nasscom

DSCI
PROMOTING DATA PROTECTION

National Centre
of Excellence
CYBERSECURITY TECHNOLOGY
AND ENTREPRENEURSHIP

इलेक्ट्रॉनिकी एवं
सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF
ELECTRONICS AND
INFORMATION TECHNOLOGY
सत्यमेव जयते

REIMAGINING SECURITY: A NEW ERA POWERED BY GENERATIVE AI

December 2024

Foreword

The objective of this report is to provide a comprehensive analysis of the current state of the cybersecurity landscape, with a particular focus on the integration of Generative AI technologies. As cyber threats continue to evolve and escalate, organizations must adapt their security strategies to safeguard their assets and maintain trust in the digital age. This report aims to highlight the challenges and opportunities presented by Generative AI in enhancing cybersecurity measures, while also examining the emerging trends within the Indian security landscape.

In this report, we cover key aspects such as the current dynamics of the security industry, the growing adoption of Generative AI solutions by user organizations, and the innovative approaches being developed by service providers. We also explore the frameworks that organizations should implement to strengthen their security posture, the best practices outlined in a playbook for security providers, and the overall outlook for the cybersecurity sector as it continues to evolve.

Looking ahead, the outlook for the cybersecurity industry is promising, with increasing investments in innovative solutions and a growing emphasis on collaboration among service providers and user organizations. As the adoption of AI-driven security solutions gains traction, organizations will be better equipped to navigate the complexities of the threat landscape, ensuring a more secure and resilient digital environment for all stakeholders.

VINAYAK GODSE
CEO
DSCI

ACHYUTA GHOSH
Senior Director and Head
Nasscom Insights

Table of Contents

Security is the cornerstone of digital trust 07

With 400+ companies in the ecosystem, India is an emerging hub for cybersecurity services 13

Global end-user enterprises are embracing Generative AI-led shifts in cybersecurity strategies 16

Security technology providers are innovating to incorporate Generative AI into their solutions portfolio 22

Recommended Generative AI-Enabled Cybersecurity Framework for End-User Enterprises 31

Security Playbook for Service Providers 32

Outlook & Recommendations 35

Case Studies 39

Executive Summary

The economic impact of Cyberattacks

$4.88 Mn Average cost of a data breach in 2024, highest average on record

88% Cybersecurity breaches caused by human error

4Mn Global shortage of Cybersecurity Professionals

91% Organizations feel employees' using Generative AI will lead to increase in productivity in next 12 months

99% Organizations will increase their cyber budgets in next 12 months

Source: IBM, Stanford, Cybersecurity Ventures, PwC, World Economic Forum, DSCI

1. Current Security Industry

a. The cybersecurity industry is experiencing significant transformation, driven by the need for innovative solutions to combat the rising threat of cyberattacks.

b. Cybersecurity market in India reached ~USD 6 billion in 2023, growing at a CAGR growth of over 30% during 2019-23.

c. India cybersecurity market is expected to account for 5% of the global market by 2028.

2. India's Security Landscape

India is emerging as a prominent hub for cybersecurity services

a. With 400+ companies in India’s cybersecurity ecosystem, a growing number of startups and established providers are focusing on innovative solutions.

b. India's maturing cybersecurity landscape, characterized by growing awareness and spending, has seen 60% of product providers emerge since 2015.

c. Bengaluru, Delhi/NCR, and Pune/Mumbai are the leading cybersecurity hubs in India, with Bengaluru holding the largest share ~35%, followed by Delhi/NCR ~29% and Pune/Mumbai ~31%. Hyderabad and Chennai are emerging tech centres.

3. User Organization Adoption of Generative AI Security Solutions

a. The adoption of Generative AI in user organizations is gradually gaining momentum, as businesses recognize the potential of AI-powered solutions to enhance threat detection and incident response.

b. The Nasscom-NCoE (DSCI) State of User Organizations Security 2024 survey reveals a ~5% annual increase in cybersecurity spending as a percentage of IT budgets, underlining its growing importance as a strategic investment for digital transformation.

c. Data analysis and insights generation, automation of various cybersecurity processes, and customer services and support are the top three use cases for Generative AI in security, globally and in India.

d. Organizations are primarily focusing on regular audits and model testing to mitigate Generative AI risks.

e. The survey highlights organizations' comprehensive approach to cybersecurity in the Generative AI era, encompassing awareness, access control, human-in-the-loop considerations, & advanced security training.

4. Service Providers Developing Solutions with Generative AI Integration

a. Cybersecurity service providers are actively developing solutions that incorporate Generative AI, aiming to automate processes and improve the efficiency of threat management.

b. Generative AI is a promising technology, with nearly 35-40% of security providers already integrating it into their offerings within just two years.

c. Model fairness and bias are key challenges for service providers using Generative AI.

d. Service providers are leveraging partnerships, industry collaborations, in-house development, and client/academic co-creation to accelerate the adoption of Generative AI in cybersecurity, enabling the development of innovative, robust, and tailored solutions.

e. Partnerships strategy has seen a significant increase in importance, likely due to the complex nature of Generative AI solutions.

5. User Organization Framework

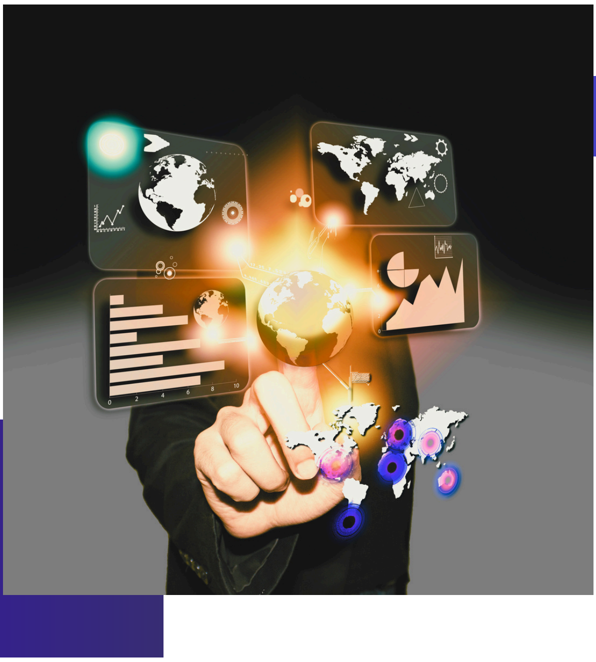
a. The Nasscom-NCoE(DSCI) framework has a structured approach that enables user organizations to effectively manage security threats while ensuring compliance with privacy regulations.

b. It can proactively allow user organizations to protect their valuable assets, maintain business continuity, and foster trust with stakeholders.

6. Playbook for Security Providers

a. The Nasscom- NCoE(DSCI)'s playbook is essential for security service providers, outlining best practices for assessment, planning, and implementation of security solutions.

b. This playbook serves as a guide for navigating the complexities of cybersecurity and ensuring a proactive response to incidents.



7. Outlook & Recommendations

a. The future of cybersecurity is poised for growth, with increasing spending on innovative technologies and a focus on collaboration among industry leaders.

b. As organizations continue to prioritize security, the integration of AI and automation will play a crucial role in enhancing their ability to combat cyber threats effectively.

Security is the cornerstone of digital trust

Security has become an increasingly critical aspect in the digital age. As technology continues to advance, and reliance on it grows, so does the risk of cyber threats. From data breaches and identity theft to critical infrastructure attacks and geopolitical espionage, the stakes have never been higher.

The rapidly rising economic cost of cybercrime

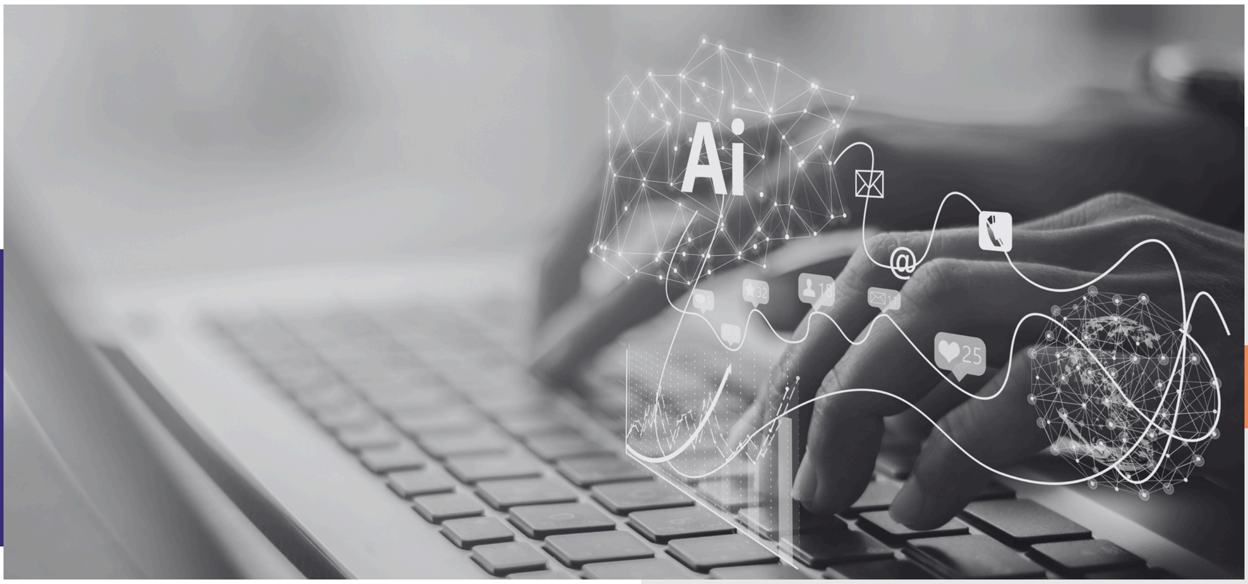
Cybercrime is a growing threat, silently stealing billions of dollars from individuals and businesses worldwide. With the increasing reliance on technology, the cost of cyberattacks is skyrocketing, impacting economies and disrupting daily life.

$4.88 Mn
Average cost of data breach, globally.

39%
Increase in cost of data breaches in India between 2020 and 2024, reaching ~$2.3 Mn.

88%
of cybersecurity breaches are due to addressable human error.

Source: IBM, Stanford, Cybersecurity Ventures, PwC, World Economic Forum



Security is evermore paramount today

The escalating threat of cybercrime demands a robust and innovative approach to cybersecurity. As our digital world expands and becomes increasingly interconnected, the stakes are higher than ever.

- **Pervasiveness leading to higher potential misuse of personal data**
  As our digital footprint expands, so does the risk of data breaches and identity theft.

- **More connected critical infrastructure**
  The increasing interconnectedness of critical infrastructure systems, such as power grids and transportation networks, makes them vulnerable to cyberattacks.

- **Increasing propensity of cyber warfare led mass collateral damage**
  Cyber warfare has the potential to cause widespread disruption and damage to critical infrastructure, economies, and societies.

- **Greater potential of economic damage with growing linkage to digital wellbeing**
  Digital technologies are essential for economic growth and social progress. However, cyberattacks can undermine these benefits and cause significant economic losses.

- **Generative AI's democratization exposes every possible interface to the risk of cyberattack**
  The widespread adoption of generative AI has created new opportunities for cyberattacks, as malicious actors can exploit these tools to launch sophisticated attacks.

Most observed cyberattacks

Major Cyberattack Pathways

Email, third party and open-source software, web applications, end-point devices, cloud-based pathways, software supply chain, mobile devices, operating systems, firmware vulnerabilities, etc.

Emerging Cyber Threats

AI/ML attacks, quantum computing threats, IoT vulnerabilities, biometric hacking, etc

Significant Vulnerabilities

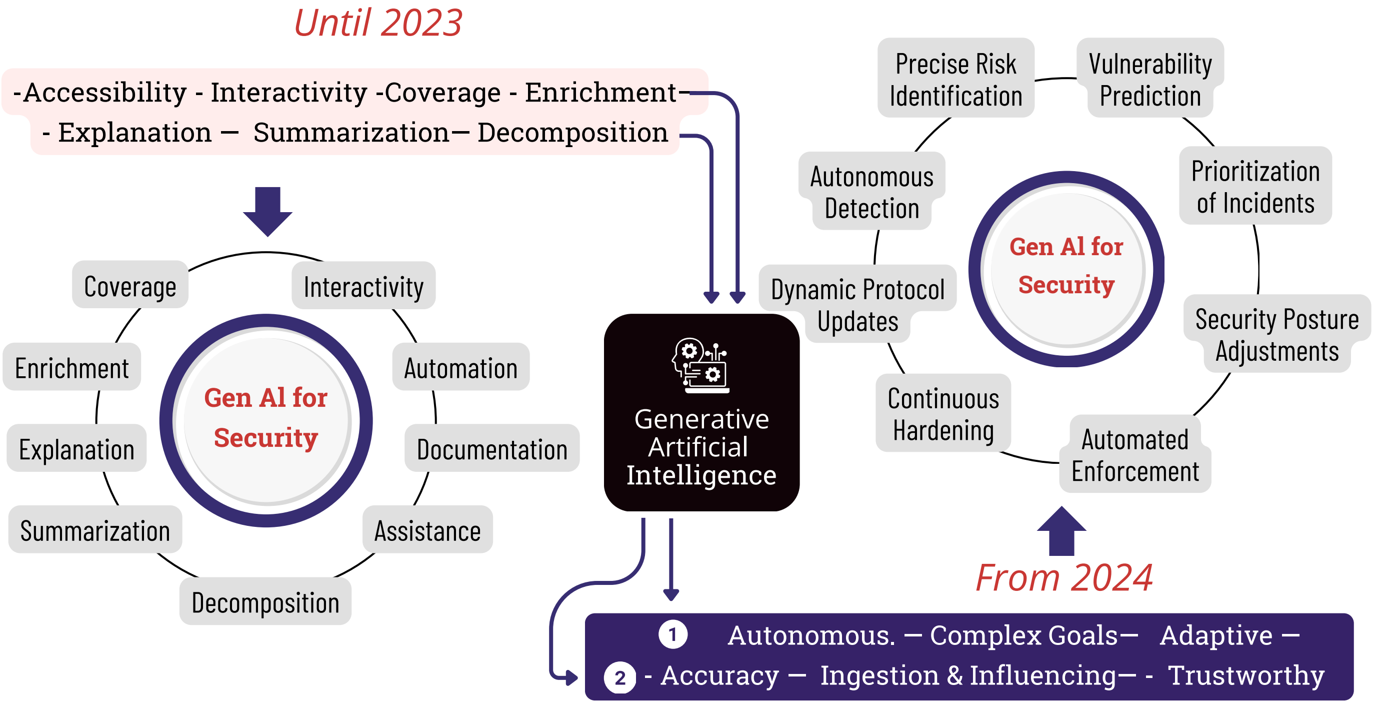
Misconfigurations, unsecured APIs, outdated/unpatched software, zero-day vulnerabilities, weak or stolen user credentials, access control/unauthorized access, web application, etc.

