Infosys®
Navigate your next

CYBERSECURITY – STRENGTHENING THE FABRIC OF DIGITAL TRUST

Infosys® | Knowledge Institute

Contents

Cybersecurity manages security risks across all stages of the business value chain and helps gain the trust of customers and stakeholders. Cybersecurity leverages technology to provide better visibility and control across cloud infrastructures. It secures modern workplaces, establishes a modern zero-trust architecture, and holistically secures transformation initiatives.

Cybersecurity threats have evolved dramatically in the last two decades. The statistics are alarming, with cyberattacks every day, everywhere. According to Check Point Research, cyberattacks on corporate networks increased by 50% in 2021 compared with 2020. Remote working environment became a norm during the pandemic, which enlarged the attack surface. Adversaries in sequence adapted quickly to the changed landscape.

The cybersecurity landscape has also advanced in the last 20 years, with better regulations, frameworks, and controls. The BS-7799/ISO 27001 standard was developed between 2000 and 2008 — an era dominated by antivirus, firewall, and virtual private network (VPN) solutions. Between 2009 and 2014, these solutions evolved further to promote application-aware firewalls, unified threat management, deep packet inspection, and malware analysis. It also brought forth the NIST framework and ISF standards of good practices. From 2015 to 2018, significant advancements happened with the inception of big data analytics, DevSecOps, MITRE ATT&CK framework, web application firewalls, threat intelligence, and threat hunting.

More recently, zero-trust network access (ZTNA) frameworks, blockchain technology, 5G networks, and the internet of things (IoT) have gained traction in response to the evolving threat landscape.

Advancements happened around DevOps, cloud-native applications with serverless platforms, container security, breach and attack simulation, and NDR/CDR solutions.

Cyber defense programs contribute to workspace transformation, cloud adoption, digital transformation, and borderless architecture. Digital technologies, including 5G, software-defined networking, artificial intelligence (AI)/machine learning (ML), blockchain, big data, and open source, are gaining prominence. Governance frameworks such as 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) are driving global baselines on data protection and privacy practices.

Cybersecurity now focuses on the efficiency of controls, predictability of costs, and constant innovations. Secure by design (SBD), cyber hardening, reduced risks and assured quality, managed services, and innovation and automation are the latest asks of stakeholders. A strong cybersecurity program also demands compliance with existing and new regulations.

The focus now is on a comprehensive cybersecurity program that is sustainable, reduces risks, and enhances customer confidence.

Cybersecurity's evolution to counter attacks

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

This study analyzes cybersecurity's evolution across the following three horizons:

Horizon 1 (H1): Cybersecurity evolved from periodic business workload monitoring that helped organizations evaluate security controls' effectiveness, configuration, and operations and keep track of security metrics. In the software development life cycle (SDLC) phase of cybersecurity evolution, the source code assurance approach helped organizations safeguard against attempts to exploit application code flaws that affected end systems.

Horizon 2 (H2): In the past few years, security automation has enabled organizations to function efficiently across security engineering, incident detection and response, cloud-native services/external security solutions deployments, and the MSS life cycle with scalability and agility. This requirement-specific approach provides customers with context-rich visibility, security governance, and compliance in a multicloud environment. H2 offers unified security for containers; serverless computing; continuous integration/continuous delivery (CI/CD) integrations in DevSecOps; security orchestration, automation, and response (SOAR); integrated governance; and underlying cloud platform ecosystems.

Horizon 3 (H3): In H3, extensive remote working has accelerated the adoption of container and serverless platform-based cloud-native applications, endpoint application isolation and containment for workplace security, and secure access service edge (SASE) solutions. Mainstream focus is on external vendor security solutions supporting a zero-trust approach.

