Infosys®
Navigate your next

CYBERSECURITY: THE GUARDIAN OF DIGITAL TRANSFORMATION

Infosys® | Knowledge Institute

Contents

Cybersecurity manages business risks throughout the value chain through processes, policies, and governance methodologies. The technology identifies, detects, protects, responds to, recovers from, and governs against cyber threats. It secures an organization's entire attack surface — cloud, workplace, IoT/OT, applications, big data, and AI models.

Daily and widespread cyberattacks persist. By 2025, Gartner projects 45% of global organizations will face supply chain software attacks. Cybercrime damage cost will rise from $8 trillion to $10.5 trillion in 2025, according to Cybersecurity Ventures.

The cybersecurity landscape has significantly advanced in the past two decades with better regulations, frameworks, and controls. The BS-7799/ ISO 27001 standard emerged between 2000 and 2008 — an era of antivirus, firewall, and virtual private network (VPN) solutions. Between 2009 and 2014, these solutions evolved to promote application-aware firewalls, unified threat management, deep packet inspection, and malware analysis. This era also introduced the National Institute of Standards and Technology (NIST) framework and Information Security Forum (ISF) standards of good practices.

From 2015 to 2018, significant advancements happened with big data analytics, DevSecOps, MITRE ATT&CK framework, web application firewalls, threat intelligence, and threat hunting.

Recent developments include secure access service edge (SASE), cloud-native application protection platform (CNAPP), zero-trust network access (ZTNA), data security fabric, blockchain, 5G, and internet of things (IoT). Advancements also happened around securing hyperautomation, privacy by design, identity detection and response (IDR), and data security posture management (DSPM) in cloud, and the recent use of generative AI in cybersecurity. This includes securing GenAI models from deep fakes and privacy concerns.

Cybersecurity has evolved alongside digital transformations like secure workspace shift, multicloud adoption, IoT growth, decentralized identities for borderless architecture, 5G, software-defined perimeter, and software bill of materials. Governance frameworks such as India's Digital Personal Data Protection (DPDP) Act 2023, Europe's General Data Protection Regulation (GDPR), the California Consumer Privacy Act of 2018 (CCPA), and the Federal Health Insurance Portability and Accountability Act (HIPAA) drive global baselines on data protection and privacy practices.

With the rise of ML and AI, especially large language model (LLM)-based generative AI, cybersecurity is no longer just about efficient controls and cost predictability. It is now also about the effectiveness of advanced technologies.

Concepts like secure by design, cyber resilience, business availability, quality assurance, managed services, and innovation remain crucial. A robust cybersecurity strategy demands adherence to both old and new regulations. Companies require a lasting cybersecurity plan that minimizes risks and boosts customer trust.

Cybersecurity's progress from horizon 1 to 3

Cybersecurity has particularly advanced across infrastructure security (IS); identity and access management (IDAM); data security; governance, risk management, and compliance (GRC); vulnerability management (VM); managed security services (MSS) and threat detection and response (TDR); IoT, OT, and 5G; cloud security; and data privacy.

In horizon 1 (H1), cybersecurity shifted from perimeter monitoring with static policies to traffic evaluation against contextual policies, where false positives and true negatives were common. Secure application development practices emerged early but limited to secure coding and dynamic testing to find security vulnerabilities.

In H2, security automation became the preferred method for efficient cybersecurity engineering, incident detection and response, secure cloud-native development, and MSS life cycle, with benefits of being human error free, scalable, and agile. This approach ensured automated governance, context-rich visibility, and regulatory compliance adherence in multicloud environment. H2 offers integrated visibility of security gaps for virtual machines, containers; serverless computing; continuous integration/continuous delivery (CI/CD) integrations in DevSecOps; security orchestration, automation, and response (SOAR); ZTNA for remote access; and integrated and automated governance for underlying multicloud platforms.

