DSCI

PROMOTING DATA PROTECTION

A NASSCOM® Initiative

INDIA CYBERSECURITY INDUSTRY

SERVICES AND PRODUCT GROWTH STORY

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

4th Floor, NASSCOM Campus
Plot No. 7-10, Sector 126, Noida
Uttar Pradesh 201303, India
E-mail: research@dsci.in

Copyright & Disclaimer

The information contained herein has been obtained from sources believed to be reliable. DSCI disclaims all warranties as to the accuracy, completeness or adequacy of such information. DSCI shall have no liability for errors, omissions or inadequacies in the information contained herein, or for interpretations thereof.

Usage of Information

Forwarding/copying/using in publications without approval from DSCI will be considered as infringement of intellectual property rights.

Foreword

Rama Vedashree

CEO, DSCI

The digital transformation journey across the globe significantly picked up pace due to the pandemic. Initially, the focus was on business continuity but now there is a notable shift in digitalisation dynamics. As organizations settle into the new reality, they are now crafting their organizational strategy to be led Digitally. As the remote working trend pushes us into a borderless network setup, the adoption of Cloud have become a key investment priority globally. This rapid digitalization has led to an increased regulatory attention from a data and privacy perspective, integration of new technology stacks to enterprise IT, and adoption of cloud, and remote collaboration tools. These trends combined with the growing awareness at board and CXO level around cyber threats is pushing the worldwide cybersecurity demand and spend. The Indian IT services with its global expertise and experience, along with the innovative Indian cybersecurity product ecosystem have been the twin growth engines securing the digital transformational journey of customers globally.

In the last two years, the Indian cybersecurity industry has witnessed significant growth. The prominent global presence of the Indian cybersecurity industry can be felt on back of its unyielding commitment to ensure a secure transformation journey spanning across all verticals and large enterprises and SMBs. It is noteworthy to mention that from a revenue perspective, the cybersecurity services industry has grown from USD ~4.3 Bn in the calendar year 2019 and is projected to clock USD ~8.5 Bn in CY 2021. The employee base surged from 110K in 2019 to reach 218K in 2021 owing to the immense demand for cybersecurity professionals. The cybersecurity start-up and product industry also exhibited robust growth, increasing from 175 companies in 2018 to around 265+ companies in 2021 and attaining an industry revenue of USD 1.37 Bn. The talent pool in the Indian Product companies has grown from 15K in 2019 and touched 27K in 2021.

The Indian cybersecurity industry is fostering a partnership mindset. The collaboration between ecosystem stakeholders such as academia, government, services majors, start-ups is creating a conducive ecosystem. DSCI has been focused on creating and growing the start-up ecosystem by facilitating incubation and acceleration programs, funding opportunities, new products through use cases, a robust talent pool, and enabling start-ups to expand their global footprint. India is indeed becoming a trusted and natural partner of choice for providing cybersecurity services and products globally.

This report aims to narrate the growth story of the Indian cybersecurity Industry and covers facets such as revenue analysis, innovation strategy, global expansion, talent initiatives, and advancements in technology adoption, process automation, deployment models and offerings. The report features a compendium of rich case studies, carefully curated to showcase how our Industry members are enabling secure digital transformation and cloud adoption. It also captures the voice of industry leaders who are pushing the boundaries to grow in this strategic domain.

We sincerely hope that this research report gives you a better insight into the Indian cybersecurity landscape and its capabilities to drive your digital transformation journey in a secure and trusted way.

Shri Ajay Prakash Sawhney
Secretary, Ministry of Electronics
& Information Technology,
Government of India

"Government of India and MeitY have a comprehensive Digital India Programme and the pandemic has provided a further push to digitalization, taking Government services online. India's Cyber Security Industry was at the forefront supporting Government and all critical sectors to manage the heightened cyber security risk in the last two years. The `India Cybersecurity Industry Report', showcases the capabilities of the Indian Cybersecurity Services and Start-ups and the continuous innovation in products and services to serve customers in India and globally. Ministry of Electronics & IT is committed to partnering with DSCI to scale up our innovation in emerging areas like 5G, Hardware, IoT Security, and through our flagship ISEA and FutureSkills Programes, meet the talent demand of the Industry."

Rajendra S Pawar

Chairman, DSCI

“Globally the pandemic has fast tracked digitization and with digital being the new norm, Cyber has now become a predominant risk at a company and country level. It is heartening to note that in line with our vision to make India a Global Hub for Cyber Security, the Products and Services Industry has scaled up to meet the rising Global and Domestic demand. While the services industry is expanding its footprint globally through a platform-led Security offerings and cloud-based managed security services, the young product industry is innovating on new solution areas with a cloud-first strategy to reach global customers. A strong synergy in the ecosystem of Services and Products players, will propel India to tap the growing Cyber Security demand and grow to USD 35 billion by 2025.”

Debjani Ghosh

President, NASSCOM

"Every crisis has a silver lining and for the pandemic, it has been the accelerated adoption of digital solutions across enterprises and government. Decade’s worth of digital transformation has taken place in the last two years and India’s technology industry has emerged as the preferred digital solutions partner with cybersecurity as a key growth vertical. Cybersecurity is now a boardroom agenda and offers tremendous opportunities for India’s tech industry to build innovative solutions and services. Enabling policies, an expanding skilled talent pool, domain expertise and a connected ecosystem with start-ups and academia, India is rapidly expanding its cybersecurity capabilities and emerging as the hub for all things digital with security and trust as its foundation."

Executive Summary

Revenue Insights

- The Indian Cybersecurity Services Industry grew from USD 4,3 Bn in 2019 to USD ~8.5 Bn in 2021
- Indian cybersecurity products grew from USD 740 Mn in 2019 to reach USD 1.37 Bn in 2021

Technology

- From the analyzed companies, 74% of the products and services companies leverage AI/ML
- Cloud and Automation driving innovation

Geographic Revenue

- Services companies garnered 80-85% of their revenue from the global market
- 60-65% of product companies revenue predominantly came from the Indian market

Offerings

- **MSS** is the leading the services segment with 63%, followed by cloud at 58%
- **Data Security** offered by 62% respondents, followed by cloud at 57%

Innovation

- Cloud based services and products, imbued with AI/MI
- Services- Privacy, IAM, GRC, Data security
- Products- ZTNA, CASB, MDR/EDR, IAM (PAM), Privacy

Talent

- In 2021, services companies have a cybersecurity workforce of 2.18 Lakhs, where as products have ~27K

Key Investment Priorities

- Services –skilling talent and expanding existing customer base
- Products companies- R&D and marketing initiatives

Platform

- 78% of Indian cybersecurity services companies analyzed offer platform-based services and ~76% product companies analyzed offer platform-based products

TABLE OF CONTENTS

Research Methodology

As part of DSCI's industry development initiative, the report titled '**India Cybersecurity Industry**' was developed through a three-month comprehensive study. This report is a result of a detailed study of 100 plus cybersecurity product and services companies.

Scope: The report aims to showcase the different facets of the Indian cybersecurity Industry such as aggregate value, global footprint, innovation drive, talent & skilling initiatives and technological advancements. It delves into the cybersecurity services & product segments and shows how the industry is creating an impact on a global level attention to the evolving threat landscape across countries. It illustrates the growing demand and necessity of cybersecurity solutions.

Objective: To showcase the capabilities of the Indian Cybersecurity industry and **its emergence as a Global hub for cybersecurity**.

IDENTIFICATION OF COMPANIES

(A near comprehensive list of 300+ Indian Cyber

Security Companies created)

PRIMARY RESEARCH

(Survey-based data gathering)

DESK RESEARCH

(Data validation and profiling of 300+ companies)

EXPERT INTERVIEWS

(Discussions with a cross section of CEOs/ Founders/Industry leaders to validate cumulative trends and obtain deeper insights)

FINAL ANALYSIS & REPORT CREATION

Global Cybersecurity

Market Overview

Global Cybersecurity Spend

Key Drivers

Emerging trend of remote working

- Outbreak of COVID-19 pandemic has surged the trend for remote working and the enterprise networks have gone borderless.
- This change is ramping up infrastructure, end point and cloud security spend.
- Gartner forecasted that 51% of Global Knowledge Workers will be remote by the end of 2021

Rising incidences of cyberattacks

- As per a report published by IBM, the data breach costs increased from USD 3.86 million to USD 4.24 million, which is the highest average total cost in the 17-years history
- The growth in edge devices without proper security and policy safeguards are increasing the attack surface and in turn increasing vulnerabilities

Adoption of IoT and advanced technologies

- IT/OT/ICS in supply chain or critical infrastructures are particularly vulnerable if not secured properly. Legacy OT systems converging with IT infra, requires protection against cyber-attacks
- IDC predicts that there will be 55.7 Bn IoT devices and will generate 73.1 zettabytes of data by 2025

Increased need for cybersecurity professionals

- Cybersecurity staffing and company-wide security training is a top priority.
- Well-trained cybersecurity professionals are in high demand and dependence on a more distributed workforce is creating a more critical need for them in 2021.
- Organizations are investing in cross skilling employees and training fresh employees to specific cyber domains

Regulatory and compliance requirements

- Data privacy is taking a larger role in the security of organizations across all industries due to global data compliance laws
- Regulatory frameworks by the government to adhere to industry standards is another prominent growth factor
- The need to secure vendors/third-parties/sub-contractors in order to have a strong cyber/privacy posture is driving demand

Rising focus towards cybersecurity

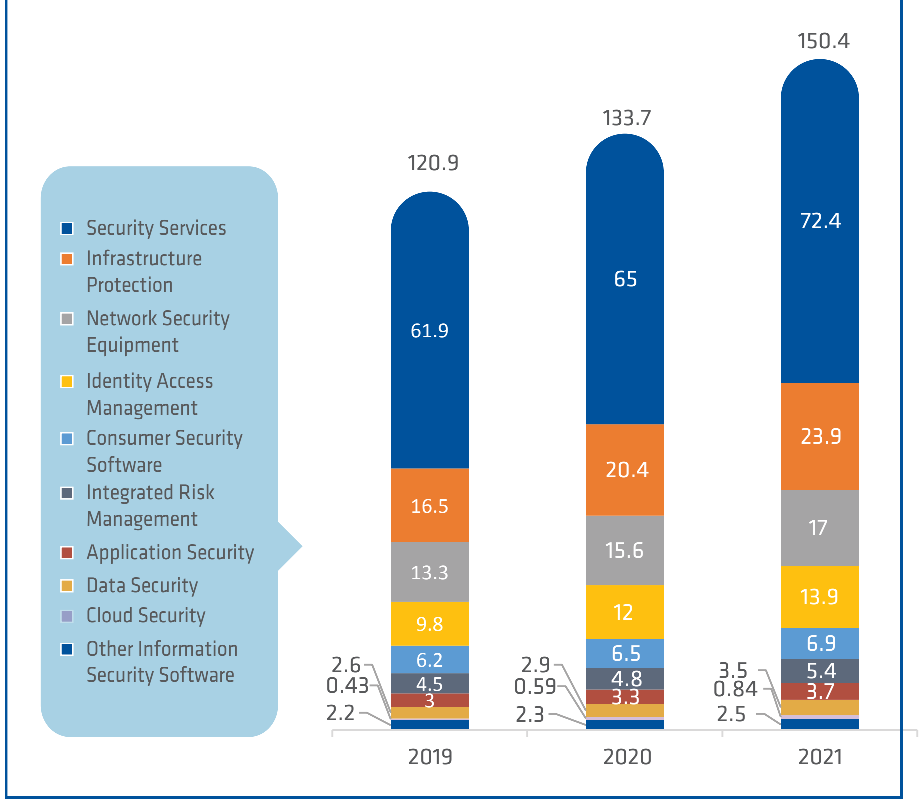
- With the increasing regulatory attention and consumer awareness towards security breaches and attacks, the enterprises large and medium are mitigating risk by security adoption
- IDC expects worldwide security spending to reach USD 174.7Bn in 2024 with a CAGR of 8.1% over the 2020-2024 forecast period

Source: Gartner, Deloitte, IDC, Gartner, IDC, IBM, Pandasecurity

Global Cybersecurity Landscape

Market Overview

Information Security & Risk Management End User Spending by Segment, 2019-2021 (USD Bn)



The global spend on information security, risk management technologies and services was predicted to grow by 12.4% and touch USD 150.4Bn in 2021

Overview

- **Remote working scenario**: The continuous surge in the demand for remote working technologies and cloud is a major driver for cybersecurity spend.
  - Software as a Service and Public Cloud adoption has seen a sharp rise, and the evolving Data Protection regulations is creating a higher compliance burden with the Cloud-First preference of businesses
- **Surge in Automation, AI & ML**: The market's focus is shifting towards automation and the adoption of machine learning technologies for cybersecurity
- **Shift in priority**: With Boards and Regulators, Governments taking cognizance of Cyber as a key risk at a company and country level, Cyber Security is getting higher budgetary allocations
- **End-users**: B2C organizations, BFSI, Healthcare are demonstrating higher maturity, and increased spend for cyber security.

Offerings

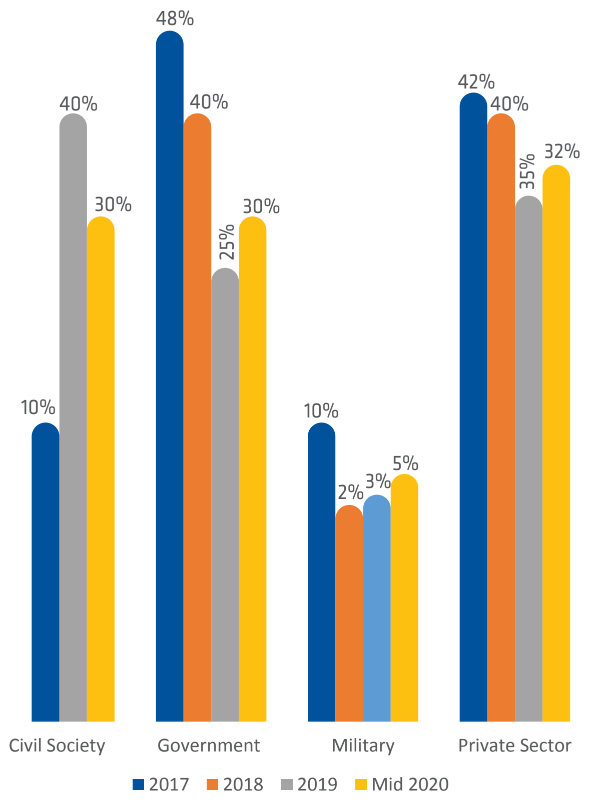
- **Security Services** - Garners the highest share of the security spend to the tune of USD 72.5Bn, spanning Consulting, MSSP, hardware services.
- **Cloud security**- cloud access security brokers (CASB), is the smallest yet fastest growing market segment to mitigate risks arising from cloud adoption
- **Integrated Risk Management (IRM)** - is witnessing a robust double-digit growth owing to the need for compliance and newly discovered risks during the global pandemic crisis. Key drivers:
  - Integration of new technology
  - Third-party risk management & supply chain management

Source: Gartner, Gartner 2020, Mckinsey, Infosys

Threat Landscape

Call for Action

Cyberattacks by Sectors



Advancements in Cyberthreats

Insider threat and vulnerabilities

1. Between 2018 and 2020, there was a 47% increase in the frequency of incidents involving Insider Threats.
   1.1. This includes malicious data exfiltration and accidental data loss.
2. Poor configuration, lack of training/awareness, and inadequate cyber policy in an organisation are increasing the risk of threats and vulnerabilities.

Increasing incidences of Ransomware as a Service (RaaS)

1. Rise in the number of threat actors who offer Ransomeware-as-a-service (RaaS)
2. Ryuk, Bitpaymer, Gandcrab, Hermes, Revil, Dharm, Egregor, Nempty, Avaddon, and Conti were common ransomware actors in 2021

DDoS attacks

1. Between January 2020 and March 2021, DDoS attacks increased by 55% while growing in complexity, with 54% of incidents using multiple attack vectors
2. The biggest attack over the past 15 months was at 500 Gbps and used at least five different attack vectors
3. The technology sector was the most targeted, receiving 27% of all DDoS attacks over the past 15 months.