Major Cyber Threats

Phishing, ransomware, DDoS attacks, social engineering, supply chain attacks, insider threats, zero-day exploits, spyware, viruses and worms, etc.

Emerging impact of Generative AI on cybersecurity

Generative AI for Cyber Security: Until 2023 and From 2024



Until 2023
-Accessibility - Interactivity -Coverage - Enrichment
- Explanation — Summarization— Decomposition
Gen AI for Security
Coverage
Interactivity
Enrichment
Automation
Explanation
Documentation
Summarization
Assistance
Decomposition
Generative Artificial Intelligence
Precise Risk Identification
Vulnerability Prediction
Autonomous Detection
Prioritization of Incidents
Dynamic Protocol Updates
Security Posture Adjustments
Continuous Hardening
Automated Enforcement
Gen AI for Security
From 2024
1 Autonomous. — Complex Goals— Adaptive —
2 - Accuracy — Ingestion & Influencing— - Trustworthy

The Generative AI in revolutionizing cybersecurity practices, from enhancing current capabilities to enabling autonomous and adaptive security solutions.

Current state of Generative AI in cybersecurity

Until 2023

Accessibility, Interactivity, Coverage, Enrichment

Generative AI can enhance accessibility to security information, enable interactive exploration of data, expand coverage of security analysis, and enrich insights through contextual understanding.

Explanation, Summarization, Decomposition

It can provide clear explanations for complex security findings, summarize lengthy reports, and break down complex security problems into manageable components.

From 2024

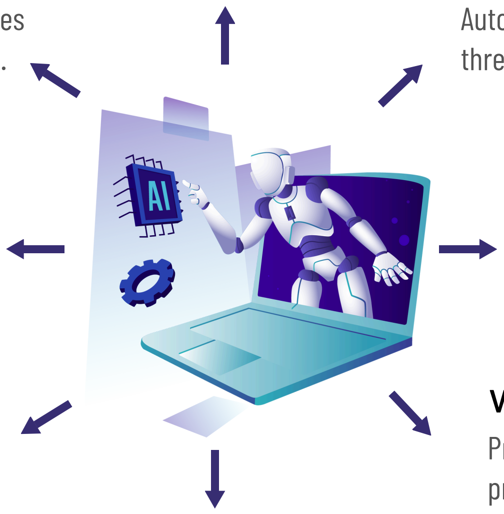
Autonomous, Complex Goals, Adaptive

Generative AI will be able to autonomously set and achieve complex security goals, adapt to evolving threats, and learn from past experiences.

Accuracy, Ingestion & Influencing, Trustworthy

It will prioritize accuracy in its outputs, seamlessly integrate with existing security systems, and build trust through transparency and explainability.

Applications of Generative AI going forward



Dynamic Protocol Updates

Generative AI automatically updates security protocols to adapt to evolving threats.

Continuous Hardening

Continuously strengthens security defenses through automated hardening techniques.

Autonomous Detection

Autonomously detects and responds to threats in real time.

Automated Enforcement

Enforces security policies and standards through automated mechanisms.

Precise Risk Identification

Identifies specific threats and models their potential impact.

Security Posture Adjustment

Adapts security controls to mitigate emerging risks.

Vulnerability Prediction

Predicts future vulnerabilities and proactively patches systems.

Prioritization of Incidents

Prioritizes incidents based on severity and impact.

Current cybersecurity capacity gaps need urgent attention and Generative AI-infusion

The global cybersecurity landscape is facing a severe shortage of professionals, with a gap of over 4 million skilled individuals. Despite this, organizations are significantly increasing their cybersecurity budgets and recognizing the potential of Generative AI to boost productivity. This presents a unique opportunity to leverage AI to bridge the skills gap and enhance cybersecurity defenses.

→ 44 Mn global shortage of cybersecurity professionals

→ 99% organizations will be increasing their cyber budgets in next 12 months

→ 91% Organizations feel employees' using Generative AI will lead to increase in productivity in next 12 months

Source: IBM, Stanford, Cybersecurity Ventures, PwC, World Economic Forum

Impact of Generative AI on Security

The impact of generative AI on security is multifaceted. While it offers significant benefits, it also introduces new challenges and risks that must be carefully considered and addressed. A balanced approach that leverages the strengths of AI while mitigating its weaknesses is essential for ensuring a secure digital future.

Advanced Threat Detection

Generative AI can analyze vast datasets to identify patterns and anomalies that may indicate malicious activity, such as phishing attempts, malware, and data breaches.

Automated Incident Response

AI-powered systems can rapidly detect and respond to security incidents, reducing time it takes to contain threats and minimize damage.

Improved Vulnerability Assessment

Generative AI can generate synthetic data to test security systems and identify vulnerabilities that might otherwise be overlooked.

Enhanced Cybersecurity Upskilling

AI can create realistic training scenarios to help security professionals develop the skills needed to address emereine threats.

Ethical Concerns

Use of AI in security raises ethical questions about privacy, bias, and accountability. It can create challenges in determining responsibility for negative outcomes.

Data Exposure

Generative AI can pose significant risks to sensitive data. If an AI system is not adequately protected against unauthorized access or manipulation, it could be used to steal or misuse sensitive information.

AI-Powered Malware

Generative AI can be used to create new, unique malware variants that can evade traditional detection methods, making it more difficult for security teams to identify & respond to threats.

Deepfake Threats

Generative AI can be used to create highly realistic deepfakes, which can be used for fraud, disinformation, and blackmail.

Source: Nasscom, DSCI Research

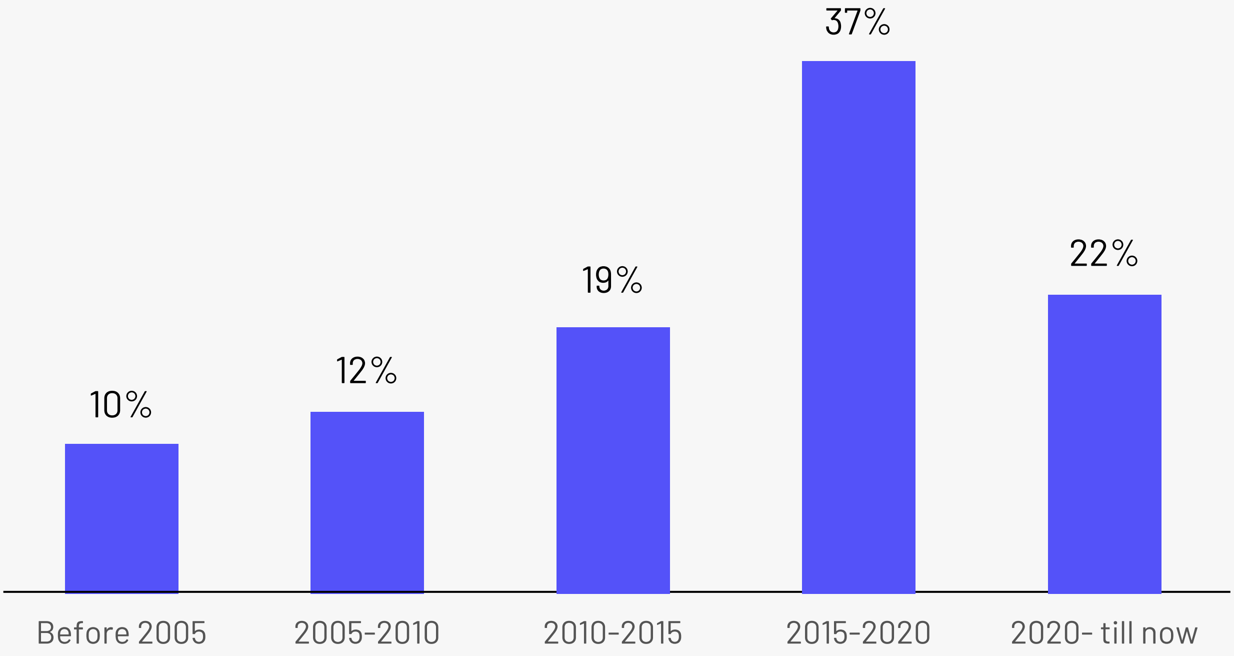
With 400+ companies in the ecosystem, India is an emerging hub for cybersecurity services

Factors driving India's emergence

India's cybersecurity ecosystem is rapidly evolving in response to increasingly sophisticated threats that are rapidly expanding attack surfaces due to digitalization of legacy sectors, faster adoption of emerging technologies, such as Generative AI, IoT, edge computing, and the still-evolving technology-related policy paradigm (DPDP Act, likely revisions to IT Act with digital nativity at the core, etc.) with less well-tested punitive measures, all of which combinedly create more opportunities for threat actors, as well as solution providers.

Damage due to cyberattacks is also becoming multi-dimensional, and increasingly complicated to quantify. Reputational risks, IP loss, and competitive pushback endanger companies' sustenance over and above one-time monetary loss. Organizations are therefore investing more in both preventative and mitigative security frameworks. Growing awareness and spending are evident in the gradually maturing cybersecurity providers' landscape in India, with 60% of the product providers having emerged since 2015, as shown in the chart below. The pandemic slowed down this trajectory somewhat, however, end user enterprises have also increased spending in security services offered by their existing tech vendors or by cloud providers through as-a-service model.

Distribution of cybersecurity product companies in India by year of incorporation