Unlike endpoint detection and response (EDR), extended detection and response (XDR) carries cross-layer TDR capabilities to provide data visibility across networks, device endpoints, and analytics to address sophisticated threats. Customer-centric data privacy controls, including privacy by design (PbD) and default in systems and technologies, data protection office as a service, quantum cryptography, and differential privacy to protect complex IT and cloud environments, are delivered with privacy-enabling technologies. Passive and agentless IoT platforms empower the connected devices ecosystem, provide real-time visibility, and offer AI/ML-based analytics to deliver actionable insights and reduce infrastructure risks with zero impact.

Cloud customers need to rethink their strategy with cloud security posture management (CSPM), cloud workload protection platform (CWPP), and cloud access security broker (CASB) solutions. The cybersecurity mesh architecture should integrate stronger policy management and governance and monitoring of digital assets to continuously optimize and manage the attack surface across the IT and cloud landscapes.

We have explored key trends across the following nine domains:

Infrastructure security

Identity and access management

Data security

Governance, risk management, and compliance

Vulnerability management

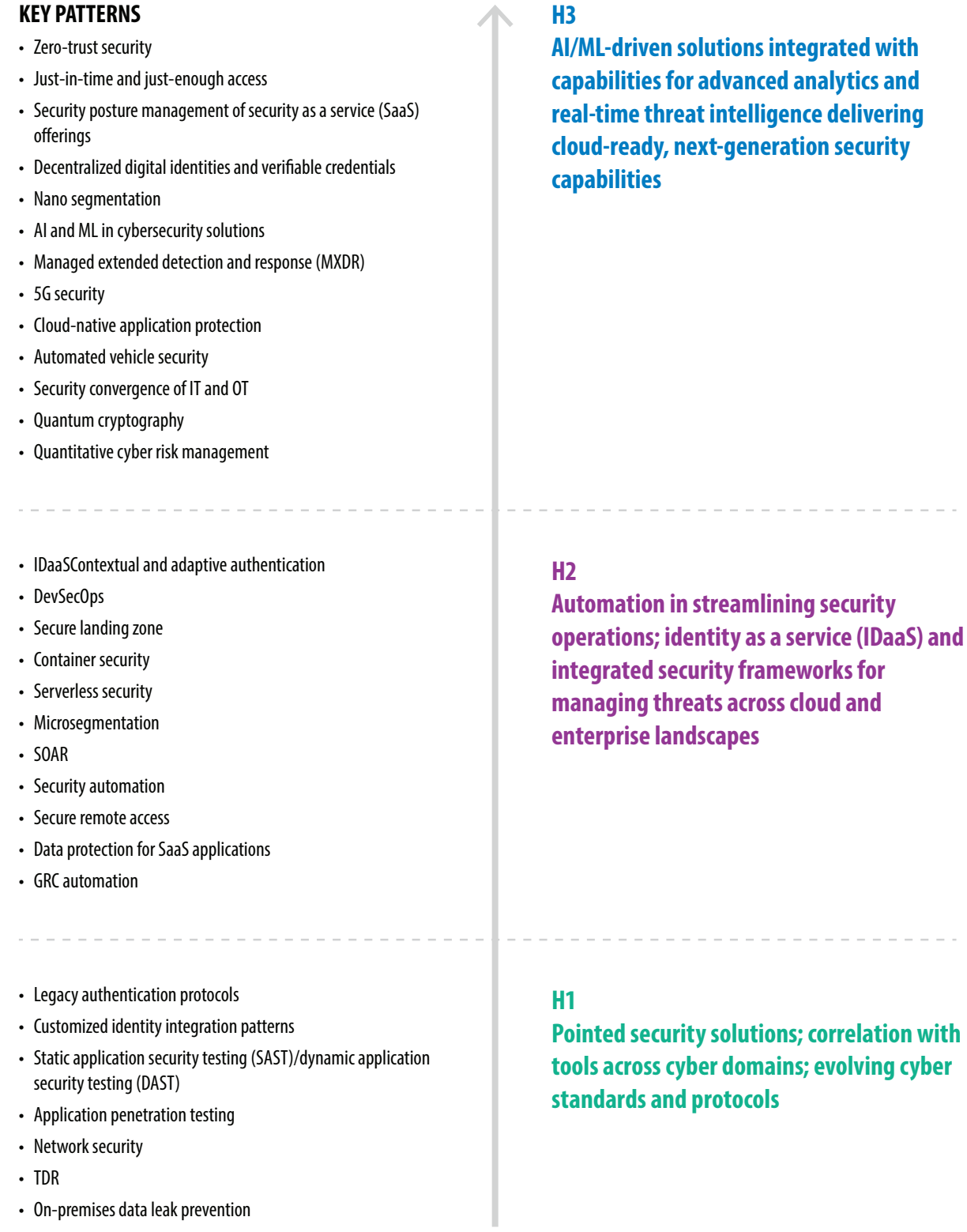
Managed security services - threat detection and response

