
<th>Telecom Service Providers (TSP)</th>
<th>System Integrator (SI)</th>
</tr>
</thead>
</table>
| The OEMs develop products for the cyber security industry that are generic and cut across industry verticals:  
  - Next Generation Threat Prevention  
  - Next Generation Firewalls  
  - Endpoint Security  
  - Network Security  
  - Intrusion Prevention System (IPS)  
  - Intrusion Detection System (IDS)  
  - Security Information and Event Management (SIEM)  
  - Vulnerability Management | The TSPs offer the following in a way of managed services to the end customers:  
  - Firewall Protection  
  - Unified Threat Management  
  - Intrusion Prevention System (IPS)  
  - Intrusion Detection System (IDS)  
  - DDoS Detection and Migration  
  - Vulnerability Management Services (VMS)  
  - Penetration Testing | The SIs integrate security products as per the customers’ needs (through customization) depending on their technical environment and applications:  
  - Consulting and Compliance  
  - System Integration  
    - Endpoint Security  
    - Network Security  
    - Data Security  
    - Identity and Access Management (IAM)  
    - Others  
  - Mobile and Application Security  
  - Network System Security  
  - Managed Security Services |

Several offerings between the TSPs and SIs often overlap on each other, thereby eating a pie of individual shares.
Indian Customers Look for a Right Mix of On-premise and Cloud-based Security Applications for their Benefit

<table>
<thead>
<tr>
<th>Vertical trends</th>
<th>On-premise</th>
</tr>
</thead>
</table>
| BFSI            | • Better control on the security features  
                 • Larger bandwidth in terms of securing multiple applications  
                 • If compliance issues are at stake  
                 • For industry verticals that are prone to frequent cyber attacks and carry sensitive information  
                 • Physical access to mission critical security is required  
                 • The back-end sensitive data is protected by on-premise security software  
                 • Several of the company owned servers and IPs are being protected by on-premise security software  
                 • The Indian Central as well as State Governments look to use the traditional on-premise security applications |
| IT/ITES         | • Less Capital and Operational expenditure for running security software  
                 • Better expertise offered by the provider as in compared to in-house team  
                 • For situations where scalability remains a factor to business success  
                 • Where continuous / real-time monitoring of security threats are required  
                 • To experience easier application management, where number of applications run at once  
                 • The front-end applications that run are protected by cloud-based security applications  
                 • The Indian IT/ITES sector being the most progressive and widely spread, the technology sector looks to use a lot of cloud-based security solutions of its globally networked work-force  
                 • The Indian Government is considered to be a late adopter of technologies; however, with the Digital India initiative put in place, cloud-based security could soon find a place in the ecosystem |
| Govt.           | • The Most Vulnerable Industry Sectors have been mentioned here |

www.innovationnorway.no
Emerging Players
# Network Security Start-up in India: INNEFU

## About

Innefu is a research-oriented Information Security consulting group specializing in meeting the Information Security needs of the consumer via specialized products and services. Its product and services are often being used by the Law Enforcement Agencies to track hackers and cyber miscreants.

## Management Team

- **Tarun Wig**: Co-founder
- **Abhishek Sharma**: Co-founder

## Products and Services

- AuthShield – Two Factor Authentication
- Internet Interception and Monitoring System
- Tactical Internet Monitoring System
- Cyber Cafe Surveillance
- Network and Web Applications Vulnerability Assessment
- Penetration Testing for Web Applications and Internal Networks
- Managed Security Services

## India Locations

New Delhi

## Website

[www.innefu.com](http://www.innefu.com)

## Established

2012

## Funding

No Funding Received
## Network Security Start-up in India: InstaSafe

### About
InstaSafe is a Cloud Security Start-up focussing on enabling businesses to adopt and embrace cloud computing technologies and applications safely and securely. The company envisions to provide a secure and safe cloud platform, acting as an intermediary addressing all the concerns for cloud adoption.

### Established
2012

### India Locations
Bangalore

### Website
www.instasafe.com

### Management Team
- **Sandip Panda**: Co-founder and CEO
- **Deepak Panigrahy**: Co-founder
- **Biju George**: Head of Cloud Operations and Customer Support
- **Prashanth Guruswamy**: Director-Sales and Business Development

### Products and Services
- Encrypted Private Network
- Multi-layer Authentication
- Cloud Web Security

### Funding
Undisclosed amount in two rounds of investment from one investor
## Endpoint Security Start-up in India: AppKnox

### About
Appknox is a mobile security company that aims at helping businesses and developers make their mobile applications more secure.

### Established
2014

### India Locations
Bangalore

### Website
www.appknox.com

### Management Team
- **Harshit Agarwal**: Co-founder and CEO
- **Subho Halder**: Co-founder and CTO
- **Prateek Panda**: Co-founder and CMO

### Products and Services
- Mobile Security
- Mobile Vulnerability Testing
- Static Application Security Testing
- Dynamic Application Security Testing
- User Behavior Analysis

### Funding
US $19.9K in two rounds of investment from five investors
Data Security Start-up in India: ShieldSquare

About
ShieldSquare protects online businesses from Content theft. The company offers invisible and comprehensive website protection from the various threats of bot scraping. It ensures that all types of online businesses are protected from the ever evolving bot threat.

Established
2013

India Locations
Bangalore
Chennai

Website
www.shieldsquare.com

Management Team
- **Pavan Thatha**: Co-founder and CEO
- **Rakesh Thatha**: Co-founder and CTO
- **Vasanth Kumar Gopalakrishnan**: Co-founder and COO
- **Jyoti Kakatkar**: Co-Founder VP-Tech

Products and Services
- Bot Prevention
- Content Scraping Protection
- Price Scraping Prevention
- Form Spam Prevention
- Credential Stuffing Prevention
- Skewed Site Analytics Prevention
- Carding Activity Prevention
- Others (Prevents Ticket Scraping, Auction Sniping, Account Aggregation)

Funding
US $350K in one round of investment from six investors
# Data Security Start-up in India: Avyaan Labs

## About

Avyaan Labs is a cyber space security company that helps fight against cyber and data breaches using its cutting edge solutions. Through its service offerings, the company helps its clients maintain highest level of digital security for web and mobile applications, web servers, IT networks, and other IT infrastructure.

## Management Team

- 

## India Locations

- Noida

## Website

- www.avyaan.com

## Established

- 2014

## Products and Services

- Web Application Audit
- External Penetration Testing
- Mobile Application and Security Testing
- Avyaan@365

## Funding

- No Funding Received
## Managed Security Services Start-up in India: Cyber Octet

### About

Cyber Octet is an IT Solution, Security, Training, and Services Company providing best solution to its clients for any development solution to securing data. Till date, the company has served several Government Institutions and private sector organisations through its end-to-end expertise.

### Established

2011

### India Locations

Ahmedabad

### Website

www.cyberoctet.com

### Management Team

- **Falgun Rathod**: Founder and Managing Director

### Products and Services

- Cyber Crime Investigation
- Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)
- Enterprise Security and Policies
- Web Application Security
- Product Security Assessment
- Security Auditing
- Training

### Funding

No Funding Received
### About

Aujas is a Global Information Risk Management (IRM) company with 400+ customers spread across 22 countries and helping them enhance their information value using the Aujas Information Risk Management solution portfolio.

### Management Team

- **Srinivas Rao**: Co-founder and CEO
- **Sameer Shelke**: Co-founder and COO
- **Navin Kotian**: Co-founder and President

### India Locations

- Bangalore

### Website

- www.aujas.com

### Products and Services

- Risk and Compliance Advisory
- Identity and Access Management
- Security Intelligence
- Threat Management
- Digital Security

### Established

- 2008

### India Locations

#### Bangalore

### Website

- www.aujas.com

### Funding

- US $11 Million in three rounds of investment from three investors
Enterprise Collaboration and Security Start-up in India: Vaultize

**About**

Vaultize provides a comprehensive enterprise file security platform that enables continuous data protection, digital rights management, and unprecedented access control for zero data loss enterprise file sharing and VPN-free secure access.

**Established**

2010

**India Locations**

Pune
Mumbai
Noida

**Website**

www.vaultize.com

**Management Team**

- **Anand A. Kekre**: Co-founder and Executive Chairman
- **Ankur Panchbudhe**: Co-founder and CTO

**Funding**

Undisclosed amount in one round of investment from one investor

**Products and Services**

- Enterprise Secure File Sharing
- FTP Replacement
- Digital Rights Management
- 3A Access
- Zero Data Leakage
- Endpoint Data Protection
- Mobile Enablement and Collaboration
Market Opportunity
Network Security

Network security is the act of protecting the cyber network with simple means of security such as usernames and passwords. In addition to these low-level security features, network security also incorporates firewalls, antivirus protection, network security scanners, intrusion detection and protection systems (IDS/IPS), and security information and event management (SIEM).

Endpoint Security

Endpoint security refers to features on email, mobile phones, tablets, printers, personal computers, and other devices that protect them from intrusion, such as antivirus software, smart cards, and biometric scanners.

Data Security

Data security is anything that protects databases from destructive forces and unwanted access by unknown users, including data masking, data recovery, and data encryption.

Managed Systems and Services

Managed systems and services allow companies and end users to outsource all or parts of their cyber security solution. These services may include firewalls, antivirus or antispyware protection, endpoint security, hardware, and file system and data encryption.
The Indian Cyber Security Market is expected a double digit growth till 2020

<table>
<thead>
<tr>
<th>Product</th>
<th>FY 15</th>
<th>CAGR</th>
<th>FY 20</th>
<th>CAGR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Security</td>
<td>258,5</td>
<td>11.03%</td>
<td>436,2</td>
<td>11.09%</td>
</tr>
<tr>
<td>Endpoint Security</td>
<td>237,2</td>
<td>11.09%</td>
<td>401,3</td>
<td>11.09%</td>
</tr>
<tr>
<td>Data Security</td>
<td>60,4</td>
<td>15.36%</td>
<td>123,5</td>
<td>15.36%</td>
</tr>
<tr>
<td>Managed Security Services</td>
<td>161,0</td>
<td>18.28%</td>
<td>372,7</td>
<td>18.28%</td>
</tr>
</tbody>
</table>

- Next Generation Firewall (NGFW) is expected to see a splurge in the use among all products of Network Security.
- With the increase of BYOD across industry verticals in India, end-point security is expected to observe a double digit growth over the next few years (until 2020).
- In 2015, India reported over 54,483 cyber security incidents, which includes phishing, spam, and malicious code. This, as a result, has made customers aware of the fact that data could not be compromised to hackers at any cost and hence would see the data security market to grow to US $123.5 Million by the end of 2020.
Banks are the top spenders towards cyber security to maintain confidentiality of transactions and customer data

Market Trends

• Hackers, world over, has been targeting the financial institutions in search of stealing data and this trend remains no different in the Indian context. BFSI would observe the largest growth with 28% market share among all other industry verticals by the end of 2020.

• The Indian healthcare industry is moving through a phase of transition where the payers and providers in the business deal with a lot of customer data. This, in a nutshell, would inflate the need of securing data and hence the healthcare pie within the cyber security space would increase.