Social Engineering

1. Emerging trend of social engineering in 2021 include: increasing 'consent phishing', deepfakes, expansion of Phishing-as-a-Service market, and deployment of customized phishing Email using AI
2. Social engineering is the most prominent way of committing crime by targeting not only businesses but individuals too

Role of Artificial Intelligence in Cyber Attacks

1. As the security evolves , threat actors are also evolving. AI/ML is being used to crack passwords, break CAPTCHA, clone voice, and find vulnerabilities
2. In 2021, FBI stated that malicious actors will leverage "synthetic content" including deep fakes for cyber and foreign influence operations in the next 12-18 months

Source: F5, Mckinsey, Infosys, FBI, Cybersecurity Works, Kaspersky 2021, WIPRO, Tessian

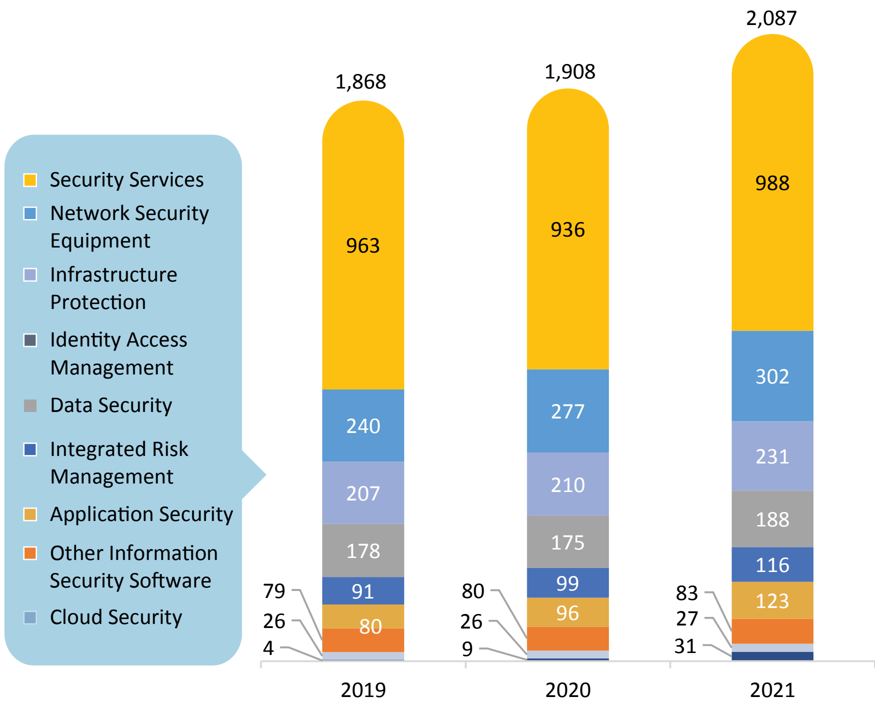
Domestic Cybersecurity

Market Overview – India

India Cybersecurity Spending

Key Insights

Information Security & Risk Management, End User Spending by Segment, 2019-2021 (USD Mn)



In India, the total Enterprise Information Security and Risk Management spend is USD 2.08 Bn in 2021, and has increased by 9.5% as compared to 2020.

Key Drivers

- **Tightening of regulatory norms** in Banking, Healthcare, Insurance, Capital Markets and Critical Information Infrastructure like Energy, Oil & Gas.
- **Stepping up of readiness** by IT Sector which services global customers across various geographies and verticals
- **The accelerated focus on digitalization** due to the pandemic and ongoing initiatives including Make in India, Digital India, National Health Mission and smart cities
- **Surge in number of Cyberattacks** - 3X increase in cyber attacks resulting in increased budgets and attention on cyber security
- **Government initiatives** such as Smart Cites, Digital Indian and sectoral regulations such as RBI Cybersecurity framework, IRDAI, and directives from CERT or NCIIPC are driving domestic demand

Trends

- Emergence of 5G - The upcoming rollout will increase the total number of connected devices and data generated. Securing and analyzing the data (for malicious packets) will grow cybersecurity demand
- Cloud adoption leading to development of new tools will drive application security demand
- IT & OT convergence - Secure integration of OT systems to internet will drive demand
- Shift in enterprise mind set - Security moving from a after thought to become an enterprise priority

Offerings

- Security services dominate the market share in terms of segments
  - MSS garners the lions share
- Cloud security growing at the fastest pace
- IAM, GRC, Application security, Data (privacy, DLP) security high In demand

Source: Gartner 2019, Gartner 2021: Economic times, DSCI

India Cybersecurity Services and Product

Industry Overview

India Cybersecurity Industry

Key Insights

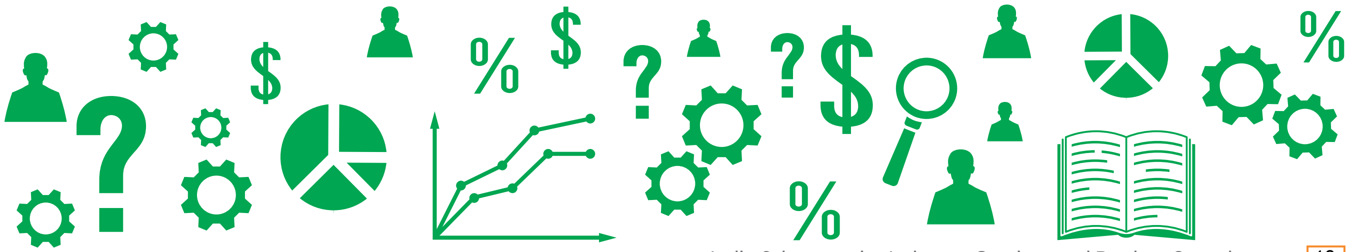
TRENDS IN THE INDUSTRY

- **Remote workforce**: Increase in digital footprint due to digitalization has led to demand of secure and compliance frameworks & infrastructure development
  - The rapid adoption of perimeter-less enterprise networks is leading to demand for secure firewalls, routers, and access management operations
  - With shift in demand dynamics, the Indian cybersecurity industry became quick to innovate, it also started offering customized and turn - key holistic security solutions.

- **The cybersecurity start-ups** are reinventing themselves with new digital marketing channels & sales process automation strategies. They have also grown their funding portfolio substantially to USD ~779 Mn cumulatively in 2021.
  - They have achieved faster product innovation cycles and created new deployment models
  - They have been growing their international presence via a robust partnership ecosystem and SaaS based delivery models
  - They are offering cutting edge threat identification and response automation products

- **Partnership models** are being forged between SI's and start-ups to explore synergies in customer offerings. The services companies acquire/partner start-ups with innovation in niche areas for specific use cases and start-ups get the advantage of sell-through partnership to a large customer base, capital, experience and infrastructure

- The services companies are leveraging their global expertise and experience for offering end-to-end transformational services and platform based services.
  - From consultation to implementation and management of security controls and frameworks, they have imbibed security right from DevOps to ensure that the clients' and end-user data & privacy are protected



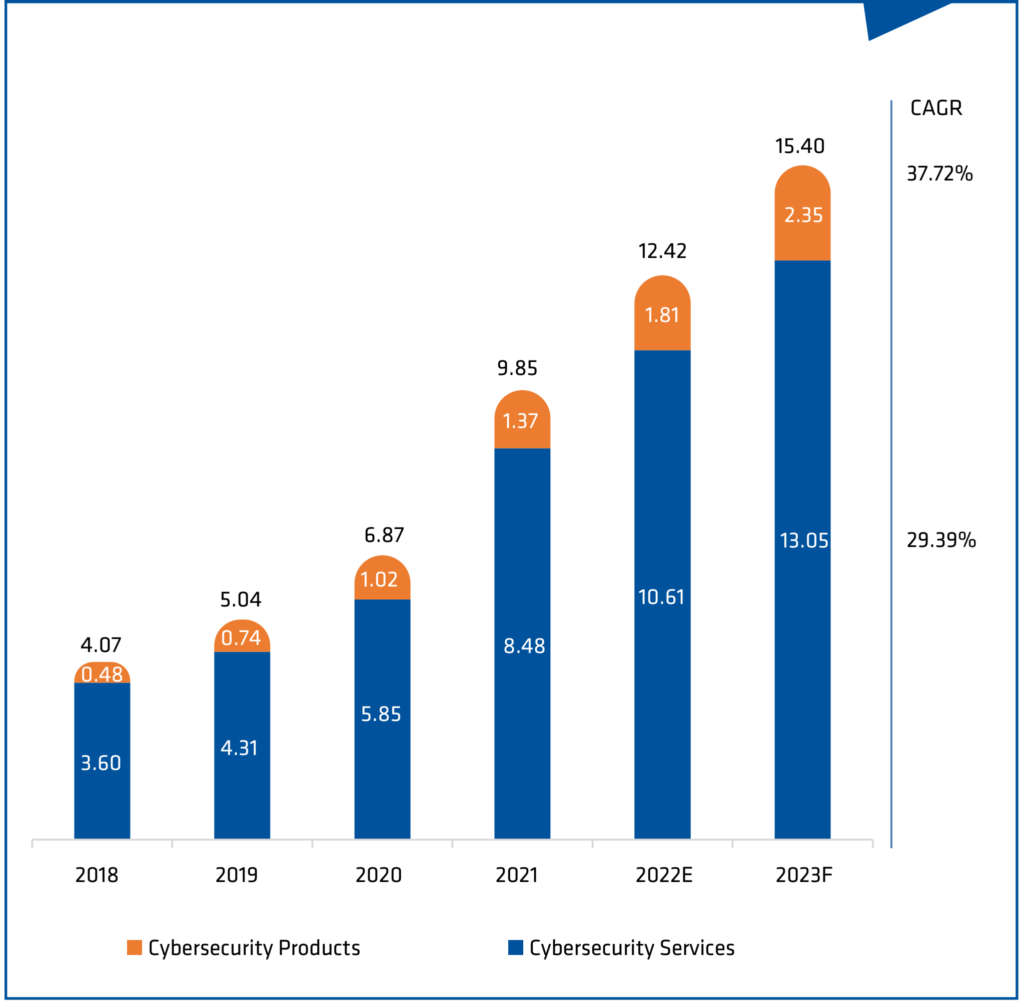
Source: DSCI Analysis and industry interviews

India Cybersecurity Industry

Overview

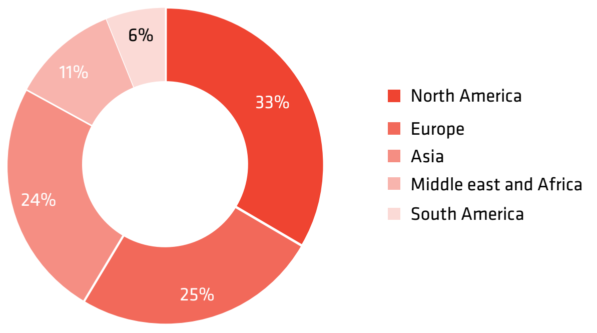
India's cybersecurity services and product industry have a combined revenue of USD 9.85 Bn in 2021

India Cybersecurity Industry Revenue (USD Bn, 2018-2023)



- The services and product industry have a total revenue of USD 9.85 Bn in 2021 and grew at a CAGR of ~40% in the last two years.
- The key drivers of the Indian cybersecurity Industry are:
  - Adoption of cloud first strategy
  - Business led innovation- remote working conditions
  - Growing threat landscape and awareness around threats
  - Global and domestic regulations around compliance, and data privacy
- North America and Europe continue to be the leading geographies for Services and Product Revenues with combined 58% revenue contribution.
- Asia and MEA are the fastest growing geographies

Geographic Revenue Split



Source: DSCI Analysis and industry interviews

Cloud

The key enabler for digitalization

01 Cloud adoption

- Last couple of years witnessed a surge in adoption of multi-Cloud, Hybrid cloud, Hyperscaler and SD-WANs & VDI's
- Migration to Cloud became a key priority for every CIO's digitization and business continuity roadmaps, and CSPs and Managed Cloud Service Providers scaled up to support cloud migration demand of an unprecedented scale.
- The shift to remote infrastructure continues to drive the demand for cloud and remote network security

02 Benefits of cloud-based security

- Decreases the total cost of ownership
- Simplifies vendor management
- Sharing of threat intel through platforms
- Ease of deployment and integration
- Offers dynamic elasticity and scalability

03 Sectoral adoption

- Cloud adoption is at different stages across the industry due to factors such as strict data compliance laws and legacy architecture
- The public sector Banks and other regulated sectors are in talks of creating consortiums for secure cloud adoption
- Private sector and SMEs are rapidly adopting cloud

Key Questions asked by organizations

- Key questions asked by organizations for secure cloud adoption
- What all needs to be secured and what is the ROI?
- How can we secure remote access to my corporate application?
- How do we provide secure access to internet applications?
- How to secure virtualized environment- VDI interface?

04 Opportunity areas

- Cloud adoption in the Public sector is more regulated and requires tighter controls ;creating the requirement for secure and compliant data migration
- Awareness and comprehension of the shared responsibility matrix is still quiet low; Cloud security strategy and consulting can be provided for creating frameworks
- Data compliance from privacy and data localization perspective is pushing demand for GRC solutions

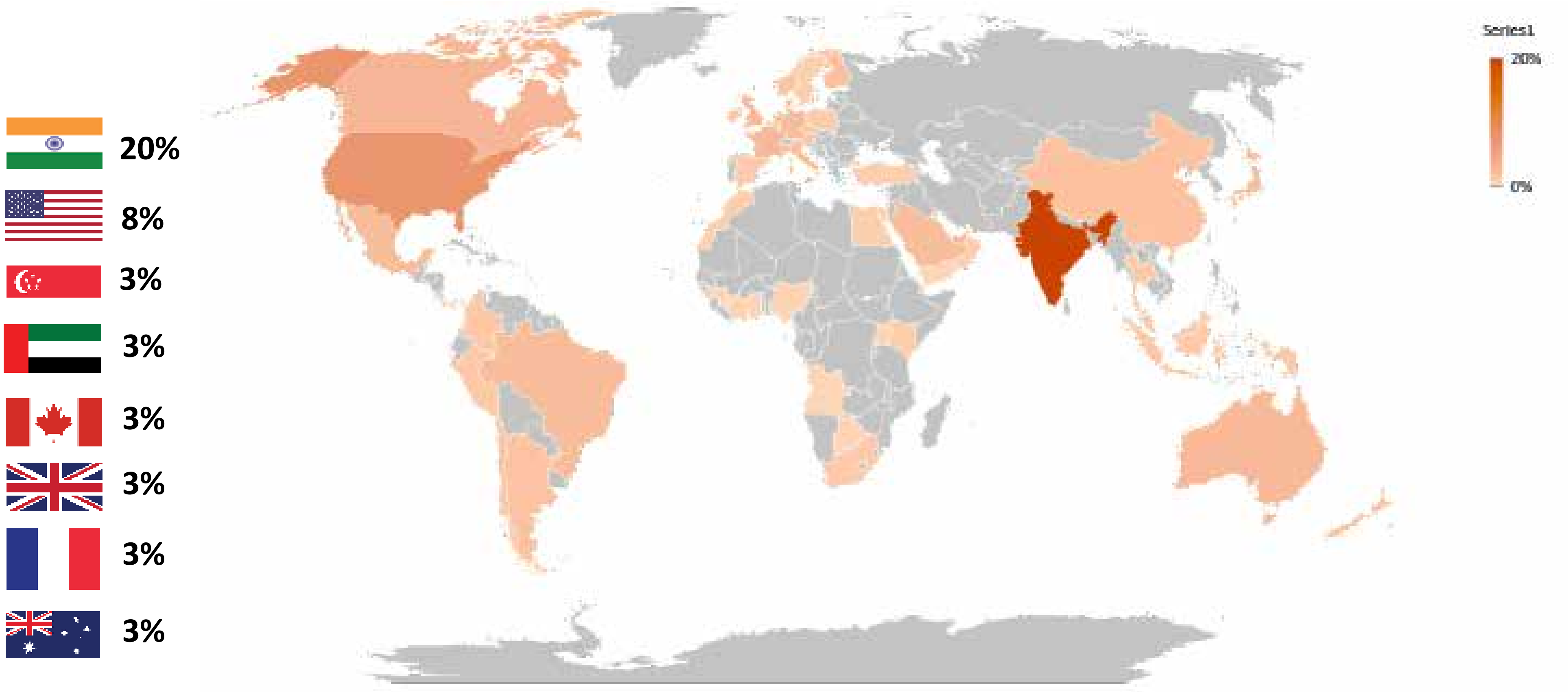
05 Key offerings

- Increased demand around data privacy, user access rights & behavior monitoring, configuration and vulnerability management, application security and compliance.
- Cloud security technology, tools and products on the rise (XDR, EDR, MDR, IAM, UEBA, ZTNA, CASB, CWPP, CSPM)
- SASE and ZTNA architecture assuming central role in cloud journey

Source: Industry interviews

India's Growing Global Footprint

Global Presence of Indian Product and Services Companies



- The product companies in India are expanding their global footprint through a robust network of channel partners. The emergence of cloud-based delivery models is further boosting sales in international markets.
- The services companies are further growing their global presence and setting up SOCs, cyber defense centers and R&D centers across the globe for serving the clients better.