Internet of things, operational technology, and 5G

Cloud security

Data privacy

Figure 1: Market dynamics across the three horizons



Source: Infosys

Figure 2: Key trends across cyber security subdomains

Infrastructure security

Trend 1 – SASE framework gains ground over legacy security controls

Trend 2 – ZTNA becomes mainstream for secure and seamless zero-trust access

Identity and access management

Trend 3 – Risk-based authentication gains prominence to minimize security risks

Trend 4 – Identity becomes a core component with zero-trust security model

Data security

Trend 5 – Enhanced security at all touchpoints with integrated data protection and classification tools

Trend 6 – Certificate life cycle management and automation gain consideration

Governance, risk management, and compliance

Trend 7 – Supply chain security and vendor risk management (VRM) gain focus

Trend 8 – New cyber controls enable effective cybersecurity governance

Vulnerability management

Trend 9 – SBD adoption embeds security early and ensures digital trust

Trend 10 – Enterprise resource planning (ERP) on cloud adoption emphasizes business-critical ERP application security

Trend 11 – Ticketless infrastructure VM minimizes manual efforts

Managed security services - threat detection and response

Trend 12 – Orchestration, automation, and response technology ease incident management

Trend 13 – Advanced security monitoring through cloud-specific protection programs

Internet of things, operational technology, and 5G

Trend 14 – IoT and OT tools enable complete network visibility

Trend 15 – Real-time security monitors help detect vulnerabilities and violations in 5G

Cloud security

Trend 16 – Secure landing zones gain prominence for cyber resilience and security as a built-in culture

Trend 17 – Cloud security as code ensures continuous compliance in production

Data privacy

Trend 18 – Integrated frameworks and privacy technologies enable effective data protection

Source: Infosys

INFRASTRUCTURE SECURITY

Organizations deal with a host of information assets due to increased cloud adoption and off-premises hosting. They are constantly updating security controls to detect real-time threats and fine-tune security control configurations to isolate, remediate, and prevent threats.

Traditional antivirus tools failed to prevent many ransomware attacks due to complexity and limited functionality for remote workforce use. Organizations have now begun mandating advanced AI/ML-based intelligent malware protection tools, including EDR and XDR controls, which no longer rely on signature updates to be distributed and deployed for malware protection.

Trend 1 — SASE framework gains ground over legacy security controls

Software-defined wide-area network adoption is already at speed. By replacing legacy multiprotocol, label-switching, and wide area networks, the SASE framework is transforming security controls to the edge. Our analysts predict that 80% of organizations will become SASE-compliant by 2024. This journey entails shifting to an "as a service" model with the SASE framework to yield better return on investments, robust security, and reduced complexity. The SASE framework also gives CXOs a single-pane view, as all technologies within the framework have full integration.

Earlier, enterprises used to acquire, deploy, configure, and build security controls in their data centers, public cloud, and private cloud within limited predefined data center locations. Thereafter, users had to access these security controls, irrespective of their geographical locations. It required high dependency on the hosted sites of security controls, resulting in network latencies and, in turn, poor user experience.

Security control technology providers are building capabilities to provide SASE security controls by themselves or with partners. They are also committing to road maps to bring them into a single management pane with tighter integration to meet the defined SASE framework. Many enterprises have started choosing SaaS while adopting the latest security controls, such as ZTNA and CASB solutions.