• The Indian Government has become strict on securing the data at their end. Although this particular sector moves on using the traditional way of security, cloud-based security applications are yet to contribute largely.
Factors Driving the Cyber Security Market (1/3)

Increasingly complex security threats and escalating number of cyber crimes impair business continuity

<table>
<thead>
<tr>
<th>Drivers</th>
<th>1-2 years</th>
<th>3-4 years</th>
<th>5-7 years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increasingly complex security threats and escalating number of cyber crimes impair business continuity</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Targeted Government investments in digital inclusion and infrastructure modernisation projects directly drive the market</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Consumerization of smartphones and bring-your-own-device (BYOD) in organizations drive the demand for network security deployment</td>
<td>H</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>Pressure from regulatory agencies and the payment card industry cause organizations to be security-compliant</td>
<td>M</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>National agencies drive the adoption of cyber security in critical national infrastructure</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Espionage by country and company is increasing the need for cyber security</td>
<td>L</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>Cyber warfare and cyber crime are creating profitable business</td>
<td>M</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>

Note: Drivers are shown in order of impact. Source: Frost & Sullivan
## Factors Driving the Cyber Security Market (2/3)

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Increasingly complex security threats and escalating number of cyber crimes impair the business continuity</td>
<td><img src="https://www.innovationnorway.no" alt="Impact" /></td>
</tr>
<tr>
<td></td>
<td>• For the last couple of years, Indian enterprises have witnessed organized security breaches, which have caused huge financial losses and have also impacted business continuity. Enterprises, both large and SMEs, have realized that these sophisticated attacks not only affect business continuity and agility but also tarnish their brand image.</td>
<td><img src="https://www.innovationnorway.no" alt="Impact" /></td>
</tr>
<tr>
<td></td>
<td>• Firms across verticals, BFSI, IT/ITeS, service providers, and Government are investing significantly in advanced security solutions to safeguard against future attacks.</td>
<td><img src="https://www.innovationnorway.no" alt="Impact" /></td>
</tr>
<tr>
<td>2</td>
<td>Targeted Government investments in digital inclusion and infrastructure modernization projects</td>
<td><img src="https://www.innovationnorway.no" alt="Impact" /></td>
</tr>
<tr>
<td></td>
<td>• India is witnessing a large increase in Government spending in the education, healthcare, construction, and infrastructure sectors. Ongoing and planned digitization programs across these verticals are likely to continue to boost the uptake for network security offerings in the region.</td>
<td><img src="https://www.innovationnorway.no" alt="Impact" /></td>
</tr>
<tr>
<td>3</td>
<td>Consumerization of smartphones and BYOD in organizations</td>
<td><img src="https://www.innovationnorway.no" alt="Impact" /></td>
</tr>
<tr>
<td></td>
<td>• The proliferation of employee-owned smartphones and tablets in the corporate network are giving rise to security solutions, especially designed for BYOD environment.</td>
<td><img src="https://www.innovationnorway.no" alt="Impact" /></td>
</tr>
<tr>
<td>4</td>
<td>Pressure from regulatory authorities and payment card industry cause organizations to be security complaint</td>
<td><img src="https://www.innovationnorway.no" alt="Impact" /></td>
</tr>
<tr>
<td></td>
<td>• In the past two years, regulatory authorities and the payment card industry have put increasing emphasis on data security in India. The cyber security market is in its early adoption stage; hence, the regulatory bodies are not very stringent on security compliance. However, the pressure to adopt strict security measures is expected to increase in two to three years.</td>
<td><img src="https://www.innovationnorway.no" alt="Impact" /></td>
</tr>
</tbody>
</table>

Source: Frost & Sullivan

www.innovationnorway.no
## National agencies drive the adoption of cyber security in critical national infrastructure

### Description
- Contemporary technologies are being implemented in critical infrastructure of the country, such as energy, defense, and transportation. This is leading to exfiltration of information by cybercriminals. The Government is focused toward improving the cyber security measures to reduce the risk of cyber terrorism.

### Impact
- **High**
- **Medium**
- **Low**

### Event
- 5

## Espionage by country and company is increasing the need for cyber security

### Description
- With the success of the Digital India initiative, there will be higher availability of digital data both from critical business perspective and national data that is at risk. There is an increasing need and emphasis from the Government as well as from organizations to secure digital information. Cyber espionage is a growing concern in Government and corporations and, with the further digitalization implementing, cyber security will be a matter of national defense.

### Impact
- **High**
- **Medium**
- **Low**

### Event
- 6

## Cyber warfare and cyber crime are creating profitable business

### Description
- The constant growth in the number of devices connected to the world wide web, is permitting cyber criminals to commit offences in a digital environment. Cybercrime has evolved from infiltrating systems for fun to infiltration for business. The current focus is on extracting personal information via phishing attacks, etc.
- Cyber warfare, which is highly feared by Governments, is strictly focused on Government and strategic infrastructure of the nation.

### Impact
- **High**
- **Medium**
- **Low**

### Event
- 7

---

Source: Frost & Sullivan

www.innovationnorway.no
Factors Restraining the Cyber Security Market (1/2)

<table>
<thead>
<tr>
<th>Restraints</th>
<th>1-2 years</th>
<th>3-4 years</th>
<th>5-7 years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of knowledge about the severity of cyber threats <strong>among</strong> decision makers</td>
<td>M</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>A <strong>highly active software market</strong> restrains corporations from fully securing information infrastructures</td>
<td>M</td>
<td>M</td>
<td>L</td>
</tr>
<tr>
<td><strong>Economic issues</strong> restrain the adoption of cyber security systems</td>
<td>H</td>
<td>M</td>
<td>M</td>
</tr>
</tbody>
</table>

Technological development in India has resulted in a complex cyber threat landscape

Note: Drivers are shown in order of impact. Source: Frost & Sullivan
www.innovationnorway.no
Factors Restraining the Cyber Security Market (2/2)

Lack of knowledge about the severity of cyber threats among decision makers
1. Cyber threats are becoming more critical by the day, and top-level decision makers, both in corporations and Government, are becoming more knowledgeable about the situation. But this increase in knowledge is still insufficient to combat the breaches.

2. Government officials are gradually gearing up to understanding the risks involved in cyber security breaches. While corporate managers view this as an IT issue and allocate insufficient budgets for cyber defense.

A highly active market restraints corporations from fully securing information infrastructures
1. The software market is constantly developing, leading to new and advanced threats appearing everyday. Developments in the cyber threat market is extremely fast and dynamic, and this is keeping the cyber security market from finding a solution that would eliminate these threats universally.

Economic issues restrain the adoption of cyber security systems
1. Cyber security as an environment consists of technology and implementation by the people and the procedures that needs to be followed. There is a cost associated with all the three areas and budget restraints negatively impacts the adoption of the cyber security systems. In a such a situation, organizations are pushed to procure older technologies or they deploy off-the-shelf products, which are much easier to breach than tailored solutions.

2. Currently, threats appear from diverse areas, ranging from advanced persistent threats (APT) to phishing attacks. With threats emerging from different dimensions, it is crucial to adopt cyber security for different layers of systems, but limited economic resources restrain enterprises and countries from adopting these much needed solutions.

Source: Frost & Sullivan
www.innovationnorway.no
Market Opportunity

Network Security
Network Security – Definitions

**Firewall / IPSec VPN**
A firewall is a system or a group of systems that enforces an access control policy between networks (blocking and/or permitting a certain kind of traffic). Thus, the principal function of a firewall is to protect resources of a private network.
IPSec VPNs operate at the network layer (layer III) of the Open System Interconnection (OSI) network architecture model.

**SSL VPN**
This is a type of VPN that does not require VPN client software on remote devices. Users can make a secure connection from any laptop or desktop with a browser using SSL standards.

**IDS / IPS**
IDS gathers and analyzes information from various areas within a computer or a network by using intelligent detection methods to identify possible security breaches, which include attacks from both outside and inside the organization. Intrusion Detection and Prevention or Intrusion Prevention Solutions not only detect attacks but also block them.
# Network Security Market — Current Market Scenario

## Market stage
- Mature, US $258.5 Million for FY 2015
- CAGR (FY 2015-2020) is 11.03%

## Competition landscape
- End-to-end network security market will continue to evolve through acquisitions or partnerships

## Other factors
- The proliferation of consumer-owned smartphones and tablet PCs on the corporate network of organizations has given rise to network security solutions that are designed specifically for BYOD

## Potential for opportunities
- Vendors must provide advanced security analytics and risk assessment of network vulnerabilities to improve their security solutions

## Industry convergence trends
- The strengthening of partnerships between network security vendors and MSSPs through the model of outsourcing

## Growth zone
- Verticals: BFSI, IT/ITeS, Government
- Horizontals: Large enterprises are main contributors

## Technology Split
- Firewall/IP Sec VPN – 13.5% growth
- IDS/IPS – 7% growth
- SSL VPN – 12% growth

<table>
<thead>
<tr>
<th>Technology Split</th>
<th>Firewall / IPsec (84%)</th>
<th>IDS / IPS / IS (13%)</th>
<th>SSL VPN (3%)</th>
</tr>
</thead>
</table>

The Firewall / IPSec VPN segment in India is likely to grow at a CAGR of around 13.5% for the period 2015-2020. There is an upsurge of cyber crime from professional cyber criminals, as a result of which detecting and managing networks has become business imperative. The NGN firewalls are likely to experience a healthy growth in the medium to long term.

The IDS / IPS experiences a moderate growth of around 7% in 2015. The short-term growth for this segment depends on the level of innovation of NGFW, which would encompass a complete range of security features, such as intrusion, detection and prevention, content filtering, anti-spam, and anti-virus.

The SSL VPN segment is likely to grow at a CAGR of around 12% for the period 2015-2020. Demand for SSL VPN primarily comes from banking, financial services, and insurance sectors. With the increase in mobile devices and other mobility products, there is a need to secure remote access to corporate networks, which is the biggest driver for SSL VPN.

The Market Estimates mentioned above are End-user estimates.
### Network Security – Vertical Analysis

**FY-15**

<table>
<thead>
<tr>
<th>Vertical</th>
<th>Adoption Trends</th>
</tr>
</thead>
<tbody>
<tr>
<td>BFSI</td>
<td><strong>BFSI</strong> is the top spender on network security solutions due to their high requirement of confidentiality in transactions and customer data.</td>
</tr>
<tr>
<td>Telecom</td>
<td><strong>Government and IT/ITeS</strong> are the second in spending in security solutions. Digital India is providing a boost to implement strong network security solutions in the Government vertical.</td>
</tr>
<tr>
<td>Oil &amp; Gas</td>
<td><strong>Telecom</strong> service providers are key contributors to the overall market revenues. With the increase in the number of datacenters in India, this vertical provides a substantial revenue potential to the overall market.</td>
</tr>
<tr>
<td>Healthcare</td>
<td><strong>Healthcare</strong> requires a reliable and integrated security network to protect their patient data as well securely transfer large medical files via a low latency network.</td>
</tr>
<tr>
<td>Govt.</td>
<td></td>
</tr>
<tr>
<td>Media</td>
<td></td>
</tr>
<tr>
<td>IT / ITeS</td>
<td></td>
</tr>
<tr>
<td>Others</td>
<td></td>
</tr>
</tbody>
</table>
Network Security – Drivers and Restraints

**Drivers**

Growth of services, such as e-Government, e-Banking, e-Commerce, e-Education, and e-Healthcare in the country is increasing

- The network security market in India has been experiencing an uptake with the growth of e-Services such as e-Commerce, e-Banking, e-Education, e-Healthcare, and e-Government. Networking vendors are expanding their solutions to cater to verticals such as healthcare, retail, education, and Government.

Increased usage of smartphones and BYOD in organizations

- The use of smartphones, tablets, and other mobile devices is rapidly increasing across organizations in India. The proliferation of consumer-owned smartphones and tablets in the corporate network of organizations has given rise to network security solutions that are designed specifically for BYOD. Networking vendors are aggressively expanding their portfolios to address the consumerisation of smartphones and tablets.

Rise in employee mobility forces organizations to implement remote access network solutions

- As the mobility of workforce increases, networking devices are increasingly being used for personal as well as professional purposes. Employees from healthcare, construction, investment banking, and insurance verticals are constantly on the move, which compels companies to provide them with access to the corporate network.

**Restraints**

Unregulated organization of distributors and management

- The organization and management of distributors and resellers in India is unregulated and unorganized. Some distributors compete with each other over the same products, while others compete with each other in the same territories. The channel lacks proper structure in terms of product price, profit potential, and regional allocation.

Organizations’ limited budget for security spending owing to cost-cutting in IT services

- Organizations have a limited budget for security. The Indian network security market is extremely price-sensitive and clients generally seek comprehensive network security solutions at reduced costs.
Network Security: Market Share Analysis, India, FY15

Cisco; 29%
Fortinet; 13%
Check Point; 24%
Others; 8%
Dell (Sonic Wall); 2%
Intel (McAfee); 4%
Juniper; 5%
IBM; 6%
Sophos; 6%

Classification of players

Tier-I
Cisco
Check Point

Tier-II
Sophos
IBM

Tier-III
Palo Alto Networks;
3%
Intel (McAfee);
4%
Juniper; 5%
IBM; 6%
Sophos; 6%
Fortinet; 13%
Check Point; 24%
Others; 8%

Others include Huawei, Pulse Secure, F5 Networks, Array Networks, HP, Gajshild, Venustech, TopSec, Sangfor, NSFOCUS, Neusoft, and other small network security vendors
## Focus Products

- **Next-Generation Firewalls (NGFW)** – NGFW is a fully integrated, threat-focused, single management interface network firewall with an effective next-gen IPS and advanced malware protection. It delivers comprehension, unified policy management of firewall functions, application control, threat prevention, and advanced malware protection from network to the endpoint.

- **Next-Generation IPS (NGIPS)** – NGIPS solution integrates real-time contextual awareness, intelligent security automation, advanced threat protection, and high performance and scalability with purpose-built appliances that incorporate a low latency and a single pass design.

- **Advanced Malware Protection (AMP)** – AMP is a subscription-based, managed through a web-based management console, and deployed on a variety of platforms – endpoints, network, email, and web. AMP also provides sandboxing, threat intelligence, and retrospective security.

- **Security Management** – Manages network security solutions for their customers via centralized operational tools, partners with best-in-class technology vendor to deliver SIEM systems. The managed services portfolio consists of – Adaptive Security Device Manager, Content Security Management Appliances, Defense Orchestrator, Firepower Management Center, and Security Manager.