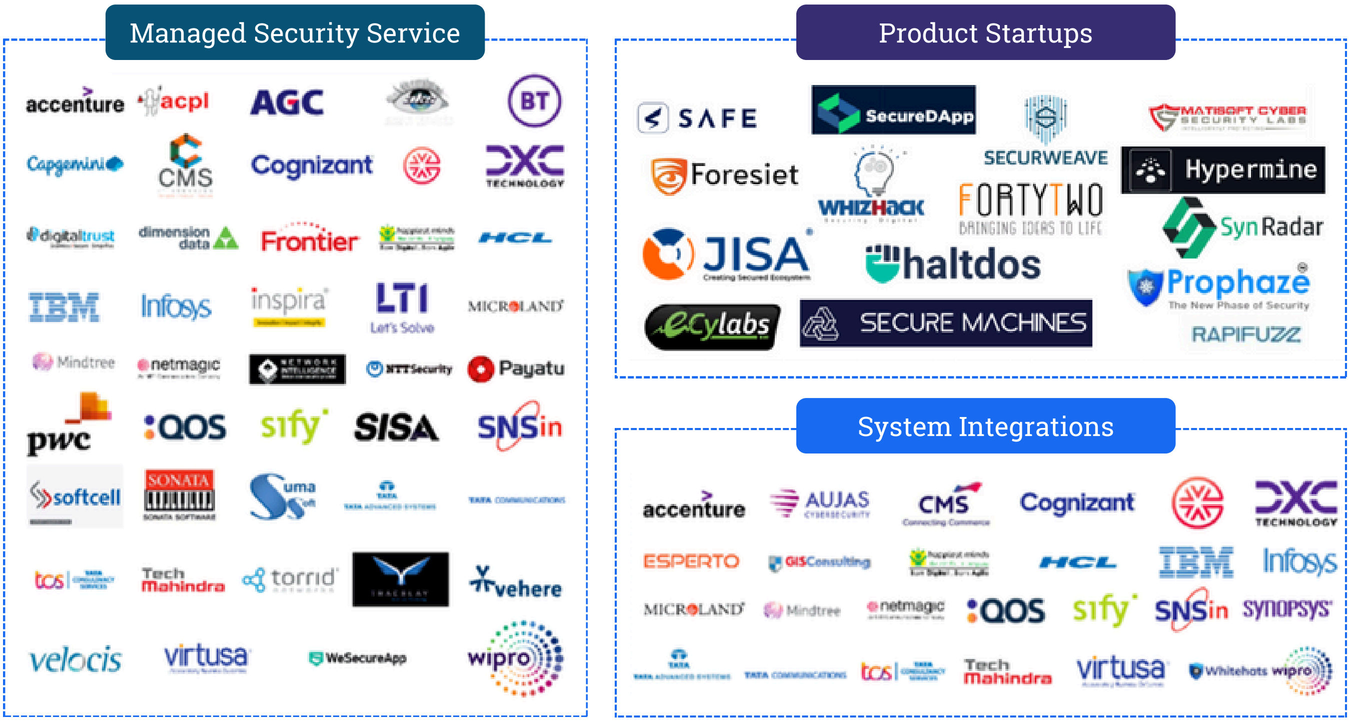


Total no. of companies - 315

Source: DSCI Survey

Evolving cybersecurity provider landscape in India

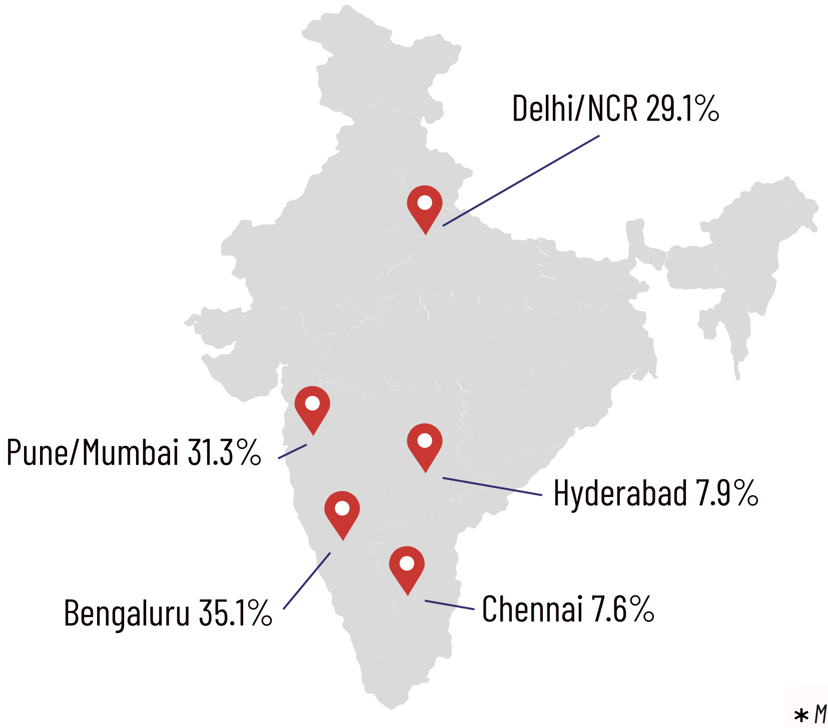
With greater demand, there has been a significant increase in the product startups in this space, along with expansion of existing managed security services and system integrator landscape, as shown below.



Illustrative list

Established and emerging locations

Where Cybersecurity Innovation Thrives in India



Total no. of companies - 315

Source: DSCI Survey

∗ *Map for representation purposes only. Map not drawn to scale.*

→ Bengaluru has highest number of cybersecurity companies with 35.1% of total presence, reinforcing its status as India's primary tech hub attracting numerous startups and established firms in cybersecurity sector.

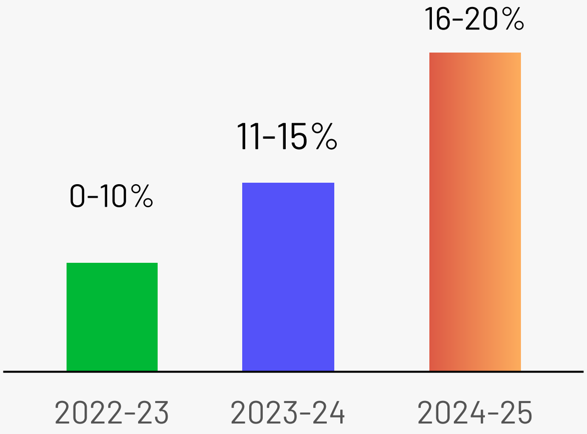
→ Delhi/NCR closely follows with 29.1%. The capital region's growth as a tech hub is evident due to increasing demand for cybersecurity solutions.

→ Combined presence of Pune and Mumbai is 31.3%. While Hyderabad and Chennai are emerging cities, growing as important centres for technology, indicating potential for future growth.

Global end-user enterprises are embracing Generative AI-led shifts in cybersecurity strategies

1. Cybersecurity Spending is Surging

Rate of growth of security as a % of IT Spending



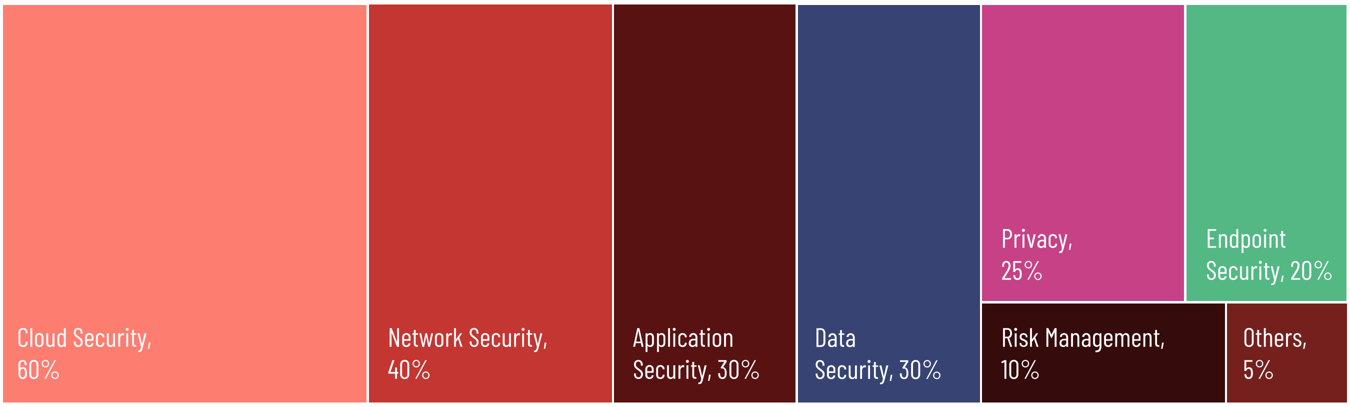
Source: Nasscom-NCoE (DSCI) State of Security User Organizations 2024 survey

Cybersecurity spending as a percentage of IT budgets has been increasing, more so since the pandemic. However, this rate of increase has accelerated with the emergence of Generative AI. Areas of investments have diversified beyond traditional threats like malware, phishing, and network intrusions, to more advanced security risks made possible by Generative AI.

The domestic security market expanded from USD 1.98 billion in 2019 to USD 6.06 billion in 2023, with the security products market growing from USD 1.03 billion to USD 3.76 billion during the same period. (DSCI)

The Nasscom-NCoE (DSCI) State of Security User Organizations 2024 survey of 104 global companies across 6 sectors, indicates a steady increase in security spending as a percentage of IT budget, with up to 5% increase in allocation each year. This trend validates growing recognition of cybersecurity as a critical digital transformation investment.

Cybersecurity Spending Priorities

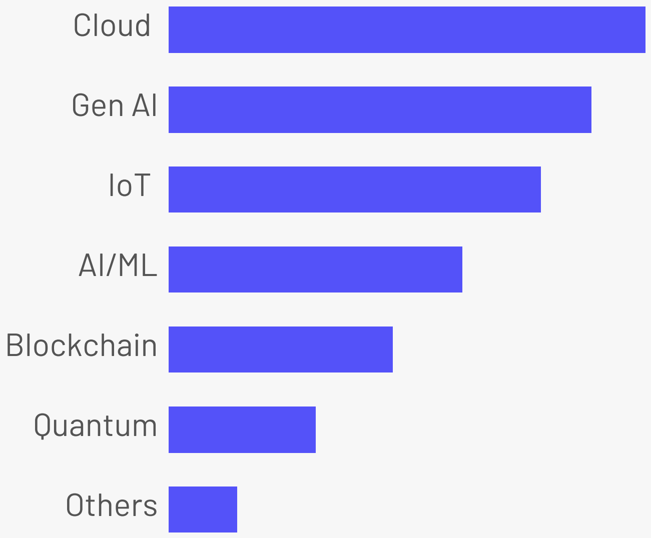


Source: Nasscom-NCoE (DSCI) State of Security User Organizations 2024 survey

Enterprises prioritized cloud security spending in 2024 YTD, followed by network, application, and data security. As the Generative AI opportunity brings laggard enterprises to adopt cloud-based/native data services and SaaS, spending on cloud security solutions is likely to accelerate through 2025 and beyond.

2. Generative AI is a top investment priority after cloud

Emerging Technologies Shaping Cybersecurity



Source: Nasscom-NCoE (DSCI) State of Security User Organizations 2024 survey

Cloud enables scalable, flexible security infrastructure.

Generative AI can automate real-time threat detection, prevention, and mitigation.

IoT-enabled device security is crucial for edge and endpoint computing.

Predictive AI/ML powers advanced threat intelligence, behavioral analysis, and anomaly detection

Blockchain can power data transparency and zero trust solutions.

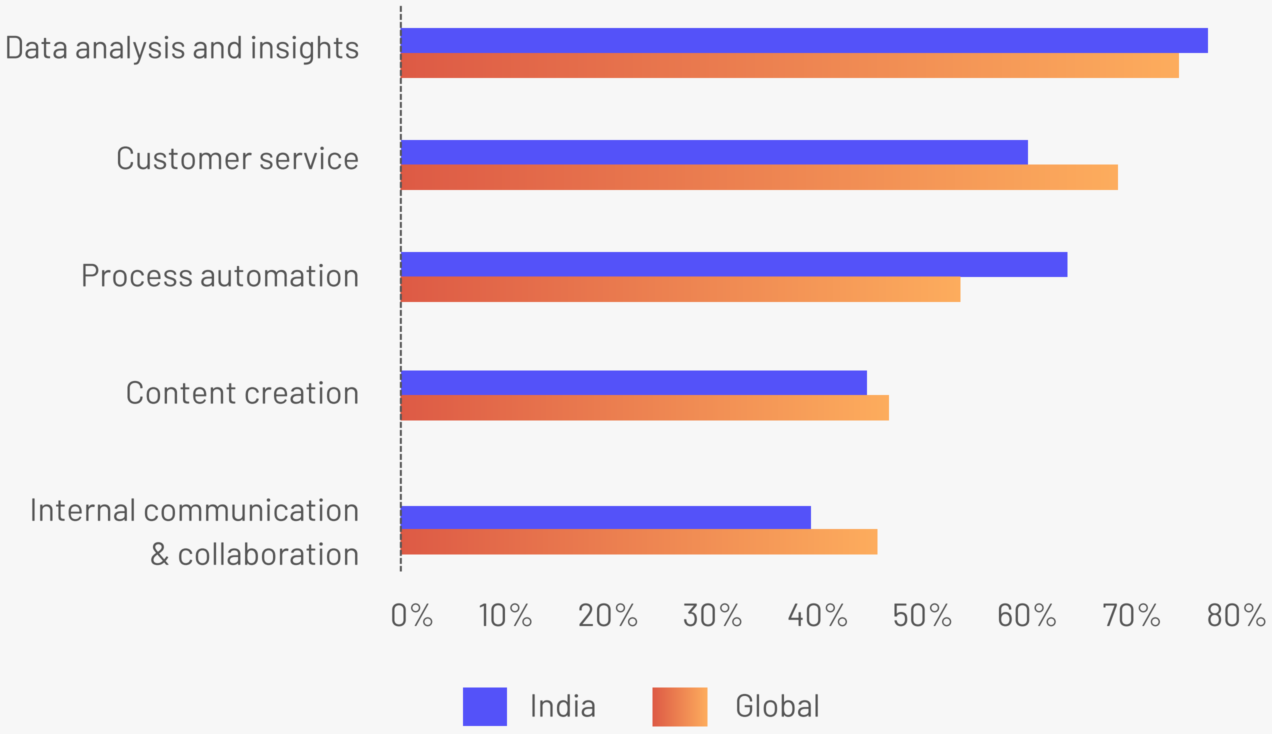
Quantum cryptography offers a revolutionary security paradigm.

The Nasscom-NCoE (DSCI) survey reveals enterprise preferences in integrating emerging technologies into their security solutions portfolios, with each tech uniquely impacting cybersecurity risks and resolution paradigms. Generative AI, of all, has risen rapidly in its influence on and for next-gen security solutions.

Data analysis and insights generation, automation of various cybersecurity processes, and customer services and support are the top three use cases for Generative AI in security, globally and in India.

Generative AI is being applied to extract valuable insights from data, enhance customer interactions, automate various tasks within organizations, and bolster security measures.