A global energy company wanted to transform its legacy network of multiple on-premises deployments. It wanted to ensure user activity traceability and secure remote site access. The company worked with Infosys to deploy SASE solutions (Zscaler ZIA, ZPA, ZPA PSE) across its global network, which enabled next-generation, perimeter-less security for 25,000+ users and enhanced enterprise-grade security for hybrid cloud and edge.

Trend 2 — ZTNA becomes mainstream for secure and seamless zero-trust access

ZTNA enforces granular, adaptive, and context-aware policies, leading to secure and seamless zero-trust access to private applications hosted across clouds and corporate data centers, from any location and device. It can be a combination of user identity, user or service location, time of day, type of service, and security posture of the device.

On the assessment of user identity, device identity, and other contextual factors, ZTNA allows "least privilege" access to specific applications rather than exposing the entire underlying network to any user with a valid login key. This reduces the attack surface risks and prevents lateral movement of threats from compromised accounts or devices.

ZTNA acts as a key enabler for SASE solutions, transforming the concept of a security perimeter from static, enterprise data centers to a more dynamic, policy-based, cloud-delivered edge to support the access requirements of the distributed workforce. Businesses should upgrade their legacy VPN solutions to ZTNA, which enables microsegmentation in the network and makes applications secure over the internet. It secures legacy application access, enhances user experience, and optimizes infrastructure and operational costs.

A global consumer products brand wanted to enhance user experience and create a more secure user access system. It transformed its Zscaler SASE solution to enable ZTNA. It introduced SASE and a zero-trust/software-defined perimeter to connect remote users with its corporate network. The company could reduce operational costs, enhance VPN to zero trust, and improve overall security by monitoring additional noncorporate networks.

IDENTITY AND ACCESS MANAGEMENT

IDAM ensures that the right users have access to the right information at the right time. Mapping to the technology standards for accelerated user provisioning enables authentication and authorization of the accessed information (applications/systems). The functional blocks in IDAM are implemented as point solutions to cater to disparate policies of federated business units and manage access of enterprise workforce users.

As businesses expand globally, IDAM has become more complex, while pointed solutions (legacy/homegrown IDAM) have become less effective. The scope of identity personas has expanded to include the enterprise workforce, vendors, partners, customers, and nonhuman (e.g., bot) identities. IDAM now focuses on establishing holistic governance across on-premises and cloud infrastructure with life cycle management applied for each identity, managing risk posture through automated provisioning and visibility of access entitlements, reducing the threat vector by managing keys to the kingdom, remediating to passwordless technologies, and adopting a zero-trust IDAM framework. This includes managing the number of privileged accounts, adopting zero standing privileges models, and establishing just-in-time frameworks for privileged access.

Trend 3 — Risk-based authentication gains prominence to minimize security risks

A strong identity helps establish robust security standards for a zero-trust model. It connects legacy and cloud applications with policies applied to manage access risks and secure attack surfaces. The zero-trust model assumes potential breaches in advance and requires each access request to be strongly authenticated, authorized, and evaluated for anomalies.

Identity is the core foundational element of a zero-trust model. Such identities include people, nonhuman (services, bots, etc.), and IoT devices; for instance, employees or external users who connect remotely to enterprise resources using managed or unmanaged devices in the current remote working environment. If such remote access policies allow weak login credentials, attackers can easily gain unauthorized access (e.g., using password sprays, compromised credentials, etc.) to enterprise jewels.

Defining policy-based contextual or adaptive multifactor authentication (MFA) can restrict access to enterprise resources. This is due to integrated

risks determined from the convergence of user, device identity, and environmental conditions. This framework for leveraging risk signals to enforce strong authentication minimizes security risks, controls access to privileged accounts, and remediates legacy (weaker) authentication protocols. It improves security posture with a balance of user productivity. It delivers a frictionless login experience, strengthening the fabric of trust while using digital services. Various MFA factors leveraged for stronger authentication include passwordless solutions (e.g., using FIDO2), push notifications (using authenticator smartphone apps, including MS Authenticator and Google Authenticator), one-time password delivery using SMS or email, automated verification call, knowledge-based questions, etc.