## Unique Value Propositions

- Cisco’s entire security portfolio is tightly linked to the underlying basic infrastructure (networks, servers, virtual machines, applications) rather than “bolted-on” and can be scaled securely.

- Cisco’s threat detection mechanism has deep visibility of the basic infrastructure, threat focused, platform-specific, and network behavior analysis.

- Cisco’s strategy in security is to embed threat centric security everywhere across the extended network. To strengthen their capability they are either building or buying or partnering with ecosystem players to embed security throughout the extended network — from network to endpoint and datacenter to cloud.
# Network Security – Vendor Profile

## Focus Products

Check Point security solutions secures their customers’ infrastructure with state-of-the-art security products for threat prevention, mobility, firewalls, and security management.

- **Next Generation Threat Prevention (NGTP)** – NGTP delivers an integrated multi-layered line of defense to enable enterprises maximize their security and minimize the security incidents. This is achieved by the following:
  - **SandBlast Zero Day Protection** – As a part of this solution, the sandboxing feature picks up the malware at the exploit phase, files are quickly quarantined, and inspected. This solution combines CPU-level inspection and OS-level sandboxing to prevent infection from the most dangerous exploits and zero-day and targeted attacks.
  - **Threat Extraction** – This capability immediately provides a safe version of the potentially malicious content to users. Access to the original suspicious version is blocked, until it can be fully analyzed by sand-blast zero day protection.

- **Next Generation Firewalls (NGF)** – NGF provides next generation security to datacenter, large enterprises, and small and medium businesses. NGF protects both north-south and east-west traffic in a datacenter environment.

## Unique Value Propositions

- Checkpoint focuses on providing end-to-end security from network to cloud to mobile devices. The solutions are built on software-defined protection where security is integrated in the management, control, and enforcement layer.
- Check Point’s security solutions are designed to address specific industry needs as well as, are ready to adapt infrastructure scaling and dynamic networks.
# Network Security – Vendor Profile

## Focus Products

<table>
<thead>
<tr>
<th>Focus Products</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enterprise Firewall</strong></td>
<td>Fortinet’s Enterprise Firewall Solution delivers one of the best-in-kind effective security solutions that provides immediate responsive and intelligent defense against malware and emerging threats with an integrated security fabric extending across borderless network.</td>
</tr>
<tr>
<td><strong>Fortinet Next Generation Firewall (NGFW) Solution</strong></td>
<td>This NGFW is a high performance network security appliance that adds to have intrusion prevention, application control, and anti-malware to the traditional firewall VPN combination. The Fortinet’s NGFW appliance combines the performance of the FortiGate Family with that of the security intelligence component of FortiGuard Labs in order to address several security pointers.</td>
</tr>
<tr>
<td><strong>Fortinet Internal Segmentation Firewall (ISFW) Solution</strong></td>
<td>The Fortinet ISFW Solution helps protect sensitive information from cyber threats once it gains entry into the perimeter network. ISFW sits in front of specific servers that contains sensitive information or a set of user drivers or web applications sitting in the cloud.</td>
</tr>
</tbody>
</table>

## Unique Value Propositions

- The Fortinet’s network security platform offers solutions for the core (internal segmentation through ISFW), the perimeter (through NGFW), and access (secure access).
- Fortinet’s network operating system is flexible enough to cater to the specific need of companies across industry verticals, sizes, and deployment types.
## Network Security – Vendor Profile

### Focus Products

<table>
<thead>
<tr>
<th>McAfee Network Security Platform</th>
<th>The McAfee Network Security Platform is a next-generation IPS that redefines how organizations block advanced threats.</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee Advanced Threat Defense</td>
<td>The McAfee Advanced Threat Defense detects targeted attacks and connects with existing defenses, converting threat intelligence into immediate action and protection.</td>
</tr>
<tr>
<td>Intrusion Prevention and Targeted Threat Detection</td>
<td>McAfee Network Security platform provides in-band traffic inspection and threat blocking through a set of malware detection technologies that are optimized for real-time execution.</td>
</tr>
</tbody>
</table>

### Unique Value Propositions

- The McAfee Network Security Platform extends beyond signature matching with layered signatures-less technologies that defend against never-seen-before threats. This is much different from the traditional way of blocking advanced threats.
- McAfee addresses the unique challenge of dynamic analysis of IPS infrastructure by combining its high performance next generation IPS sensor with McAfee Advanced Threat Defense.
Market Opportunity

Endpoint Security
**Endpoint Security – Definitions**

<table>
<thead>
<tr>
<th>Endpoint considered</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Physical endpoints — Laptops, Desktops</td>
</tr>
<tr>
<td>• Virtual endpoints — VDI, Terminal servers</td>
</tr>
<tr>
<td>• Point of Sale Machines</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mobile device management</th>
</tr>
</thead>
<tbody>
<tr>
<td>• For the purpose of this study, the endpoint protection market does not include Mobile Device Management (MDM): The ability to define device use policies and controls for IT management capabilities. A small subset of traditional MDM functions is included in endpoint protection solutions, such as remote wipe and lock</td>
</tr>
</tbody>
</table>

**Cloud-based solutions**

SaaS Endpoint Protection is hosted and maintained by service provider to deliver up-to-date security without requiring a management server in client premises. Administration is typically handled through a Web-based portal that provides management information, configuration tools, service statistics, and reports in real time, enabling the cloud administrator to monitor how the service is performing.

**On-premise-based solutions**

On-premise solutions involve one or more hardened servers physically installed between the network boundary and internal resources like the email servers and endpoint clients. An IT resource is required to monitor the latest malware trends, adjust the appliance settings, and provide technical support to internal users.

The research covers both cloud-based and on-premise-based solutions. The cloud solution is mostly adopted by SMBs.
## Endpoint Security – Definitions

<table>
<thead>
<tr>
<th>Endpoint security</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Antivirus / Antimalware</strong></td>
<td>Protects endpoints, on or off the corporate network, against viruses, Trojans, worms, spyware, ransomware, and new variants as they emerge.</td>
</tr>
<tr>
<td><strong>Firewall and IPS</strong></td>
<td>Analyzes packet headers and enforces policy based on protocol type, source address, destination address, source port, and/or destination port. Packets that do not match policy or know events are rejected.</td>
</tr>
<tr>
<td><strong>Application and Device Control</strong></td>
<td>Prevents potential damage from unwanted or unknown applications (executables, DLLs, Windows App store apps, device drivers, control panels, and other Portable Executable (PE) files). Allows to specify and categorize, which external devices may or may not be used, and enforce what data can and cannot be transferred to these devices.</td>
</tr>
<tr>
<td><strong>Web filtering</strong></td>
<td>Allows URL Filtering and browser filtering to set quota time, browsing policies.</td>
</tr>
<tr>
<td><strong>Encryption</strong></td>
<td>Encrypts data on a wide range of devices — PC and Macintosh laptops, desktops, CDs, DVDs, USB drives, and any other removable media to prevent unauthorized access and use of private information.</td>
</tr>
<tr>
<td><strong>Data Loss prevention</strong></td>
<td>Gain visibility and control of your sensitive data and prevent data loss via USB, email, SaaS applications, web, mobile devices, and cloud storage.</td>
</tr>
<tr>
<td><strong>Control Manager</strong></td>
<td>Provides instant visibility into security status, events, and direct access to management for unified control of all your security and compliance tools.</td>
</tr>
</tbody>
</table>
## Endpoint Security Market — Present Market Scenario

### Market stage
- Highly commoditized market with low potential for differentiation.

### Competition landscape
- Enterprise class solutions are dominated by top three players.
- The SMB class solutions is a highly fragmented market with many solutions in the market.

### Other factors
- Due to the presence of free solutions, premium solutions are being hit by price negotiations. Endpoint security solution is usually bundled with high-end security solutions rather than it being sold as stand-alone solution.

### Potential for custom sales
- Cloud-based security solutions cover few modules only unlike on premise installations. Hence, SMBs prefer the cloud solutions rather than large enterprises.

### Industry convergence trends
- Forensic analytics and single management for all platforms — on-premise, cloud or hybrid solutions is the ongoing trend.

### Growth zone
- Verticals: Government, Defense, IT/ITES, BFSI, Manufacturing, Education
- Horizontals: Large enterprise is a major contributor

### Product split
- Product focus: Antivirus, Firewall, application control, device control, Web control
- Services focus: Management of alerts and notifications (SoC)

| On premise (75%) | Cloud based (25%) |
The market for endpoint security is flattening from a revenue perspective. Product efficacy questions and the rise of free solutions challenge pricing power.

Traditional antivirus is an important part of network security, providing effective protection against non-targeted malware.

Mobile devices provide new opportunities for endpoint protection vendors, but monetizing mobile offerings has been a challenge.

Emerging protection is evolving to include new types of protection. Device sensors that feed data to analytics platforms is an example.

Security suites are increasingly important as the added features provide additional value, helping to justify premium (paid) solutions from free solutions.
### Endpoint Security – Vertical Analysis

**FY-15**

<table>
<thead>
<tr>
<th>Vertical</th>
<th>Adoption Trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>BFSI</td>
<td>Across verticals, spending on Endpoint security remains stable.</td>
</tr>
<tr>
<td>Telecom</td>
<td>The most influential markets are <strong>Government, defense, the finance industry, IT/ITES, and education.</strong></td>
</tr>
<tr>
<td>Oil &amp; Gas</td>
<td>Typically, the more heavily regulated verticals are the top spenders for security.</td>
</tr>
<tr>
<td>Healthcare</td>
<td>The financial vertical, including <strong>banks</strong>, is heavily regulated and must follow strict security requirements. As a result, financial verticals are more interested in a breadth of solutions, which may include Network Access Control (NAC), Data Loss Prevention (DLP), and vulnerability management.</td>
</tr>
<tr>
<td>Govt.</td>
<td></td>
</tr>
<tr>
<td>Media</td>
<td></td>
</tr>
<tr>
<td>IT / ITeS</td>
<td></td>
</tr>
<tr>
<td>Others</td>
<td></td>
</tr>
</tbody>
</table>
Endpoint Security – Drivers and Restraints

**Drivers**

**Increasingly complex and advanced cyber crimes**
- As the businesses are growing, new, and sophisticated threats such as zero-day malwares, Trojans, and advanced persistent threats are created everyday putting company’s critical data at risk. This has encouraged organizations to deploy endpoint security solution to safeguard their endpoints and networks against potential cyber-attacks.

**Compliance**
- From potential fines for non-compliance to litigation launched by damaged customers, partners, and others, the risks associated with a successful attack can be significant. When organizations suffer data losses, they must turn their focus away from growth and expansion to control damage, repair reputations, and reclaim competitive position.

**Career Impacts**
- Following the disclosure of a major breach, enterprises sometimes find that the first step in rebuilding trust is to accept the resignations of high-level executives up to and including the CEO many times. Hence, it is important to be protected by the right security service provider.

**Social networking sites and increased Internet usage**
- The use of social networking sites increases the need for endpoint security with Web usage controls.
- Increased Internet usage creates greater need for users to protect personal and corporate data.

**Restrains**

**The presence of free substandard solutions is eating the enterprise class solution market share**
- The highly competitive, saturated, and commoditized market inhibits pricing power by endpoint security solutions providers. The highly competitive, saturated, and commoditized market inhibits pricing power by endpoint security solutions providers.

**Advanced security solutions eating the endpoint security budget**
- Advanced security solutions around server security, information, and cyber security is eating away the budgets of endpoint security and by and large rising an opportunity to compare it with the free products.