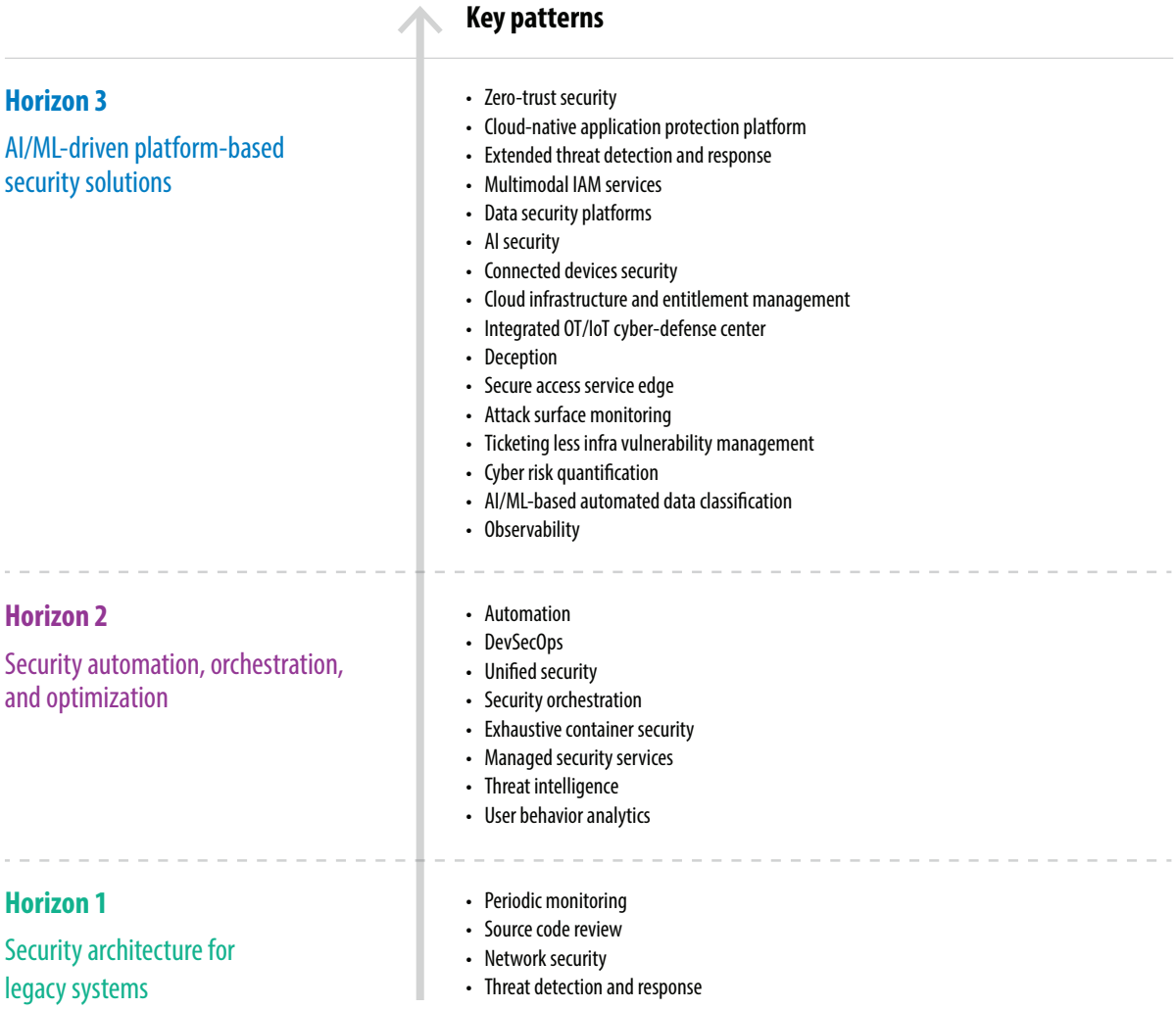
The Association of Corporate Counsel Foundation (ACC) report highlights the growing significance of legal departments within enterprises in shaping cybersecurity strategies. The percentage of chief legal officers (CLOs) has increased to 84% in 2023 from 76% in 2020. In H3, organizations realize the necessity of enhanced cross-functional collaboration among legal, IT, security, and business units to deal with cybersecurity threats. NIST's cybersecurity framework (CSF 2.0) added the govern dimension to the existing identify, detect, protect, respond, and recover sequence to emphasize cyber governance alongside people, process, policies, control, and compliance.

As digital takes center stage in business initiatives, cloud emerges as the nucleus of digital transformation. Digital Identities serve as the new

perimeter for cloud platforms. The exponential surge in human and non-human identities and their respective entitlements in cloud have complicated identity and access governance. IDR within cloud infrastructure and entitlement management (CIEM) solutions has evolved as a streamlined solution.

Platform-led services revolutionize enterprise security against advanced cyber threats via a service-oriented approach. SASE, CNAPP, data security fabrics, and extended threat detection and response (XDR) are prominent platform-based solutions. They are mainstream for integrated cyber protection, context sharing, and convergence of use cases in one platform, aligned with zero-trust approach. Amid generative AI's prominence, securing against deep fakes, data poisoning during learning large language models, and ensuring data privacy become crucial. Observability has also evolved to provide visibility beyond intrusion timing to intruder actions within enterprise boundaries to identify potential cyber risks. The cybersecurity mesh should merge robust policy management and governance, asset monitoring, and surface optimization across IT, OT, and cloud landscapes. Cyber risk visibility and integrated IT and OT security via unified cyber defense centers are crucial for the entities exposed to critical infrastructure.

Figure 1. Evolution of cybersecurity from horizon 1 to 3



Source: Infosys

Figure 2. Key trends across cybersecurity subdomains

Infrastructure security	**Trend 1.** Developments in microsegmentation enable zero-trust alignment **Trend 2.** Proactive decoys and lures gain prominence for advanced cybersecurity and zero trust
Identity and access management	**Trend 3.** Advanced threat detection capabilities strengthen security measures in identity management **Trend 4.** Verifiable credentials/decentralized identity and passwordless authentication strengthen digital identity ecosystem security
Data security	**Trend 5.** Data security platforms become a necessity to safeguard information **Trend 6.** Growing cloud workloads demand data security posture management
Governance, risk management, and compliance	**Trend 7.** Organizations increasingly adopt unified control frameworks to strengthen compliance and optimize costs **Trend 8.** AI/ML and integrated and quantitative approaches help manage third-party risks
Vulnerability management	**Trend 9.** A paradigm shift to microservices-based architecture and API security **Trend 10.** Safeguarding supply chains against cyber threats
Managed security services - threat detection and response	**Trend 11.** GenAI-powered security operations gain wider acceptance **Trend 12.** Data pipelines for effective cybersecurity
Emerging technologies	**Trend 13.** IT-OT security convergence gains popularity for unified, rapid protection **Trend 14.** Organizations embrace zero-trust security in OT/IoT network
Cloud security	**Trend 15.** Cloud-native application protection platform elevates multicloud security for businesses **Trend 16.** Firms secure hyperautomation to future proof their businesses
Data privacy	**Trend 17.** Privacy compliance becomes key to digital transformation **Trend 18.** Customer trust hinges on robust privacy controls