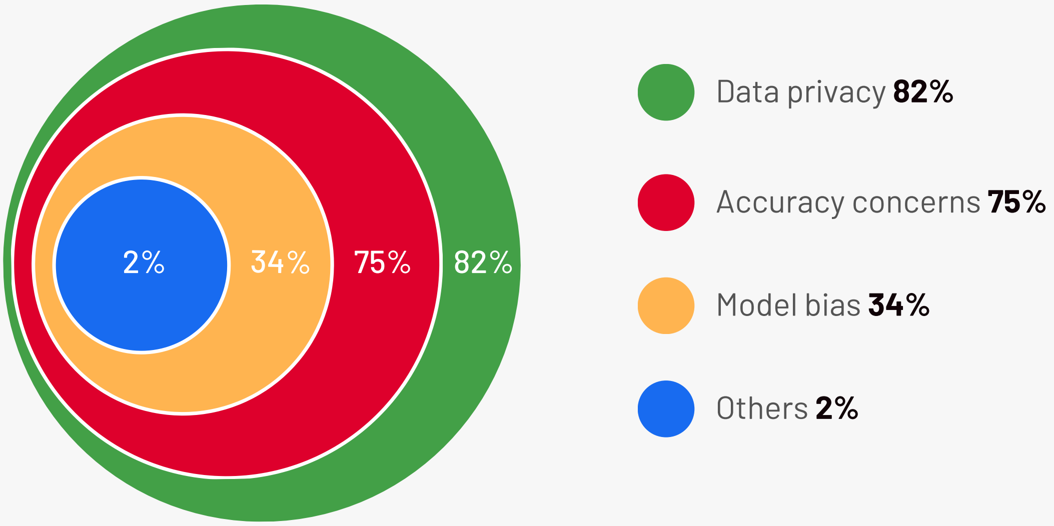
How organizations are using Generative AI



Source: Nasscom-NCoE (DSCI) State of Security User Organizations 2024 survey

3. Data privacy is a major concern with Generative AI

Risk associated with Generative AI



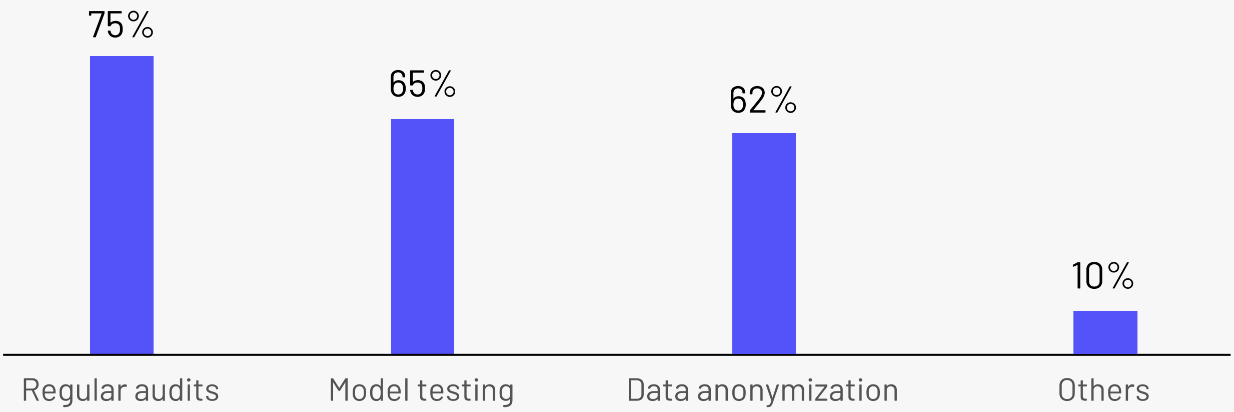
Source: Nasscom-NCoE (DSCI) State of Security User Organizations 2024 survey

Global enterprises continue to face challenges in data privacy, output accuracy, and model bias with the use of Generative AI, limiting integration with existing security solutions. Data privacy is the primary concern when using foundation or finetuned models without adequate security guardrails. Output accuracy compromises can be a major risk with undetected type I and type II errors in risk detection. Model bias can lead to incorrect classification of risks and non-risk factors, exposing security frameworks to potentially damaging attacks. Addressing these risks is crucial for ensuring responsible and secure development and deployment of generative AI technologies.

4. Organizations are primarily focusing on regular audits and model testing to mitigate Generative AI risks

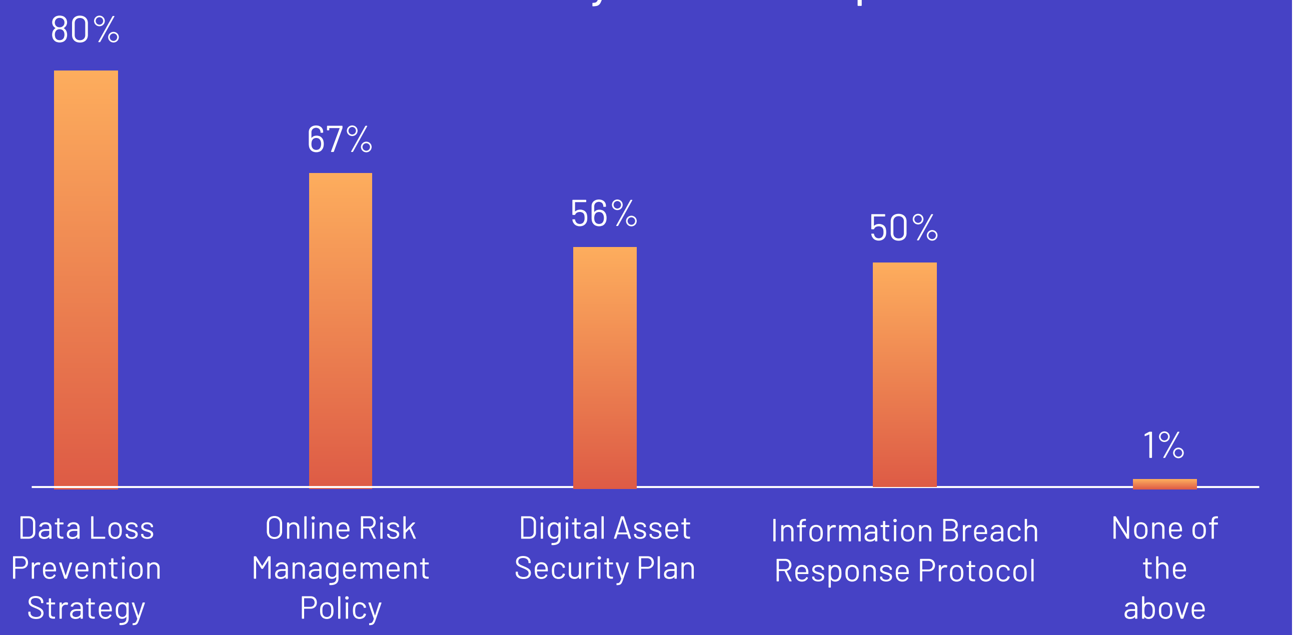
The survey also assessed the priority organizations assign to mitigating risks associated with Generative AI infused security solutions. The results reveal a strong focus on data anonymization (ranked 3), model testing (ranked 2), and regular audits (ranked 1). This indicates a keen awareness of the potential risks, particularly data privacy concerns.

How organizations are mitigating Generative AI risks



Source: Nasscom-NCoE (DSCI) State of Security User Organizations 2024 survey

Current security measures in place



Source: Nasscom-NCoE (DSCI) State of Security User Organizations 2024 survey

End-users are prioritizing data privacy and security by anonymizing sensitive information before inputting it into Generative AI security solutions. Also, they are likely cross-verifying AI-generated insights with other sources, underscoring a cautious approach to relying solely on AI-driven outcomes. Integrating Generative AI risk mitigation approaches with the currently established enterprise risk and security management systems will be crucial for a seamless enterprise risk and security framework.

5. Generative AI-enabled cybersecurity best practices

The survey reveals that organizations are focusing on multi-layered approaches to cybersecurity. Beginning with Generative AI awareness and basic literacy to cybersecurity awareness and shifts due to Generative AI, to the critical role of human-in-the-loop, building robust access controls, and role-based Generative AI usage, to more advanced security trainings in the Generative AI era, all aspects are being thought through by companies.

Top Three Followed Best Practices

1

Regular Security Awareness Training

Organizations are providing regular training on responsible & ethical use of Generative AI as well as role-based Generative AI literacy sessions and continuous updates with technology evolution.

2

Continuous Monitoring and Patching

They are also regularly monitoring Generative AI usage within the enterprise, randomized scanning of data ingestion at source, prompts, and generated output for accuracy, blas, data leaks across the Generative AI pipeline.

3

Robust Access Controls

Organizations are implementing strong password policies, requiring complex passwords and frequent changes. Additionally, they are introducing role-based access to enterprise data accessible through Generative AI interfaces, over and above or integrated with existing access control measures

Source: Nasscom-NCoE (DSCI) State of Security User Organizations 2024 survey

Interestingly, the survey suggests that organizations in the healthcare industry are particularly cautious, with a higher adoption of advanced security measures, likely driven by stringent compliance requirements and the sensitive nature of patient data. With Generative AI usage growing, companies across sectors must look at sensitive data and differential usage policies of such data sources through Generative AI assistants or productivity tools on-premises or through remote work locations.

Security technology providers are innovating to incorporate Generative AI into their solutions portfolio

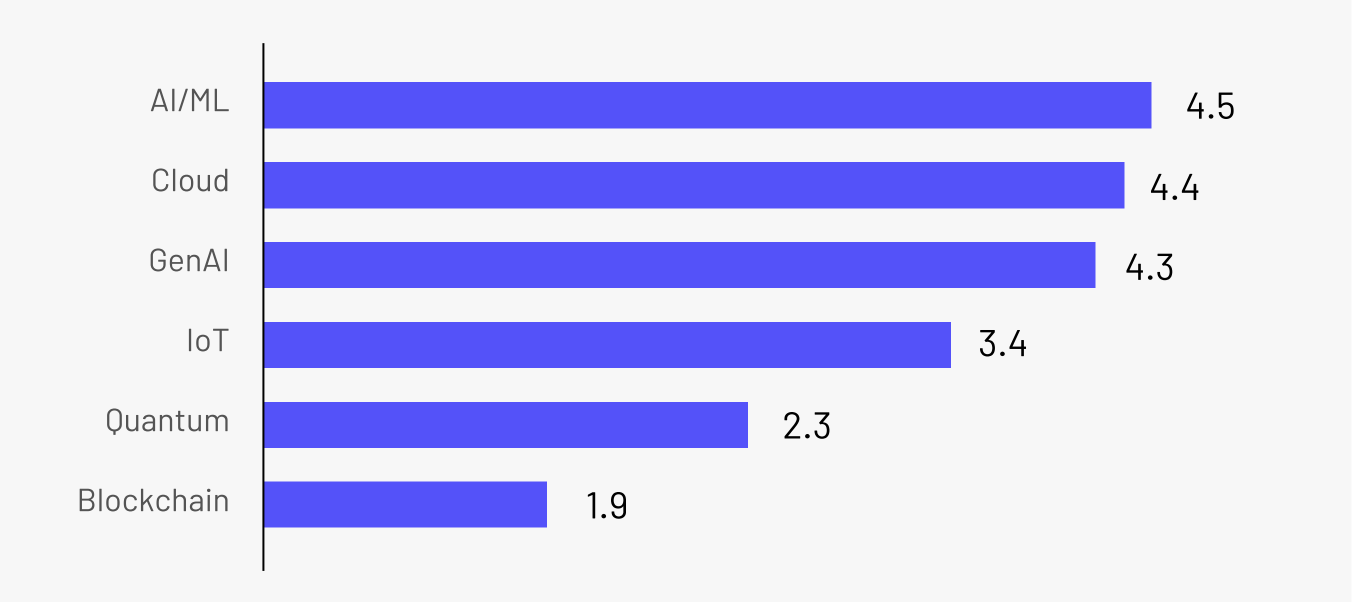
1. AI/ML and cloud are transforming security service offerings

AI/ML and cloud continue to be the preeminent technology priorities of cybersecurity providers in 2024. Leveraging AI/ML and cloud technology, cybersecurity providers can create new market opportunities and value propositions, provide subscription-based security, deliver scalable offerings, and reduce operational costs.

AI/ML applications in security

- Advanced threat detection through data-driven pattern analysis and anomaly detection using data from diverse sources.
- Automated threat response with predefined actions like IP blocking and system isolation.
- Anomaly detection through behavioral analysis by comparing user activity to established baselines.
- Potential threat and vulnerability detection by analyzing historical data patterns.