**Social networking sites and increased internet usage**
- Cloud-based security solutions have a challenge that enterprises are unwilling to move their sensitive data on to cloud
Endpoint Security: Market Share Analysis, India, FY15

- Symnatec; 32%
- McAfee (Intel); 16%
- Trend Micro; 10%
- Kaspersky Lab; 10%
- ESET; 7%
- Sophos; 4%
- AVG; 4%
- Others; 17%

Others include F-Secure, Panda Security, IBM, GFI, BitDefender, AVIRA, AVAST Software, iSheriff, Webroot, CheckPoint, eEye Digital

Classification of players

- Tier-I: Symantec, McAfee
- Tier-II: Sophos, AVG, Kaspersky Lab
- Tier-III: CheckPoint, IBM Security, F-Secure, Microsoft Security Essentials, AVIRA
## Endpoint Security – Vendor Profile

<table>
<thead>
<tr>
<th>Focus Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Endpoint Protection is an in-depth set of multi-layered defense mechanism which includes:</td>
</tr>
<tr>
<td>• <strong>Symantec Online Network for Advanced Responses (SONAR)</strong> – This performs behavioral analysis and prevents malware designed to appear legitimate.</td>
</tr>
<tr>
<td>• <strong>Symantec Insight and Network threat Protection</strong> – This goes beyond the traditional signatures for protection from advanced targeted attacks.</td>
</tr>
<tr>
<td>• <strong>Norton Power Eraser</strong> – This is an advanced repair tool integrated with Symantec Endpoint Protection client.</td>
</tr>
<tr>
<td>• <strong>Symantec’s Security Technology And Response (STAR)</strong> – This enables to detect the evidence of compromise scanning on the endpoint via Symantec Endpoint Protection. Further, this is utilized by Symantec Managed Security Service and ATP.</td>
</tr>
<tr>
<td>• <strong>Cynic</strong> – A cloud-based sandboxing platform, this provides bare-metal hardware and network sandboxing analysis of objects yielded by ATP, Endpoint Protection, and email.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unique Value Propositions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Symantec focuses on providing unrivalled security across physical and virtual platforms and supports the latest operating systems. Multiple layers of defense, simple management across platforms with visibility, and efficiency through a single console.</td>
</tr>
<tr>
<td>• Symantec Endpoint Protection (SEP) is the fastest and lightest endpoint protection system available today. These solutions stays out of the way from business solutions and performs non-critical security tasks when the system is idle. SEP also eases management of security on virtual machines by enabling clients running in virtual machines to be automatically identified and separately managed.</td>
</tr>
</tbody>
</table>
## Endpoint Security – Vendor Profile

### Focus Products

Trend Micro is one of the largest Endpoint Protection (EPP) vendors and have significant investments in the areas of application control, vulnerability detection and shielding, malware sandboxing, and EMM capabilities.

- **Office Scan Security** – Provides a range of malware protection options, such as malicious URL filtering, critical resource and process protection, browser exploit protection, vulnerability detection and shielding, and behavioral monitoring.
- **Worry-free Business Security Services** – Protects Windows, Mac, and Android devices with cloud-based anti-malware and threat protection, managed via a secure web-based console.
- **Endpoint Application Control** – Safeguards against unwanted and unknown applications executing on endpoints.
- **Vulnerability Protection** – Delivers intelligent virtual patching to block exploits and zero day threats.
- **Endpoint Encryption** – Ensures data privacy by encrypting data stored on your endpoints, including DVDs and USB drives.
- **Mobile Security** – Expands protection to gain visibility and control of mobile devices and data in motion.

### Unique Value Propositions

- Trend Micro endpoint solutions deliver the most complete user protection available against evolving threat landscape, across every device and application. Their solutions provide ultimate flexibility to deploy endpoint security on-premise, in the cloud, or using a combination of both. Also, it allows to manage users across threat vectors and deployment models from a single management console.
- Trend Micro endpoint security solutions ensure complete mobile and desktop protection against everything from traditional threats to the latest sophisticated targeted attacks. The solutions are developed to defend both virtual and physical endpoints with multiple layers of anti-threat capabilities.
## Endpoint Security – Vendor Profile

**Focus Products**

McAfee’s Complete Endpoint Protection Solutions protect major operating systems like Windows, Macs, and Linux from zero-day exploits and advanced targeted attacks.

- **McAfee Complete Endpoint Protection, Enterprise** – This includes the most advanced endpoint security for large enterprises: collaborative advanced threat defense, zero-impact user scans, and dynamic whitelisting. In addition to this, the particular security software provides essential endpoint antivirus, antispam, web security, integrated firewall, and Intrusion Prevention (IP) for desktops and laptops.

- **McAfee Complete Endpoint Protection, Business** – The McAfee Complete Endpoint Protection is an all-in-one solution that provides endpoint security for key devices within a business entity. This includes PCs, Macs, Linux Systems, Physical and Virtual Systems, Windows Tablets, as well as security for data in cloud storage.

- **McAfee Endpoint Protection for SMB** – The McAfee Endpoint Protection for SMBs are targeted particularly for companies with low technical resources and provide protection from cyber-criminals and hackers.

- **McAfee Active Response** – This is an threat detection and response tool that protects endpoints so that security breaches and threats could easily be identified.

**Unique Value Propositions**

- McAfee provide security tools that can easily be deployed, be it in the cloud or on-premise.
- McAfee provides security tools that are simplified for a better investigation.
Market Opportunity

Data Security
Email Security

Email Security provides both signature- and reputation-based anti-spam detection and prevention. The email is highly encrypted and has a correlation with ATP solutions for effective mitigation in zero-day malware attacks.

Web security

The ability to block undesired content through category whitelisting / blacklisting, powered by reputation-enabled website filtering. Synchronized with real-time threat intelligence to reduce possible download of malicious files or accessing phishing sites.
### Data Security Market — Current Market Scenario

**Market stage**
- Growth, US $60.4 Million for FY 2015.
- Data security is slowly becoming commoditized and are being slowly integrated with advanced security solutions.

**Competition landscape**
- Cisco is a prominent player in the email security segment, while content providers and cloud-based email providers are also gaining acceptance.
- Forcepoint followed by Bluecoat are the dominant players in the web security.

**Competitive factors**
- Cost, performance, branding, sales support, reliability, integrated capabilities, channel partners, supporting technology needs, such as the ability to inspect SSL-encrypted traffic.

**Distribution structure**
- Through distributors, resellers, SIs, service providers, and direct sales.

**Industry trends**
- Web security solutions drive the market growth, while email security is gradually becoming saturated due to the popularity of cloud-based email.

**Growth zone**
- Verticals: BFSI, IT/ITeS, Government
- Horizontals: SMBs are gearing to the adoption of email and web security

**Product split**
- Product focus: Web Security

| Web Security (60%) | Email Security (40%) |
The data security market will witness a moderate growth in its two sub-segments – email security and web security. However, with the enforcement of cyber security policies in the SMBs will bring momentum to the growth.

MNCs that operate out of India, primarily in the BFSI vertical are witnesses to adopt data security, to enforce their user policies for their corporate network access.

Email service offered by content providers, such as Google, Yahoo, Microsoft adoption are on the rise. This adoption trend is causing a dip in the need in the for dedicated email security systems.

Cloud-based SaaS email providers are gaining acceptance due to the ease of deployment that they offer and also, users are not involved in the liability of the email security.

Government and large enterprises focus on mitigating the malicious social media traffic and URLs; thereby, driving the web security market in India.

The Market Estimates mentioned above are end-user estimates.

US $1 = INR 64
www.innovationnorway.no
### Adoption Trends

#### Email Security
- **BFSI** is the major contributor toward email security revenues due to adoption by the MNCs banks in India.
- **Telecom service providers** are increasing their market share in this segment, as they see the need to combat spam.
- The **Government** vertical saw an increase in their share due to ban on private email for official communication across all its organizations.

#### Web Security
- **BFSI, e-Commerce, and Retail** contribute largely to this segment.
- The **Government** is a key contributor, implementing web filtering for a nation-wide campaign to block websites containing objectionable content causing disruption to law and order. This filtering also enables the Government / organizations to tackle online pornography and social media related terrorism.

<table>
<thead>
<tr>
<th>Vertical</th>
<th>Revenue Share</th>
</tr>
</thead>
<tbody>
<tr>
<td>BFSI</td>
<td>24%</td>
</tr>
<tr>
<td>Telecom</td>
<td>12%</td>
</tr>
<tr>
<td>Oil &amp; Gas</td>
<td>4%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>6%</td>
</tr>
<tr>
<td>Govt.</td>
<td>18%</td>
</tr>
<tr>
<td>Media</td>
<td>8%</td>
</tr>
<tr>
<td>IT / ITeS</td>
<td>26%</td>
</tr>
<tr>
<td>Others</td>
<td>2%</td>
</tr>
</tbody>
</table>

Revenue numbers are to be validated; these are F&S estimates

www.innovationnorway.no
Data Security – Drivers and Restraints

**DRIVERS**

**Sophisticated threats via email and web vectors**
- Growing concerns about sophisticated threats through email and web vectors stimulate spending on content security solutions.

**Need to enhance workplace productivity**
- The need to enhance productivity in the workplace drives enterprises to adopt content filtering technologies to protect their employees from un-desired content.

**Need to protect intellectual assets**
- The need to protect intellectual assets from advanced attacks pushes enterprises to deploy content security solutions to prevent the data loss caused by phishing emails and embedded malicious URLs.

**Emergence of other advanced security technologies**
- The emergence of other advanced security technologies, such as APT, web application firewall (WAF), and DDoS, shifts enterprises’ attention away from traditional content security solutions.

**RESTRAINTS**

**The maturity of the email security segment**
- The maturity of the email security segment is likely to restrain overall market growth.

**Increased adoption of cloud based services**
- The growing preference for cloud-based services hinders spending on product solutions.

**Increased adoption of cloud based services**
- The growing preference for cloud-based services hinders spending on product solutions.
Data Security: Market Share Analysis, India, FY15

Classification of players

**Tier-I**
- Cisco (Ironport); 38%
- Symantec; 13%
- Trend Micro; 10%

**Tier-II**
- Forcepoint; 42%
- Axway (Tumbleweed); 4%
- Intel Security; 6%

**Tier-III**
- Blue Coat; 21%
- Others**; 12%

*Others include Dell (Sonic Wall), CA, Trustwave, Fortinet, Kaspersky, F-Secure, Watchguard, Sophos, Cellopoint.
**Others include F-Secure, Lyceum Capital (Clearswift), Kaspersky, Dell (SonicWall), Barracuda, Sophos, Fortinet, Trustwave (M86), WatchGuard (Borderware)
Focus Products

Forcepoint is a joint venture combining the user protection, data security, and cloud expertise of Websense, defense-grade insider threat, and analytics technology of Raytheon and next-generation network protection capabilities of Stonesoft.

• **Triton AP-Email** – This provides security to the email from the multi-stage advanced threats that penetrate the IT landscape. It has the following features:
  − Cloud, on-premise, and hybrid deployment
  − Enterprise-grade DLP
  − Real-time behavioral sandboxing, threat intelligence
  − Advanced email encryption, archiving, image analysis

• **Triton AP-Web** – This provides defense against productivity draining web content and threats to operations. It has the following features:
  − Cloud, on-premise, and hybrid deployment
  − Enterprise-grade DLP protection
  − Behavioral sandboxing for advanced threat identification
  − Allow seamless access to web resources on mobile devices when they are used outside your corporate network

Unique Value Propositions

• Forcepoint empower organizations to drive their business forward by safely embracing transformative technologies through a unified, cloud-centric platform that safeguards users, networks, and data while eliminating the inefficiencies involved in managing a collection of point security products.

• Forcepoint’s platform simplifies and strengthens security as part of a holistic strategy that includes people, process, and technology is a far more compelling value proposition than a simple point solution; it focuses on insider threat protection, cloud data protection, and network security.
The Blue Coat Advanced Web Security Solutions is built on proxy-based architecture, and can be delivered as a cloud service, on-premise appliance or hybrid of the two.

- **Proxy SG (On-premise Appliance)** – provides the security and control of web traffic, bandwidth management capabilities, user authentication, web filtering, data loss prevention, encrypted traffic visibility, content caching, stream-splitting and more.
- **Web Security Service (Cloud service)** - on-demand web security, customizable reporting and actionable intelligence
- **Mobile Device Security Service** - enterprise-grade threat protection and policy controls to mobile devices (iOS and Android).
- **Content Analysis** - delivers advanced threat protection to detect, analyze and block the increasingly sophisticated attacks.
- **Malware Analysis** – provides actionable intelligence that combines static, dynamic and reputational analysis techniques to help to mitigate unknown malware and zero-day attacks. This adaptive and customizable sandbox solution delivers comprehensive, enterprise-class malware detonation and analysis to expose advanced attacks.

- Blue Coat offers solutions that provide the visibility, acceleration, and security required to optimize and secure the flow of information to any user, on any network, anywhere.
# Data Security – Vendor Profile

## Focus Products

McAfee’s Data Security service offerings are considered the best in the industry. This largely includes multiple versions of Web Security and Data Loss Prevention (DLP) software.

- **Web Security** – The McAfee Web Security solutions simplify and secure access to cloud applications while protecting organizations against advanced malware and other hidden threats. Multiple versions of Web Security include McAfee Web Protection, McAfee Web Gateway and McAfee SaaS Web Protection.

- **Data Protection and Encryption** – This particular security solution provides multi-layered protection for data regardless of where the data actually resides: on the network, cloud or endpoint. Encryption options include enterprise-grade drive encryption or management of native encryption. Various types of McAfee Data Protection software includes McAfee Complete Data Protection—Advanced, McAfee Complete Data Protection, McAfee Complete Data Protection—Essential and McAfee Total Protection for Data Loss Prevention.

## Unique Value Propositions

- As a part of the McAfee Security Connected framework, enterprise data protection solutions are fully integrated with McAfee e-Policy Orchestrator software, which unifies and simplifies data security management. This is quite unique as compared with its peer group software.