Source: Infosys

INFRASTRUCTURE SECURITY

Modern enterprises seek digital transformation and dynamic security controls. Strengthening cybersecurity for the hybrid work and zero trust begins with infrastructure modernization The shift toward digitalization necessitates restructuring to deploy modern security controls against emerging threats.

Companies shift from static to automated dynamic security controls. They transform their secure web gateway (SWG) architecture from traditional appliances to cloud-based services as needed at various stages.

CISOs and CIOs prioritize zero-trust adoption at the infrastructure layer itself. After the success of secure access service edge (SASE) and zero-trust network access (ZTNA), Infosys advances organizations toward full zero-trust adoption using cutting-edge technologies. This aligns with the macro trend of vendor consolidation and platform-led services in the cybersecurity space, where SASE enhances infrastructure security.

Trend 1 — Developments in microsegmentation enable zero-trust alignment

Microsegmentation, once error-prone and disruptive, has evolved to become more focused and ROI-driven through modern advancements. Both host-based and network-based microsegmentation options allow for customized solutions based on the customer's environment. It enables precise infrastructure segmentation and a least-privilege access approach, rooted in zero-trust principles. Microsegmentation achieves a dual goal — minimizes blast radius and eradicates lateral movement — bringing organizations closer to a zero-trust alignment.

A major US financial organization, in collaboration with Infosys, is currently engineering a microsegmentation solution. This endeavor is particularly challenging because of the enterprise's extensive Kubernetes deployment with multiple tenants. Infosys is designing the solution to first establish precise transaction visibility and subsequently apply granular zoning rules across all infrastructure and application workloads.

Trend 2 — Proactive decoys and lures gain prominence for advanced cybersecurity and zero trust

Proactive lures and decoys, as part of deterring security control, will soon become a technology must-have. This cutting-edge technology possesses the ability to comprehend threat patterns and mimic attacker behaviors, offering a robust defense mechanism. Infosys' cybersecurity engineering facilitates decoy deployment, policy enforcement against web and insider threats, and early threat detection for swift action. This approach ensures that businesses stay ahead of evolving cyber threats, safeguarding their digital assets and maintaining robust security controls.

A Belgian government organization worked with Infosys to deploy deception technology using lures at the perimeter and within internal shared services like active directory. This initiative has strengthened the organization's offensive security with deeper zero-trust integration and earned customer appreciation.

IDENTITY AND ACCESS MANAGEMENT

Identity and access management (IAM) is vital for secure and seamless user experiences. It has evolved from a simple username-password and manual provisioning model to single sign-on, multifactor authentication (MFA), centralized identity management, role-based access control, and access certification.

Recognizing password limitations in the face of ever-sophisticated cyber threats, IAM shifted toward passwordless authentication methods, such as biometrics (facial recognition, fingerprint scans, and iris recognition). This shift eliminated credential compromise risk and became the new norm. AI/ML and blockchain-based decentralized identity enhances governance control. It uses ML to analyze user behavior and access requests, giving users more control through self-sovereign identities. As the digital ecosystem becomes more complex, organizations adopt an identity fabric approach aligned with cybersecurity mesh architecture and zero-trust principles. The convergence of identity and governance services ensures consistent and secure access management for all human and non-human identities across various resources, including on-premises, on-cloud, and third-party.

Trend 3 — Advanced threat detection capabilities strengthen security measures in identity management

Traditional IAM security controls such as MFA are ineffective against modern identity threats. IAM and infrastructure security controls often have significant detection gaps. Identity threat detection and response (ITDR) is a security principle that encloses threat intelligence, processes, tools, and best practices to protect the identity system.

ITDR brings predefined identity threat-specific actions to cover identity breaches and other identity infrastructure attacks. It integrates with existing enterprise security solutions such as extended detection and response (XDR) and endpoint detection and response (EDR). Organizations with mature IAM should focus on the following aspects to address detection gaps and enhance cyberattack preparedness:

- Perform an audit on the existing IAM infrastructure to address known vulnerabilities in preparation for ITDR.

- Implement controls with emphasis on identity detection that prioritizes identity tactics, techniques, and procedures (TTPs).
- Execute a robust response using tools and processes to eradicate, recover from, and remediate identity threats.

Advanced AI assists and improvises the user behavior detection process by analyzing and profiling patterns and responding to threats. Organizations integrate tools and processes, evaluate existing tools aligned with ITDR architecture, and incrementally deploy zero-trust capabilities to enhance ITDR.