Security solutions tech priorities in 2024 (5 highest, 1 lowest)



Source: Nasscom-NCoE (DSCI) State of Security Service Providers 2024 survey

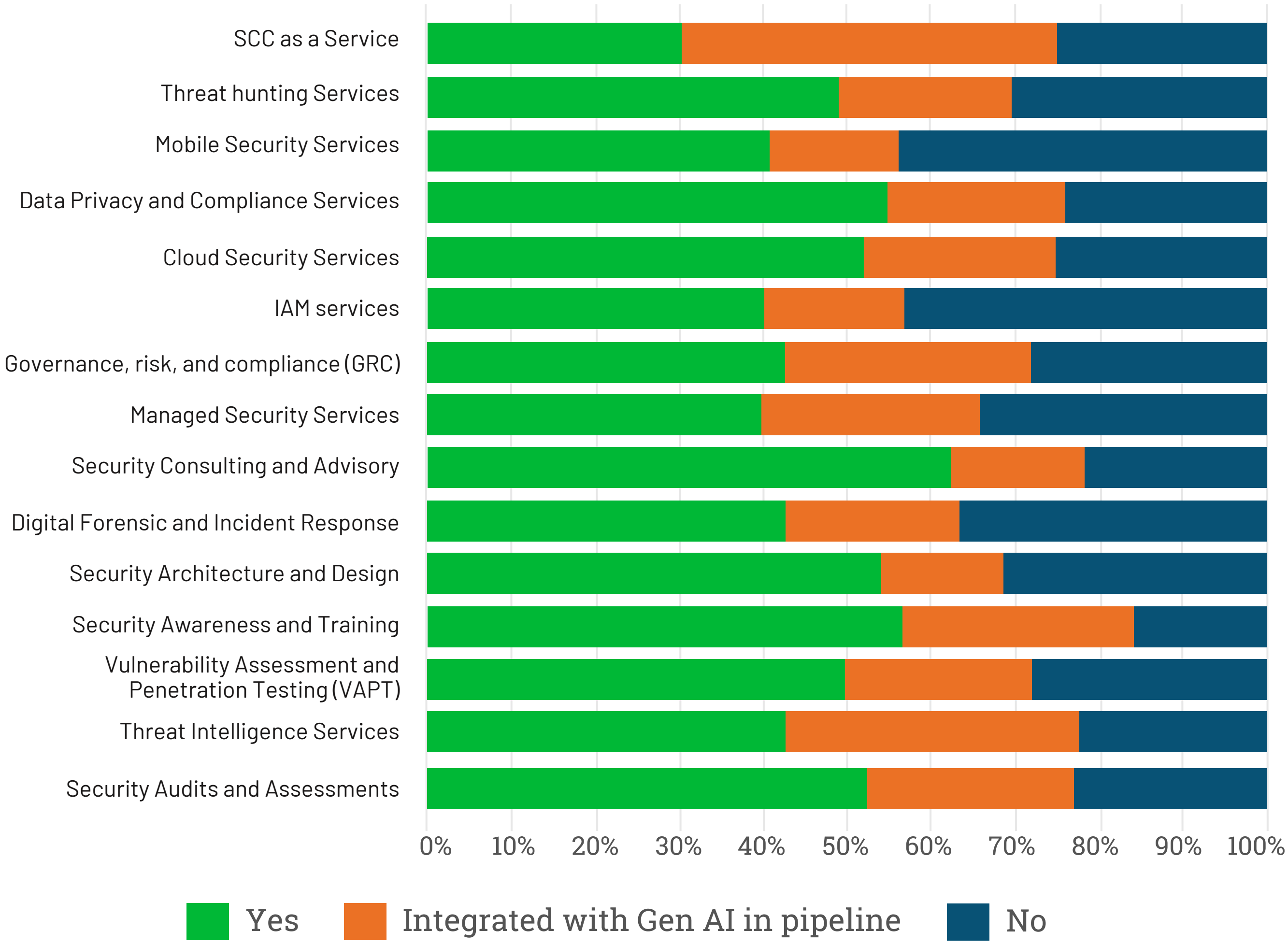
As Generative AI adoption grows, several security processes, such as data collection, aggregation, and analysis, behavior or sentiment pattern segmentation for anomaly detection, etc. will likely be automated, thereby enabling security professionals to focus on advanced threat assessments needing human intuition and expertise.

Case Spotlights

TCS Partners with Google Cloud, leveraging Google Security Operations to offer AI-powered MDR and Secure Cloud Foundation solutions. It will use AI for investigation and response workflows.

Wipro launched a new AI innovation hub, AI360, and its Generative AI lab, Lab45, and committed to investing USD 1 billion over three years to enhance its AI technology. This investment aims to integrate AI into all Wipro's products and internal operations, including cybersecurity.

2. Generative AI is a promising tech and within a span of 2 years, nearly 35-40% security providers have already integrated it into their offerings

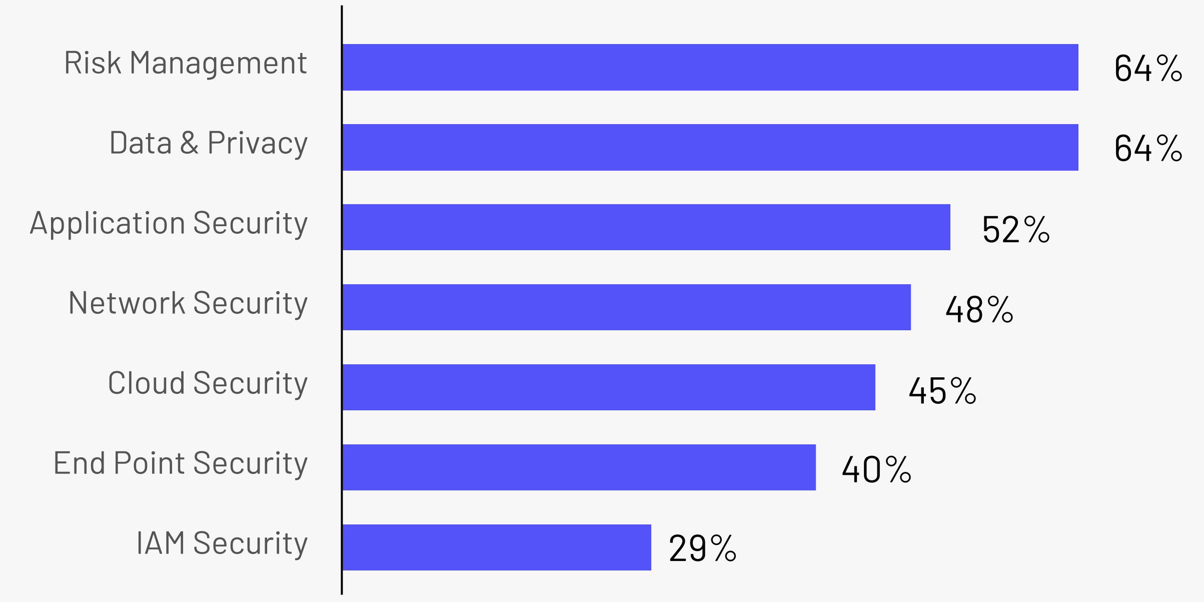


Source: Nasscom-NCoE (DSCI) State of Security Service Providers 2024 survey

Generative AI offers great opportunities in cybersecurity, offering the ability to automate tasks such as triaging alerts and incident responses, and managing data loss prevention (DLP) alerts. However, the adoption of Generative AI-enabled cybersecurity offerings is still in its early stages, with limited organizations utilizing them.

Key services where organizations are leveraging or plan to leverage Generative AI are threat intelligence, security audits and assessments, and GRC for automated threat detection, incident response, compliance check, vulnerability scanning and risk management.

Promising opportunities for leveraging Generative AI in security services

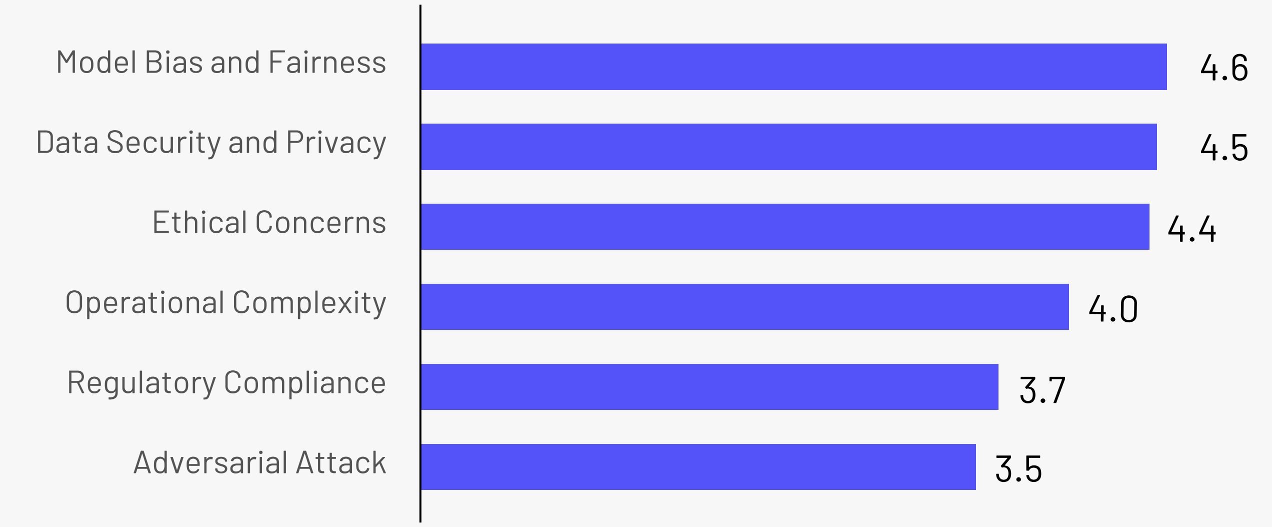


Source: Nasscom-NCoE (DSCI) State of Security Service Providers 2024 survey

BFSI and Manufacturing sectors exhibit the highest adoption rates among large enterprises, followed by healthcare and retail. More hi-tech and telecom SMEs are embracing Generative AI-enabled security services.

3. Model fairness and bias are key challenges for service providers using Generative AI

Challenges to Generative AI integration in security solutions



Source: Nasscom-NCoE (DSCI) State of Security Service Providers 2024 survey

Top three key challenges in integrating Generative AI into security solutions

Data Quality and Bias

Generative AI models are only as good as the data they are trained on. Biased or inaccurate training data can lead to biased outputs, which can have serious consequences in security applications.

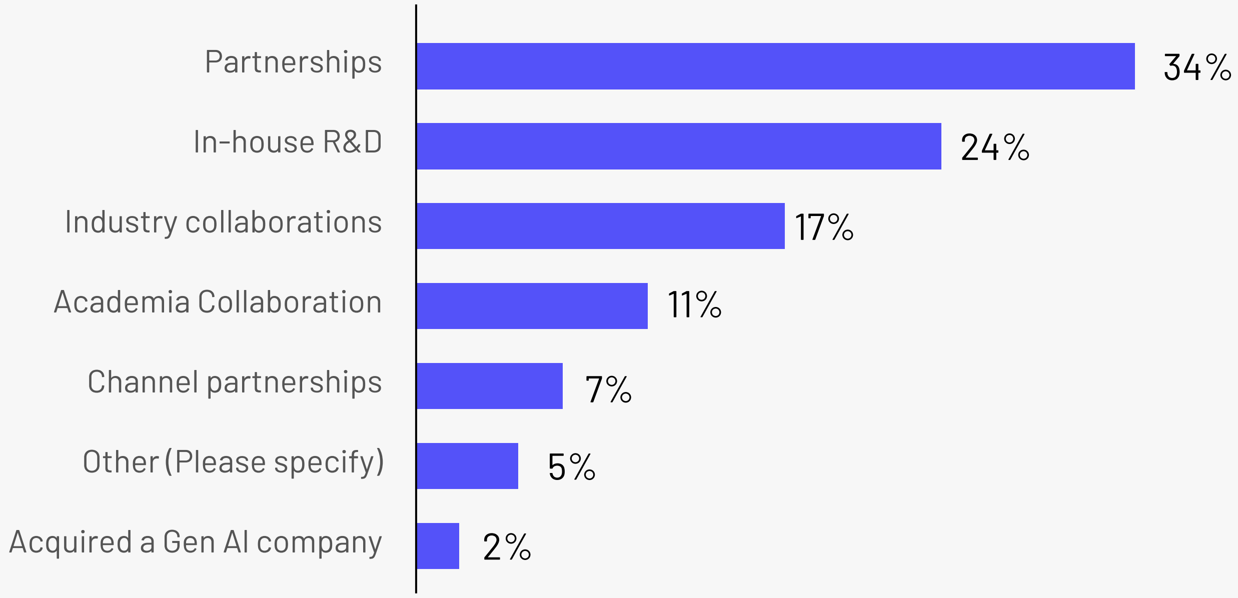
Model Interpretability and Explainability

It can be difficult to understand how Generative AI models arrive at their decisions, making it challenging to trust their outputs and identify potential errors.

Security Risks

Large language models are trained on massive datasets that may contain sensitive information. This makes them potential targets for attacks that could compromise the model or the data it was trained on.

Generative AI capability development strategies preferred by security providers



Source: Nasscom-NCoE (DSCI) State of Security Service Providers 2024 survey

Partnerships and industry collaborations are a quick way to start the Generative AI journey with combined resources and knowledge in data sharing, compute optimization, and expertise access enabling creation of robust and innovative solutions.

In-house Generative AI development, on the other hand, takes longer but enables firms to build custom solutions, ensure smooth integration with existing systems, and establish early-mover advantages in cost-value impact.