A Europe-based postal services major wanted to modernize its access management framework for its enterprise and customer user segments. It worked with Infosys to roll out a strong authentication framework that was integrated with the identity risk model to enable a secure and frictionless login and session management experience for protected applications.

Trend 4 — Identity becomes a core component with zero-trust security model

The zero-trust model maintains that all users or devices, irrespective of their access location, are authenticated and authorized to access requested applications or services. It encompasses the following:

- Identity as the central focus.
- Minimal reliance on traditional edge firewalls with VPN.
- Frictionless and secure access to resources with MFA (i.e., identity/device verification).
- Assurance of security principles enforcement across all access tiers.

When designing a zero-trust model, the principles mentioned above should be considered for securing access to enterprise applications and services, whether they are setup on-premises or in the cloud. Tools such as Microsoft Azure AD, PingID, Okta, and CyberArk can help here.

A U.S.-based food and beverage major modernized its identity management and access governance framework by establishing holistic visibility of "who has access to what" across on-premises and cloud resources. It automated access requests and provisioning processes, life cycle management, setup of business-centric roles, and setup of governance processes. The outcome was a strong policy framework for least-privileged models and the adoption of a zero-trust framework.

DATA SECURITY

Earlier, data security focused on perimeter-based protection with limited encryption, especially for drives and application-level secure socket layer (SSL)/ transport layer security (TLS) protection. Database protection was limited to the native vendor-provided encryption capabilities such as SQL and Oracle TDE, often managed by the DBA Group.

The evolution of zero trust led to data security technologies maturing in depth and coverage. As data moved to different landscapes, the focus shifted to protecting the data wherever it resided.

Advances in blockchain, AI/ML, homomorphic encryption, and multiparty computing are now used in data protection, merging the protection of data at rest, in transit, and in usage. However, none of these technologies possess transformational data protection capabilities for enterprises without a coordinated data governance process that applies uniform policies. An infonomics focus on quantifying data value is expected to further drive data security governance investment decisions in the coming years.

Trend 5 — Enhanced security at all touchpoints with integrated data protection and classification tools

Data loss prevention (DLP) tools protect on-premises data at endpoints, during transit, and at rest. DLP can be integrated with a CASB to ensure the same DLP policies are applied to cloud-hosted data. User entity behavior analysis capabilities in a CASB can be used to provide role-based access control to applications or cloud-hosted data and detect suspicious user access activity. Anomalies and incidents are logged and available for audit and better decision-making.

Further, DLP detection capabilities can be augmented with data classification solutions. These solutions can add metadata fields to sensitive documents and emails, which can help DLP tools identify sensitive information faster with fewer false positives and fewer rules. The classification tools can also call various encryption applications, such as information rights management (IRM) for protecting files and emails

containing sensitive information, especially when sent outside the organization.

All these data protection technologies must further integrate with security information and event management (SIEM) tools for correlation and incident detection. The central security operations team can act as needed.

A Switzerland-based agro trading company wanted to implement an integrated data protection strategy to protect its intellectual property and sensitive information. After a holistic assessment, multiple data protection tools were implemented, including Symantec DLP, O365 DLP with AIP data classification, IRM, and an MCAS solution. These were integrated with the Azure Sentinel SIEM for centralized event correlation and SNOW, an online ticketing system. A Microsoft Power BI-based solution was also implemented for analytics and reporting.

Trend 6 — Certificate life cycle management and automation gain consideration

With increasing cloud adoption and remote connections, the number of certificates in the environment has gone up drastically. In the transition phase, a valid certificate for secure communication became essential. Generally, enterprise-level certificates will have two years of expiry. In recent times, where most companies have completed two years of cloud adoption, we have seen many application downtime issues because of expired certificates. There are multiple reasons for this, including:

- Manual tracking and management of SSL keys and certificates.
- The time-consuming, application-dependent, four-step process for certificate request generation.
- Unplanned certificate-related outages causing business disruption.
- Downtime due to certificate renewal and replacement.