A top German specialty chemical company sought a standardized identity security operation model to proactively detect identity-related threats and vulnerabilities. Infosys helped it establish robust protection control processes using Microsoft tools, including ITDR.

Trend 4 — Verifiable credentials/ decentralized identity and passwordless authentication strengthen digital identity ecosystem security

As IAM evolves, organizations should embrace AI-driven governance, decentralized identity models, and a user-centric approach. Continuous compliance monitoring and context-aware access control strengthen security, while integration with emerging technologies ensures relevance. This transformation promotes decentralized identity solutions built on blockchain technology and passwordless authentication to eliminate credential compromise. Users get enhanced control over their data through self-sovereign identity frameworks, backed by blockchain's immutability, preventing identity theft and data breaches.

A North American food and support services player aimed to transform its access management user experience through passwordless authentication. Infosys helped the firm design, implement, and roll out Windows Hello for Business (WHFB) for its enterprise users.

DATA SECURITY

The zero-trust approach has revolutionized data security. The focus has shifted from perimeter protection to data safeguarding, regardless of location. This paradigm shift ensures a robust and comprehensive approach to data security. Advanced data security tools such as AI-ML data classification, data security platforms, insider risk assessment, and data security posture management for cloud platforms help businesses safeguard sensitive data, minimize cyber threats, and stay competitive.

AI-ML data classification categorizes and labels vast data troves, enabling precise control and tailored data protection measures. Data security platforms enhance visibility, centralize data protection mechanisms, and proactively detect and prevent potential threats in real time. Insider risk assessment tools identify and mitigate internal threats, such as data breaches and information leaks in real time. Data security posture management for cloud platforms ensures data security and compliance, allowing organizations to fully leverage cloud computing with integrity and privacy.

Trend 5 — Data security platforms become a necessity to safeguard information

Organizations increasingly prioritize data protection from unauthorized access, use, disclosure, disruption, modification, and destruction. Higher data volumes, more cyberattacks, and stricter data protection regulations drive the adoption of data security platforms. Organizations centralize management, automate workflows, and access threat intelligence through data security platforms. These platforms enable market consolidation through acquisitions, drive innovation with new features, and bolster organizations' security postures with comprehensive measures.

A leading US beverage and bottler manufacturer required a platform to safeguard intellectual property and sensitive information. Infosys helped it implement a robust data protection platform through tools such as AIP data classification, IRM, O365 DLP, and MCAS. The company remarkably enhanced data security, centralized management, reporting, and day-to-day operational tasks. With enhanced visibility, the company makes informed decisions and responds effectively to potential threats in a robust and secure data environment.

Trend 6 — Growing cloud workloads demand data security posture management

DSPM involves proactive monitoring and evaluation of cloud workloads to uphold best practices and compliance standards. The cloud shift drives demand for customized security solutions. Organizations recognize the need for real-time visibility, potential vulnerability identification, and prompt security gap address. DSPM tools automate these processes and provide insights into cloud workload security, ensuring data integrity, confidentiality, and availability.

DSPM strengthens cloud security, mitigates risks, bolsters compliance with regulations like GDPR, streamlines tasks for efficiency, and improves cloud visibility for swift risk mitigation.

Infosys assisted a US health insurer select and deploy a tailored DSPM solution for its multicloud environment. The firm reduced data breach risks, minimized potential regulatory fines, and improved overall security posture. This enhanced trust and confidence among its customers and stakeholders.

GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE

Boards/CxOs prioritize GRC and security as critical business concerns, with an evolving regulatory/compliance landscape and maturing risk management frameworks. Security and privacy as ESG/investor priorities drive integration and aggregation across diverse tools using governance frameworks and business-aligned SMART metrics/KPIs. GRC innovates as a competitive differentiator, driving resilience, transparency, trust, and confidence beyond compliance/risk management and financial impact.

Organizations prioritize digital transformation amid geopolitical changes and the post-pandemic landscape. They must navigate expanding threat surfaces with a focus on maximum return on security investment (ROSI). Cyber risk quantification, common control frameworks, cognitive GRC, AI/ML-driven digital GRC, data analytics, and automation, protect critical assets and sensitive data, and mitigate enterprise and supply chain risks.

Infosys offers a wide range of GRC services and solutions, leveraging AI-powered, agile, scalable/upgradable platforms, partnerships, IPs, and extensive industry experience. It assists customers through a successful GRC transformation journey.

Trend 7 — Organizations increasingly adopt unified control frameworks to strengthen compliance and optimize costs

Globally, regulatory/compliance landscape evolves, expands, and becomes more stringent, while risk prioritization and cost-benefit analyses grow more complex. Organizations spanning sectors, functions, and geographies face this issue due to larger scale and complexity.

Organizations need common control frameworks and stringent enforcement and monitoring of controls for better compliance and cost optimization. An optimal, business-aligned common control framework enhances synergies across compliance programs, offers an integrated view, and boosts efficiency. Consistent processes, automation at various levels (control implementation, control testing, and evidence collection), including configuring GRC platform native features, workflow customization, and RPA and AI-driven bots, strengthen the framework.