Source: DSCI Analysis and industry interviews

Innovation in Cybersecurity

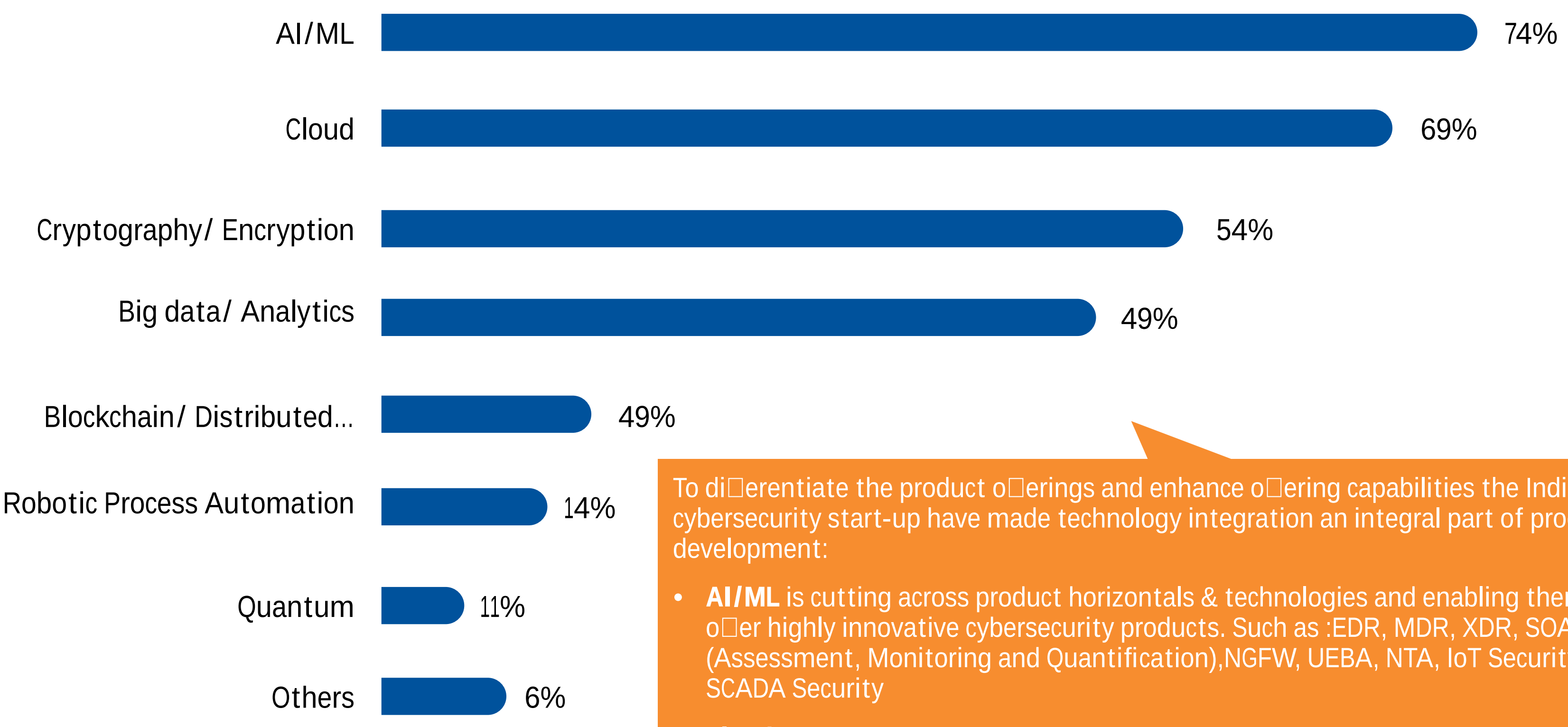
	PRODUCT	PLATFORM BENEFITS	SERVICES
ENDPOINT SECURITY AND MOBILE SECURITY	AI/ML based threat detection and response Threat graph and telemetry, threat hunting,	Real time attack prevention	End point monitoring and response
SECURITY OPERATIONS	Processing large amounts of security data , SOAR, MDR, AI/ML based threat detection and response	Remediation of response	Managed SOC, Cloud SOC
THREAT AND VULNERABILITY MANAGEMENT	Sandbox threat simulation, zero-day exploit, deception	Active defence	Proactive threat/breach simulations and patching SIaaS, VMaaS
CLOUD SECURITY	Continuous visibility of assets, misconfiguration management, cloud native, Artifact scanning	Blindspot management	Shift left, GRC Automation, Secure app development
RISK MANAGEMENT	Risk Quantification contextualization and prioritization	Prioritize and proportionate risk handling	Instant threat sharing and mitigation, metrics driven delivery
SECURITY ARCHITECTURE	SASE framework with advanced bundled products	Zero trust	Robust cybersecurity architecture design and deployment

Source: Industry interviews

Technology Integration

Enhancing Cybersecurity Product Offerings

TECHNOLOGIES FOR ENHANCING CYBERSECURITY PRODUCT OFFERINGS



To differentiate the product offerings and enhance offering capabilities the Indian cybersecurity start-up have made technology integration an integral part of product development:

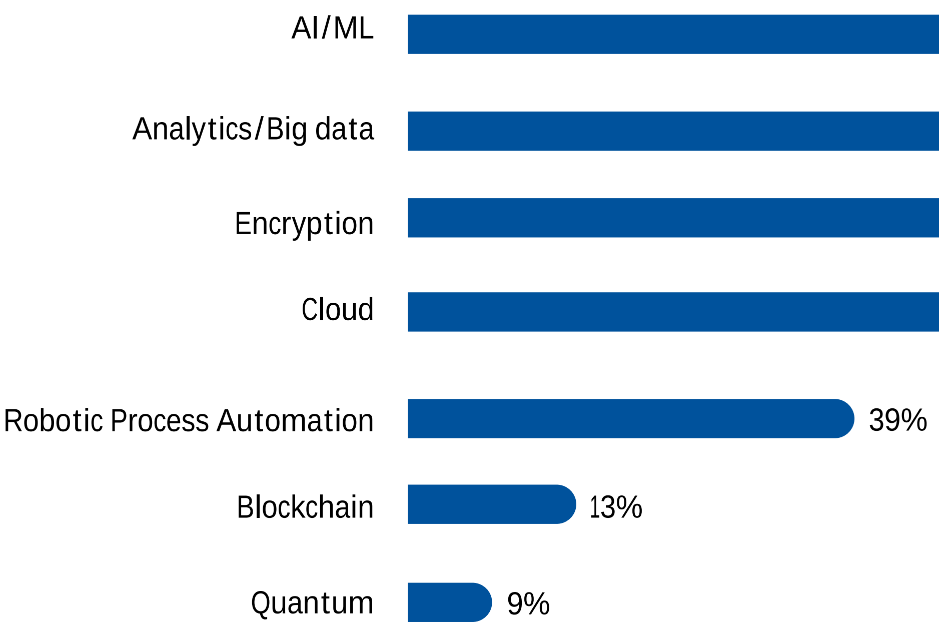
- **AI/ML** is cutting across product horizontals & technologies and enabling them to offer highly innovative cybersecurity products. Such as :EDR, MDR, XDR, SOAR, Risk (Assessment, Monitoring and Quantification),NGFW, UEBA, NTA, IoT Security and OT & SCADA Security
- **Cloud** offers scalable cybersecurity solutions to consumers with greater flexibility, agility and lesser infrastructure investment. Such as CASB, CSPM, ZTNA and UEBA
- **Cryptography**; distributed ledgers, zero-knowledge technologies, and privacy technologies are using advanced cryptography to secure data.

Source: DSCI Analysis and industry interviews

Technology Integration

Enhancing Cybersecurity Service Offerings

TECHNOLOGIES FOR ENHANCING CYBERSECURITY SERVICE OFFERINGS



The surge in data flow and growth in surface area of attacks has led in accelerated adoption of technology stacks to enhance current cybersecurity offerings:

- **Cloud**- The ubiquitous adoption of cloud has led to creation of security offerings imbued with cloud capabilities
- **AI/ML**- Industry is developing augmented ML models to detect/predict complex threats and respond to breaches
- **Big data and data analytics** tools are being adopted invariably to structure the data lakes being generated and detect anomalies & patterns in real-time
- **RPA** -AI and behavioral analytics are appending advancement to security automation
- **Blockchain**- Decentralized authentication solutions and public-key encryption mutually help in risk-based authentication and secure data communication
- **Quantum** key distribution and quantum cryptography are still in nascent stages, and are poised for growth with the advent of quantum computing

Source: DSCI Analysis and industry interviews

India’s Cybersecurity Services

Industry Overview

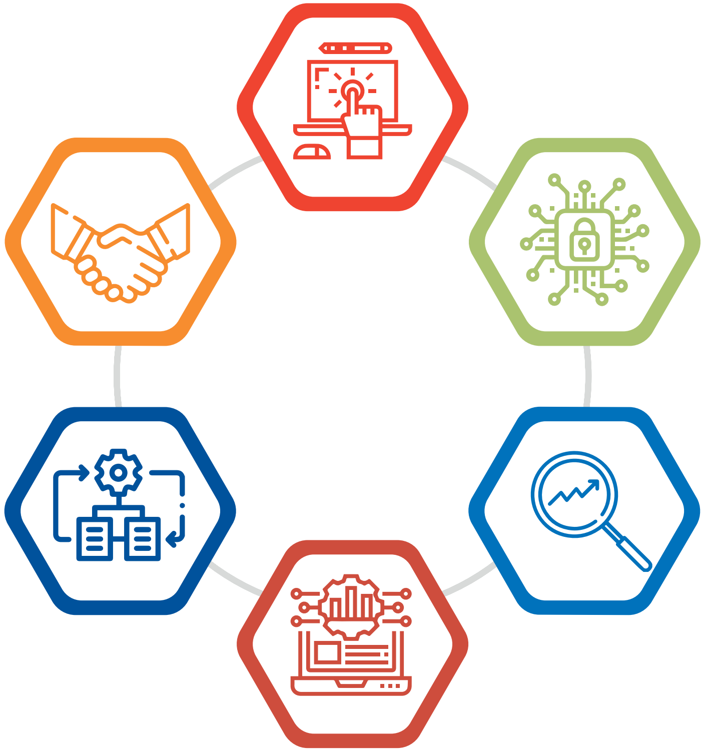
India’s Cybersecurity Services

Industry Overview

Digitalization

The ubiquitous growth of remote working models have created perimeter-less organization network, which has increased focus on securing remote connectivity and leakage points for a seamless digital experience

The closing of digital divide in developing countries is further generating demand for cybersecurity



Start-up collaboration

The cybersecurity service providers are engaging with Indian start-ups for R&D and innovation, thereby creating customization and differentiated offerings.

Cybersecurity offerings

There has been a surge in demand for data privacy, cloud security (ZTNA, CASB), GRC (Internal & Vendor risk management and quantification of risk), IDAM solutions (UEBA), SecOps (breach simulation, patch & vulnerability management).

Technology– moving towards automation

The providers are investing in AI and RPA for pushing automation of cybersecurity functions to offer comprehensive, and enhanced cybersecurity. This will push the Y-o-Y consumer spend on security down and gradually transform into an economical suite of security for all organizations.

Areas of focus- IAG, IDAM, GRC, SOC, IR, Cloud compliance and NGFW

Enterprise trends - emergence of new mindset

As organizations embrace business led innovation and digital transformation, the services providers enable implementation of security by design. DevSecOps helps accelerate time to market from months to weeks minimizing bugs and vulnerabilities

Shift in service models

Organizations are demanding outcome-based offerings and SaaS based Managed and Shared services (Cloud SOC, platforms) through a consumptive/subscription model.

Requirement for simplified vendor management and reducing capex is on the rise.

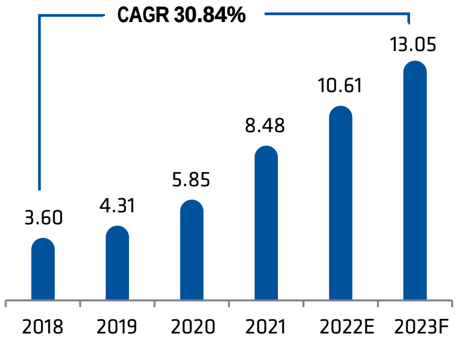
Platform based service models are gaining traction on back of ease of deployment, agility (Premises agnostic) and ability to integrate disparate tools

Source: Industry interviews

India’s Cybersecurity Services Industry

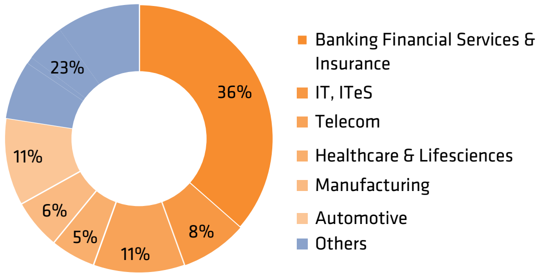
Revenue Outlook

Revenue growth 2018-2023, (USD Bn)



- The tremendous growth can be attributed to surge in demand for securing infrastructure & networks on private networks & cloud. Also from managing secure Application development, IDAM, TVM and GRC.
- The Increase in ransomware attacks led to increased cybersecurity awareness and adoption across large enterprises and SMEs alike
- Cybersecurity has now moved from providing just security to become a business enabler and is driving cybersecurity spends
- The growth in awareness levels of CXO’s around cybersecurity to protect brand value and proactively implement security control is another driver

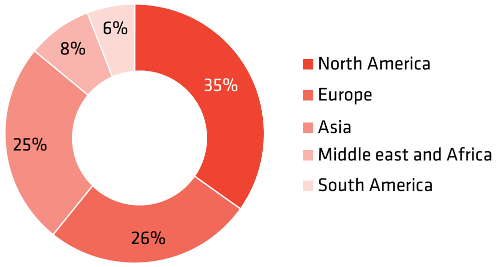
End-user revenue contribution, 2021



Other will include: Retail, Entertainment, Education, Transportation, E-commerce etc

- The highly regulated industries continues to drive revenue for the services players owing to their cyber maturity levels. The need for GRC, data protection and privacy has grown significantly while moving to remote working infrastructure
- The IT and ITeS industry has demonstrated and inspired secure cloud adoption
- Manufacturing and critical infra have gained significant traction as focus on OT and IoT security grows
- Globally, Government with their 5G and smart city projects are emerging as potential market opportunities
- B2C sectors, retail and e-commerce are deemed to grow at a very robust pace in the next 2-3 years

Geographic contribution, 2021



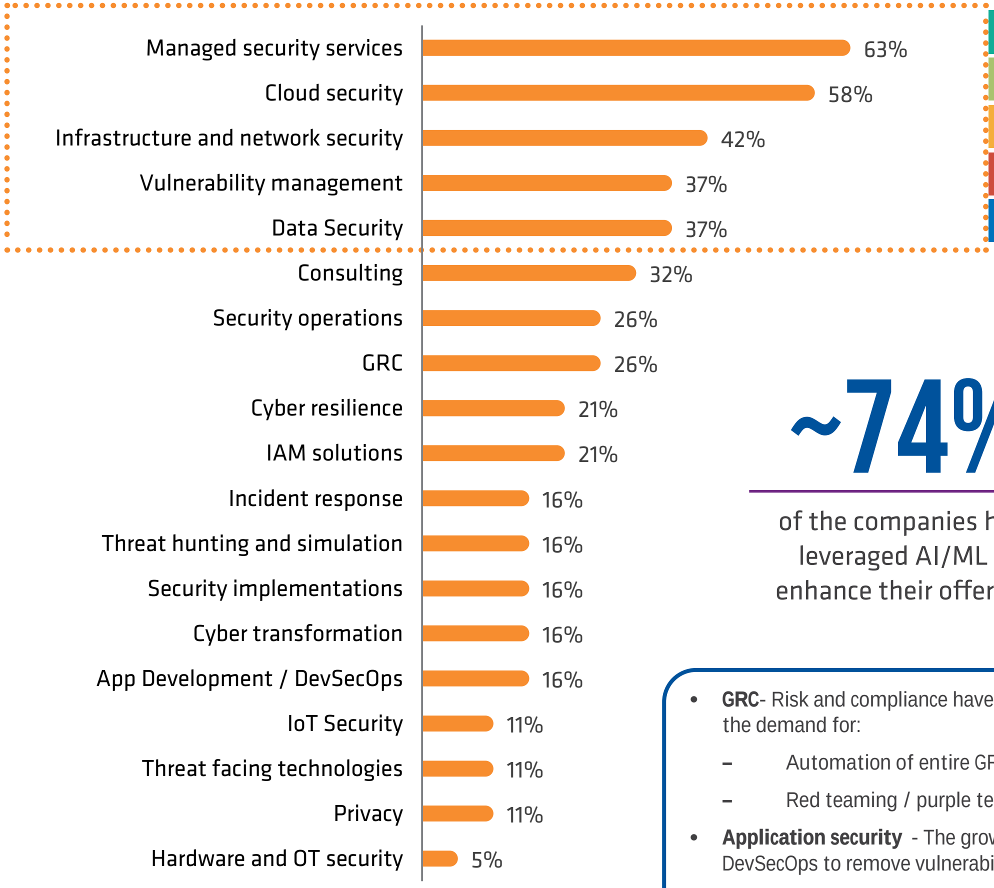
- The Indian services industry caters to global customers and from a revenue perspective the global market contributes 80-85% and domestic market 15-20%
- The developed countries have been a lucrative market, as adoption drive is higher due to stringent regulation, higher awareness levels & cybersecurity budget, and quicker decision-making process
- The top companies are focusing on regions such as US and Europe as there are a greater number of cyberattacks incidences. Moreover, they have more legacy tech that is being revamped, renovated and upscaled. This is driving more spending in US and Europe primarily in banking, manufacturing, energy, travel and transportation sector.
- From a mid-size org perspective- markets such as Australia, US, European countries, UAE, and Singapore have a strong pull.