- McAfee provides one of the best in the industry, a comprehensive web security solution, from granular application control to web filtering, deep content inspection, and advanced malware protection.
Market Opportunity

Managed Security Services
Managed Security Services – Definitions

Hosted / Cloud-based services
This include shared or dedicated security services delivered based on equipment housed in service provider’s premises and fully managed by the service provider’s security operations center or networks operations center (NOC). The customer is not required to buy, install, and maintain any security equipment and is able to enjoy similar functions to those of security equipment installed on the customer premises. The following hosted services are covered:

- Firewall
- IDS / IPS
- Content Security
- Others*

Management / Monitoring services
Managing, monitoring and maintenance of potential security breaches and security equipment, which is housed in customer’s premises, from a security operations center or networks operations center or by dedicated onsite personnel. These monitoring services may be real time or periodic. The device management and network monitoring services are covered:

- 24X7 monitoring
- Firewall
- IDS/IPS
- Content Security
- Others**

Assessment services
Assessment services are provided for diagnostic and forensic purposes to determine the security posture of the customer’s IT infrastructure. The results of assessment can be used to provide consulting on architecture and policy design / implementation for risk mitigation to the corporate network. The services include:

- Vulnerability assessment
- Penetration testing
- Security consulting

*Others include authentication (tokens, smart card, biometrics, PINs, passcodes), APT protection, website monitoring, DDoS protection, DLP, WAF, SIEM).

**Others include authentication, APT protection, website monitoring, DDoS protection, etc.
# Managed Security Services – Market Overview

## Managed Security Services Market — Present Market Scenario

| **Market stage** | • Growth, US $161.0 Million for FY 2015.  
                  • Growth potential market, opportunity for new service offerings, such as cyber insurance. |
|------------------|------------------------------------------------------------------------------------------|
| **Competition landscape** | • Wipro, IBM, HP, TCS, Infosys, HCL technologies  
                               • Tata Communications, Reliance, Sify. |
| **Other factors** | • Branding, services portfolio, R&D investment, reliability, integration capabilities, partnerships, and long-term viability of the service provider. |
| **Potential for sales** | • Both LEs and SMBs are investing in security infrastructure, maintenance and upgrades. For this, they are eager to adopt reliable third-party security services. |
| **New service offering** | • The forensic and incident response services segment is a newly differentiated segment and growing rapidly in India due to the susceptible nature. |
| **Growth zone** | • Verticals: BFSI, IT/ITeS, Government, Manufacturing  
                     • Horizontals: LE: 85%::SMB:15% |
| **Product split** | • Services focus: Forensic and Incident Response Services  
                      Management / Monitoring services (50%)  
                      Assessment services (20%)  
                      Hosted / Cloud services (30%) |
Managed Security Services – Market Forecasts

CAGR: 18.3%%

Trends

1. An MSS boom is inevitable considering technology advancement and its acceptance. Models such as virtualization, cloud storage, IoT, and BYOD encourage MSS adoption. Also, Initiatives such as e-Governance, e-Kranti, and digital India also add to MSS growth.

2. With the increasing cyber security threats and breaches to enterprises becoming grave, assessment services are likely to have a stronger share among the large enterprises.

3. Extending the regulatory compliance measures to SMBs is likely to cause an overwhelming increase in adoption of MSS services by them.

4. The management/monitoring services segment is poised to a healthy growth is expected to be the highest growing segment. Assessment services and hosted / cloud-based services segment also will witness a growth momentum.

5. With new participants entering, the Indian market will set the competition to grow. Services such as DDoS protection, web and email security, SIEM, and risk assessment services will witness greater demand from large enterprises.

The Market Estimates mentioned above are End-user estimates

Revenue numbers in US $Million

<table>
<thead>
<tr>
<th>Year</th>
<th>Revenue</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>161,0</td>
</tr>
<tr>
<td>2016</td>
<td>185,7</td>
</tr>
<tr>
<td>2017</td>
<td>216,3</td>
</tr>
<tr>
<td>2018</td>
<td>255,4</td>
</tr>
<tr>
<td>2019</td>
<td>305,5</td>
</tr>
<tr>
<td>2020</td>
<td>372,7</td>
</tr>
</tbody>
</table>

US $1 = INR 64
# Managed Security Services – Vertical Analysis

## FY-15

<table>
<thead>
<tr>
<th>Vertical</th>
<th>Adoption Trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>BFSI</td>
<td>39%</td>
</tr>
<tr>
<td>Telecom</td>
<td>11%</td>
</tr>
<tr>
<td>Oil &amp; Gas</td>
<td>11%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>9%</td>
</tr>
<tr>
<td>Govt.</td>
<td>15%</td>
</tr>
<tr>
<td>Media</td>
<td>4%</td>
</tr>
<tr>
<td>IT / ITeS</td>
<td>9%</td>
</tr>
<tr>
<td>Others</td>
<td>2%</td>
</tr>
</tbody>
</table>

### Adoption Trends

- **BFSI and IT/ITeS** are the top spenders in this segment. These two verticals are the top contributors toward management / monitoring services, as compared to the other services.

- The stringent compliance and regulatory measures to safeguard transactions in the BFSI vertical allows them to contribute largely to the MSSP revenues.

- The **Government** vertical is a prominent contributor in the MSS market. As part of the defense strategy, the Government is adhering to MSS in order to secure vital information. Several security incidents such as web defacement attacks signalled the alert for more comprehensive cyber protection.

- The **Manufacturing** sector also exhibits increased spending on security services due to the “Make in India” boost to this sector.
Managed Security Services – Drivers and Restraints

**DRIVERS**

**Complex and Hybrid IT architecture in an enterprise**
- An increasingly sophisticated security landscape fundamentally challenges the capability and capacity of many enterprises’ IT set-up and forces them to turn to MSSP for complementary and advanced services.

**Shortage of cyber security professionals**
- Shortage of cyber security experts turn enterprises to MSSP. The expert shortage issue is so common across all countries in Asia-Pacific (APAC) that enterprises are facing challenges to acquire and retain resources.

**Regulatory and Compliance**
- Regulation and compliance mark another driving force towards adoption. Updated or new industry guidelines provide more in-depth and detailed advice to follow.

**Cloud-based security services**
- Actual adoption of cloud technology in the market drives the demand for cloud-based security services. Enterprises are attracted by the flexibility and scalability it offers.

**RESTRAINTS**

**Concerns over QoS**
- Concerns over service quality and reliability continue to impede market adoption.

**On-premise solution slows cloud adoption**
- The high propensity to retain on-premise product ownership for security concerns prevents enterprises from considering cloud-based security services.

**Lack of structured regulatory and compliance in certain verticals**
- Lack of industry compliance and regulation in some verticals and some developing countries attributes to the low market awareness and adoption rate.
Managed Security Services – Competition Landscape

Managed Security Services: Market Share Analysis, India, FY15

Classification of players

Tier-I
- Wipro
- Sify
- HCL
- Accenture
- Tata Consultancy Services

Tier-II
- IBM
- Microland
- CSC
- HP
- Dimension Data
- Symantec

Tier-III
- Singtel
- Tata Communications
- CtrlS
- nextra data

Others include NTT, Dimension Data, Symantec, CMS

Others include Reliance, TCL, Netmagic, Nxtgen, Wipro InfoTech, Sify, NxtraData, IBM, HCL Technologies, Net4, Tulip, HP, Infosys, AT&T, BT.

www.innovationnorway.no
Wipro’s comprehensive Managed Security Services are powered by its core service platform that encompasses all aspects of security. Key solutions and services that Wipro provides with their custom service delivery are:

- Security Intelligence as a Service
- Cyber Threat Management
- Platform Security Assurance
- Next Generation NAC
- Security Intelligence Center
- Wipro Identity Cloud
- Infrastructure Security Operations
- Infrastructure Security Monitoring
- Unified Threat and Vulnerability Management
- Advanced Security Services
- Security Support Services

Wipro has a customizable engagement model to suite diverse customer requirements. Wipro deploys best-of-breed solutions with a standard delivery framework.
## Managed Security Services – Vendor Profile

### Focus Products

Dell Managed Security Services enable a completely secure infrastructure, managing day-to-day security operations and proactively addressing the real threats to corporate networks.

- **Information Security Management Services** — Protect information assets, improve regulatory compliance, reduce costs, and remove the complexity in an enterprise.

- **Security Operations and Engineering Services** — Includes full outsourcing, co-management, monitoring, automated correlation and reporting, threat assessment, and security consulting.

- **Network Security Services** — Manage all network security devices including firewalls, intrusion detection systems, intrusion prevention systems, and access control technologies.

- **User Account Administration Services** — Offer complete solutions for provisioning user accounts for secure authentication and access to applications; provide control and management processes to create and delete user IDs, passwords, and security tokens required to protect information assets and address regulatory compliance requirements.

### Unique Value Propositions

- Dell Managed Security Services integrate seamlessly into any complex enterprise environment with service delivery tailored to suite each engagement, thus becoming an extension of enterprises’ security teams.

- Dell focuses on protecting enterprises’ digital assets against cyber threat, provide an intelligent defense that combines technology with global threat visibility, and industry-recognized expertise.
## Managed Security Services – Vendor Profile

<table>
<thead>
<tr>
<th>Focus Products</th>
<th>HCL offers Managed Security Services (MSS) to its customers through four of its Security Operation Centers. The company has a balanced approach, compliance, proactive security, techno-centric focus, and flexible delivery model to serve its global audience. The overall MSS portfolio of the company could be bundled as:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>Security Solution Management (on-site / remote)</strong> — Includes Policy Management, Change Management, Configuration Management, Signature Updates, Device fine tuning, Version Upgrade, and Reporting.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Managed Endpoint Security Services</strong> — Includes Virus / Malware / Spyware Monitoring, Outbreak Prevention, Signatures Update, Compliance Management, Deviation Reporting, Uniform Policy Management, and Configuration Management.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Anti-Phishing</strong> — Includes Proactive Domain and Phishing URLs Monitoring, Abuse Email Forwarding, Phishing Website Takedown, Reporting, and Forensics Analysis.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Anti-Malware</strong> — Web Application Malware Monitoring, Web Application Malware, Malicious Code Sandbox Analysis, Forensics, and Malware Reporting.</td>
</tr>
</tbody>
</table>

| Unique Value Propositions | • HCL’s Security Operation Centers (SOC) are ISO 27001, ISO 9001 and ISO 20000 certified. |
|                          | • The company offers 24x7 monitoring and management of security devices, network devices, servers, databases, applications, and Endpoints using HCL’s own Security Event Correlation framework. |
Market Opportunity

Advanced Threat Protection
Advanced Threat Protection solutions perform the task of preventing zero-day malware from penetrating the enterprise environment. In an event, where a polymorphic malware has managed to infiltrate the enterprise systems or network, these solutions perform real-time monitoring to check if the malware may detonate and initiate certain activities such as communications with the control and command center to push out corporate data.

| Sand boxing        | • On-premise / cloud-based virtual detonation or emulation for zero-day file analysis, correlate threat intelligence with other nodes.  
|                   | • Forward and scan / tap mode will need to incorporate remediation technology. |
| Remediation        | • Correlation with either endpoints or network security devices for scoping the attack, corrective actions on the users’ device such as file quarantines. |
| Rules-based Analytics / Heuristics | • Real-time threat intelligence feeds to help speed up identification and provide an investigative workbench to spot other unusual activities that could indicate new forms of attack. |
| Exploit detection  | • The ability to investigate at the code level of execution files, detect vulnerabilities that have been exploited, and remediate the risk. |
The ATP Solutions Market is Nascent, Growing and Fragmented

### Trends

<table>
<thead>
<tr>
<th></th>
<th>The ATP Solutions Market is in its nascent growth stage and is also highly fragmented, with several vendors offering diverse solutions, thereby driving the growth. Leveraging the growing concerns about the sophisticated threat landscape, many vendors carrying out extensive marketing activities to promote their products and solutions, which also resulted in increased adoption.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The rising concerns around advanced malware and other zero-day attacks bring in traction for Advanced Threat Protection (ATP) solutions among enterprises. MNC organizations in India are the primary adopters of ATP as a measure of their organizational global best practices. Again, dedicated on-premise solutions are preferred choice with enterprises as compared with their cloud-based counterparts.</td>
</tr>
<tr>
<td>2</td>
<td>Advanced security breaches have occurred in verticals, such as, BFSI, Government, Telecom, Energy that deal with sensitive and valuable information. These verticals are key adopters of ATP and will continue to drive the market in the future as well.</td>
</tr>
<tr>
<td>3</td>
<td>Indian enterprises are more reactive in terms of adoption of ATP solutions as compared to their global counterparts. Also, solution providers need to put in efforts in educating their customers about the comprehensive vision for advanced and targeted attacks.</td>
</tr>
<tr>
<td>4</td>
<td>Cyber criminals are using advanced tools and methods to launch targeted attacks and enterprises everyday face the challenge of threat mitigation from these sophisticate and evasive techniques. The use of social engineering, infected media, and zero-day exploits, email phishing will remain the mainstream approaches in the launch of APT attacks. In addition, the use of watering hole techniques to launch mass infections for a randomly potential target will also increase. System and web application vulnerability exploitation and data analytics will become the popular techniques used to understand and define targets before an attack.</td>
</tr>
</tbody>
</table>
Advanced Threat Protection – Drivers and Restraints

DRIVERS

The increase in APT-type attacks and other advanced malware threats

- With the emergence of new and advanced attacks that use multiple vectors and kill chains have caused huge data breaches across verticals.
- Legacy security technologies fail to defend against these types of threats, and as a result increasing number of enterprises look at new technologies and solutions.