An American multinational tobacco company collaborated with Infosys to establish a common control framework and control testing (design and effectiveness). The firm used a structured audit schedule to conduct control tests at different intervals (monthly, quarterly, annually) and coordinate tasks with the GRC tool. This enhanced customer visibility, ensured continuous control assurance, improved SOX compliance, and drove efficiencies, resulting in cost savings.

Trend 8 — AI/ML and integrated and quantitative approaches help manage third-party risks

Increasing third-party incidents, a growing threat landscape (especially post-pandemic), and the ever-changing supply chain environment necessitate monitoring of and adherence to cybersecurity compliance in the supply chain. Robust tiering methodologies, tools, and automation improve operational/cost efficiencies and enhance integrated view. Integrated risk management also gains traction for better business alignment and maximum stakeholder value through improved integrated real-time quantitative risk visibility (and reporting) across functions (including supplier risks and outside-in threat intelligence). This helps in informed decision-making, such as prioritization of interventions and investments, including M&A initiatives.

Traditional vendor risk assessments fall short to address emerging risks. AI/ML and digital GRC methods boost digitization within the company and among suppliers. A comprehensive, dynamic quantitative risk assessment, encompassing people, processes, and technologies, combined with inside-out and outside-in digital footprint evaluations, ongoing real-time monitoring, and full 360° visibility, effectively handle third-party risks.

A leading US healthcare provider wanted data-backed, continuous visibility on risk posture, covering internal and third-party environments, with a focus on PHI-related systems. Infosys helped it implement the SAFE security partner solution to quantify breach likelihood scores (and trends) across people, policies, technologies, cyber products, and third parties. This optimized security risks through prioritized remediation from proactive and predictive analytics of aggregated vulnerabilities and external threat intelligence.

VULNERABILITY MANAGEMENT

Vulnerability management is crucial for enterprises to maintain digital security. It identifies and addresses system, application, and network weaknesses and reduces cyberattack risks. Businesses stay ahead of potential threats, safeguard sensitive data, and protect customer trust. Effective vulnerability management with timely patching and updates prevents breaches and enhances an enterprise's resilience to cyber threats.

Vulnerability management has evolved rapidly in the past decade due to technological advances, shifting threats, and complex IT environments, with notable contributions from automation, AI, and ML. Organizations now embrace DevSecOps to integrate security early in the SDLC pipeline. This shift-left approach incorporates the SBD principle to secure applications, infrastructure, and data.

Cloud adoption spurs the mainstream use of container security, API, microservices-based architecture, and risk-based prioritization. New technologies enable automated patching.

Trend 9 — A paradigm shift to microservices-based architecture and API security

In an era of Agile work and faster GTM, microservices-based architecture is a game changer. Granular components' bigger attack surface makes them prime targets for hacktivists, as shown by recent attacks on industry giants like Facebook and Twitter. Insecure APIs create a ripple effect, allowing attackers to exploit vulnerabilities and gain access throughout the supply chain. While traditional solutions like Burp suite, SOAP UI, and Postman did the trick, niche solutions from vendors such as App Sentinel, NoName, Salt, and Cequence provide end-to-end protection of business-critical APIs.

Securing APIs throughout the development process is now a CXO priority. This involves finding important APIs, assessing their business risks, uncovering vulnerabilities, and regular risk monitoring.

Organizations need tools and processes to detect and fix weaknesses in APIs; continuously assess API security controls to meet compliance requirements and enforce configurations to harden systems; control and mitigate risks during change, whether routine code, application, or modernization to the cloud.

A European company adopted an agile application development approach and incorporated security testing tools in its CI/CD pipeline. However, it lacked API security assessments. Infosys helped it set up an automated API security assessment process to precede code deployment to production. The firm conducted security assessments for all APIs in the same sprint they were developed.

Trend 10 — Safeguarding supply chains against cyber threats

Supply chain security protects the interconnected network of vendors, suppliers, partners, and third-party service providers that contribute to an organization's products or services. Supply chain security is on the rise due to growing cyberattacks that exploit vulnerabilities in the supply chain to gain unauthorized access to organizations' systems and data. Many industries require organizations to follow specific regulations for supply chain security. Compliance with these regulations is crucial not just to avoid penalties but also enhance security practices.

Modern businesses rely on a complex ecosystem of suppliers, partners, and vendors to deliver goods and services. Each entity in this network potentially introduces vulnerabilities that cybercriminals can exploit to target the ultimate target organization. A third-party breach can cascade into security risks for the organizations they serve. Attackers often target weaker links in the supply chain as entry points to more valuable targets, underscoring the need to assess all entities' cybersecurity.

Supply chain security involves evaluating the security practices of vendors and partners before engaging with them. Continuous monitoring of security measures ensures ample security throughout the partnership. Organizations must validate software and hardware integrity to prevent such risks and stay informed about third-party components and their software bill of material (SBOM) for continuous scanning and vulnerability mitigation.

Zero trust, vendor assessments, continuous vulnerability scanning, threat intelligence sharing, and robust incident response plans are essential vulnerability management components to safeguard the supply chain.

A US semiconductor company aimed to standardize supply chain security procedures across its enterprise and establish a software bill of material (SBOM). Infosys helped the firm set up a security tool that identifies SBOM vulnerabilities and establishes effective vulnerability management processes.