Source: DSCI Analysis and industry interviews

India's Cybersecurity Services Industry

Offering Analysis

Key Cybersecurity Segments in Demand



- MSS and Shared Services are being adopted across verticals and industries for partial or complete workloads.
- Platform based services offer attractive benefits and flexibility, thereby experiencing significant growth in demand

- Cloud adoption is propelling demand for cloud security solutions
- There has been a surge in revenue gained through deployment of frameworks (DevsScOps), architectures (Zero Trust, SASE) and platform based services (Cloud SOC)

- Infrastructure and network security continues to play a key role in digital transformation journey, especially for large organizations
- SD-WAN, VDI and cloud networks are driving demand

- The industry is taking shift left approach. The addition of new devices, open networks and IoT devices has led growth in cybersecurity demand
- Breach, patch and vulnerability management in an outcome-based and self-services models are gaining traction

- Data privacy, security and compliance are undergoing innovation to enable the organizations to anonymously run analytics for their clients and provide hyper personalization services using Big data and AI

~74%

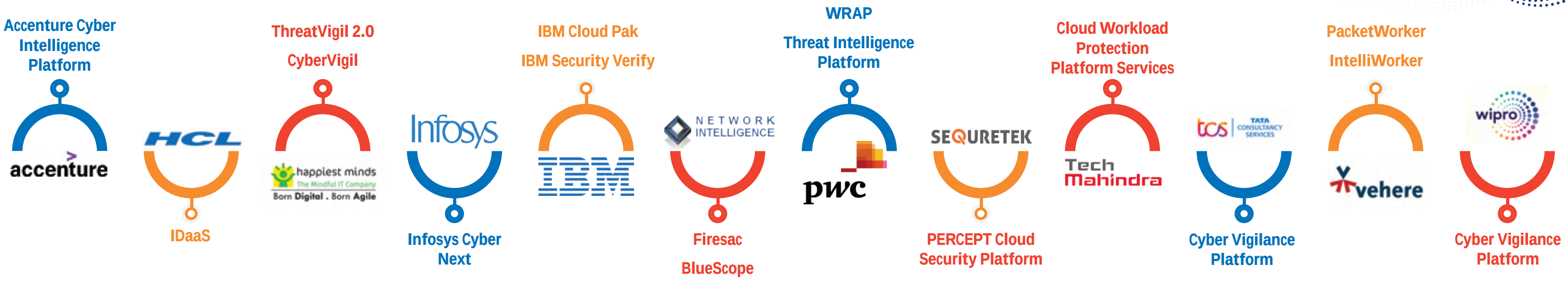
of the companies have leveraged AI/ML to enhance their offerings

Industry offering trends

- **GRC**- Risk and compliance have seen significant growth as client need to adhere to global data protection regulations. This has increased the demand for:
  - Automation of entire GRC processes for an efficient IT risk assessment gaining traction
  - Red teaming / purple teaming and breach simulations are going from sporadic to continuous models
- **Application security** - The growing number of cloud-based applications & tools are propelling demand for Application security and also DevSecOps to remove vulnerabilities and provide robust applications to consumers from day zero
- **IDAM** - IDAM with UEBA is growing in demand for clients, their employees as well as their customers
- **End-point security** - With WFH scenario persisting, endpoint security, controls and measurements have gained huge traction
- **OT & IoT security** - The focus on OT and IoT security is growing due to need for connected device discovery and management. Unique OT security solutions are being implemented upon request

Source: DSCI Analysis and industry interviews

Emergence of Platform based Services



Platforms

- A platform offers cybersecurity services imbued with latest technology and bundled with a set of complementing cybersecurity products in a shared or managed model.
- They can be offered in customized models, platform as a service, or SOC as a service.
- Platforms can leverage hybrid working models where data can reside on premise and analytics can run on the cloud, they can be metered on consumption
- The platform can run on multiple data centers across different geographies, and can be on different instances on different data centers in a multi tenant model
- With a curation of SOPs (use cases)- the time to market to deploy new solutions is decreased significantly
- The platforms emulates enterprise security as a service, and can offer a wide range of services including but not limited to :Threat Intelligence, red team services, breach simulation, IDAM, risk monitoring & visualization, pro active threat hunting & vulnerability management, incident response products, cloud assessment provisioning, vendor risks, data privacy, and analytics & management of Data lakes, data fabrics and data governance with in-built security

The platform advantage

- Quick and simpler integration and implementation- faster time to market
- Shortened time frame for use-case deployment
- Offers ability to integrate disparate tools
- Enables orchestration and tool simplification
- log segregation and correlation can be done on cloud for acquiring intelligence
- Provides shared threat intelligence
- Include a suite of products
- New services can be added to the existing platform
- Offer flexible solutions
- Premises agnostic & Tool agnostic
- Cloud SOC can connect over VPN
- Reduced cost of ownership
- Enables integrated security management of tools.

78% of the respondent services companies offer platform-based services

Trends:

- The providers are developing a curated model focused on outcomes i.e. Opex based model with pre-defined use cases for quick deployment
- The customization of products are growing in demand specially for automated identification, and remediation of vulnerabilities
- Cloud SOCs gaining momentum
- Virtual CISO function is emerging especially in the SMEs
- Platforms have the ability to be configured/ extended through APIs
- Standardization is important, going ahead, through evolving industry standards, e.g. ETSI, NIST, etc.

Content source: DSCI analysis, company websites

Note: These are illustrative examples and do not showcase the entire ecosystem

India's Cybersecurity Services Industry

Investment Priorities

For successful growth and expansion strategies, the services providers are prioritizing their investments and paving a growth trajectory

Investment Priorities for growing the cybersecurity services revenue

Expanding customer base and offerings in existing verticals is first priority

32%

- Offering self services models with value added, network-based security solutions and secure transformational services to existing customer.
- Leveraging enterprise security platforms to cater to industries in the same verticals

Enhancing offerings with technology is second priority

27%

- Strengthening existing offerings by leveraging tech stacks such as AI/ML, RPA, Blockchain and cloud along with UEBA.
- E.g, automate sec-ops and Incident monitoring & response

Venturing into new verticals/ industries is third priority

22%

- The global demand coming from Manufacturing & Critical infrastructure (OT security), Large conglomerates (transformation and SOC services), Governments (holistic solution), Telecom (5G SOCs) is pushing the providers to expand verticals

Expanding geographies are fourth priority

19%

- Creating new Cyber defense and fusion centers across geographies ,to offer better customer service

Innovation investment strategy and priorities

32%

Talent reskilling for innovation is given the highest priority, through various cross skilling and upskilling initiatives. The companies are rapidly expanding employee base as there is huge capacity to absorb, through funding Universities and lateral hiring

32%

Internal incubation of ideas, spending on R&D, and incubation of start-ups – Spending on R&D and incubation of start-ups are growing immensely for creating robust offerings as demand for securing remote networks and automating remediation has increased

For product integration:

65% of the respondents engage in partnership with Indian cybersecurity products and start-ups

27%

Partnerships are on the rise as platforms are emerging and multiple best of breed products from different vendors are being integrated. Start-up with unique product offerings are leveraged

10%

M&A acquisition of niche product offerings are preferred for acquisition however an incubation or partnership model is preferred

Source: DSCI Analysis and industry interviews

Experts Speak

The demand for cybersecurity is increasing multi-fold, which is leading to expansion of cybersecurity capabilities from start-ups to tech giants and other big conglomerates with an objective to become cyber resilient and ensure business continuity. Multiple industry sectors, including energy, healthcare, and manufacturing are also expected to gain significant cyber traction over a short duration with operational technology coming under threat from cyber intrusion. Indian corporations are looking to leverage innovative solutions while optimizing cost and driving efficiency. Continuous innovation by Indian product companies, in areas of MDR, Identity & Access Management, GRC, vulnerability management, using AI and ML to address the dynamic nature of risk, is driving cybersecurity demand.

Atul Gupta

Partner and Head, Digital Trust; India Cyber Security Lead, KPMG

The accelerated digital transformation during the pandemic combined coupled with increased awareness around cyberattacks have been the key driving factors for these customers. There has been an increase in ransomware attacks, especially amongst SMEs. This has led them to adopt end-to-end solutions such as managed services. The successful Indian start-ups are entering into partnerships with SI's for implementing their technologies. On the other hand, Indian cybersecurity providers are able to customize their offerings, helping their Indian and international customers enhance their security posture.

K K Mookhey

Founder, Network Intelligence Pvt. Ltd.

"The era of brand is over and today is the era of the consumer"

The global demand for cyber security is being driven by the paradigm shifts being seen across business. As businesses reinvent themselves to restore relevance and regrow, there is also an increasing sense of sustainability and trust that CXOs are imbibing as part of their growth strategy. We strongly believe cyber security needs to be integrated into the very fabric of the business than applying a "band aid" approach so that growth is not only sustainable but secure and responsible as well. in In the face of increasing business complexities and ever changing attack surface, Accenture combines comprehensive Security capabilities with industry expertise and "glocal" presence thus helping clients outpace threats both "known" and "unknown" on an ongoing basis.

Muthu Raja Sankar

Lead/ Managing Director, Accenture Security India Business

Experts Speak

Enterprise customers are focusing on Threat Intelligence, red team service offering, simulation and insights & representation/visualization of cybersecurity posture. They are also moving towards using shared services for partial workloads and leveraging them for Technologies such as PAM and automation. SMEs are investing in MSS services such as EDR and PAM. The current priority of Happiest Minds remains skilling and training of talent in order to strengthen the existing sec ops, add automation, threat intel and brand monitoring and provide holistic offerings from India.

Priya Kanduri

CTO & Vice President, Cyber Security services, Happiest Minds Technologies

The convergence of network security and cloud workloads is driving demand for cybersecurity. Customers are looking for secure functionality of business applications and are focusing on cost optimization. With a robust alliance ecosystem in India, the creation of innovative solutions & services is able to enable customers to reinforce their cyber resilience. The fast-paced global adoption of 5G networks coupled with IT transformation will further push the demand for advanced cybersecurity solutions from India and enable India to become the destination for remote SaaS delivery.

Rajesh Dhuddu,

VP & Practice Leader -
Blockchain & Cybersecurity,
Tech Mahindra

The pandemic had organizations focusing on remote working models and business continuity in the short term, which quickly transitioned into business resilience. We saw a shift in protection strategies from securing the perimeter to securing data. There has been a surge in demand for cybersecurity offerings such as GRC, IDAM, Data security (DLP, Encryption) and Cloud security. Cybersecurity spends are growing globally on the back of increased awareness around cyber threats, digitalization and sectoral/government regulations. India is catering to this surge in demand with its robust talent pool and innovative mindset.

Samir Khare,

Vice President
CIS APAC Cybersecurity
Cybersecurity Unit GDC India
- Capegemini

Experts Speak

India is growing its global footprint and enabling secure digital transformation of enterprises across the globe. Nurturing the domestic cybersecurity ecosystem by innovating through local start-ups in a partnership model, funding them and also adopting their products onto our platform, along with investing in pre-skilled employable workforce in India will pave way for a robust cybersecurity talent and technology value proposition.

Santha Subramoni

Head-Cyber Security Unit,
Tata Consultancy Services

There has been tremendous growth in the services industry in terms of people, process and technology. India's conducive environment for nurturing start-ups coupled with the rise of e-learning modules is helping grow the skilled cybersecurity workforce, however, there is still a significant gap between demand and supply. The models of delivering services are advancing, creation of platforms and assets that can automate certain portions of the service delivery so that the number of people required to engage in repetitive non-value-adding work can be reduced. These advancements are critical to ensure that we address the workforce challenge.

Siddharth Vishwanath

Partner - Risk Advisory &
Cyber Security Leader, PwC
India

The organizations are aiming to achieve a secure workplace & digital experience. This has led to the consumption of outcome-based security as a service model. Cloud SOC i.e. platforms are being pushed as they offer quick and simpler integration & implementation, flexibility, secure connectivity, IDAM features. Holistic offerings that are tool agnostic are gaining traction and helping shorten the time to market. Currently, the talent demand is high, and the market has a huge capacity to absorb. Key sectors that are estimated to drive the market are Manufacturing (FMCGs), Retail food distribution, logistics besides Banking & Finance. With a 360-degree scale-up taking place in India in terms of innovation, bolstering the talent pool is resulting in growth in depth, breadth and scale of cybersecurity offering from India

Srinivasan CR

Chief Digital Officer, Tata
Communications

The global economy is transcending into a Data and AI led world. This transformation is driving the need for advanced cybersecurity platforms as organizations are moving towards a shared services model and aiming to automate cyber functions to optimize cost. The incubation and partnership with Indian startups is facilitating the creation of next gen cybersecurity platforms by leveraging cutting edge technologies.

Vishal Salvi

Chief Information
Security Officer
and Head of
Cybersecurity, Infosys

India's Cybersecurity Services Industry

Case Studies

Company name	Industry	Problem Statement	Solution Deployed	Outcome
accenture	**Major Multinational Retailer in Europe**	• Significant level of DevOps adoption across the Tech landscape • Intent to Shift Security to the Left - Integrate security scanning capabilities into DevOps to identify and remediate vulnerabilities earlier in the SDLC • To improve the overall security and compliance of applications • Reduce application security risk while enhancing development speed	• Implemented shift-left security, by designing and implementing (automated, simple-to-use, re-usable, one-click onboarding, pipeline agnostic) DevSecOps framework and vulnerability management process for scanning applications to identify, report and track security vulnerabilities while application features were being developed.	• 40% decrease in security vulnerabilities • 15% cost reduction across Secure-SDLC by shifting security left • 50% reduction in Security effort required to support Secure Development • Accelerated adoption of security assessments during Development phase by 80% • Increased ability to monitor, track and manage application security risks on-demand
CMS IT SERVICES	**Power (National Critical Infrastructure)**	• The customer needed essential products and services for the datacentre, disaster recovery centre, and integrated network and security operations and command centre. • 24x7 data privacy, critical system availability, and near real-time incident resolution are the cornerstones of Power Distribution companies.	• Deployed CMS IT Defensible Cybersecurity Platform Components of Cybersecurity System Integration, Managed Detection & Response, Identity and Access Management, and GRC Audits and Assessments	• >99% SLA uptimes and 24x7 Advanced Security Monitoring, detection, and response integrates with security controls in IT/ OT/ IoT environment • Enhanced threat detection and response capabilities for complex attacks with adaptable TTPs • Continuous visibility to Vulnerabilities and immediate improvement of Cyber Defense Posture

Source: Accenture, CMS IT Services

*Note: These are Illustrative examples and do not cover the entire ecosystem

India's Cybersecurity Services Industry

Case Studies

Company name	Industry	Problem Statement	Solution Deployed	Outcome
HCL	**Leading gas distributor in the UK**	• The company needed to securely migrate all their workloads to a public AWS cloud. • They sought to radically improve consumer experience, through next-gen workplace services with robust security controls. • They also wanted to safeguard the workloads while enacting specialized cloud governance and compliance policies.	**CloudSecurity-as-a-Service (CSaaS) solution for:** • 4,000+ users • 6,000+ endpoints • Privileged access to 200+ admins	• Improved IDAM, Enhanced PAM, and Data security-enabled PKI and HSM management • Robust malware advisory and vulnerability assessment • Digital endpoint security-enabled DLP, encryption, and AMP management
happiest minds The Mindful IT Company Born Digital . Born Agile	**Major civil aviation infrastructure services**	• The client needed a secure cloud portal for ensuring signed digital permissions of an unmanned aircraft, ensure compliance and protection of sensitive data of citizens, confidential information on the cloud, secure access and processing, and end to end logging & monitoring	• Cost effective solution by the maximum use of AWS security components • Defense-in-depth solution by use of multiple security products and services from different vendors	• Secured cloud design • 24*7 monitoring • MDR and 99.999% availability • Privacy design to ensure protection for all sensitive data stored on cloud

Source: Accenture, CMS IT Services, HCL

*Note: These are Illustrative examples and do not cover the entire ecosystem

India's Cybersecurity Services Industry

Case Studies

Company name	Industry	Problem Statement	Solution Deployed	Outcome
KPMG	A telecom player	The client offers a multitude of technology enabled products and services which handle a large volume of critical data including personal information of close to 320 million subscribers. Telecom operations is a critical infrastructure prone to multiple threats. Hence, it's of paramount importance to have proactive and effective threat, vulnerability and privacy management program.	KPMG in India developed holistic security operations framework, Security by Design, Secure Deploy and Secure Operations. Helped the client to design, implement and run a comprehensive security and privacy assurance program to proactively assess, govern and mitigate the security and privacy risks for IT and Telecom assets. KPMG in India also built a platform to: • manage the security assessment lifecycle integrated with security tools • maintain Centralized repository for vulnerabilities and realtime tracking and security posture update	• Reduced 80% of security risks with effective risk management and governance • Implemented Zero Day Process to identify zero day vulnerabilities. • Reduced 75% of time and effort for Tracking Risks CxO Dashboard, KPIs through automation • Assisted in identifying and compiling documentation for audits with regulatory authorities
Infosys	Leading telecom company	• The core requirement by the company was to build a strong platform with the best-of-breed agile services which can support their digital transformation journey. • They were facing increased complexity due to heterogeneous IT security stack and high AMC due to multiple vendors	Digital Transformation to become Cloud Native with NexGen Security Solutions- • Built a security framework • Implemented network, data and endpoint security along with IAM • Installed NexGen firewalls with hyperscale capabilities to reduce complexity, management efforts and opex cost	• Reduced 99% of P1 outages • Enhanced the security posture and reduced overall network risk • Reduced the risk from cyber threats • Improved scalability and reduced redundancy • Optimized operation efforts by implementing public cloud solution

India's Cybersecurity Services Industry

Case Studies

Company name	Industry	Problem Statement	Solution Deployed	Outcome
TATA COMMUNICATIONS	Sharekhan	• The client wanted different ways to defend its network/systems against DDoS attacks at Layers 3, 4 and 7. • System needed to be compatible with BNP Paribas security architecture, while meeting RBI and SEBI regulatory controls.	• Hybrid on-premise/cloud DDoS protection system. which helped it protect its customers' online trading activities, while preserving the integrity of its entire cybersecurity architecture.	• Succeeded in dealing with various DDoS attack signatures, offer stronger cybersecurity assurances with many DDoS attack signatures
Tech Mahindra	A leading Australian Telco	• The client wanted to secure, control & monitor access of privileged users to IT infrastructure and ensure compliance to their security policy and to group security policy	• Designed & implemented centralized PIM solution integrated with IT infra • Implemented CyberArk / PUAM solution to control privilege access and Role Base Access Control, 2FA and assessment of internal applications and privilege ID monitoring	• Control and manage insider threats to sensitive data leakage • Defend outsider threat more effectively by protecting the privileged and service accounts • Defend outsider threat more effectively by protecting the privileged and service account
tcs TATA CONSULTANCY SERVICES	Energy major	• The client needed to enhance its security operations and identity and access management • The lack of real-time centralized threat visibility in the company resulted in increased turnaround time to identify, respond and remediate business threats, and caused poor user experience due to lack of advanced security analytics	• Centralized security monitoring for the energy major's IT and OT systems. • TCS prepared a multi-year roadmap to modernize and automate SecOps and IAM processes, improving user experience and integrating processes and technologies.	• $170K - per year cost benefit by creating synergies within team 40% more operational stability • $1.5M - in cost avoidance with license optimization • 30% increased SOC maturity and 100% remediation of demilitarized zone vulnerabilities and 70% Windows-based historic vulnerabilities for a 40% overall risk reduction