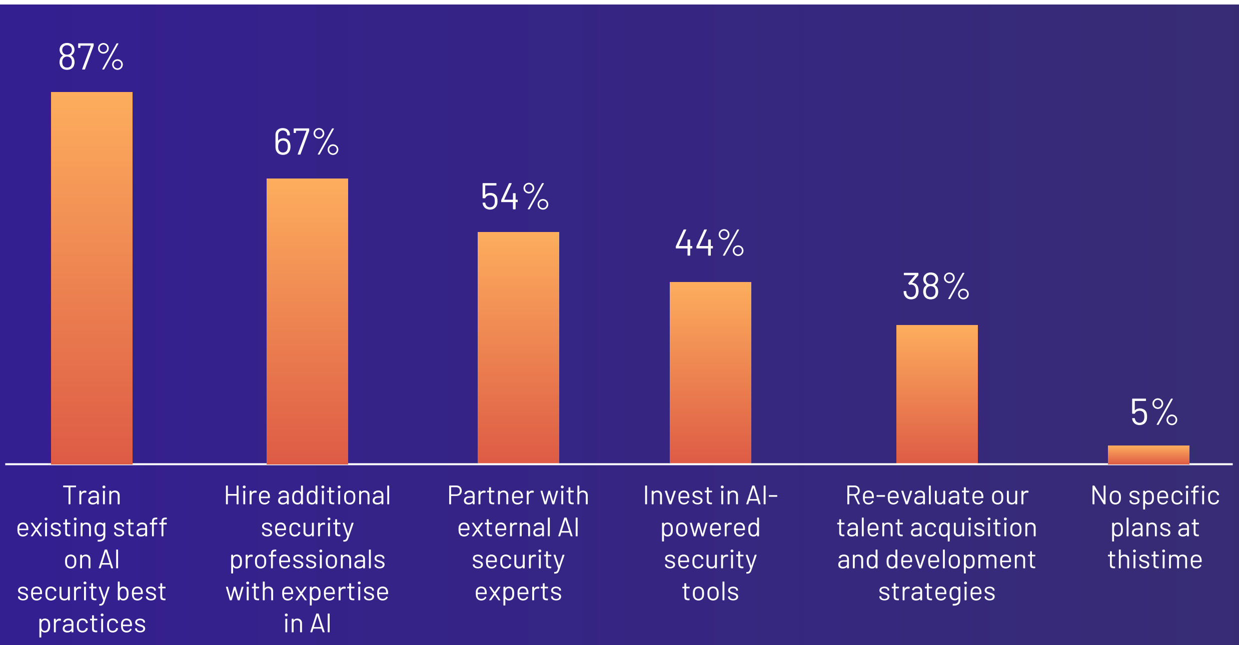
While in early stages, co-creation with clients, or R&D partnerships with academia can unlock the next level of innovation and IP creation for security providers over time.

Case Spotlights

NTT Data is exploring and applying generative AI to improve network security and enhance cybersecurity training, through network traffic and user behaviour anomaly detection, and malware samples generation.

CrowdStrike and NVIDIA collaborated to enhance the CrowdStrike Falcon XDR platform by integrating NVIDIA's AI capabilities, including new Generative AI microservices, NVIDIA NIM, to provide customers with better visibility into potential threats.

Skills and talent development

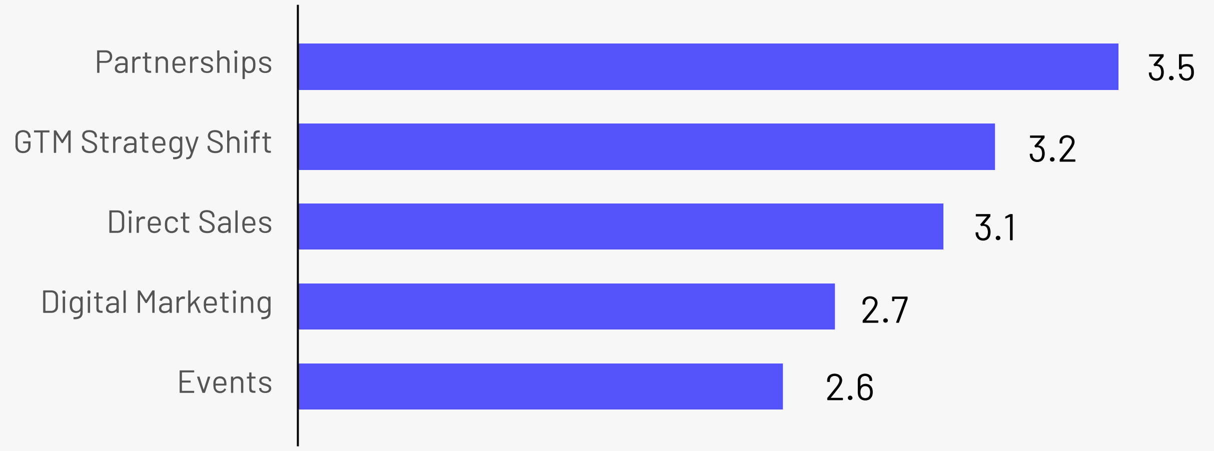


Source: Nasscom-NCoE (DSCI) State of Security Service Providers 2024 survey

Security organizations are focusing on training of existing non-AI tech workforce and external specialist hiring to prepare their workforce for the impending AI/Generative AI-led cybersecurity transformation. According to ISC2, 88% of its members believe AI is influencing their current jobs, primarily positively through increased efficiency, though concerns about job redundancy persist.

5. Security service providers are rethinking go-to-market (GTM) in the age of Generative AI

Shifting focus on GTM strategies



Source: Nasscom-NCoE (DSCI) State of Security Service Providers 2024 survey

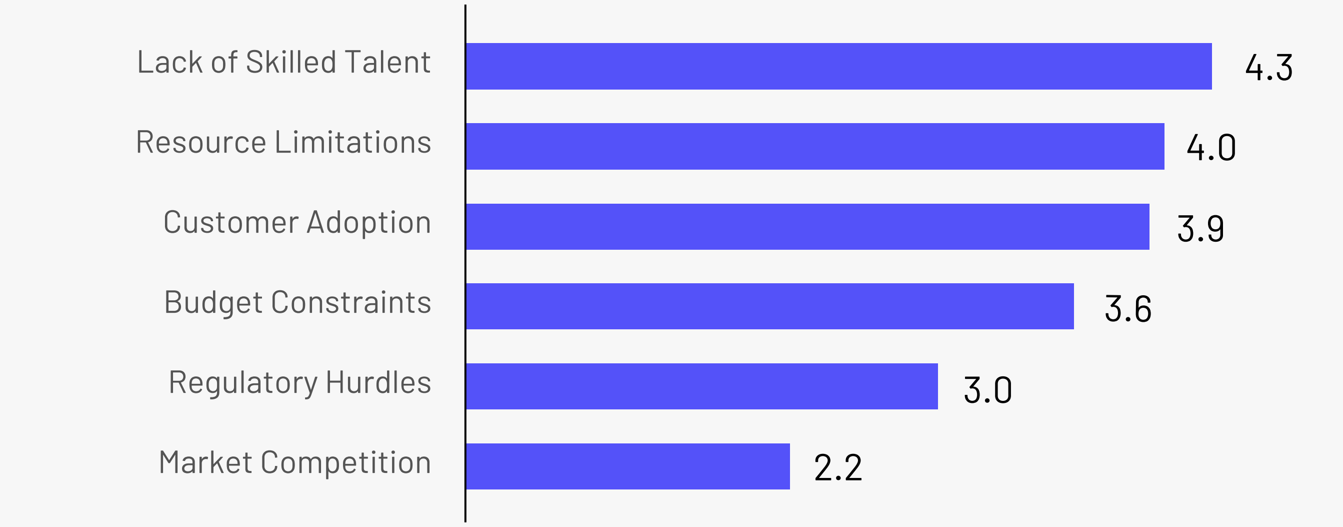
Partnerships with technology services or system integrator companies, cloud providers, and even startups offering unique solutions is the preferred GTM strategy for security providers to navigate the Generative AI transition. Partnerships strategy has seen a significant increase in importance, likely due to the complex nature of Generative AI solutions.

Case Spotlights

Tata Communications announced partnership with Palo Alto Networks in October of 2024 to provide advanced cybersecurity solutions worldwide, including security consulting, network and cloud security, and threat detection and response.

In April 2024, Quick Heal's enterprise arm, Seqrite, appointed M. Tech Solutions as value-added distributor to expand its presence in India with focus on Enterprise and Government segments.

6. Challenges in offering Generative AI-powered security services



Source: Nasscom-NCoE (DSCI) State of Security Service Providers 2024 survey

Lack of talent skilled in cybersecurity and AI/Generative AI, and concerns about reliability, security, and privacy, are hindering Generative AI adoption across organizations irrespective of size or sector.

Some key challenges of integrating Generative AI into security solutions

Technical

Integrating Generative AI models into existing solutions requires significant computational resources and complex modeling techniques. Optimizing models for performance without compromising capabilities is a significant hurdle.

Data

Obtaining sufficient and high-quality security incident data for training Generative AI models is difficult due to privacy concerns and data sensitivity.

Operational

Real-time threat detection and response using Generative AI can be hindered by the computational demands of data processing. Integrating Generative AI across diverse cybersecurity domains and platforms requires seamless compatibility. Also, ensuring compliance with local privacy regulations while protecting user data is a complex task for organizations.

Recommended Generative AI-Enabled Cybersecurity Framework for End-User Enterprises

By adopting a comprehensive cybersecurity framework, organizations can proactively protect their valuable assets, maintain business continuity, and build trust with their stakeholders.

01

Monitor

behaviors, activities, usage, access, evolutions, interactions and conversations, dependencies, exchanges, updates, evolutions, external developments, and actions.

02

Generate

scenarios that mimic varying levels of vulnerabilities across security layers, personas, and access controls to build response strategies across multiple dimensions.

03

Develop Threat & Risk Cognition

by building pattern modeling capabilities, deriving impact-worthy insights from pattern monitoring, building contextualized decision-enabling visualizations for various stakeholders, and utilizing models to further quantify the impact of various response scenarios (including scenario of not adopting Generative AI-based security posture) to facilitate future actions.

04

Protect

through integrity verification and validation, continual validation, context isolation, laying down dynamic safety boundaries, linage tracking, multi-tiered access control, automated enforcements, input and output controls and filtering, and privacy enhancing methods.

05

Seek Conformance

to boundaries, output limitations, security protocols, accuracy range, performance metrics, consistency expectations, and transparency & explainability levels.

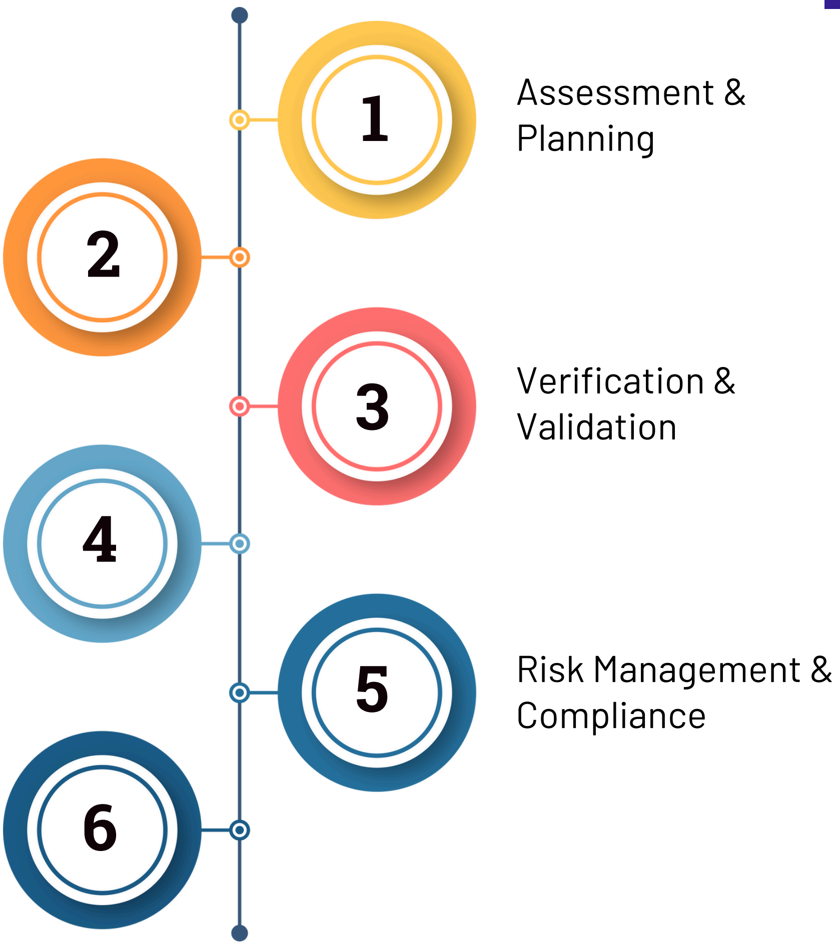
06

Adapt

detection, protection, and remediations for new scenarios, boundary conditions, edge cases, advancements in threats, evolution of underlying models, operating environments, business contexts, operating scenarios, behavior changes, and alignment expectations.

Source: Nasscom, NCoE (DSCI)

Recommended Security Playbook for Service Providers


1
Assessment & Planning
2
Architecture Design & Implementation
3
Verification & Validation
4
Monitoring & Detection
5
Risk Management & Compliance
6
Incident Response & Recovery

Source: Tech Mahindra, Nasscom, NCoE (DSCI)

1. Assessment and Planning

Evaluate the client's current security controls and processes.

Benchmark the planned solution, the current security state, and the organization's maturity level against industry standards to identify gaps.

Time-box the assessment to a decided timeline. Also, assess the feasibility of integrating emerging technologies, if any.

2. Architecture Design & Implementation

- Develop customized security solutions that align with the client's specific needs and risk profile.
- Create detailed design specifications for the security architecture, including:
  - **High-level design:** Outline the overall security framework and components.
  - **Low-level design:** Specify the technical details of individual security controls and systems.
- Develop a comprehensive implementation plan that outlines the steps, resources, and timelines required to deploy the security solutions.

3. Verification & Validation

Comprehensive Testing

Security verification and validation services involve a range of testing methodologies, including penetration testing, vulnerability scanning, and security code reviews.

Proactive Risk Mitigation

By rigorously testing clients' systems, service providers can identify and address potential vulnerabilities before they are exploited, improving the overall security posture of the organization.

Enhanced Client Confidence

The ability to identify and mitigate risks strengthens client confidence in the effectiveness of their security controls.