MANAGED SECURITY SERVICES - THREAT DETECTION AND RESPONSE

TDR has shifted from reactive to proactive, using threat intelligence and automation. Breach and attack simulations, beyond tabletop exercises, test internal controls and processes in a controlled environment. The trend shifts from managed detection and response (MDR) to managed protection detection and response (MPDR), with an emphasis on ITDR due to evolving identity threats.

As threats advance, the security data lake empowers analysts to query and extract relevant events for threat hunting, enhanced by telemetry from deceptive decoys and extended detection and response (XDR) agents. Cyber Kill Chain and MITRE ATT&CK remain vital in content engineering, while emerging trends include data pipelines, GenAI, and observability.

Trend 11 — GenAI-powered security operations gain wider acceptance

GenAI is an industry buzzword widely applied for its cognitive capabilities. It employs dataset crawling for model training and responding to human queries, predominantly used by security analysts for investigation and analysis. GenAI models carry risks such as data poisoning, extraction attacks, and erroneous incident analysis decisions. Organizations must consider these risks during model training.

The technology empowers security operations with an automation-first, intelligence-driven, risk-based, threat-centric approach, ensuring swift incident response, threat containment, and insights into threat actors and their tactics. It also enhances information asset security preparedness.

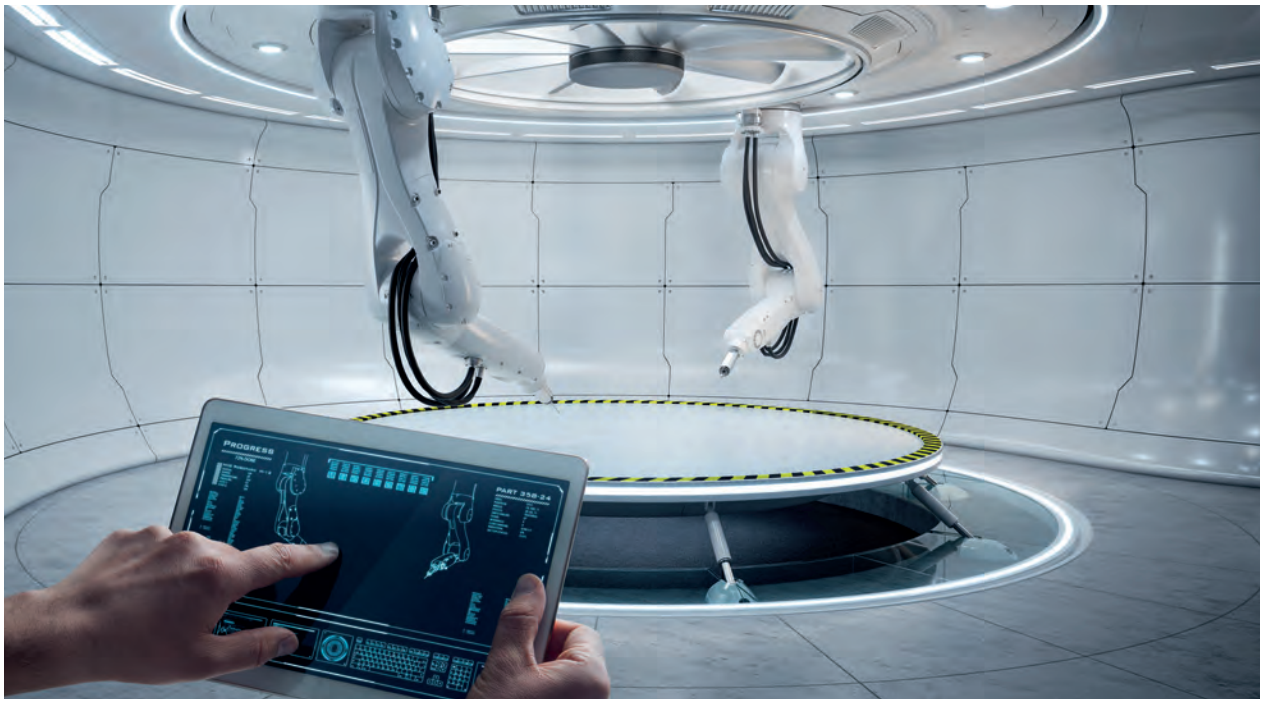
> A European postal operator wanted to improve its cybersecurity investigations. Infosys assisted by leveraging LLMs to provide context, attribution, and MITRE Att&ck mapping for security alerts. Resultantly, analysts conduct advanced analysis and threat hunting to uncover unknown threats and enhance cybersecurity effectiveness.

Trend 12 — Data pipelines for effective cybersecurity

Capturing all essential events during a major cyber incident is crucial for analysts to correlate and assess its impact accurately. In such situations, the volume of generated events may become unpredictable and significantly increase. Frequently, critical events may be missed during ingestion into the SIEM platform due to volume or EPS-based subscription limitations. To overcome such situations, data pipeline solutions collect, process, and route data (event logs) by filtering out unnecessary data or by aggregating data into more manageable chunks. It prevents the ingestion of duplicate and nonessential events into the SIEM platform.