Incomplete set of capabilities of legacy security approaches

- Legacy security solutions use signature-based technologies and fail to detect and prevent advanced malware. Thus, enterprises are looking for advanced security solutions that use signature-less detection technologies to identify threats. The new solutions must be integrated with signature-less technologies that are able to detect, prevent, and remediate the advanced threats in the network and endpoint, be it in the physical, virtual, or cloud environments.
- Key technologies that businesses are looking at include sandboxing, emulation, Big Data analytics, and anomaly behavior analysis. These technologies can be integrated with other protection solutions to conduct remediation and enhance protection levels across infrastructure.

RESTRAINTS

High cost and the rising complexity of APT solutions prevent customers from investing in dedicated technologies

- Enterprises find APT solutions to be expensive (especially, hardware appliance-based solutions). This raises major concerns in terms of the total cost of ownership of the solutions. As a result, many enterprises still opt for cost-effective security solutions, such as UTMs, firewalls, IPS, and content and endpoint security solutions.
- In addition, the complexity of the solutions and the need to integrate them into existing security infrastructure restrain companies from investing in them. The lack of skilled security professionals with expertise in advanced malware analysis and forensics dissuades companies from making use of these advanced solutions.

Numerous technologies offered by vendors may cause confusion in terms of businesses choosing the right solution

- An increasing number of security vendors have launched new products and solutions for APT and claim that their technologies are superior to the offerings of their competitors. Most of these products and solutions have left customers confused about what to adopt and may have contributed to the market leadership of the sandboxing technology. The situation also led to uncertainty among enterprises about the capability of the proposed solution, which may prevent them from adopting any of the offerings. A technology framework and strategy standard will help clients choose the right solutions for their needs.
Advanced Threat Protection – Vendor Profile

Focus Products

• FireEye is a specialized network security company that provides automated threat forensics and dynamic malware protection against advanced cyber threats. The company is focused on delivering comprehensive APT solutions across vectors, such as networks, content, endpoints, and mobile devices.

  – **Products**: Network security (NX Series), email security, (EX Series), content security (FX Series), endpoint security (HX Series), and forensics analytics (comprises the PX Series and the IA Series for enterprise forensics and the AX Series for malware analysis).

  – **Cloud-based Solutions**: Cloud-based email and mobile threat prevention platforms and the threat analytics platform.

  – All these solutions are powered by the company’s Multi-Vector Virtual Execution (MVX) technology and Dynamic Threat Intelligence (DTI) Cloud, which allow the sharing of actionable threat intelligence across the world.

  – FireEye MVX Engine, which provides organizations with signature-less detection capability to help protect against advanced malware and unknown and APT-type threats across the web, email, content, and mobile vectors. This is done by identifying and detonating suspicious content across multiple network flows, file types, Web objects, and email attachments within an instrumented and hardened proprietary hypervisor. FireEye also provides MVX-IPS as an optional license on the NX Series, which delivers the extended MVX technology to help detect advanced threats that bypassed traditional IPS solutions.

  – The MVX Engine is also powered by FireEye’s DTI Cloud that facilitates the distribution of critical threat intelligence from organizations across the world. This means that all these security products can connect with the FireEye DTI Cloud, which helps correlate multi-vector threat intelligence across products, locally and globally, and provides Big Data analytics-type capability to detect trends and identify potential or actual targets.

Unique Value Propositions

• FireEye continues to benefit from its strong reputation as a security specialist focusing on advanced malware, zero day, and APT solutions based on its signature-less detection technology.
## Advanced Threat Protection – Vendor Profile

Palo Alto Networks is a leading innovative network security vendor and is globally famous for its cutting-edge NGFW platform. In addition to the firewall platform, the company has been offering WildFire.

### Focus Products
- **Products**: WildFire, a public service in Palo Alto’s NGFW; WF-500, a dedicated appliance for private cloud.
  - WildFire is a cloud-based APT solution that is integrated with NGFW appliances, provides customers with flexible deployment models for its WildFire solution, which includes the WildFire subscription service and the on-premise appliance-based solution. In both cases, the WildFire solution works in conjunction with the NGFW platform to monitor advanced attacks caused by malware, such as zero day, by looking at both network traffic (domain name system (DNS)-based botnet signature detection) and individual files for the inspection of advanced malware.
  - While the NGFW platform helps protect the network with the traditional signature-based detection technologies, WildFire adds in the signature-less malware protection with the cloud-based sandbox that will analyze all suspicious traffic and files for advanced malware. The analysis insights will then be updated to all other security solutions to enhance protection capabilities.

### Unique Value Propositions
- The provision of an end-to-end security platform that covers network layer to endpoint and on-premise to cloud security has helped Palo Alto Networks secure a prominent position in the market. The vision to focus on prevention and remediation also sets it apart from the other vendors that focus on detection capabilities.
Cyber Security Product / Service Lifecycle Analysis

Market Value

- On-premise email security
- Firewall / IPsec VPN
- SSL VPN
- Management / monitoring services
- Next Generation Firewalls
- Sandboxing
- Forensic and Incident Response Services
- Mobile Security
- Security / Threat Intelligence

Time

Development → Growth → Maturity → Decline

Source: Frost & Sullivan
www.innovationnorway.no
Threats in Verticals
“Securing the cyberspace has become an important priority for governments, businesses, and citizens across the world. In line with the Prime Minister’s vision of making India a cyber-security expert nation and his recent exhortation to the industry, we have created the cyber security task force. This taskforce aims to make India a global hub for providing cyber security solutions including cyber security products and services. The taskforce will focus on the four key pillars of Industry development, Policy enablement, Technology development and Skill development.”

Mr. Rajendra Pawar, Chair, NASSCOM Cyber Security Task Force and Chairman, NIIT

Factors affecting cybercrimes in verticals

- Cyber criminals profile and motivation.
- Vertical-wise data and its importance in the dark net.
- Vertical-wise cyber security implementation.
- Well-defined IT regulatory framework and cyber laws.
- Skilled cyber law enforcement departments to identify cyber criminals.
- Prudent judicial system to assess the nature of the cyber crime and provide justice.
e-Commerce Transactions are More Prone to Cyber Attacks

**Trends**

- Use of mobile devices and apps for consumer banking.
- Introduction of financial services and offerings tailored to address the younger generations’ requirements.
- Information security threats originating from other nations.

**Vulnerabilities / Attacks**

- Phishing emails to employees, vendors, and customers to access to sensitive data in the web servers.
- Potent malwares to steal information such as credit card details, banking passwords, and email credentials from computers and mobile phones.
- Denial of Service (DoS) attacks damage trading systems network by blocking regular users to access the network / systems.
- Payment processors and gateways are frequently attacked by cyber attackers during e-Commerce and third-party payments by customers.
- Malicious software, websites, messages, mobile apps to access account information and credential of users during mobile transactions.
Critical National Infrastructure are Prone to Cyber Terrorism

Trends

- Digital India provides electronic services to their citizens such as digital locker, e-Education, e-Health, e-Sign, and national scholarship portal.
- Smart Cities to provide a conducive environment for both individual and commercial activities and overall development.

Vulnerabilities / Attacks

- Absence of dedicated data privacy and data protection laws may lead to unauthorized access to personal information and manipulation of citizens’ data.
- Under developed regulatory and legal framework, parliamentary oversight for e-Governance.
- Lack of offensive and defensive cyber security capabilities makes critical national infrastructure vulnerable.
- Inadequate cyber warfare and cyber terrorism policy leads to vulnerabilities in the Indian national defense and security.
Cyber Criminals Infiltrate Telecom Networks for Cyber Espionage

**Trends**

- Consolidation of telecom operators by mergers and acquisitions or spectrum sharing.
- Investment toward infrastructure capacity augmentation to provide high quality network services.
- OEMS to rise up the value chain by leveraging their potential in using analytics and other intelligent solutions.
- Strict regulations to be implemented to maintain quality of service and transparency.

**Vulnerabilities / Attacks**

- Leased infrastructure equipment from ISPs (home routers) are vulnerable to cyber attacks. The compromised equipment can be used to steal data, launch other malicious software anonymously, store exfiltrated data or access expensive services.
- Agencies (both public and private) may infiltrate telecom operators’ network to establish surreptitious surveillance.
- Sensitive customer data can be stolen from telecom operators’ data center and can be used to conduct identity theft, launch further attacks or blackmail customers.
Company Networks are Breached to Gain Access to Trade Secrets

**Trends**

- Susceptible to supply and pricing shocks due to large dependencies on imported fuel.
- Drive toward fuel efficiency due to reduce dependency on crude imports.
- Low domestic production, inadequate transmission, and distribution infrastructure in natural gas.

**Vulnerabilities / Attacks**

- Breached company networks (DDoS attacks) to gain access to trade secrets, sensitive financial information, client data.
- Malicious control of the operational technology and systems, such as software, sensors, SCADA systems that operate and control pipelines, power plants, and transmission and distribution grids.
- Damage physical infrastructure (such as cutting the fiber-optic cables).
Third-party Vendor Supply Chain is the Weakest Link in Hospital IT Systems

Trends

- Investment toward low-cost hospitals and other accessible points of healthcare delivery such as telemedicine.
- Increased penetration of medical insurance and access via mobile apps.
- Increased adoption of mobile health apps and medical wearable devices.
- Emergence of IoT platforms to integrate healthcare applications, devices, and things.

Vulnerabilities / Attacks

- Patient data theft due to employee negligence, accidental exposure or insider theft and lead to financial loss or exposing data to other nations for cyber warfare.
- IT systems and hospital networks have evolved over time resulting into a complex hybrid environment. This level of complexity poses a vulnerability in terms of managing the infrastructure and deploying a single security platform.
- Sharing of data with third parties, such as storing data in the cloud, poses a vulnerable situation for healthcare data.
- The third-party vendor supply chain is a vulnerable area for cyber attacks, where the hospital IT systems interact with third-party vendors’ systems for supply chain management.
DDoS Attacks are Commonplace Occurrence to Steal Media Content

Trends

- Rise of over-the-top (OTT) video services and videos on demand.
- Media content available across multiple platforms and also screens.
- Growth in Internet advertising, especially mobile.
- Upsurge of new video opportunities through connected devices.

Vulnerabilities / Attacks

- Media production networks, media storage locations are vulnerable to DDoS attacks, whereby the intruder gains access to content for malicious usage.
Maturity in India
CISOs to Step Up in Enhancing the Cyber Maturity of India

Indian security professionals are confident about their readiness in protecting enterprise networks since they adopt many security tools.

Indian organizations prefer cloud-based solutions and pay as you models for their security requirements.

Indian cyber security policy (2013) does not mandate Indian organizations to report security breaches for legal proceedings.

Indian organizations find it difficult to retain talent; hence, they are willing to outsourcing some security services.

CISOs / CSOs are likely to adopt analytical tools to analyze breaches and proactively eliminate security incidents.

Security as a platform gained traction from Indian CISOs as compared to series of point products or devices on the network. They believe that continuous monitoring threats will help more than having the best-of-breed products.
Cyber Security is an Emerging Market in India

**Market Trends**

**2012-2014**

*Consolidation, Partnerships*

Consolidation of market resulted in better distribution structure and improved technical competency. Several vendors have formed strategic partnerships to offer comprehensive solutions.

**2015-2017**

*Evolving market*

The proliferation of consumer-owned smartphones and tablets in the corporate network of organizations has given rise to security solutions that are designed specifically for BYOD. Networking vendors will aggressively expand their portfolios to address the consumerization of smartphones and tablets.

**2018-2020**

*Increasing role of hosted services*

The trend of strengthening partnerships between network security vendors and MSS providers will drive the adoption of hosted network security services, which will give rise to a pay-as-you-go model and provide more flexibility and scalability options for small- and mid-sized businesses.

Source: Frost & Sullivan analysis
Key Elements to Market Entry
The CISO Usually Makes the Final Decision of Procuring a Security Solution in India

**Solution Package**
- Enterprises prefer to opt for Security Product Suites over stand-alone offerings.
- Smaller companies look to use stand-alone products or SaaS-based security modules.