4. Monitoring and Detection

Proactive Threat Management

Managed Security Services (MSS) providers offer real-time threat monitoring, incident response, security analytics, and vulnerability management to proactively detect and address security risks.

Rapid Incident Response

By leveraging advanced tools and experienced professionals, MSS providers can quickly detect, analyze, and respond to security incidents, minimizing damage and reducing recovery time.

Enhanced Security Posture

The proactive nature of MSS services helps organizations maintain a strong security posture and mitigate potential threats.

5. Risk Management and Compliance Measures

Risk Identification and Assessment

Conducting regular assessments to identify potential threats to IT systems and data, including vulnerabilities, malware, and unauthorized access.

Risk Mitigation and Elimination

Develop and implement strategies to address identified risks, such as security controls, incident response planning and employee training.

Compliance Adherence

Ensure compliance with relevant industry regulations and standards, such as- data privacy laws, security frameworks, and industry-specific standards.

6. Monitoring Incident Response & Recovery and Detection

Prepare for Incident Response

Create a detailed plan outlining procedures to follow in case of a security breach. Educate employees on how to recognize and report potential security incidents. Create standardized guidelines for handling common types of security incidents.

Implement Data Backup

Regularly back up client's important data and store it in a secure location. Implement measures to protect backup data from unauthorized access or corruption.

Outlook & Recommendations

Currently, the adoption of generative AI in cybersecurity is relatively low, primarily due to concerns about trust, complexity, and integration with existing systems. While there's potential for enhanced threat detection and automated response, widespread adoption could lead to unintended consequences like more sophisticated attacks and new vulnerabilities in AI-powered systems. Thus, cautious integration with robust safeguards is crucial. The future of cybersecurity demands a multifaceted approach. By adopting the following recommendations, different stakeholders can navigate the evolving threat landscape:

Security Service Providers

1. Invest in AI Expertise

Hire or train AI experts to develop and maintain robust Generative AI solutions.

2. Prioritize Data Security

Implement stringent data protection measures to safeguard sensitive information used for training and model development.

Security User Organizations

1. Evaluate AI Solutions Critically

Conduct thorough risk assessments before adopting Generative AI tools to identify potential vulnerabilities.

2. Foster AI Literacy

Educate employees about the potential benefits and risks of Generative AI to promote informed decision-making.

Startups

1. Focus on Niche Applications

Develop specialized Generative AI solutions for specific security challenges to gain a competitive edge.

2. Collaborate with Established Players

Partner with security service providers or user organizations to validate and refine AI models.

Government

1. Establish Clear AI Regulations

Develop comprehensive regulations to govern the development and deployment of Generative AI in cybersecurity, balancing innovation with security.

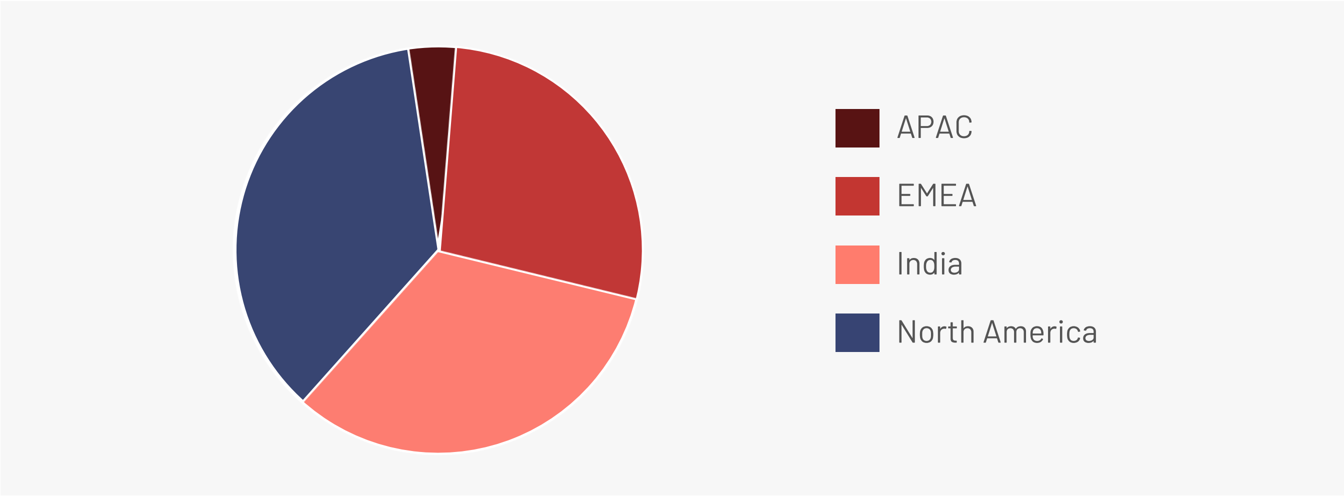
2. Promote AI Research and Development

Invest in research to advance AI techniques and foster a thriving AI ecosystem.

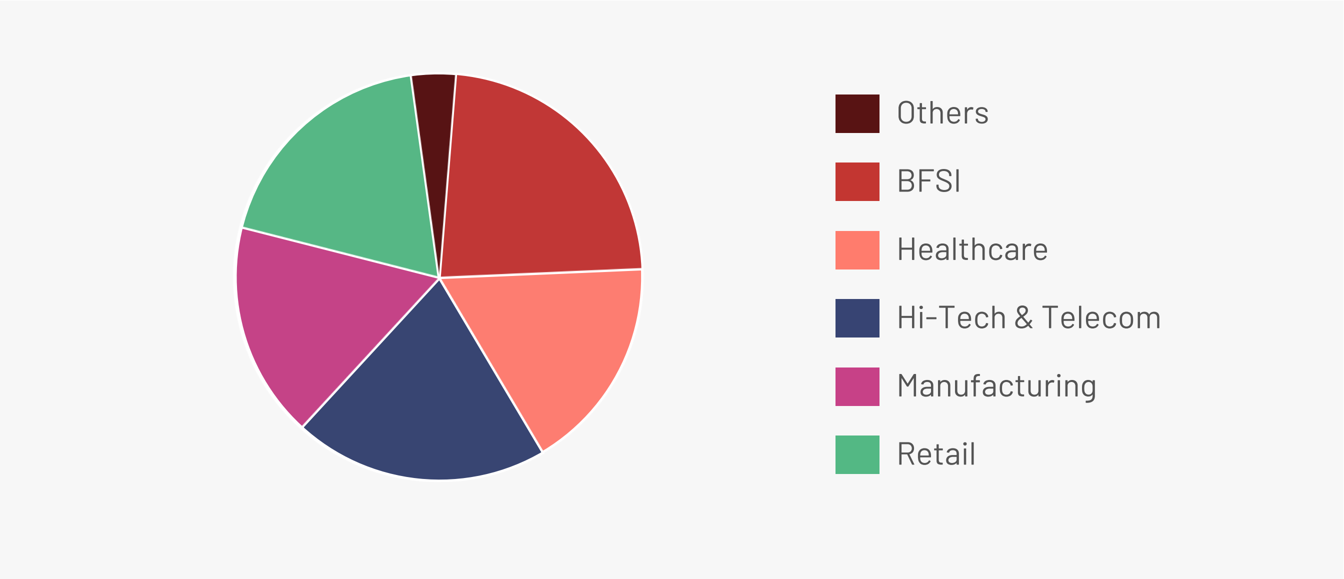
Appendix

Nasscom-NCoE (DSCI) State of Security User Organizations 2024 survey (number = 104 organisations)

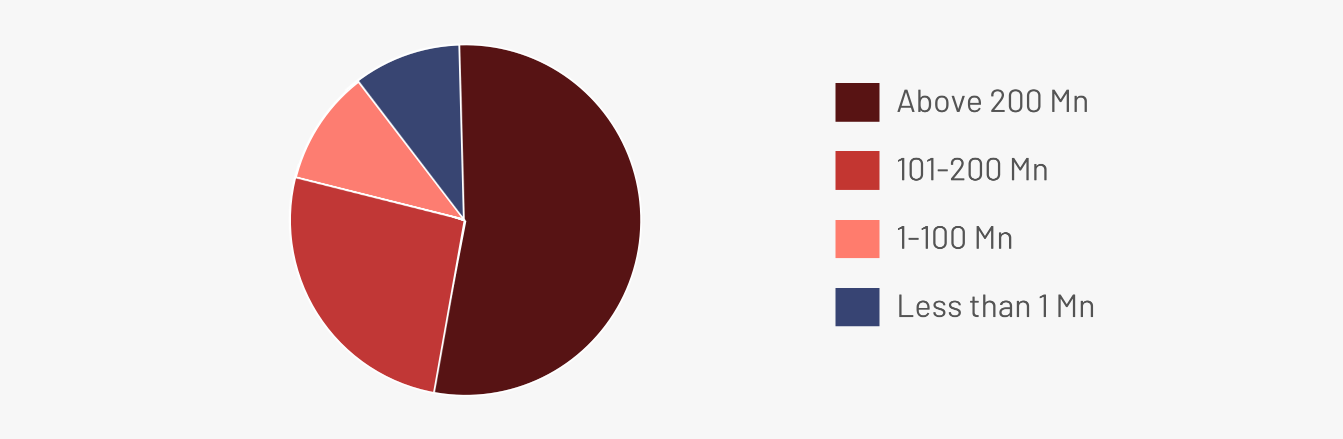
- 91% of the respondents were Heads of IT, CISO, CSO, Global or regional CIOs, CTOs, Head of IT, Head of Digital Transformation, Director/VP levels in IT
- Survey participants location



- Survey participant organization vertical

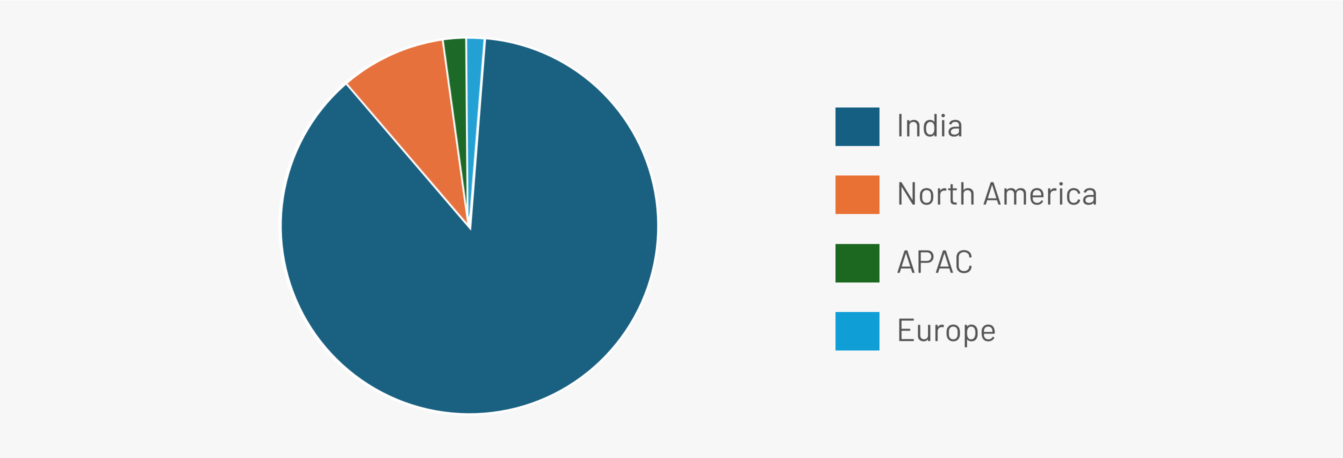


Survey participant organisation size

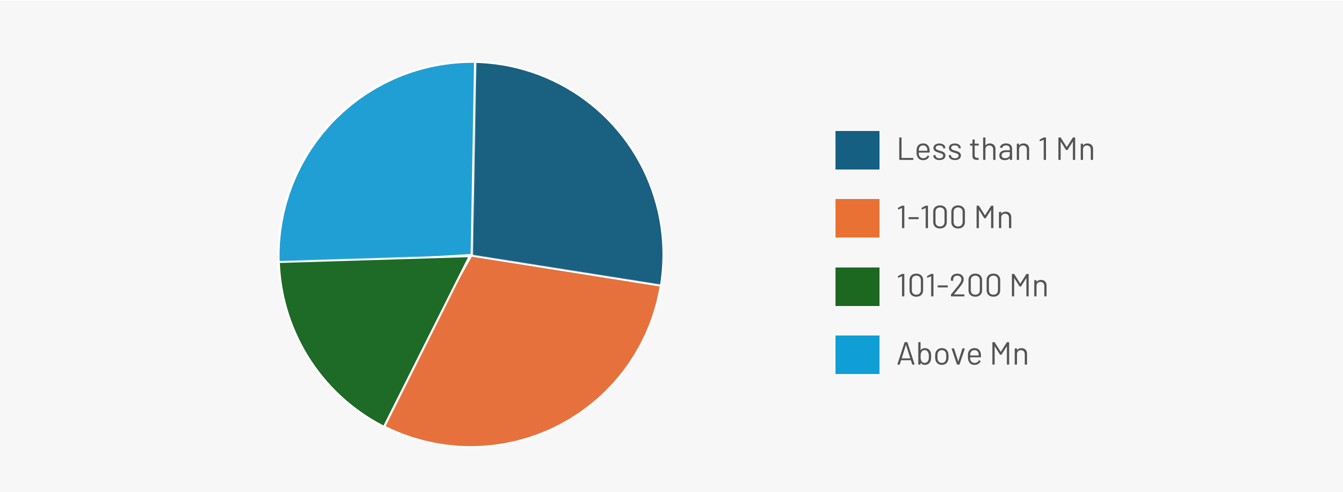


Nasscom-NCoE (DSCI) State of Security Service Providers 2024 survey (number = 104 organisations)

Survey participant organization location



Survey participant organization size



Case Studies

1. Company Name: RavenMail

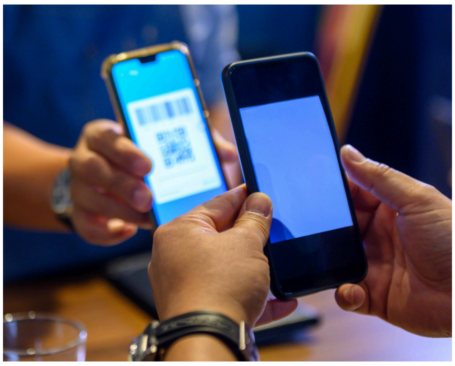
Solution

ContextAI is a LLM Detection engine for highly targeted AI-Phishing.