Source: TCS, Vehere, WIPRO

*Note: These are Illustrative examples and do not cover the entire ecosystem

India's Cybersecurity Services Industry

Case Studies

Company name	Industry	Problem Statement	Solution Deployed	Outcome
vehere	Banking	- The company was facing audit failure, limited visibility of the network (risk of breach), and ineffective and time-consuming alert management.	- NDR & NF across 2 data-centres - Data Retention for 90 Days - Comprehensive monitoring of all network assets - Vehere PS to build dashboards to support business reporting & integration with SIEM (Streamline and automate event analysis, triage and incident response)	- Compliance: Address regulatory compliance requirement for deployment of NBAD and, Network Forensics - Reduced risk of Breach and increased SOC operations efficiency - Fastest route towards implementation of Security Analytics program - Near real-time support for monitoring of new business applications
wipro	Australian Government's leading road and public infrastructure safety agency	- Looking to secure migration of 150+ sensitive business applications to the AWS cloud. - Build a strategy to securely migrate reduce administrative overhead and cost with optimal efficiency. - AWS-ready security monitoring and incident response capabilities with latest use cases. - To identify application security vulnerabilities and identify risks before go-live and maintain GRC.	- Performed end-to-end AWS security strategy and architecture design with the principles of Secure by Design - Established and operationalized SOC and TVM on AWS - Deployed SIaaS and VMaaS	- Enhanced security posture - Rapid applications development and migration at scale - Early identification of security risks -faster migration to AWS - Cybersecurity and threat posture visibility to management - Enhanced ability to respond to potential security breaches

India: Emerging Hub for Cybersecurity Services

Managed Security Services

- accenture
- acpl
- AGC
- AKS IT SERVICES
- BT
- Capgemini
- CMS IT SERVICES
- Cognizant
- DXC TECHNOLOGY
- digitaltrust
- dimension data
- Frontier
- happiest minds Born Digital . Born Agile
- HCL
- IBM
- Infosys
- inspira
- LTI Let's Solve
- MICROLAND
- Mindtree
- netmagic
- NETWORK INTELLIGENCE
- NTTSecurity
- Payatu
- pwc
- QOS
- sify
- SISA
- SNSin
- softcell
- SONATA SONATA SOFTWARE
- Suma Soft
- TATA ADVANCED SYSTEMS
- TATA COMMUNICATIONS
- tcs TATA CONSULTANCY SERVICES
- Tech Mahindra
- torrid networks
- TRACELAY
- vehere
- velocis
- virtusa Accelerating Business Outcomes
- WeSecureApp
- wipro

Cybersecurity Consulting & Auditing

- AAA
- accenture
- acpl
- AGC
- ARC Advisory Group
- BDO
- BT
- DXC TECHNOLOGY
- Deloitte
- dimension data
- ESPERTO
- EY Building a better working world
- Frontier
- GISConsulting
- Grant Thornton
- IBM
- Infosys
- inspira
- KPMG
- mazars
- MICROLAND
- netmagic
- NSE
- NTTSecurity
- Payatu
- PC Solutions
- protiviti
- pwc
- SB SECURITY BRIGADE Immunity for your IT
- SISA
- SNSin
- softcell
- Suma Soft
- TCG DIGITAL
- tcs TATA CONSULTANCY SERVICES
- Tech Mahindra
- VARUTRA
- WeSecureApp

System Integrators

- accenture
- AUJAS CYBERSECURITY
- CMS Connecting Commerce
- Cognizant
- DXC TECHNOLOGY
- ESPERTO
- GISConsulting
- happiest minds Born Digital . Born Agile
- HCL
- IBM
- Infosys
- MICROLAND
- Mindtree
- netmagic
- QOS
- sify
- SNSin
- SYNOPSYS
- TATA ADVANCED SYSTEMS
- TATA COMMUNICATIONS
- tcs TATA CONSULTANCY SERVICES
- Tech Mahindra
- virtusa Accelerating Business Outcomes
- Whitehats
- wipro

Note*: These are Illustrative examples, and do not cover the entire ecosystem

Indian Cybersecurity Start-up & Product

Industry Overview

Indian Cybersecurity Start-up & Product Industry

Key Trends

Cybersecurity offerings:

- The providers are offering custom domain specific solution (supply chain) as well as holistic turnkey platform
- All products traditionally offered on-premise are being imbued with cloud capabilities
- Consolidation of security controls to offer holistic solution is driving demand for platform-based products

Tighter regulation pushing demand for products:

- Regulators such as RBI, SEBI, and others are pushing cybersecurity compliance by implementing mandatory policies, regulations, regular audits and report sharing related to cybersecurity assessment

Funding and acquisitions:

- Total estimated cybersecurity funding was at USD 778 Mn with a cumulative funding over 5 years
- The number of start-ups have grown from 175 in 2018 to 265 plus in 2021
- Indian cybersecurity products reached USD 1.37 Bn in 2021. Niche products offering that are domain specific are gaining higher traction
- US security technology start-ups are showing higher interest in acquiring Indian start-ups to harness the R&D and engineering talent Indian companies for acquisition and growing their capabilities while saving R&D expense

Demand dynamics:

- Momentum towards cloud migration from on-premise data centers is driving adoption of CSaaS
- Organizations are requiring complete visibility of all assets, endpoints and users to create the right cybersecurity strategy
- BFSI continues to be the highest spender
- SMEs are adopting cybersecurity to maintain brand value
- Organizations have introduced lighter optimized architecture to host the product
- For consolidation of security controls, customer need one stop shop for all security needs

Go-to market strategies:

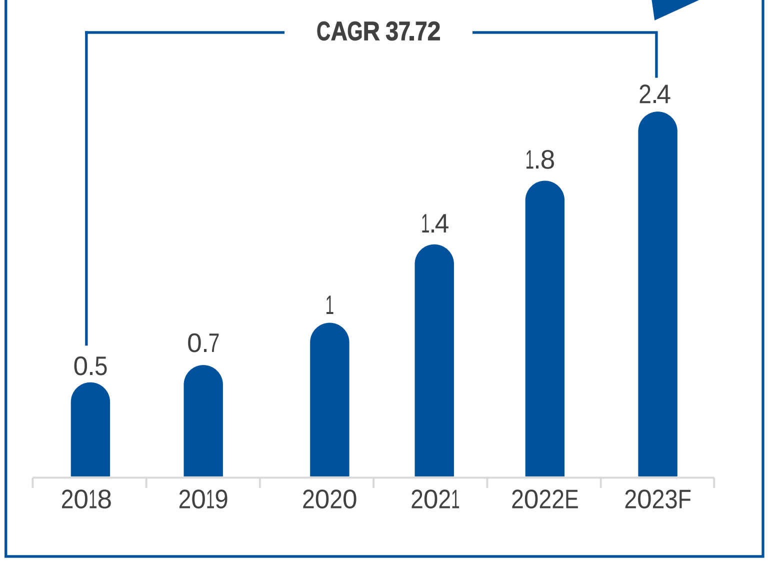
- Investment in expanding geographic presence through channel partners and value add resellers enabling growth
- Sales Process Automation taking place to boost marketing initiative and crack new deals
- Partnering with SI's and consulting firms for product integration and re-selling is another prominent revenue source

Source: DSCI Analysis and industry interviews

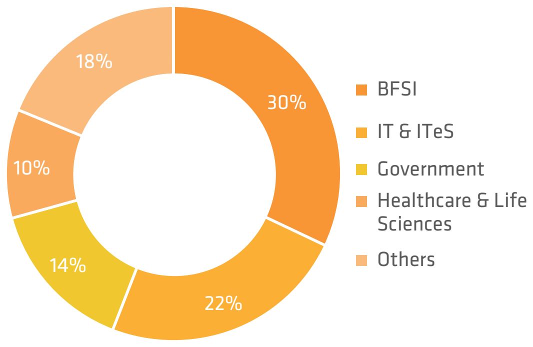
Indian Cybersecurity Product Industry

Revenue Outlook

Cybersecurity Product Industry revenue, (USD Bn)

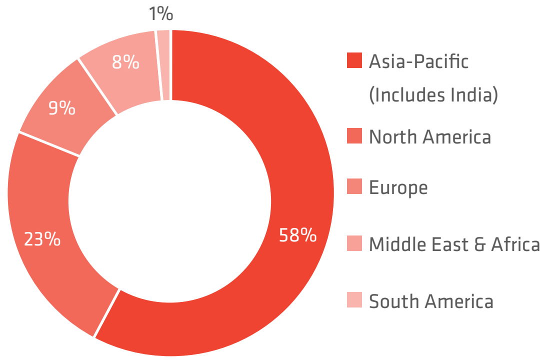


Revenue spilt by End-User



Others include Retail, E-Commerce, Education, Critical Infrastructure, Energy, Automotive, Consumers etc.

Revenue spilt by Geography



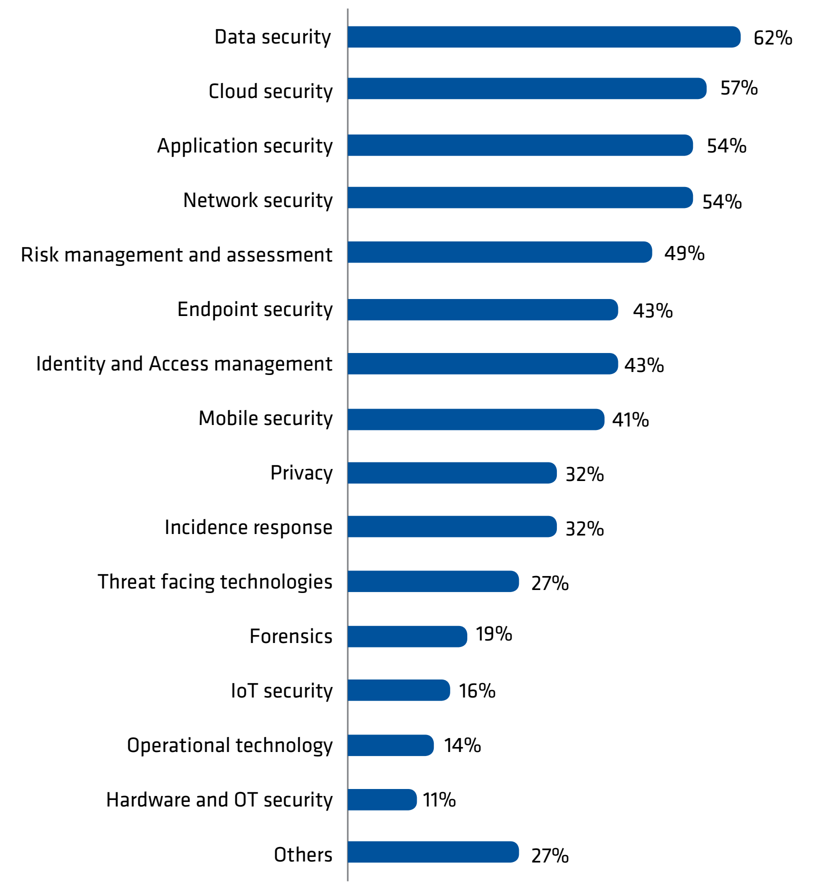
- In 2021, the industry observed a robust growth rate of 31% and reached USD 1.37 Bn with at a YoY of 35%
- Business continuity, remote working model, growing awareness around threat landscape, and maintaining brand image are a few key drivers that are driving the market
- Dynamic marketing strategies, robust partnership ecosystem across the globe and creation of best of breed point products and platforms through R&D is further driving the revenue stream

- The mature regulated sectors continue to dominate the product industry revenue, on back of data privacy, security, compliance and risk management requirements
- The demand for holistic end-to-end solutions are emerging across industries and pushing demand for platforms
- Manufacturing, e-commerce and retail sector are estimated to grow adoption of cybersecurity products at a fast pace in the next 2-3 years

- The Asian market leads in the overall revenue contribution, as it represents 58% of the overall revenue generated
- Demand from North America was robust during the pandemic, and almost doubled from the last year
- A robust product distribution channel of partners, SI's, whole-sellers and value adding resellers are expanding the global footprint

Next-Gen Product Offerings

Product offerings



Key offerings in focus

Three major offering shift in the cybersecurity product industry are happening in the field of visibility holistic detection (detection of threat or behavior or patterns), and the ability to respond while moving from passive to active defense

Visibility: By bringing multiple protocol and sets of data ranging from OT data to traditional logs into single viewpoint visibility is improved.

Detection: Intense innovation is happening in the industry leveraging AI, to detect anomalies in real time.

Response: Mix of automation and ML are used to the response engine. AI /ML are facilitating replacement of manual correlation rules with automation.

Key offerings:

- Data security DLP, Encryption (privacy, security products) and Cloud security (policy and Access) lead the product offering portfolio in terms of demand – cloud adoption has pushed demand for new products
- Application security growing with increased usages of cloud-based tools
- Network security is gaining traction as organization networks are going borderless and need to be secured using ZTAN, SASE, NTA, SOAR and MDR type of products
- Products focused on Compliance assessment, vulnerability management and threat intelligence are gaining popularity.

Upcoming offerings: Authentication-as-a-Service |ZTNA| Continuous Security Validation | Cyber Risk Quantification |Threat Intelligence |Data Classification; Anonymization | IAM (PAM,PIM) | Data Erasure [Data Destruction | Secure Hardware Encryption| NextGen Operations Platform| Internet Isolation | QKD Hub and Spoke | Satellite QKD | EDRM | NDR |Secure multi-computation Zero Knowledge proof

Patent research is being done in areas of Access Technology & Identity, Authentication, ML Algorithm for malicious URL detection, Key-Exchange, AI/ML based Antivirus, Systema and method for determining an asset maturity score, Non-Linear Secret Sharing, WAFER Series in 2021 xx companies filed for patents

~78% of the organizations offer platform based products such as EDR, MDR, XDR, ZTNA, SOAR, and WAF.

Others Include: Zero Trust Access, Continuous Security Validation, Video Collaboration, Cyber Risk Quantification, Threat Intelligence

Source: DSCI Analysis and industry interviews

Product Development & Deployment Strategies

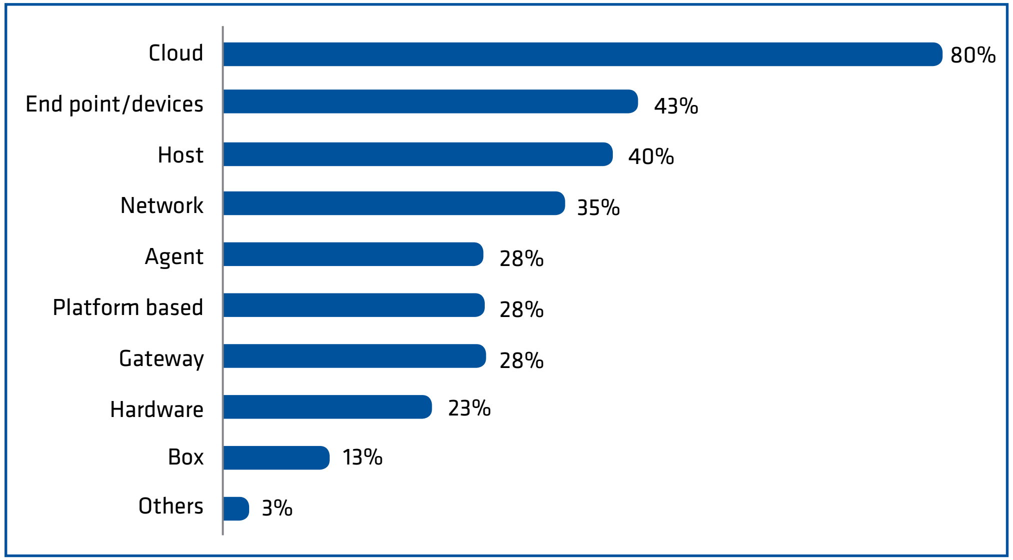
Product development strategies:

- The methodologies of product development has evolved with increased focus on R&D and technology integration–shorter product development cycles are now being realized.
- Within a window of 3-4 weeks, new solutions were developed ground-up to secure the remote work collaboration environment.
- Focus is on getting first-mover advantage and innovate for scale, efficiency, interoperability and agility, while keeping the product lean and robust.
- All companies are evolving their products and platforms to cloud based to cater to the customer needs

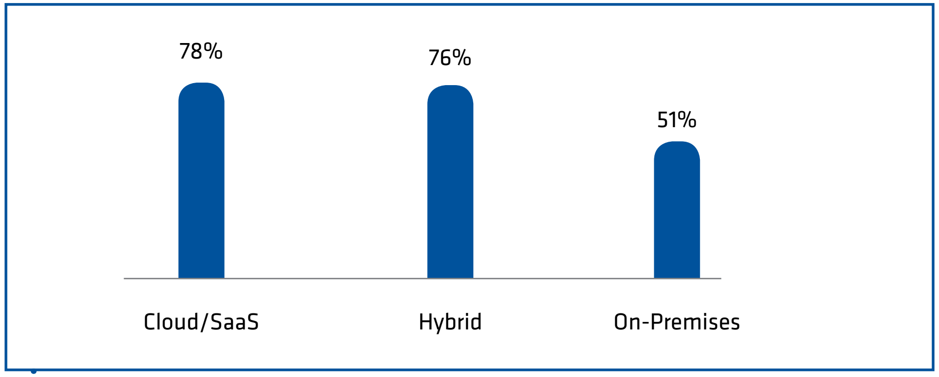
Product deployment strategies:

- Cloud has taken up a central role in the cybersecurity industry due to adoption of multi cloud ecosystem, hyperscalers and remote networks
- The cloud-based deployment has enabled shorter time to market, scalability, ease of integration and platform-based approach.
- The platforms-based cybersecurity products are being offered in a CSaaS model primarily on a subscription model to reduce capex.
- The cloud based delivery models are very attractive to SMBs migrating to the cloud and companies being born in cloud
- As large enterprises are migrating workloads to the cloud, cloud based next gen products are high in demand

Product – point of integration



Preferred product deployment model



Product Licensing Model

- **97.6%** - Subscription based
- **29.3%** - Perpetual-one time licensing
- **24.4%** - Consumptive /Pay as per use

Source: DSCI Analysis and industry interviews

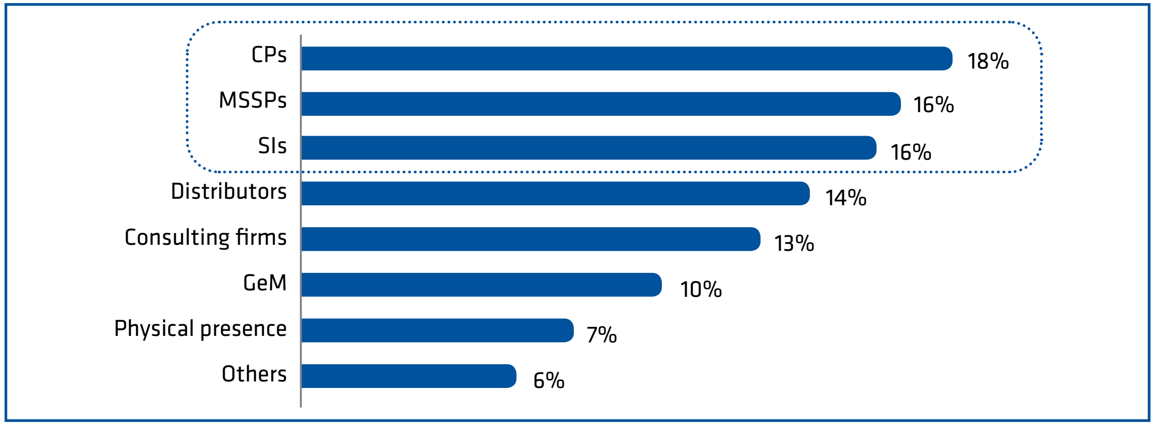
Go-to-Market Strategies

Expanding global footprint:

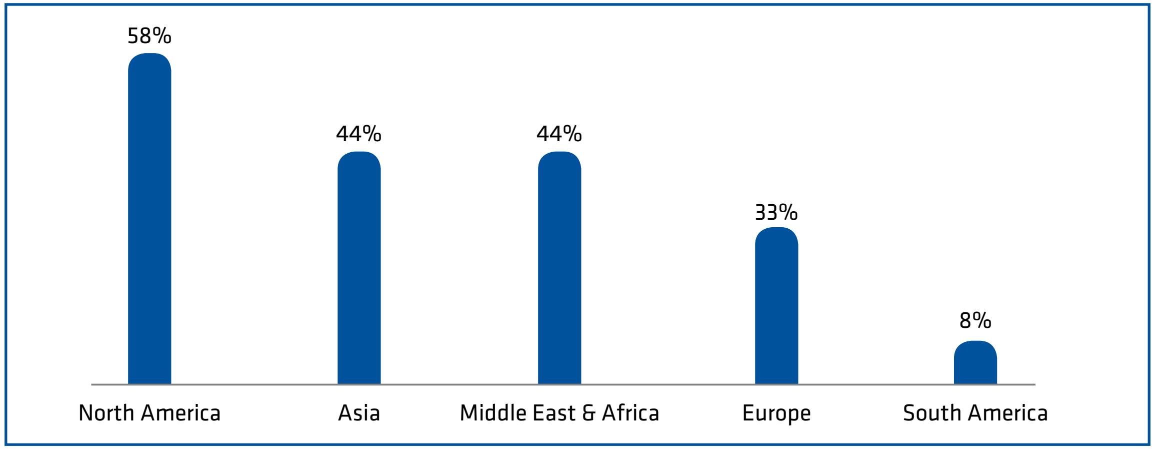
- Product and start-ups are overcoming geographic boundaries through an agile sales and marketing approach to improve connect with buyers and collaboration with the ecosystem partners
- A lot of companies have adopted digital marketing channels in this new reality, however for India and ASEAN market direct sales presence is preferred in close proximity physical presence is preferred
- For quick and eective geographic expansion strategy a partnership model is preferred
- Tie-up with MSSPs, channel partners, and Sis are enabling penetration of of global markets
  - Value add resellers and SI's also facilitate services
- Key markets of future focus are North America, Europe, followed by Middle East & Africa
  - The focus is more on developing strategic accounts and bagging Government projects
  - 24% of the product companies plan to expand into North America, 20% plan to expand into Europe and around 19 % of the companies plan to expand its footprints into Asia market
  - North America and Europe are deemed most lucrative, due to their rampant cloud migration from legacy infra
- The medium and large sized companies prioritize direct sales over partnership models for expansion.

Source: DSCI Analysis and industry interviews

Preferred Distribution Channels



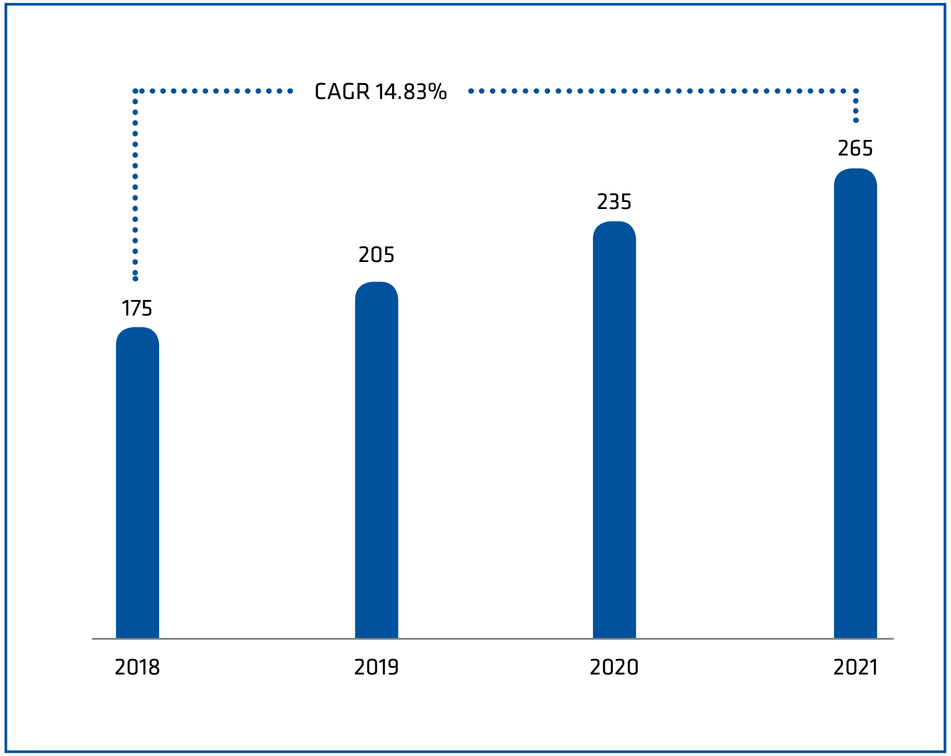
Regions recently added (2021)



Government & Industry Initiatives

Start-ups & Talent Acceleration

Product & Start-up Companies



Source: DSCI - Indian Cybersecurity Product Landscape 2.0, DSCI analysis

Government and Industry Initiatives:

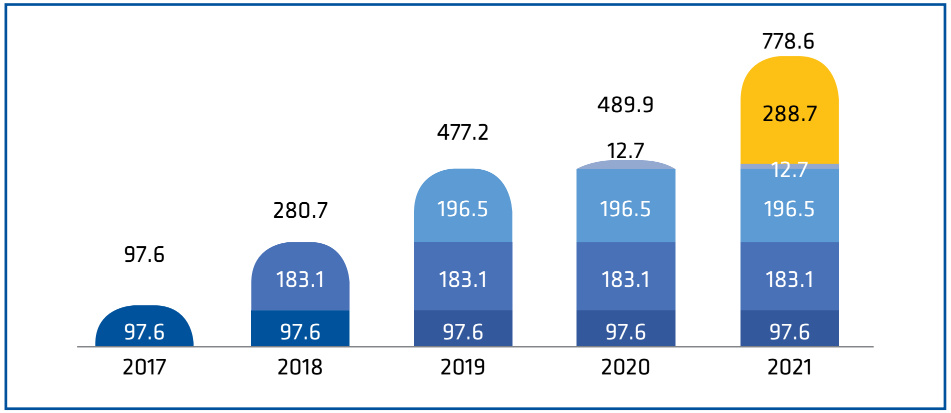
- **NCoE-** It's National COE, established by DSCI and MeitY to incubate deep tech security startups and multiply cyber security technology development in the country. One of the key objectives are translating R&D to Cybersecurity Products.
- **CCoE-** It is a joint initiative of the Government of Telangana and DSCI to catalyze innovation, entrepreneurship and capability building in cybersecurity and privacy. It promotes incubation, acceleration of security of privacy startups i n the state and make Telangana a preferred state for cybersecurity.
- **Grand Challenge-** In order to promote a culture of innovation and entrepreneurship in the cyber security domain, MeitY and DSCI launched the 'Cyber Security Grand Challenge' with award money of INR 3.2 Crore to motivate start-ups. SecurelyShare, and Payatu and Monoxor were the winners of the first grand challenge.
- **UCCH-** It's a DSCI initiative in collaboration with MeitY to promote the culture of innovation by discovering niche use-cases and conducting application challenges.
- **GeM-** Government E-Market place is facilitating start-up inception by driving initiatives like Startup Runway 2.0 that presents an opportunity for Startups to showcase their innovative products and services to Government buyers and engage in public procurement. GeM also provides Preferential Market Access granted to Indian start-ups and product companies to boost Make in India initiative.

Commercialization funding programs by Technology Development Board of DST & other funding activities by the ecosystem stake holders is further driving start-up inception and growth.

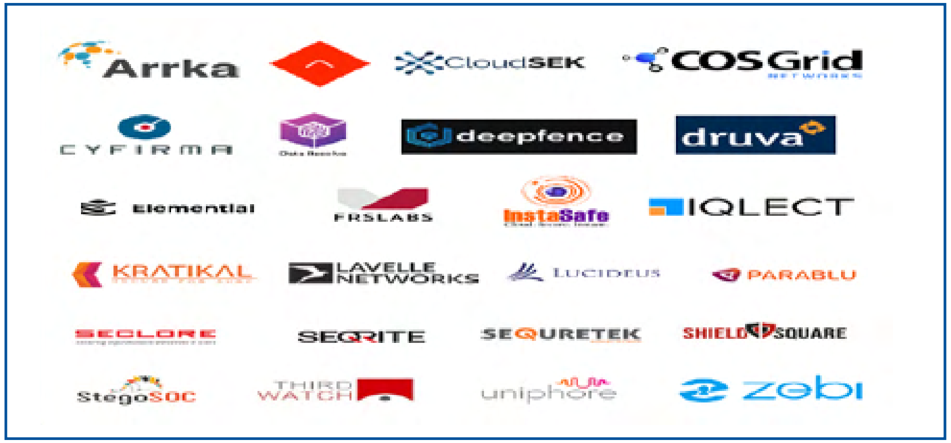
Indian Cybersecurity Product Industry

Funding Landscape

Cybersecurity Funding (USD Mn)



Cybersecurity Companies Funded



Source: DSCI Analysis and Crunchbase

*Note: These are Illustrative examples and do not cover the entire ecosystem

Total Cybersecurity Funding (2017 2021) | **USD 778 Mn**

- 2020 had huge head-winds in the funding of security start-ups. The funding landscape in India is in nascent stages as compared to US, Europe, and other regions. However, India's ability to produce unicorns in digital start-ups holds the potential to also transform the funding landscape of security start-ups too.
- There has been an increase in terms of awareness among the users over the last two years, due to the impact created by new cyber attacks such as ransomware as a service.
- From the investor's perspective, the niche solutions and platform-based companies are being valued, as the customers are looking for end-to-end solutions.
- Geographic overview: US remains a major investor from global perspective, investments are increasing gradually.
- In terms of status of engagement with cybersecurity startups and product companies, around 27% Indian cybersecurity service providers are actively funding Indian cybersecurity start-ups.

Interest areas for funding:

- Data privacy and secure multi party computation, verify encryption
- Data analytics to draw out intelligence
- Leverage data- run ML while preserving the privacy
- MDR gaining traction
- IDAM and zero trust focus
- Cloud networking
- End point security and management
- Security breach analytics and management
- Decoy infra and SASE- technologies

Indian Cybersecurity Product Industry

Mergers & Acquisitions

Mergers & Acquisitions:

- India is becoming a hotspot for global Cybersecurity technology companies, as acquisitions of Indian companies is growing, which is enabling the inorganic growth plans for geographic broad basing.
- Good traction is building up as global large cybersecurity firms are rapidly acquiring cybersecurity start-ups.
- Global companies are looking for start-ups to acquire products from niche areas.
- The Indian start-ups are looking for inorganic opportunities to expand their presence, get access to large customer base and capital.
- Overall, a lot of Indian start-ups are gaining traction for their innovative product R&D, Qualys and Zscaler were active M&A players in 2020, 2021.

Company name	Acquirer	Speciality	Details
Cybernet Security Solution Private Limited	BEK Communications Cooperative	Cybersecurity solutions	2021 - One of the objectives of the acquisition was to expand CyberNet Security's quality communication services to North Dakota businesses and nine other states BEK servers
Smokescreen Technologies	Zscaler	Solutions to predict threats, detect attacks, and respond to breaches	2021 - The acquisition allowed integration of Smokescreen into the Zscaler Zero Trust Exchange. It also helped to augment its capabilities for the detection of targeted attacks, lateral movement attempts, and ransomware
Cloudneeti India Private Limited	Zscaler, Inc.	Zscaler Cloud Security Platform	2020 - The main aim of the acquisition was to provide its customers with industry-leading data protection covered through the Zscaler Cloud Security Platform. It also enhanced organizations' cloud security by discovering and eliminating a few common causes of data breaches and compliance violations
Spell Security	Qualys	Endpoint Security	2020 - Acquisition brought an advanced endpoint behavior detection and additional telemetry to the Qualys Cloud Platform while strengthening Qualys' security and threat research capabilities
Aristi Labs	Exploit Hunters	SIEM	2020 - Technical operations of Exploit Hunters can take place in India from Bhopal. The deal was expected to also allow Aristi to expand its services in the Global markets
Paladion	Atos	MDR	2020 - This acquisition brought in some key Managed Detection & Response (MDR) capabilities to the Atosportfolio. It also expanded the global coverage for cybersecurity monitoring and response with Pladion'sSOCs. It enabled the creation of the next generation of Atos' Prescriptive SOC offering

Source: Zscaler Inc., BEK Communications, Zscaler

Indian Cybersecurity Product Industry

Mergers & Acquisitions

Company name	Acquirer	Speciality	Details
ShieldSquare	Radware	Bot Management	2019 - Radware leveraged ShieldSquare's product line to expand its portfolio and offered bot mitigation and management product line under its new Radware Bot Manager product line.
Lakhshya Cyber Security Labs	Lakhshya Cyber Security Labs	malware analysis, cyber breach investigation	2019 - Lakhshya Labd added a team of more than 40 professionals with expertise across sectors and with real-time 24/7 monitoring services through its SOC facility. This added significant value to Zacco and enabled the combined entity to address the clients' Digital Asset Protection in a holistic manner
Adya	Qualys	Cloud Security	2019 - The objective of the deal was to use the software products of Adya to consolidate the administration of Qualys' 'Software as a Service'(SaaS) apps through a single console
AforeCybersec Technology	AforeCybersec Technology	Multi-Segment	2019 - The acquisition enabled AforeCybersec customers to benefit immediately from Terralogic's extensive service capabilities, including the UI/UX Design, Automation, DevOps, IIOT and AI/ML Solutions. Terralogic's global customers will be provided with access to enhanced Cybersecurity
AuthMe ID Services	Airtel	Authentication	2018 - As part of the deal, the core team of AuthMe joined Airtel and become a part of Airtel X Labs. In addition, Airtel also acquired the intellectual proprietary rights for two flagship Authentication solutions developed by AuthMe
1Mobility	Qualys	Mobile & IoT Security	2018 - With the acquisition, Qualys provides visibility across mobile and IoT environments along with existing on-premises, endpoints, cloud(s)

Source: DSCI

Indian Cybersecurity Product Industry

Case Studies

Company name	Industry	Problem Statement	Solution Deployed	Outcome
APPSECURE	Oil and Gas	- The company was having issues related to several demanding and complex regulatory & security requirements and required to deploy an integrated approach towards IT Risk and Security Vulnerability Governance to meet their increasing threat landscape and regulatory requirements.	- Solution for risk, compliance and security vulnerability program	- 60% reduction in time spend for threat identification
CHIP SPIRIT	VLSI Design	- The client was facing issues related to software/core based cyber security solutions which were having a high possibility of being compromised at multiple levels like backdoors, Trojans and loopholes in the procured devices/ firmware. - This was mainly because procurement of encryption related semiconductor solution chips have supply chain risks.	- Proposed and developing a product that is completely hardware (VLSI chip design within FPGA with multiple levels of key handling) based encryption device developed in India.	- High speed crypto solution with minimal software intervention to protect highly sensitive data
DIMA Cyber Security	Cybersecurity | Network Security	- The company was looking for new models as the traditional on-premise multi-vendor security techniques such as Firewall, End-point security, Wireless LAN controller were leading to lower network security, higher investment costs on the physical hardware and periodic license renewable, and higher maintenance costs.	- Developed a one-stop solution, a software as a security client agent that complies with the SASE(Secure Access Service Edge) model, Zero Trust Architecture, Multilevel Security(MLS) powered by Threat Intelligence, DNS Firewall and Secure Web Gateway.	- Reduced capital expenditure and operational expenditure - Zero Manual Intervention - Achieved clear and filtered traffic that completely eradicates ransomware and phishing attacks forever

Source: Provider organization

*Note: These are Illustrative examples and do not cover the entire ecosystem

Indian Cybersecurity Product Industry

Case Studies

Company name	Industry	Problem Statement	Solution Deployed	Outcome
GAJSHIELD Data Security Firewall	FMCG	• The client was compromised on the security measures and server security. • Another challenge faced by the company was the authentication of users.	• Firewall • Multiple ISP support • URL and Application Filtering	• Secured network effectively • Successfully managing and tracking users
InstaSafe Cloud. Secure. Instant.	ITES	• The customer needed to evaluate secure access solutions to different applications hosted in multiple Data Centers around the world and were looking for Cloud based Zero Trust Access solution for their private Applications and softwares hosted across various countries including India, to access their applications remotely and securely.	• InstaSafe Zero Trust Application Access	• Scaled up remote access from 500 to 30000 users in 5 days, with greater compliance adherence, better remote security • 60% reductions in setup and maintenance costs
KRATIKAL SECURE FOR SURE	NBFC	• The company was facing brand abuse due to email spoofing, low email deliverability rate, and unsuccessful email marketing campaigns.	• Generated a DMARC record for the company's email domain.	• Gained full insight into its outbound email channel and authenticated outbound emails with a DKIM signature and configured all the legitimate sources to make them DMARC-compliant • Raised the average DMARC compliance and improved email deliverability rate and reduced spam score and protection against email spoofing attacks.