**Procurement Process**
- The CISO takes the inputs from the IT Head understanding the IT challenges much specific to the company’s needs and resorts to the best Security Solution.
- Many companies procure multiple vendor trial packages, thereafter selecting the one suitting both the process and budgeting necessities.

**Decision Maker**
CISO / CSO

**Solution Knowledge**
- Several Service providers reach out to the company with improvements in their offerings and pricing. The company evaluates the products and does a cost comparison of switching.

**Preferred Channels**
- The perception that direct sales has more dedicated customer support is waning as vendors are focusing on bettering their channel partners through training thus increasing the partner sales in India.
- In cases of high brand value vendors / re-sellers are also considered for competitive pricing options.

Purchasing decisions happen at the highest level and only get approval once a strong enough business case is made to weigh the benefits versus the investment (CapEx and Opex).
India being a Large and Complicated society, Security Vendors Tend to Increase their Spread through a Network of Trusted Partners

<table>
<thead>
<tr>
<th>Market Structure</th>
<th>Competition</th>
<th>Customer Needs</th>
</tr>
</thead>
</table>
| • The large enterprises remain a lucrative market in terms of licensing the security products. Vendors target this set of companies in acquiring such accounts and renewing them Year-on-Year.  
• The increase in cyber attacks on the Financial Sector across the world makes it easy for the security vendors to pitch in for advanced security solutions and tools. The increasing RBI mandates and the Indian cyber regulations push the financial companies to opt for the needs.  
• A significant chunk of revenue is expected to roll out from the SMB market. SaaS-based security services gels out well in this segment. | • Since the overall cyber security market is largely diversified, an environment of competition exists across security product lines (Network Security, Endpoint Security, Data Security, MSS) and type of vendors (Security Vendor, TSP, Distributor, SI, VAR). | • Customer needs differ depending on the size and the sector they cater to.  
• For example, the Financial Sector looks for complete security suites to maintain their sensitive information. While the backend of the data is being maintained by the on-premise security solutions, the front-end of the applications are addressed by the cloud-based models. Similarly, for an SMB, the security needs are largely very specific. They opt for stand-alone security tools in the form of SaaS-based model. |
Security Vendors Look to Push their Products in the Indian Market through Distributers, MSS Providers, and SI

<table>
<thead>
<tr>
<th>Sales Model</th>
<th>Pros / Cons</th>
<th>Key Success Factors</th>
</tr>
</thead>
</table>
| **Direct Sales Model**           | • High Profit Margins  
• More Controlled Pricing Structure  
• Cost Effective                  | • Brand value / Brand awareness, highly driving dominant market players’ solution sales  
• Price competitiveness rendered due to increase in customer base resulting to huge sales  
• Massive scope to tailor customer specific solutions driving further sales growth |
| **Pros**                         | • Huge CapEx structure for better market penetration  
• Hard to develop market awareness without channel partner / vendor outreach |                                                                                     |
| **Cons**                         |                                                                                           |                                                                                     |
| **Indirect Sales Model**         | • Larger reach through the network of the partners  
• Leverage the knowledge and roots already established by the partner | • Brand awareness of the reseller / distributor, which directly attracts more buyers  
• Geographic outreach capabilities, often lacking in dominant players with restricted penetration abilities  
• Strength across various regions and verticals |
| **Pros**                         | • Difficult to identify the right partner to build a network                                                   |
| **Cons**                         |                                                                                           |                                                                                     |
Indirect Sales Model is Very Common in India for Cyber Security Products

In this model, the partner takes most of the responsibilities of making the sale and setting up the solution for the customer

<table>
<thead>
<tr>
<th></th>
<th>Pre-sales</th>
<th>Contract sign-off</th>
<th>Customer Support</th>
<th>Integration / Customization</th>
<th>Billing</th>
</tr>
</thead>
</table>
| Distributor / Value-added Distributor | ![check](https://www.innovationnorway.no) | ![check](https://www.innovationnorway.no) | • As per SLA  
• Email, Hotline / Web-live support | ![check](https://www.innovationnorway.no) | ![check](https://www.innovationnorway.no) |
| MSS Provider         | ![check](https://www.innovationnorway.no) | ![check](https://www.innovationnorway.no) | • As per SLA  
• Email / Web-live support | ![check](https://www.innovationnorway.no) | ![check](https://www.innovationnorway.no) |
| Resellers / SI       | ![check](https://www.innovationnorway.no) | ![check](https://www.innovationnorway.no) | • As per SLA  
• Ticketing System | ![check](https://www.innovationnorway.no) | ![check](https://www.innovationnorway.no) |

- Partners usually provide customer support up to L1, which is the first line / front line customer support, and L2 levels, which is a more in-depth administrative level support,
- Vendors are only involved if there is an L3, which is the highest level of support in a three-tiered technical support model, responsible for handling the most difficult or advanced problems or L4 level of support, which is the escalation point beyond the organization.
- Other responsibilities lie with the partner with a level of revenue sharing as per the commitment between the vendor and the partner.
The Documental Formalities in Setting up the Companies could be Done Online

### Registering a New Business

<table>
<thead>
<tr>
<th>Registering in MCA</th>
<th>Obtaining Director Identification Number (DIN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Register in the Ministry of Corporate Affairs (MCA), by the Registrar of Companies for the state</td>
<td>• Register on MCA website</td>
</tr>
<tr>
<td>• The registration includes acquiring:</td>
<td>• Create a login ID by filling the DIN form and paying the mentioned fees</td>
</tr>
<tr>
<td>– Digital Signature Certificate (DSC)</td>
<td>• DIN generated</td>
</tr>
<tr>
<td>– Director Identity Number (DIN)</td>
<td></td>
</tr>
<tr>
<td>– Filing an e-Form / new user registration</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Business Entity Types</th>
<th>Offices of Foreign Entities in India</th>
<th>Obtaining Digital Signature Certificate (DSC)</th>
<th>Final Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary Legal Entities</strong></td>
<td><em>Liaison Office</em></td>
<td><em>DSC to be acquired from agencies appointed by the Controller of Certifying Authorities (CCA)</em></td>
<td><em>Incorporating company name, registering the office address and notice of appointment of company directors, managers, secretary, etc.</em></td>
</tr>
<tr>
<td>• Public Limited Company</td>
<td><em>Representative Office</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Private Limited Company</td>
<td><em>Project Office</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Unlimited Company</td>
<td><em>Branch Office</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Partnership</td>
<td><em>Wholly owned Subsidiary Company</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Sole Proprietorship</td>
<td><em>Joint Venture Company</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Offices of Foreign Entities in India</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Liaison Office</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Representative Office</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Project Office</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Branch Office</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Wholly owned Subsidiary Company</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Joint Venture Company</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The Indian Landscape
India is the seventh-largest country and the second most populous country in the world. By UN estimates, India’s population will exceed China’s by 2028.

In 2016-17, GDP growth is expected to be slightly better at around 7.8%.

The manufacturing sector under industry showed strong growth during 2015-16, and led to the overall growth of the industry sector at 7.3%.

While agricultural growth recovered, services experienced a slowdown.

The real per capita income during 2015-16 is estimated to reach INR 77,431 as against INR 72,889 in 2014-15.

Indian exports have been shrinking on account of a global slowdown in demand.

The current account deficit is expected to shrink to 1 to 1.3% by the end of 2015-16.

India was among the top 10 FDI host countries across the world in 2015-16.
India has a Relatively Young and Urban Population

- The **second most populous country** in the world, the UN estimates that India will exceed China’s population by the year 2028.
- The country has a **relatively young demographic profile**, with a median age of 27 years.
- India is in the midst of a **massive wave of urbanization** as approximately 10 Million people move to towns and cities each year in search of better economic opportunities.

- At 65.8%, the middle age group belonging to 15-64 years has the largest share of the total population (2014 est).
- The 0-14 age group comprises 28.5% of the total.
- 5.7% are over the age of 65 years, resulting in an elderly dependency ratio of 8.1%.
- The total dependency ratio is 51.8%.

**Total Population Estimation, India, 2010-2020**

- **2010**: 1.2 Billion
- **2013**: 1.25 Billion
- **2015**: 1.28 Billion
- **2020**: 1.35 Billion

**Population by Gender, India, 2014**

Sources: UN, CIA, World Population Review
The Government Focuses on Several Programs to Drive Economic Growth

Domestic Politics

Political Stability

- In May 2014, the National Democratic Alliance (NDA)-led by Narendra Modi from Bharatiya Janata Party came into power with a vast majority.
- The Modi Government will provide political stability and has improved India’s image.
- However, with a small presence in the Upper House, the new Government’s reform agenda is being thwarted by the opposition.

Internal Security

- Currently, the Maoist movement in the eastern part of the country is the single biggest internal security challenge for India.
- Insurgency in Jammu and Kashmir continues to impact the civilian population the most resulting in human casualty, refugee generation and economic stagnation.

Social Stability

- High and erratic inflation has corroded away household purchasing power.
- Meanwhile, the demographic surge of coming years will have to be positively utilised to ensure that all sections benefit from economic prosperity of the nation.

Policies

- The Modi Government has been focusing on its key programs of Digital India, Make in India, Pradhan Mantri Jan Dhan Yojana, Swachh Bharat Abhiyan, and Saansad Adarsh Gram Yojana to drive economic growth and prosperity.
- During the Digital India week in July, over 250 services were launched in areas including health information, utility services, smart public distribution system card, land record services, social welfare and pension services, electoral services, online court services, police services, and employment exchange services.
Agriculture, Industry, and Services are the Three Pillars of Growth

**Economy**
- The India economy is the seventh-largest in the world in terms of nominal GDP and the third largest in terms of purchasing power parity.
- The main growth engine of the economy is the export-oriented services sector.
- India grew at a rate of 7.2% in 2014.
- The country had a GDP per capita of US $1,627 in 2014.

**Agriculture**
- Agriculture contributes 17.9% to the GDP.
- India is a major exporter of agricultural products.
- The sector employs 49% of labor force.
- Key agricultural products include rice, wheat, oilseed, cotton, jute, tea, sugarcane, and lentils.

**Industry**
- Industry accounts for 24.2% of the GDP.
- The sector employs 20% of the labor force.
- Key industries are textiles, chemicals, steel, cement, and food processing.
- The Government is promoting manufacturing through its ‘Make in India’ program to increase the share of manufacturing to 25% of GDP.

**Services**
- The Services sector contributes 57.9% to the GDP.
- India has the second fastest growing services sector growing at a CAGR of 9%.
- The sector employs almost 31% of the labor force.
- Key industries include financial services, telecommunication, tourism, and insurance.

Sources: CIA, The Hindu, India Brand Equity Foundation, World Bank

www.innovationnorway.no
Political Stability has Brought Socio-eco-technological Progress in India

PESTLE Analysis, India, 2015

There is a high level of political stability with timely elections and a Government that won a thumping majority.

- **Political**: 3.5
- **Economic**: 4.5
- **Social**: 3
- **Technological**: 3.5
- **Legal**: 2.5
- **Environmental**: 3

India’s population and economic progress is taking a toil on its environment.

Outdated and archaic laws constrain the overall business climate and are in need of reform.

India’s ability to innovate and its skilled force in the digital space is a strong positive.

Long-term economic prospects for India are bright even as the country is on a rising growth trajectory.

Poor human development scores and income inequality constrain overall environment.

Rating indicates level of impact of PESTLE factors on growth. Scale = 0 to 5, where 0 is low impact & 5 is high impact.

Source: Frost & Sullivan analysis.
Important Factors that Garner Growth in India (1/2)

POLITICAL

• India, the world’s largest democracy, is enjoying political stability as the last general elections in 2014 returned the Modi Government with an overwhelming majority and a political mandate for reform.
• The new government India has helped to improve the country’s image and made some headway on the reform agenda.
• Long standing security concerns on the Jammu and Kashmir issue and rising Maoist insurgency continue to be problem areas for the Government.
• The absence of majority in the Upper House is likely to impact the Government’s ability to bring in legislative changes such as the Goods and Services Tax Act.

ECONOMIC

• India is the world’s seventh-largest economy in nominal terms and the third-largest economy in purchasing power parity terms.
• More importantly, India is one of the few emerging countries that has continued to grow and is expected to continue on the same trajectory amidst all the uncertainty and turmoil in other parts of the world.
• India is expected to grow at an average of 7.6% during 2015-2020.
• Other macroeconomic fundamentals such as inflation, fiscal deficit, and current account deficit have improved in recent months to provide a stable economic environment.
• India is a lower middle income country with a per capita income of US $1,808 in 2015.