Approach

RavenMail security adds LLM-based detectors on top of existing mail security thereby able to detect threats using organization, business and threat context. The solution also uses Multi-modal capability of understanding images, text, and overlaying with business and detection logic.

2. Industry: Digital Payments



Problem

The client needed to safeguard sensitive data, secure hybrid workloads, detect threats proactively, and meet CERT-In and PCI DSS compliance.

Solution

Deployed its platform in two phases—covering on-premise systems and AWS cloud—providing 24/7 monitoring with 990 MITRE ATT&CK-aligned detection use cases.

Outcome

- ✓ 72% faster threat detection and 64% quicker response times.
- ✓ Improved accuracy in alerts and reduced false positives.
- ✓ Achieved compliance and enhanced overall security posture.

3. Company Name: WhizHack Technologies Pvt. Ltd.

Solution

We have developed ZeroHack Query (ZQ) which is part of the ZeroHack Platform. This is a Whizhack Generative AI (GenAI) solution that enhances Cybersecurity operations through advanced SIEM integration, processing large number of events per second with low latency.

Approach

The system employs Natural Language Understanding (NLU) for log parsing and Computer Vision algorithms for analyzing security-related visual data, while maintaining connections with 20+ Threat Intelligence Platforms (TIPs) via STIX/TAXII [Trusted Automated exchange of Intelligence Information] protocols. This Large Language Model (LLM) solution generates context-aware remediation playbooks mapped to the MITRE ATT&CK framework, integrating with log platforms for automated response.

Supporting JSON log formats, the system provides comprehensive threat visibility and predictive detection, achieving above 90% up-time for consistent security monitoring and rapid incident response.

4. Company Name: Fortytwo42 Technology Innovations Pvt Ltd

Solution

Fortytwo Labs successfully deployed its π-Control Platform, leveraging proprietary Post-Quantum Cryptography, to enable secure communication for a prominent user agency.

Approach

This solution underwent stringent evaluation by DRDO Lab and IIT Chennai, culminating in the prestigious SIDM Defence Champion Award 2023, presented by the Honorable Defense Minister. Users have expressed profound satisfaction, highlighting the solution's exceptional performance, reliability, and security, exceeding their expectations.

Effective messaging solutions require robust security fundamentals: identity and authentication, confidentiality, integrity, non-repudiation, and privacy. Fortytwo Labs addressed this challenge with its innovative Pi-Control platform, leveraging proprietary Post-Quantum Cryptography (PQC) algorithms.

5. Company Name: Quick Heal Technologies

Quick Heal Technologies, a global leader in cybersecurity, offering solutions under the Seqrite brand for organizations of all sizes.

Challenges

- Overwhelming alert volumes causing analyst fatigue.
- Prolonged triage and incident response times.
- Increased security risks due to unaddressed alerts and backlogs.

Solution

Quick Heal integrated Generative AI into its XDR platform to streamline operations.
The AI assisted in: Summarizing incidents by extracting critical details like threat vectors.
Providing interactive, context-specific answers to analysts' queries in real-time.

Outcome

✓ 70% reduction in incident resolution time.

✓ Enhanced threat-hunting capabilities with better IOC analysis.

✓ Significant backlog reduction, improving alert-handling efficiency.

✓ Boosted analyst productivity by automating repetitive tasks.

This strategic adoption improved proactive threat management, enabling Quick Heal to adapt effectively to evolving cybersecurity challenges.

6. Company Name: Chipspirit Technologies Pvt Ltd

Solution

Hardware based platform for with no software or OS.

Approach

By removing the software and OS components, malwares or viruses cannot be used as they will need a host that is the software or OS and remote attacks are completely eliminated.

7. Company Name: Astranova Labs Pvt Ltd

ASTRANOVA LABS

Solution

Leveraging data integrated with our identity governance and administration solution, we intend to give insights with clear prescriptive actionable for organisations to act upon.

Approach

The solution integrates multiple attribute data pertaining to digital identity and their access (including Non-Human identities) and leverages AI for sharing recommendations customized to an organisation as per training dataset provided.

8. Company Name: tinycrows private limited

Solution

We found that resolving security gaps was time-consuming because developers lacked the necessary resources to efficiently address identified vulnerabilities.

Approach

To streamline this process, we leveraged generative AI to create a customized prompt, providing developers with clear, illustrated explanations of each vulnerability along with straightforward, language-specific guidance on 'How to Fix a Vulnerability' tailored to the code's context.

This exercise highlighted how generative AI can significantly enhance the efficiency of security champion programs.

9. Case Study Summary: Tech Mahindra's Vulnerability Management Solution

Industry

Railway Manufacturing (OEM)

Client

A global railways OEM

Challenges

- Daily vulnerability scanning for hybrid environments (on-premises and cloud).
- Root cause analysis for identified vulnerabilities.
- Enhancing overall vulnerability management and reporting processes.

Solution

Tech Mahindra assessed the client's vulnerability management process against the NIST Cybersecurity Framework (CSF), improved reporting KPIs, and automated workflows using Generative AI to:

- Conduct periodic server scans.
- Generate daily vulnerability dashboards showing trends.
- Cross-reference vulnerabilities from the CVE list and NVD for actionable insights.
- Document SOPs for threat, vulnerability, and patch management.

Outcomes

✓ 70% reduction in incident resolution time.

✓ Enhanced visibility into security trends with AI-driven dashboards.

✓ Improved process efficiency through fine-tuned KPIs and automated reporting.

This solution streamlined the client's vulnerability management, enabling quicker responses and more efficient processes aligned with industry standards.

10. E-commerce Company

Used Infoblox threat intelligence and blocked suspicious domains, stopping attacks instantly.

Problem

Detected data exfiltration attempts after seven queries but prevented breaches using advanced analytics.

Outcome

Infoblox's AI-driven DNS solutions enhance proactive threat mitigation, detect long-duration threats, and improve security response. By leveraging machine learning and real-time intelligence, organizations safeguard their operations effectively in an evolving threat landscape. DNS's scalability makes it a cornerstone for modern cybersecurity strategies.

11. Company Name: Athenian Tech

Solution

Athenian Tech provides cutting-edge cybersecurity solutions through its proprietary platforms: Digital Risk Monitoring (DRM) for continuous threat detection and compliance management, Prime for advanced threat intelligence, and Thunderbolt for executive protection monitoring.

Approach

These solutions utilize AI and machine learning to deliver real-time monitoring, predictive analytics, and comprehensive digital risk mitigation, ensuring robust and proactive defense against evolving threats.

In an era dominated by Gen AI, Athenian Tech's innovative solutions provide organizations with a forward-thinking approach to cybersecurity, emphasizing proactive threat management and continuous adaptation to evolving digital risks.

12. Company Name: Sequretek

Solution

Sequretek utilizes Generative AI and AI technologies across several key areas to tackle these challenges effectively, including autonomous parsing, attack path analysis, and proactive threat hunting.

Approach

The system employs AI-powered Response Automation Playbooks, AI-triggered SOAR, and a proactive approach to vulnerability-based attack surface management.

Sequretek's holistic approach integrates AI technologies to continuously improve cybersecurity operations, collaborating with stakeholders to strengthen defenses and share threat intelligence.

13. Company Name: Cy5 Private Limited

Solution

A platform that's built grounds-up using a cloud-native architecture that detects misconfigurations and security threats in near-realtime leveraging entity behaviour analytics, a security data lake and serverless infrastructure.

Approach

Cloud Native Security Platform with integration support across top three hyperscalers viz AWS, Azure and Google Cloud.

14. Company Name: Threatcop

Solution

The identification of suspicious content is done using a predetermined threshold or set of criteria, including fraud detection, cybersecurity, and content moderation.

Approach

It analyzes content type, historical data, content analysis, metadata, and behavioral analysis to identify phishing and suspicious activities.

15. Company Name: Indusface

Solution

AppTrana DDoS mitigation powered by behavioral AI capabilities and managed services, deployed default and custom DDoS policies to bring these attacks down to zero.

Approach

The AI engine blocked external requests to URLs not meant for public access and suggested rate-limiting rules, geo-fencing, and custom blocking rules to prevent DDoS attacks.

The AI auto-updated tolerance levels for high-rate DDoS attacks and blocked IPs accessing blacklisted URLs.

16. Company Name: Bosch Global Software Technologies (BGSW)

Client & Industry

Automotive

Problem

The automotive industry's shift towards software-driven vehicles creates new cybersecurity risks. Traditional methods are insufficient to protect against emerging threats like remote exploits, supply chain attacks, and data breaches.

Solution

AI-powered cybersecurity solutions offer a proactive and adaptive approach to mitigate these risks. By analyzing vast amounts of data, AI can detect and respond to threats in real-time, safeguarding vehicles and protecting sensitive information.

Approach

BGSW's two-pronged approach leverages AI to:

1. **Proactively Defend:** Assess risks, design secure systems, and implement preventive measures.
2. **Actively Defend:** Monitor for threats, detect attacks, and respond in real-time.
3. **Respond and Recover:** Handle incidents, recover from attacks, and ensure business continuity.

By integrating AI into every phase of the product lifecycle, BGSW helps automotive companies build a robust and resilient cybersecurity posture.

Acknowledgement

We would like to express sincere gratitude to the industry leaders whose insightful contributions have significantly shaped this report. Their valuable perspectives and expertise have been instrumental in providing a comprehensive and actionable analysis of the cybersecurity landscape.

Special thanks to Akhilesh Soni, Global Cybersecurity CoE Leader, Tech Mahindra for his invaluable input and unwavering support throughout the research process.

Methodology

This report's methodology involved a multifaceted approach to gather comprehensive insights into the cybersecurity landscape. Two primary surveys were conducted: one targeting user organizations to understand their evolving security needs and challenges, and another focusing on service providers to gauge their capabilities and offerings. In addition, in-depth interviews were conducted with key security leaders from various industries to gain expert perspectives on emerging trends and best practices. To complement these primary research efforts, a thorough review of secondary research materials, including industry reports, academic papers, and news articles, was undertaken to provide a broader context and identify relevant benchmarks. This combined approach ensured a well-rounded understanding of the cybersecurity ecosystem and enabled the formulation of actionable recommendations.

Authors

ACHYUTA GHOSH
Senior Director and Head
Nasscom Insights

VINAYAK GODSE
CEO
DSCI

NAMITA JAIN
Director
Nasscom Insights

TEJA CHINTALAPATI
Senior Program Manager
DSCI, NCoE

SNEHA SHARMA
Manager
Nasscom Insights

NIHARIKA SINGH
Associate R&D
DSCI, NCoE

About Us

Nasscom represents the voice of the $250 billion+ technology industry in India with the vision to establish the nation as the world's leading technology ecosystem. Boasting a diverse and influential community of over 3000 member companies our network spans the entire spectrum of the industry from DeepTech and AI start-ups to multinationals and from products to services, Global Capability Centres to Engineering firms. Guided by our vision, our strategic imperatives are to accelerate skilling at scale for future-ready talent, strengthen the innovation quotient across industry verticals, create new market opportunities - both international and domestic, drive policy advocacy to advance innovation and ease of doing business, and build the industry narrative with a focus on Trust, and Innovation. And, in everything we do, we will continue to champion the need for diversity and equal opportunity.

Nasscom Insights is the in-house research and analytics arm of nasscom generating insights and driving thought leadership for today's business leaders and entrepreneurs to strengthen India's position as a hub for digital technologies and innovation.

About DSCI

Data Security Council of India (DSCI) is a not-for-profit, industry body on data protection in India, setup by NASSCOM®, committed towards making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI works together with the Government and their agencies, law enforcement agencies, industry sectors including IT-BPM, BFSI, CII, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

Disclaimer

The information contained herein has been obtained from sources believed to be reliable. nasscom and its advisors & service providers disclaim all warranties as to the accuracy, completeness or adequacy of such information. nasscom and its advisors & service providers shall have no liability for errors, omissions or inadequacies in the information contained herein, or for interpretations thereof. The material or information is not intended to be relied upon as the sole basis for any decision which may affect any business. Before making any decision or taking any action that might affect anybody's personal finances or business, they should consult a qualified professional adviser.

Use or reference of companies/third parties in the report is merely for the purpose of exemplifying the trends in the industry and that no bias is intended towards any company. This report does not purport to represent the views of the companies mentioned in the report. Reference herein to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by nasscom or any agency thereof or its contractors or subcontractors.

Usage of Information

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

AI