Source: Provider organization

*Note: These are Illustrative examples and do not cover the entire ecosystem

Indian Cybersecurity Product Industry

Case Studies

Company name	Industry	Problem Statement	Solution Deployed	Outcome
Q→NU	PSU	• The client was facing challenges related to manual courier of Encryption keys (ciphers) to every defense field units which couldn't be refreshed fast enough for hackers to harvest or break.	• Using Quantum Secure Symmetric pair of keys, the company demonstrated transport of its ciphers across the public network in the real time. • Integrated Armos product with client's manual cipher generation gun and offered Quantum safe keys to the client product for transporting their ciphers.	• Saved cost of more than 100 crores every year for end customers • Created new revenue stream for customers from Defense • Will lead to total transformation of secure key distribution in Indian defense and during war time • New revenue stream for customer from Defense will give a business of $100M over next 5 years
Ram	IT-SAAS Cyber Security Industry 4.0	• The client was looking for new solution as traditional antivirus detection cannot offer zero-day malware protection, obfuscated malware, and newborn ransomware variant.	• Using Machine Learning Technology, the client was able to detect new-born malware and Ransomware using predictive methodologies and offer zero-day protection	• Better detection ratio • Light weighted product

Source: Provider organization

*Note: These are Illustrative examples and do not cover the entire ecosystem

Indian Cybersecurity Product Industry

Case Studies

Company name	Industry	Problem Statement	Solution Deployed	Outcome
SEQURETEK	**A global home furnishings company headquartered in California**	• Existing vendor's on-premise implementation stagnated • Only 12 devices integrated over 12 months, with only day shift coverage • Analyst dependence for rules configuration • No formal incident response process • Total of 250 devices to be integrated for monitoring	• Implemented Percept Extended Detection and Response (Percept XDR) solution to ensure end-to-end security for the enterprise	• Protected existing vendor's investment in Phase 1 with ingesting data from those. All sources integrated within 6 weeks • AI based detection to self identify the patterns & create correlation rules • Single and complete view over customer's enterprise security & risk posture • Time saved for IT Teams leveraging SOAR based automated response mechanisms & lower false positives • Significant reduction in the Total Cost of Ownership (TCO) for the enterprise
SECONIZE	**Financial Services**	• The client was facing challenges to manage security across the cloud and applications. • There was a need for NBFC regulatory and other security requirements for the deployment of an integrated approach towards IT Risk and Security Vulnerability Governance.	• Deployment of Seconize DeRisk Centre (DRC) to identify different vulnerabilities in the Cloud infrastructure and applications and identifying potential risks. • Provided remediation and auto-remediation to DeRisk the organization and exhaustive dashboards. • Comprehensive and exhaustive dashboards helped the management for efficient operation	• Quick remediation • 5000+ issues identified in the cloud configurations were automatically remediated • Cybersecurity Maturity improved from Level 1 to Level 4 • 80% reduction in exposure & 60% reduction in effort

Source: Provider organization

*Note: These are Illustrative examples and do not cover the entire ecosystem

Indian Cybersecurity Product Industry

Case Studies

Company name	Industry	Problem Statement	Solution Deployed	Outcome
SecOps	Fintech and BFSI	• The client was having a huge business development blocker while working with a nationalised bank and wanted to identify and patch the existing security threats before the bank conducted its final audit.	• SecOps's AI-powered agentless platform for Vulnerability Management and remediating misconfigurations in applications and cloud.	• 93% faster security risk identification and 67% reduction in time spent on patching vulnerabilities • Saved 30% of total engineering costs in security fixes and increased company revenue by 45%
SISA	Banking and IT/ITES	• The customer was having issues in complying with Global PII regulations. • They were looking for solution to identify and classify sensitive data in structured and unstructured formats as per privacy guidelines.	• Deployed on-premise version of SISA Radar tool and data discovery and classification solution. • Customized the solution to integrate with other DLP solutions for better data protection.	• Identification of sensitive data in more than 10,000+ locations • Scanned 3000 endpoints and 24,000,365 accounts in limited time • Deleted the sensitive data which was no longer required for the business • Moving identified sensitive data to secured/isolated locations • Masking, truncating and encrypting the data based on the policies

Source: Provider organization

*Note: These are Illustrative examples and do not cover the entire ecosystem

Experts Speak

The domestic market is witnessing growth in demand due to digitalization, and there has been an increase in cybersecurity spending of SMEs. SaaS-based offerings are pushing demand and the good talent pool in India specially for product building is helping build robust cybersecurity products and solutions. From a global perspective, more investors are coming forward to invest in Indian cybersecurity start-ups due to their niche capabilities.

Chethan Anand

CEO and Co-Founder
Seconize

India is witnessing enormous cloud adoption and thereby the cloud solutions have gained traction over the past few years. Increasing volume and value of digital payments coupled with other digitalization factors is driving demand for secure digital adoption initiatives. From market point of view, best of breed products integrated with AI capabilities are dominating the market. Further, the scale of attacks has reduced however the complexity of the attacks has increased in the pandemic which has led to increased awareness levels and adoption of cybersecurity among large and small enterprises alike.

Shomiron Das Gupta

Founder, CEO - DNIF

Businesses are adopting cloud and in response, industry is coming up with cloud versions for all their product offerings. Thus, the solutions earlier available only on-premises, are now also available as SaaS offerings. From a sectoral standpoint, manufacturing industry has seen a steep growth, thanks to Digital Transformation and IoT. They have started leveraging cutting-edge AI-based cybersecurity solutions to help detect, protect, and respond to next-generation cyber threats. India is fast becoming a hotspot for investments. It is thus a potential market for a lot of cybersecurity vendors to acquire Indian companies.

Anand Naik

Co-founder and CEO-
Sequretek

Maintaining business continuity and unrestricted operations in organizations are the non-tech drivers that would drive the market. The industry is seeing the demand for new kinds of domain-specific solutions, such as supply chain security. Further, cybersecurity-related to risk is driving the demand for products. The industry is focusing on R&D and increasing investments in technology as the ROI realized is higher for enhanced products in cybersecurity.

Ashish Sonal

CEO
ORKASH Labs Pvt Ltd

Experts Speak

There has been a significant increase in the number of Indian cybersecurity start-ups in the last 3-4 years, due to a hospitable environment created by the government and industry stakeholders. A boost in traction from the international market is visible due to remote sales models. The growing awareness globally around cybersecurity has fast tracked the process of approvals, from 3-4 months to 3-4 weeks. Automation is taking a central role from a provider and consumer perspective, security automation using bots is another trend that can be witnessed. Further, the rising focus of the investor community towards Indian products is growing.

Dhruv Khanna

Co-Founder & CBO
Data Resolve

Security Products are getting converged and customers are preferring a comprehensive platform for manageability ease, synchronisation & reduced cost. This demand is owing to the movement towards cloud-delivered services in the private sector. Every large security company is now focusing on building comprehensive security suites and driving demand. In the same pursuit, US-based companies are targeting Indian companies for acquisitions on back of robust cybersecurity product offerings.

Karmesh Gupta

Co-Founder & CEO
WiJungle

The demand for compliance is growing significantly, the mature cybersecurity players have been quick to adopt and now companies being born in cloud are requesting for secure cloud adoption strategies to stay data and privacy compliant. As the awareness levels related to cyberattacks and RaaS, specifically in the manufacturing sector are growing, Supply chain, OT and Web application security are gaining traction. The highly regulated industries want to make sure the solutions implemented are certified and becoming more comfortable with Indian providers.

Anshul Saxena

Chief Executive Officer -
Haltdos

Indian Cybersecurity Product Landscape

Application Security
accops, Advantal, astra, BYTESEQ, deepfence, ECYLABS, FORTY TWO, haltDos, AppSecure, INDUSFACE, INNEFU, JUTO, KRATIKAL, Moneser, SBOXR, SecOps, Secure Eye, SECURITY ESCAPE, TAC Security, WeSecureApp, Rām

Cloud Security
accops, AGNI, ASSERTION, BLOCK ARMOUR, CloudCodes, cloudneeti, deepfence, haltDos, InstaSafe, LAVELLE NETWORKS, LTS Secure, Aeridio, PROACTEYE, Prophaze, risesharp, SecLogic, SecOps, SECURE, SEQRITE, StegoSOC, vehere, zebi

Forensics
brahmi systems, Clari5, secugile, FRSLABS, nanobi, prodiscover, PYRAMID, Saraansh, SECLABS, SECURE INDIA, Sentrapi, Simplifyd, SysTools, THIRD WATCH, TrustCheckr

Identity Access Management
accops, ADDROI, AppsPicket, Arcon, Shield, Digital Signature, digitaltrust, Elemental, emudhra, finahub, FORTY TWO, ilantus, iraje, LTS Secure, marlabs, Nviera, ogive, Sectona, Secure ID, Sentrapi, SEQURETEK, Tuebora, uniphore

Operational Security
aegify, AGNI, ALERT FUSION, arctos networks, ATTACKFENCE, DNIF, CYBERPACT, Flexible IR, IQLECT, LTS Secure, Newton's Apple, Nviera, QOS, SBOXR, SecOps, SHADOWMAP, secpod, securaa, SEQURETEK, SECVIEW, technisanct

OT and SCADA Security
CHIP SPIRIT, SECTRIO, Payatu

Data Security*
ardent, Arrka, axon, brahmi systems, BYTESEQ, diro, DISECTO, druva, EDER, GAJSHIELD, Klassify, oneDPO, Q-NU, SISA, SOMISH, stellar, TAQBit, vaultize, Whitehats, ZIROH Labs

End-Point Security
3Frames, accops, Arcon, CCURE, eScan, Foresiet, K7 COMPUTING, MATISOFT CYBER SECURITY LABS, MAXSECURE, mitsogo, NPAV, Quick Heal, Rām, REVE antivirus, Safecrypt, secpod, SECURE, SEQRITE, SEQURETEK, SKYNET, SISA, WhiteList Global

IoT Security*
3Frames, BLOCK ARMOUR, FORTY TWO, Payatu, SUBEX, SYSTOLE

Gateway Security
AGNI, BUGSKAN, DIADEM, DISECTO, haltDos, LAVELLE NETWORKS, PROCYBT, TeamF1, TECHDEFENCELABS

Network Security
AGNI, cipl, COSGrid, cyqure, GAJSHIELD, haltDos, InstaSafe, IQS, LTS Secure, Newton's Apple, NIVETTI SYSTEMS, SEQRITE, SOPHOS, SUBEX, UNLEASH networks, vehere, Wi-Jungle

Risk Management
CloudSEK, Cytelligent, CYBER, Data Resolve, FIXNIX, Foresiet, KALIBRATE, ORKASH, SECONIZE, secpod, SecLogic, SecureCH, SAFE, SHADOWMAP, SISA, SKYNET, TAC, technisanct, Through bit, vaultize, Whitehats

Threat Facing Products
aadi, AGNI, ALBOT, appknox, Arcon, astra, BLUSAPPHIRE, CYFIRMA, DIGINTRUDE, DIMA, DNIF, FireCompass, Foresiet, FOURCORE LABS, KRATIKAL, LTS Secure, Newton's Apple, Payatu, PROACTEYE, Rām, SecOps, secninjaz, SHADOWMAP, SISA, SKYNET, Syn Radar, tornd, VOLON

*Data security includes privacy

*IAM includes Authentication

Note: Overlaps exist between categories, These are Illustrative examples and do not completely reflect the ecosystem

Indian Cybersecurity Product Landscape — Product Landscape Capabilities

ASM/CART
CloudSEK, ECYLABS, FireCompass

Bot Mitigation
haltDos, JUTO

CASB CSPM
CloudCodes ZERO TRUST APPROACH, eScan, haltDos, PROACTEYE, SecLogic

Data Privacy automation/ Management
ardent — Data privacy simplified and automated, Arrka, DISECTO — Cyber Security and Privacy Solutions, EDER, Karippal innovations, oneDPO

DAST/MAS
INDUSFACE, WeSecureApp

DDoS
haltDos, INDUSFACE, Foresiet

Deception
ALGOSMIC CYBER SECURITY, SMOKESCREEN, SUBEX, Secfence

DLP, Data Classification, Data security and Governance
CloudCodes ZERO TRUST APPROACH, Data Resolve, Klassify, Wi-Jungle, SISA

EDR MDR XDR
BYTESEQ, eScan, Foresiet, Microworld Software Services, SISA, technisanct

EDRM
QUIKPROTO, SECLORE, vaultize

End-point Protection
K7 COMPUTING, mitsogo, MATISOFT CYBER SECURITY LABS, MAXSECURE, NEXULUS, Quick Heal, SEQURETEK

IAM/PAM/ Authentication
arcon, Elemental, FORTY TWO, INNEFU, iraje, marlabs, Sectona

Note: Overlaps exist between categories, These are Illustrative examples and do not completely reflect the ecosystem

Indian Cybersecurity Product Landscape — Product Landscape Capabilities

NDR- Network Detection and response
NIVETTI SYSTEMS, SUBEX, TechMax Technologies, UNLEASH networks

NGFW
COSGrid NETWORKS, GAJSHIELD Data Security Firewall, Wi-Jungle Unified Network Security Gateway

Quantum
Q-NU, TAQBit

Risk Quantification/ Monitoring/Management
Data Resolve, LUCIDEUS, SecLogic, SECONIZE, SHADOWMAP, SISA, TAC Security

SDP/ZTNA
accops, arcon, ATTACKFENCE, BLOCK ARMOUR, cyqure, Foresiet

SD-WAN
COSGrid NETWORKS, Infinity labs, InstaSafe, LAVELLE NETWORKS

Secure communication
CONTUS, XGEN PLUS, DBAUX

SIEM-SOAR
arctos networks, ATTACKFENCE, BYTESEQ, DNIF, eClerx, KHIKA, LTS Secure, Nviera, securaa

SMPC- Secure multi-computation Zero Knowledge proof FHE- Full Homeworking Encryption
ZIROH Labs

UEBA
arcon, Data Resolve, haltDos, Hesperus Infosec, PROACTEYE, SEQURETEK, SISA

WAF
ARISTI, BUGSKAN Cyber Security Solutions, haltDos, INDUSFACE

Note: Overlaps exist between categories, These are Illustrative examples and do not completely reflect the ecosystem

*Note: These are Illustrative examples and do not cover the entire ecosystem

India Cybersecurity Industry

Talent Overview

Talent Pool and Skills

Talent Overview

- The cybersecurity services providers are aggressively looking to expand the workforce in India. There is a huge demand for cyber projects but with a significant shortage in availability of skilled cybersecurity talent, which is leading to many challenges for the providers, such as taking up new projects and retaining the existing talent.
- The providers are engaging in multiple skilling and talent development activities, such as internal and external investments for specific talents growth. In India, the companies are going for partnerships with universities by funding cybersecurity training, including setting up of infrastructure. Threat management centers outside India are also being set up to attract talent and inculcate talent globally.
- The focus is shifting towards having set training modules to hire freshers and training them into skilled employees .

Challenges

- War for talent leading to sharp spike in compensation; Salaries are growing up to 2X-3X for lower and mid level workforce
- Churn rate is also increasing proportionally, experts say – experienced employee committing to join have multiple offers in hand and conversion ratio has gone done roughly from 80% to 50-60%.