SOCIAL

• India’s ranking in terms of its social indicators is low. About 71.2% of its population are literate. Life expectancy at birth is around 66.4 years.
• India is ranked 135th as per the Human Development Index with a score of 0.586 in 2013 and is termed as a country with medium level of human development.
• Furthermore, there is a lot of income disparity across regions and income groups.

Sources: Frost & Sullivan Analysis, CIA, India celebrating
**TECHNOLOGICAL**

- As per the Global Competitiveness Reports by the World Economic Forum, India was 52nd in terms of innovation and sophistication factors, whereas it ranked 121st in terms of technological readiness in 2014-15.
- India was ranked 110th in terms of availability of latest technology.
- India possesses one of the strongest IT sectors in the world and the Government focus on digitalization and technology can help the country to leapfrog into an advanced age.

**LEGAL**

- The Government is trying to bring change in labor law of the country. The new law is expected to integrate three labor laws into a single law — Industrial Disputes Act, 1947, the Trade Unions Act, 1926, and the Industrial Employment (Standing Orders) Act, 1946.
- Few changes such as the ability of a firm with over 300 staff to fire its employees without any prior notice and the need for 10% of the employees or 100 workers to register a trade union will help to improve the ease of doing business.
- In recent budget session, the Government of India deferred GAAR by two years and pledged not to initiate new cases under the country’s retroactive-tax law easing some of the worries of the investor community.

**ENVIRONMENTAL**

- India makes up 2.4% of the world’s land, while supporting 16% of the world’s population resulting in a burden in the form of unsustainable use of natural resources for several generations.
- Mismanagement and overuse of India’s once abundant forests has resulted in desertification, contamination, and soil depletion throughout the sub-continent.
- India is trying to use more of renewable resources to generate electricity and focus is on solar power.

Sources: Frost & Sullivan analysis, Wall Street Journal, India Briefing, Global Competitiveness report, One India.
2016-2017 is Expected to Witness Healthy GDP Growth

**Economic growth**

- GDP growth is expected to be the same or slightly better than 2015-16 clocking in at around 7.6-7.8% in 2016-17.
- Low commodity prices, recovery in consumer demand, and a normal monsoon will aid growth.

**El Nino Effect**

- The current El Nino that started in February 2015 is expected to continue to at least till the mid of 2016 and will result in prolonged moisture stress.
- On the upside, based on historical records, there is a possibility of La Nina being repeated toward late 2016 resulting in bumper crops.

**Targeting inflation**

- Below-potential growth will result in declining capacity utilization and downward pressure on inflation even as a normal monsoon will see food prices stabilizing.
- Other deflationary forces will arise from low commodity prices and slowing Chinese growth.
- Consequently, there is a change that inflation may be below the target of 5% by March 2017.

**Twin Balance Sheet Challenge**

- The twin balance sheet problem caused by non-performing assets of public sector banks and high leverage of large corporate houses has been impeding private investment and curbing a full-fledged economic recovery.
- How the Government recognizes, recapitalizes, resolves, and reforms these weaknesses will determine the robustness of recovery.

**Controlling Twin Deficits**

- According to World Bank — Commodity Markets Outlook 2016, commodity prices are expected to remain low while oil prices are expected to stay at current level. This will likely help the current account deficit to remain moderate in the coming fiscal year.
- The math to achieve the fiscal deficit target of 3.5% of GDP for 2016-17 can be upset if strategic sale target does not materialize.

Sources: The Hindu, NDTV, India Today, Economic Times, DNA India, India Incorporated
India Brings to Table Opportunities for Firms to Invest


- In the above radar chart, the distance to frontier (DTF) ratings have been near about same for most of the indicators for both the years except for the Protecting investors indicator where the DTF was up by 7.37 points meaning India strengthened minority investor protections by requiring greater disclosure of conflicts of interest by board members, increasing the remedies available in case of prejudicial related-party transactions and introducing additional safeguards for shareholders of privately held companies.
- The getting electricity showed a good progress as compared to last year by making electricity less costly by reducing the security deposit for a new connection.

Note: The above radar diagram is based on the distance to frontier (DTF) measure, where it depicts how much the regulatory environment for local entrepreneurs in the country has changed over time in absolute terms. And DTF numbers in the bracket indicate 2015 as against 2014 (2015/2014)

Source: World Bank
These findings are from a World Bank report that analyzed the implementation of reforms by the Indian states during the first half of calendar year 2015. Seven states were found to be in the aspiring leader group with scores between 50% and 75%. These were Andhra Pradesh, Chhattisgarh, Gujarat, Jharkhand, Madhya Pradesh, Odisha, and Rajasthan. Gujarat is the closest to being a leader (score above 75%) at 71.14%.

Source: Department of Industrial Policy and Promotion, World Bank, Ministry of External Affairs
State Performance on Key Requirements for Investments

**Industrial Land Allotment** is one of the basic criteria for any investor wanting to set up a facility while obtaining infrastructural utilities is essential for any sector. The fewer and easier the processes are the more convenient and cost-efficient the sector is. Lastly, labor regulations covering licensing, registration, approval or renewal processes are key to the success of labor-centric sectors.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>State</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Land allotment and obtaining construction permit</td>
<td>Madhya Pradesh</td>
<td>Availability of information on industrial land banks</td>
</tr>
<tr>
<td></td>
<td>Gujarat</td>
<td>Robust Geographic Information System to track industrial land and ensure key infrastructure such as road and water</td>
</tr>
<tr>
<td></td>
<td>Tamil Nadu</td>
<td>Online zonal plans for industrial lands available to aid building plans</td>
</tr>
<tr>
<td>Labor Compliance</td>
<td>Gujarat</td>
<td>Online labor department processes – licensing and renewal of licenses</td>
</tr>
<tr>
<td></td>
<td>Jharkhand</td>
<td>Online portal offering registration, licensing, and renewals</td>
</tr>
<tr>
<td></td>
<td>Andhra Pradesh</td>
<td>Offers factory plan approval processes</td>
</tr>
<tr>
<td>Obtaining infrastructural utilities</td>
<td>Gujarat</td>
<td>Utility connections given within 15 days</td>
</tr>
<tr>
<td></td>
<td>Maharashtra</td>
<td>Offers investor friendly services</td>
</tr>
<tr>
<td></td>
<td>Madhya Pradesh</td>
<td>Reduction in the number of documents to two</td>
</tr>
</tbody>
</table>

Source: State Assessment Report 2015, World Bank, Times of India, DNA India, India Today 142
Foreign direct investment inflows into India rose to US $27.7 Billion during April-December 2015, up from US $21.9 Billion a year ago.

Recently, the Government made a radical change by relaxing FDI norms in as many as 15 sectors, including defence, single brand retail, construction development, civil aviation, and LLPs, to boost FDI in the country.

According to the UNCTAD Report 2016, India ranks seventh with FDI flows of US $59 Billion in 2015 and is among the top 10 FDI host economies of the world.

Foreign institutional investor (FII) flows into India have slowed down during CY2015, on account of subdued quarterly earnings and fear of a possible rate hike by the US Federal Reserve and global slowdown.

Sources: DIPP, Economic times, Financial Express, Hindustan Times
<table>
<thead>
<tr>
<th>Reasons to Invest in India</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Favourable Demographics</strong></td>
</tr>
<tr>
<td>• According to World bank, India’s population will increase to 1.35 Billion by 2020, up from 1.2 Billion in 2015.</td>
</tr>
<tr>
<td>• Nearly 70% (906 Million) will be of working age.</td>
</tr>
<tr>
<td>• With 356 Million in the age group of 10-24 years, India has the world’s largest youth population.</td>
</tr>
<tr>
<td>• Highest university graduates by 2020.</td>
</tr>
<tr>
<td>• University educated workforce expected to rise from 54-56 Million to 114 Million by 2020.</td>
</tr>
<tr>
<td><strong>Growth Story</strong></td>
</tr>
<tr>
<td>• According to the IMF, India is likely to grow at an average of 7.6% during 2016-2020, as compared to average 6.2% growth in China.</td>
</tr>
<tr>
<td>• Growth acceleration to be driven by business-oriented reforms and improved investor sentiment.</td>
</tr>
<tr>
<td>• Growth to benefit from recent policy reforms, a consequent pick-up in investment, and lower oil prices.</td>
</tr>
<tr>
<td>• FDI in India is expected to rise by 45% in 2016.</td>
</tr>
<tr>
<td>• Foreign investment limits raised in several sectors including private banks, defense, and non-news entertainment media.</td>
</tr>
<tr>
<td><strong>Consumption Growth Story</strong></td>
</tr>
<tr>
<td>• Consumption accounts for around 68% of the GDP of India.</td>
</tr>
<tr>
<td>• Expanding middle class, rising incomes, and increasing spending power along with a large youth population and rapid urbanization will continue to boost consumption.</td>
</tr>
<tr>
<td>• According to Ernst &amp; Young, India’s middle class, which is about 50 Million or 5% of the population, will reach 200 Million by 2020.</td>
</tr>
<tr>
<td>• India will add more people than China to the global middle class by 2030 creating a huge market for companies.</td>
</tr>
</tbody>
</table>

Source: IMF, United Nation, Ernst & Young, BCG, Morgan Stanley, PIB
Appendix
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>USD</td>
<td>United States Dollars</td>
</tr>
<tr>
<td>CAGR</td>
<td>Compound Annual Growth Rate</td>
</tr>
<tr>
<td>Fintech</td>
<td>Financial Technology, technologies developed to make financial services efficient. These companies are mostly start-ups, like Paytm, Mobikwik.</td>
</tr>
<tr>
<td>SME</td>
<td>Small and Medium Enterprises</td>
</tr>
<tr>
<td>BFSI</td>
<td>Banking and Financial Services Industry</td>
</tr>
<tr>
<td>CISO</td>
<td>Chief Information Security Officer</td>
</tr>
<tr>
<td>CSO</td>
<td>Chief Security Officer</td>
</tr>
<tr>
<td>POS</td>
<td>Point of Sale</td>
</tr>
<tr>
<td>DeitY</td>
<td>Department of Electronics and Information Communication</td>
</tr>
<tr>
<td>R&amp;D</td>
<td>Research and Development</td>
</tr>
<tr>
<td>NCIIPC</td>
<td>National Critical Information Infrastructure Protection Centre</td>
</tr>
<tr>
<td>DSCI</td>
<td>Data Security Council of India</td>
</tr>
<tr>
<td>CAT</td>
<td>Cyber Appellate Tribunal</td>
</tr>
<tr>
<td>CRAT</td>
<td>Cyber Regulations Appellate Tribunal</td>
</tr>
<tr>
<td>CERT-In</td>
<td>Indian Computer Emergency Response Team</td>
</tr>
<tr>
<td>CCA</td>
<td>Controller of Certifying Authorities</td>
</tr>
<tr>
<td>STQC</td>
<td>Standardisation Testing and Quality Certification</td>
</tr>
<tr>
<td>EDS</td>
<td>Electronic Delivery of Services</td>
</tr>
<tr>
<td>NTRO</td>
<td>National Technical Research Organization</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>MSS</td>
<td>Managed Security Services</td>
</tr>
<tr>
<td>TSP</td>
<td>Telecom Service Providers</td>
</tr>
<tr>
<td>BYOD</td>
<td>Bring Your Own Device</td>
</tr>
<tr>
<td>APT</td>
<td>Advanced Persistent Threat</td>
</tr>
<tr>
<td>GTM</td>
<td>Go-to-Market</td>
</tr>
<tr>
<td>MSE</td>
<td>Micro and Small Enterprises</td>
</tr>
<tr>
<td>RBI</td>
<td>Reserve Bank of India</td>
</tr>
<tr>
<td>OEM</td>
<td>Original Equipment Manufacturer</td>
</tr>
<tr>
<td>SI</td>
<td>System Integrator</td>
</tr>
<tr>
<td>IAM</td>
<td>Identity and Access Management</td>
</tr>
<tr>
<td>VMS</td>
<td>Vulnerability Management services</td>
</tr>
<tr>
<td>DDoS</td>
<td>Dedicated Denial of Service</td>
</tr>
<tr>
<td>SIEM</td>
<td>Security Information and Event Management</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Prevention System</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>NGFW</td>
<td>Next Generation Firewall</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>NGIPS</td>
<td>Next Generation IPS</td>
</tr>
<tr>
<td>AMP</td>
<td>Advanced Malware Protection</td>
</tr>
<tr>
<td>DLP</td>
<td>Data Loss Prevention</td>
</tr>
<tr>
<td>MNC</td>
<td>Multi National Corporation</td>
</tr>
<tr>
<td>CSP</td>
<td>Conferencing Service Provider</td>
</tr>
<tr>
<td>FDI</td>
<td>Foreign Direct Investment</td>
</tr>
<tr>
<td>ITeS</td>
<td>Information Technology-enabled Services</td>
</tr>
</tbody>
</table>
Thank You