A US food processing company, in collaboration with Infosys, onboarded a data pipeline solution to optimize data ingestion into its SIEM platform, ensuring flexibility, scalability, and cost effectiveness. This reduced the firm's EPS subscription by 30%, without missing any critical correlation event.

EMERGING TECHNOLOGIES



With Industry 4.0 (IIOT 4.0), ICS/OT sectors embrace digital transformation, robotics, digital twins, and advanced tech shifts, converging IT and OT networks. This enables automation, data exchange, and informed decisions but introduces risks. While security experts tackle IT, OT remains isolated and lacks adequate security. Malicious actors exploit this weakness.

IT and OT systems evolved with different purposes. IT has become a standardized and interoperable business enabler. OT systems were historically isolated and built with proprietary protocols and hardware. Initially, there was little or no effort to integrate the two, and the logical isolation of OT systems provided a level of security. Offline systems were safe from remote threats. However, the growing interconnection of OT and IT systems is eroding these differences. Now, even OT systems with no direct internet connections are indirectly accessed through an organization's business networks, exposing OT to new threats.

Trend 13 — IT-OT security convergence gains popularity for unified, rapid protection

As IT and OT merge, treat them equally. Apply IT security controls to OT. Collaborate, don't isolate, IT and OT teams. A skill gap exists between OT and cyber teams. Security teams lack awareness of OT device vulnerabilities and patches. The OT team doesn't grasp business risks from vulnerabilities. Security issues in OT devices can harm systems and human safety. So, organizations should monitor IT and OT systems and correlate logs to understand vulnerabilities and take necessary actions.

Managing IT and OT environments from a unified perspective helps the cyber team understand the threat landscape across networks and correlate alerts, incidents, and vulnerabilities.

Major IT SIEM providers like Splunk, Qradar, and Azure Sentinel integrate with OT security platforms such as Claroty, Nozomi, and MDIoT. They send alerts, events, and logs for monitoring and action. Before, hidden OT incidents caused delays in addressing threats. This integration offers quick action, removes OT blind spots, and addresses cybersecurity worries.

A major US beverage company aimed to monitor its IT and OT environments from a single interface for enhanced cybersecurity. It previously used an SIEM solution for the IT environment, and separately monitored OT, leading to unnoticed alerts and vulnerabilities. In collaboration with Infosys, it integrated an IT-OT SOC monitoring solution with its existing SIEM and Claroty OT platforms. This streamlined event and alert handling and provided quicker incident responses. The IT-OT SOC team now monitors both IT and OT environments from a single platform that requires less resources.

Trend 14 — Organizations embrace zero-trust security in OT/IoT network

Zero-trust principles in OT/IoT networks gain importance in cybersecurity. Old perimeter-centric security isn't enough against advanced threats. With more devices and IT-OT convergence, a proactive and adaptive approach is vital.

Zero trust is an innovative security framework that assumes no implicit trust, inside or outside the network perimeter. It verifies and authenticates every user and device, regardless of location or network connection. Zero-trust architecture reduces attack surface, minimizes threat movement, and enhances network security.

Zero trust gains importance in IT-OT networks that involve critical processes and are vulnerable to cyberattacks. Stringent access controls and continuous device monitoring enable organizations to secure critical infrastructure and reduce risks related to unauthorized access, tampering, and disruptions.

Zero trust suits IT-OT settings with legacy and modern systems. Despite diverse protocols, it grants detailed control for secure communication and integration among devices and systems.

A global manufacturing company with 22 OT plants faced challenges like poor asset visibility, security gaps, and a lack of skilled OT security staff. Infosys helped the firm establish a zero-trust framework by identifying cybersecurity gaps. It prioritized key infrastructure, reduced cyberattack risks, strengthened OT security against targeted attacks, and raised vulnerability awareness. The company also introduced 24/7 security monitoring to spot OT-related threats.

CLOUD SECURITY

Companies speed up digital efforts and see a substantial cloud shift. From lift & shift — where a few noncritical applications migrate to cloud through infrastructure as a service — to multicloud with cloud-native applications in cloud-exclusive enterprises.

Cloud-native applications accelerate migration, enhance standardization, and lead to error-free development. Yet, they widen the attack surface, which requires fresh strategies against cyber threats. For cyber resilience, vital cloud tenets — posture, identity, data, compliance, and code — demand next-gen security. Cloud-native security should provide a unified view of cyber risks across these tenets with shared contextual information citing a comprehensive perspective.

Trend 15 — Cloud-native application protection platform elevates multicloud security for businesses

Enterprises embrace cloud-native approaches in multicloud platforms such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). They use microservices architecture with evolved workloads like containers and serverless to develop scalable cloud-ready applications. In multicloud with a native approach, new security aspects and attack vectors emerge. Cloud-native application protection covers posture, compliance, workload protection, identity response, micro-segmentation, software bill of materials, etc., in a modular but integrated manner. CNAPP offers a unified view of cyber risks across clouds. It proactively identifies security risks from day zero to ensure secure by design in application development and infrastructure provisioning.

A leading US technology company in conversational commerce and AI software partnered with Infosys to create CNAPP modules on GCP. Infosys ensured cloud security, regulatory compliance, and managed vulnerabilities for GCP's various workloads, from serverless to containers and Kubernetes.