TATA CONSULTANCY SERVICES

- TCS has entered a partnership with Heriot Watt University to collaborate on research, co-innovation, talent development and encourage the exchange of ideas and resources among teachers, scholars, students, researchers, staff, and TCS' business partners.

Tech Mahindra

- Tech Mahindra will be working closely with IIT Kanpur on research projects to develop and foster an environment to deal with automation in cyber security and to enhance digital resilience of critical national infrastructure.

TATA COMMUNICATIONS

- Tata Communications partnered with SASTRA University to fund and establish a cyber security lab at the university. With this partnership, Tata Communications aims to co-create an ecosystem by partnering with universities globally and build the skills and capabilities.

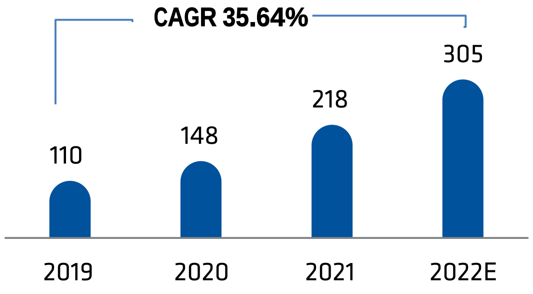
HCL

- HCL Tech inks pact with IIT Kanpur to build up competence in cybersecurity, and also hosting annual hackaton

Infosys

- NIIT University, in association with Infosys has designed an Industry Linked Postgraduate Programme, M.Tech in Cyber Security for aspiring professionals of Infosys, who are keen to explore and exploit the latest trends in Cyber Security Technologies.

Services Talent Pool in Thousands



There is an overall demand for cybersecurity talent across functions, few key cybersecurity areas in demand are:

- Identity & Access management and governance
  - Full stack IAM specialist with DevOps skills
- Digital transformation and consulting
- Business enabler
  - Business aware CISOs
- Secure cloud implementation
  - Enterprise architect
  - Cloud security architect
- Governance, risk and compliance
  - Domain specialists
  - SOC Analyst
- Audit facilitation and automation
  - Developers and specialists
- Security monitoring and operation center
  - Data scientist /security engineer

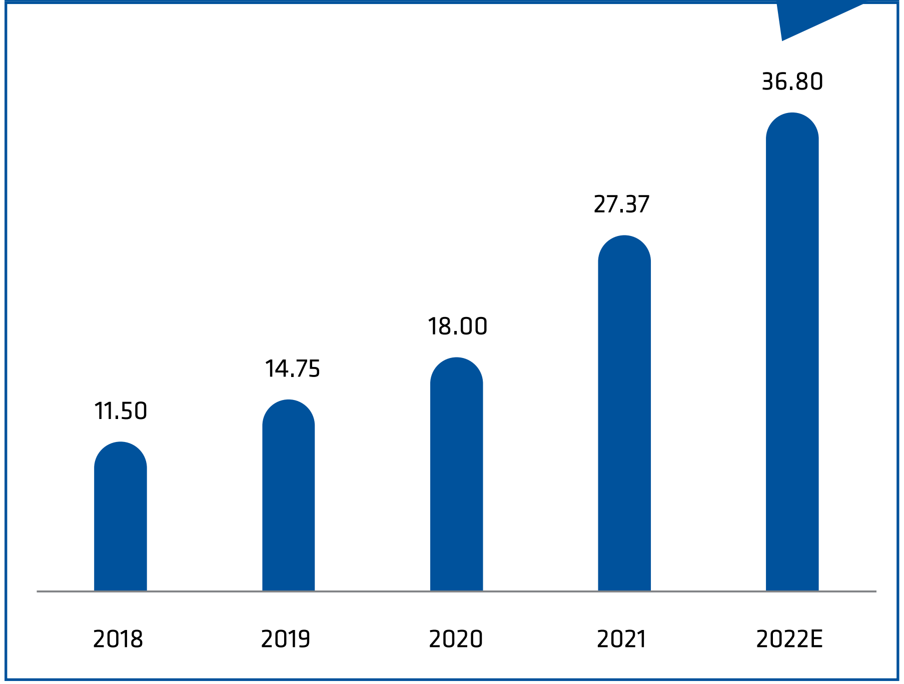
*Note: These are Illustrative examples and do not cover the entire ecosystem

Source: DSCI - Indian Cybersecurity Product Landscape 2.0, Indian Cyber Security Report 2020, TCS, Tech Mahindra , HCL, Infosys

Product Industry

Talent Pool and Skilling Initiatives

Product & Start-up Talent Pool



Key positions in demand

- SecOps- Scripters/ developers
- Security engineering
- Hardware design
- Cloud Security architect

Skills required

- Coding skills- AI/ML algo creation
- Knowledge of data science, Digital Logic implementation
- Proficiency in Cloud Security

MeitY's flagship ISEA skilling project has now entered phase 3. ISEA has key focus on cultivating BTech, MTech and PHD candidates in cybersecurity domain to boost the ecosystem.

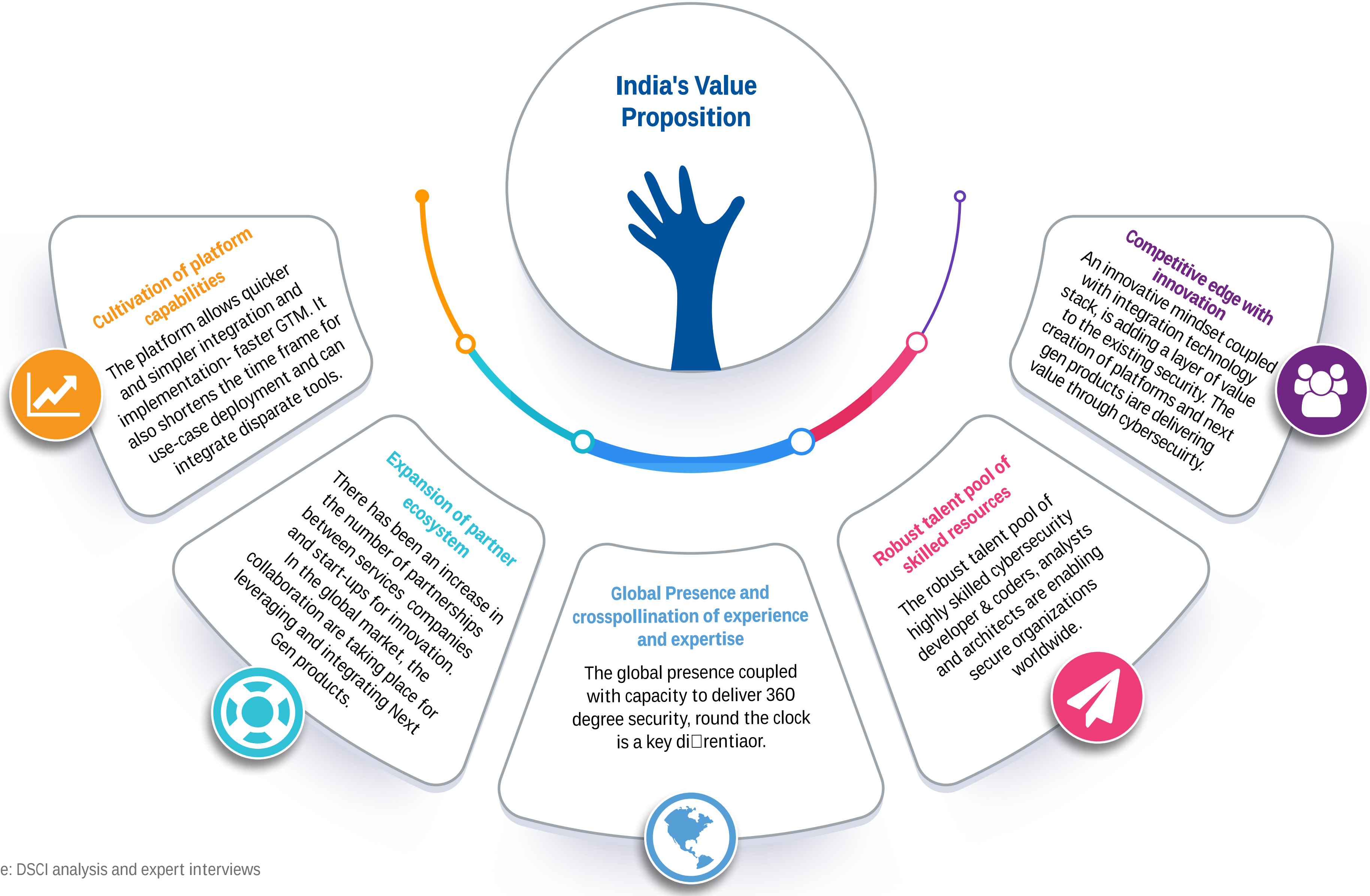
NASSCOM and DSCI aim to take the number of cyber security professionals in the country to a million.

NASSCOM FutureSkills is enabling thousands of IT professionals to be future-ready by creating a culture of continuous learning, collaboration and co-creation.

DSCI in collaboration with Microsoft have joined forces in 'Cyber Shikshaa' for skilling women engineering graduates in the niche field of Cyber Security.

Source: DSCI analysis, expert interviews ISEA

India's Value Proposition



India's Value Proposition

Cultivation of platform capabilities

The platform allows quicker and simpler integration and implementation- faster GTM. It also shortens the time frame for use-case deployment and can integrate disparate tools.

Expansion of partner ecosystem

There has been an increase in the number of partnerships between services companies and start-ups for innovation. In the global market, the collaboration are taking place for leveraging and integrating Next Gen products.

Global Presence and crosspollination of experience and expertise

The global presence coupled with capacity to deliver 360 degree security, round the clock is a key differentiaor.

Robust talent pool of skilled resources

The robust talent pool of highly skilled cybersecurity developer & coders, analysts and architects are enabling secure organizations worldwide.

Competitive edge with innovation

An innovative mindset coupled with integration technology stack, is adding a layer of value to the existing security. The creation of platforms and next gen products iare delivering value through cybersecuirty.

Source: DSCI analysis and expert interviews

Appendix

Definitions

Product	Definition
Cloud Access Security Broker (CASB)	It is designed to solve the challenges of protecting an organization's cloud applications. They are now an essential elements of cloud security strategies, that helps security and risk management leaders to discover cloud services and assess cloud risk. They also help to identify and protect sensitive information, detect and mitigate threats, and institute effective cloud governance and compliance.
Differential Privacy	Differential privacy is a system for sharing information about a dataset while withholding or distorting certain information elements about individuals in the dataset. The system uses an exact mathematical algorithm that randomly inserts noise into the data and ensures that the resulting analysis of the data does not significantly change whether the individual's data is included or not.
Endpoint Detection and Response (EDR)	It Is a modern endpoint security product with detection and response capabilities, built into a single lightweight agent. It can be deployed through cloud and unifies many cybersecurity tools in one console while offering further integration options.
Extended detection and response (XDR)	Extended detection and response (XDR) is a vendor-specific, threat detection and incident response tool that unifies multiple security products into a security operations system. Primary functions include centralization and normalization of data in a repository for analysis and query, improved protection and detection sensitivity resulting from simplified configuration and security product coordination. The incident response capability can change the state of individual security products as part of the recovery process.
Managed Detection and Response (MDR)	It offers a turnkey solution covering endpoints, networks, cloud services, operational technology (OT)/Internet of Things (IoT) and other sources, to collect relevant logs, data and other telemetry. This telemetry is analyzed using a range of analytics, threat intelligence and manual analysis to detect and respond to the threat
Next Gen Firewall (NGFW)-	They are firewalls offering bidirectional controls (both egress and ingress) for securing networks. They offer additional capabilities such as application awareness and control, intrusion detection and prevention, advanced malware detection, logging, and reporting, Which has led to their growth in demand, and cloud-based delivery is preferred
Privileged Access Management (PAM)	PAM tool can mitigate the risk arising from the existence of privileged accounts.. PAM tools provide robust and granular control, transparency, scalability, and more accountability for privileged access compared to manual controls and custom or generic tools

Source: Gartner

Definitions

Product	Definition
SCADA & Hardware Security	Hardware security has become crucial to secure the critical infra and manufacturing sectors. Cybersecurity solutions are being implemented to minimize and eliminate all kinds of risks posed by hackers, malware, cyber espionage, and other threats.
Secure access service edge (SASE)	It provides a fully integrated security stack, and delivers multiple capabilities such as SD-WAN, SWG, CASB, NGFW and zero trust network access (ZTNA). SASE's cloud-delivered set of services on back of the pandemic effect, is driving rapid adoption of SASE.
Security Orchestration, Analytics and Response (SOAR)	SOAR tools are primarily leveraged by organizations with a security operations center for general productivity, efficiency and consistency improvements. It combines incident response, orchestration and automation, and threat intelligence (TI) management capabilities in a single platform. SOAR tools are also used to document and implement processes (aka playbooks, workflows and processes)
Software-defined WAN (SD-WAN):	As cloud adoption has increased rapidly, organizations are turning their intention towards SD-WAN. Software defined WAN helps to improve user experience, especially for SaaS and IaaS applications in multi-cloud environment. SD-WAN provides security functionalities such as application-aware firewall, IDS/IPS and can be configured as per application policy.
User Entity Behavior Analytics (UEBA)	UEBA solutions use packaged analytics to evaluate the activity of users and other entities. They discover threats that is anomalous to the standard profiles and behaviors of users and entities. The most common use cases sought by enterprises are threat detection and response, as well as insider threat detection and response
Zero Trust Network Access (ZTNA)	It creates an identity- and context-based, logical-access boundary encompassing a user and an application or set of applications. It provides adaptive, identity-aware and precision access. ZTNA improves the flexibility, agility and scalability of application access, enabling digital businesses to thrive without exposing internal applications directly to the internet, reducing risk of attack

Source: Gartner

Abbreviations

AI/ML	Artificial Intelligence/Artificial Intelligence
AMC	Annual Maintainence Charge
AWS	Amazon Web Services
APAC	Asia Pacific
B2C	Business to Consumer
BFSI	Banking, Financial Services and Insurance
CAGR	Compounded Annual Growth Rate
CISO	Chief Information Security Officer
CASB	CASB
CERT	Computer Emergency Response Team
CSPM	Cloud Security Posture Management
CPs	Channel Partners
CSP	Cloud Servcie Providers
CWPP	CWPP
DDoS	DDoS
DevSecOps	Development, Security and Operations
DLP	Data Leakage Prevetion
IRDAI	Insurance Regulatory and Development Authority

FPGA	Field Programable Gate Array
EDR	Endpoint Detection and Response
GeM	Government e-marketplace
GCC	Global Capability Centres
GDPR	GDPR
GRC	Governance, Risk and Compliance
HSM	Hardware security module
IAM	IAM
ICS	Industrial Control Systems
IoT	IoT
IRM	IRM
ISEA	Information Security Education and Awareness
ITeS	Information Technology
IR	Incidence Response
IT	Information technology
LAN	Local Area Network
MDR	Managed Detection Response
MEA	Middle East and Africa
MDR	Managed detection and response

MSS	Managed Security Services
MSSP	Managed Security Service Provider
NDR	Network Detection & Response
NCIIPC	National Critical Information Infrastructure Protection Centre
NGFW	Next Gen Firewall
NIST	NIST
OT	Operational Technology
OEM	Original Equipment Manufacturer
PAM	Privileged access management
PKI	Public Key Infrastructure
RaaS	Ransomware-as-a-service
SaaS	Software as a Service
RPA	Robotic Process Automation
SIs	System Integrators
SASE	Security Access Service Edge
SCADA	Supervisory control and data acquisition is a control system architecture
SD-WAN	Software-defined Wide Area Network
SI	System Integrators

Abbreviations

SIEM	Security Information and Event Management
SLA	Service Level Agreement
SMEs	Small and Medium-scale Enterprises
SOAR	Security Orchestration Automation and Remediation
SOC	Security Operations Centre
TCS	Tata Consultancy Services
UEBA	User Entity Behaviour Analysis
TVM	Threat and Vulnerability Management
VAPT	Vulnerability Assessment and Penetration Testing
VDI	Virtual desktop infrastructure
VLSI	Veri Large Scale System Integrators
VPN	Virtual Private Network
VMaaS	Vulnerability Management as a Service
WAF	Web Application Firewall
XDR	Extended Detection and Response
ZTNA	Zero Trust Network Access

Acknowledgement

We sincerely thank the cybersecurity industry members who participated in the study and provided valuable insights. On behalf of DSCI, we would like to express our gratitude to all the industry leaders and professionals for their valuable contribution and support, without which this report would not have been possible.

Authors:

Anand Raman, Assistant Manager-Research

Rama Vedashree, Chief Executive Officer

Contributors:

Atul Kumar, Lead, Government Initiatives

Amit Ghosh, Manager, Communications

Dr. Sriram Birudavolu, CEO, Cybersecurity Centre of Excellence

Vinayak Godse, Sr. Vice President

and Industry leaders

About DSCI

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by NASSCOM®, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI brings together governments and their agencies, industry sectors including IT-BPM, BFSI, Telecom, industry associations, data protection authorities and think-tanks for policy advocacy, thought leadership, capacity building and outreach initiatives. For more info, please visit www.dsci.in

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

DATA SECURITY COUNCIL OF INDIA
NASSCOM CAMPUS, 4th Floor, Plot. No. 7-10, Sector 126, Noida, UP - 201303
For any queries contact
P: +91-120-4990253 | E: research@dsci.in | W: www.dsci.in

DSCI_Connect dsci.connect dsci.connect
data-security-council-of-india dscivideo