Following strategies, including certificate life cycle management and possibly automation of certificate rotation solutions, are gaining attention:

- Cost management by finalizing architecture and future-proof planning for the use case that can be fulfilled with an internal or external certificate.
- Inventory standardization for certificate discovery and application mapping.
- Reduction in human errors by automating the certificate request generation and installation processes.
- Prevention and remediation of unplanned outages of applications due to certificate expiry.
- Improvement in governance and reporting for crypto compliance and standards.
- Automation of certificate generation and renewal.

A global financial services firm implemented a certificate life cycle management solution for its North American unit. This was done using Venafi's solution to improve client experience. With the help of Infosys, the company integrated the solution into its environment to leverage out-of-the-box drivers and implement certificate renewal automation.

GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE

Most GRC tools provide integrated risk management and automating processes. However, there are still multiple white spaces in the market. Infosys, in partnership with Cyber Next and Living Labs, has developed several tools such as Cyber Gaze to manage security metrics.

GRC technology innovations offer real-time dashboards for better visibility supporting governance, supply chain risk management, enterprisewide risk quantification, and trend analysis. Technology companies such as RSA, MetricStream, ServiceNow, IBM, and OneTrust provide tools for automated compliance assessments, while platform companies such as CyberCompass help integrate the process and technology controls for enterprisewide visibility.

Trend 7 — Supply chain security and vendor risk management (VRM) gain focus

As organizations increasingly collaborate with partners and outsource work, the risk of compromise also increases in the supply chain. VRM identifies a business' vendor relationships and associated cyber risks. The tool categorizes risks from vendors and helps track and mitigate those risks. VRM also tests potential suppliers before they are approved as vendors. Multiple regulations, including the GDPR, put the onus of VRM on the organization, holding it responsible for any breach or data loss.

GRC automation platforms from RSA, MetricStream, and ServiceNow provide integrated VRM capabilities. Most solutions are now available in the cloud as SaaS models, reducing implementation time and operations costs. The challenge of large volumes of vendor assessments has led to a new category of vendors like CyberGRX and OneTrust that provide risk exchange capabilities for cost reduction. Like BitSight and RiskLens, others provide continuous vendor assessments using publicly exposed assets and information on the dark web.

> A leading packaged food retailer in the U.S., in association with Infosys, defined its VRM process and the vendor tiering criteria to create tier-specific security assessments meeting its risk appetite. All workflows and processes were automated using the RSA Archer product. Post-implementation, Infosys provides vendor risk assessments and ongoing remediation governance as a managed service.

Trend 8 — New cyber controls enable effective cybersecurity governance

With evolving cyber threats, CISOs struggle to measure and track the effectiveness of their control measures. Transaction systems such as SIEMs provide only a snapshot of their status and include excessive data for a strategic review. Using GRC automation tools for cyber metrics management is a long and expensive process. Most of these tools do not provide an intuitive and flexible user interface with rich dashboards and trend analysis.

To ensure the organization's security, inputs from multiple groups and stakeholders are required. These inputs are beyond those obtained from IS or IT teams. This is possible with well-defined cyber metrics supporting data-driven governance and providing specific improvement inputs to each team. The ability to drill down to specific periods and business units/ geographies helps executives measure and track the effectiveness of the control implementations.

A leading U.S.-based health care service organization was using traditional spreadsheets to manage metrics. Infosys implemented the Cyber Gaze platform to help the CISO, the CIO, and IT leadership track and analyze over 160 cyber metrics. The flexible platform allows quick implementation of new metrics (new cyber controls). It can also be used to collaborate across the IS and other teams for effective cybersecurity governance.