Trend 16 — Firms secure hyperautomation to future proof their businesses

Hyperautomation reshapes digital transformation through rapid, scalable, and extensive automation. It brings efficiency and cost benefits but opens an all-new attack surface. Securing hyperautomation employs DevSecOps to identify security loopholes and vulnerabilities at each stage of "dev," "build," and "run" in the automated application development or infrastructure provisioning life cycle. Unlike reactive cloud security, it safeguards the entire automation landscape. It ensures secure CI/CD pipelines using IAST/SAST/DAST/SCA controls for continuous compliance and vulnerability-free code delivery.

A German multinational investment bank and financial services company partnered with Infosys to build a GCP-based cloud data leakage prevention (DLP) platform. Infosys used JAVA microservices, Terraform scripts, and hyperautomation. It followed DevSecOps to identify security risks with gating controls in the CI/CD pipeline stages.

DATA PRIVACY

Organizations have remarkably transformed in the last five years. They embraced innovations through emerging technologies while ensuring compliance with global privacy laws. Their privacy journey started with comprehensive privacy assessments to identify gaps and formulate a road map to comply with regulations such as GDPR and CCPA. As regulations multiply, organizations must adhere to multiple laws across jurisdictions. So, they shift to global standards like ISO 27701 and the NIST Privacy Framework, all while incorporating privacy by design principles.

Rising AI/ML, cloud computing, and metaverse/ blockchain raises data privacy concerns. Technologies like homomorphic encryption, multiparty computing, and zero-knowledge proofs ensure privacy and regulatory compliance.

Trend 17 — Privacy compliance becomes key to digital transformation

Digital transformation amplifies business processes, products, services, and customer experiences. In this data-driven landscape, privacy is crucial for successful transformation. Safeguarding the personal data of customers, employees, and partners fosters trust, loyalty, and competitive advantage in a regulated market. It curbs breaches, bolsters confidence, and provides a competitive edge.

A global company wanted to upgrade its website for enhanced user experience, workflow, and global reach while maintaining privacy compliance. Infosys digitally transformed the website using HubSpot for marketing and communication. The firm tackled consent and privacy compliance challenges for third-party platforms like HubSpot and MS Azure by adhering to GDPR and CCPA standards. This enhanced customer confidence and reliability.

Trend 18 — Customer trust hinges on robust privacy controls

In today's digital world, customers are increasingly concerned about their privacy. They are more likely to do business with companies that have a strong reputation for protecting data. Additionally, many countries have strict privacy regulations, and businesses that want to operate in these markets must comply with these regulations. Privacy controls are essential for businesses to build customer trust and protect data. Strong privacy controls reduce data breach risks, improve customer satisfaction, and boost revenue. Customers are more inclined to share accurate information when they trust a company's commitment to data protection. Enhanced customer satisfaction improves brand reputation and provides repeat business.

A major Belgian cross-border delivery service provider manages sensitive data across hybrid systems (on-premises and cloud). This necessitates strict adherence to Article 30 of GDPR relating to data governance. The firm, in collaboration with Infosys, established a data platform that categorizes and secures information and helps achieve 100% GDPR compliance. The platform safeguards offshore data through automated masking. Enhanced privacy controls boosted revenue, data integrity, customer trust, and experience.

Advisory Council

Mohammed Rafee Tarafdar
EVP and Chief Technology Officer

Shambhulingayya Aralelemath
AVP & Global Delivery Head, Cybersecurity

Lalit Mohan Sanagavarapu
AVP, Cybersecurity

Kishore Susarla
Senior Delivery Manager, Cybersecurity

Sujatha Mudulodu
Practice Manager, Cybersecurity

Manish Kumar Pandey
Delivery Manager, Cybersecurity

Vishwanath Nagaraj
Senior Industry Principal, Cybersecurity

Karthik Andhiyur Nagarajan
Senior Industry Principal

Anil J Rajan
Senior Industry Principal, Cybersecurity

Nitin Ainath Tagalpallewar
Senior Industry Principal, Cybersecurity

Manish Jain
Group Manager, ISG

Abayavidya Rengahari
Group Manager, ISG

Prakash Vishwakarma
Principal Technology Architect, Cybersecurity

Venkata Ganesh Swaminathan Mangudy
Industry Principal, Cybersecurity

Contributors

Mohit Jain

Darshan Singh

Vinit Ajgaonkar

Shahidhussian Sayyed

Nitin Bajpai

Varadaraj Palaniswamy

Saurabh Sharma

Amit Kadam

Oommen Thomas

Prabhakaran Mahalingam

Abhijit Madhav Vaze

Sangamesh Shivaputrappa

Sesha Phani Babu Turimella

Mohammad Anjum Nasim

Biswajit Pattnayak

Producers

Ramesh N
Infosys Knowledge Institute

Pragya Rai
Infosys Knowledge Institute

About Infosys Knowledge Institute

The Infosys Knowledge Institute helps industry leaders develop a deeper understanding of business and technology trends through compelling thought leadership. Our researchers and subject matter experts provide a fact base that aids decision-making on critical business and technology issues.

To view our research, visit Infosys Knowledge Institute at infosys.com/IKI or email us at iki@infosys.com.

For more information, contact askus@infosys.com