VULNERABILITY MANAGEMENT

VM is the core prevention measure in cybersecurity that can prevent more than 80% of breaches. It handles the identification, prioritization, governance, and treatment of weaknesses throughout the infrastructure, network, and application layers.

Though early interventions in the VM area were compliance-driven, especially within the payment card industry, all enterprises now have a formal process and multiple scanning tools to identify weaknesses across the threat surface continuously.

Now organizations are moving to DevSecOps to secure their SDLC, integrating security early in the pipeline. With DevSecOps adoption and a shift-left approach, application development is incorporating the SBD principle to enhance the security of applications, infrastructure, and data.

Cloud adoption has helped evolve container security and make it a mainstream practice along with risk-based prioritization approaches. Similarly, new technologies are now available for automated patching.

Trend 9 — SBD adoption embeds security early and ensures digital trust

SBD identifies and verifies security requirements during the build and test phases before go-live.

Similarly, privacy regulations, such as GDPR, mandate PbD, ensuring the consent is captured and managed via data collection. The personally identifiable information must be secured while in use and destroyed when no longer needed.

Organizations are developing enterprise-level security policies, design frameworks, guidelines, and checklists, along with approved tools and components. Established gating criteria and governance processes ensure required security measures.

Secure architecture reviews and threat modeling identify design and architecture flaws. DevSecOps enables the identification and closure of weaknesses during the development and operation phases. Organizations need a central team to provide white-listed components and to vet and approve any new open source components, if required.

Vendors such as Microsoft and Myappsec provide threat modeling tools, while Micro Focus, Qualys, Nessus, Rapid7, Veracode, CheckMark, SonarQube, Palo Alto, Onapsis, and Black Duck scan and identify weaknesses. A central process and platform are needed to ensure governance and traceability for effective implementation of SBD and secure SDLC.

A global software platform and services provider wanted to strengthen its product security implementation processes. Infosys helped the company enable SBD through SDLC implementation for its product development life cycle. DevSecOps was implemented for automated scans with continuous monitoring to reduce the cost of security inclusion and enable developer self-help.

Trend 10 — Enterprise resource planning (ERP) on cloud adoption emphasizes business-critical ERP application security

With ERP solutions now exposed to the cloud, hacker activities have significantly increased. While ERP vendors have native solutions, there are niche solutions from vendors such as Onapsis that provide end-to-end protection of business-critical ERP solutions.

It is critical to detect and prevent unauthorized changes and configurations that expose an ERP solution's vulnerabilities. Hence, holistic business-critical application security or ERP security is now a priority for CXOs.

Organizations need tools and processes to detect and fix weaknesses in custom third-party applications; continuously assess IT controls to meet compliance requirements and enforce configurations to harden the systems; control and mitigate risks during change, be it routine code, application, and system maintenance or patching or modernization to the cloud; and get real-time visibility and alerts to respond to breaches.

A leading U.S.-based pharmaceutical company wanted to improve its SAP ERP security posture and reduce compliance cost. It partnered with Infosys to implement the Onapsis platform and integrate an IT service management tool. The company benefited from continuous vulnerability scanning and alerts, improved workflows, and compensating controls to maintain compliance between audits.

Trend 11 — Ticketless infrastructure VM minimizes manual efforts

Infrastructure vulnerabilities are identified using automated scanning tools in real time. Post-identification, the critical step is to prioritize and remediate the vulnerabilities. The tracking and assignment of these vulnerabilities were done manually using spreadsheets until the recent past.

The ticketless (self-service) and platform-based VM requires no manual effort. Using the shift-left approach, remediation teams and asset owners are given access to vulnerability dashboards designed specifically for them. They can analyze vulnerabilities in the assets owned by them and work on remediation accordingly. This makes vulnerability tracking error-free, providing more time to the remediation team to fix vulnerabilities.

A European postal services company wanted to reduce time, effort, and cost of its VM and remediation processes. The company leveraged Infosys' Cyber Scan platform to implement ticketless VM and establish a more secure infrastructure.

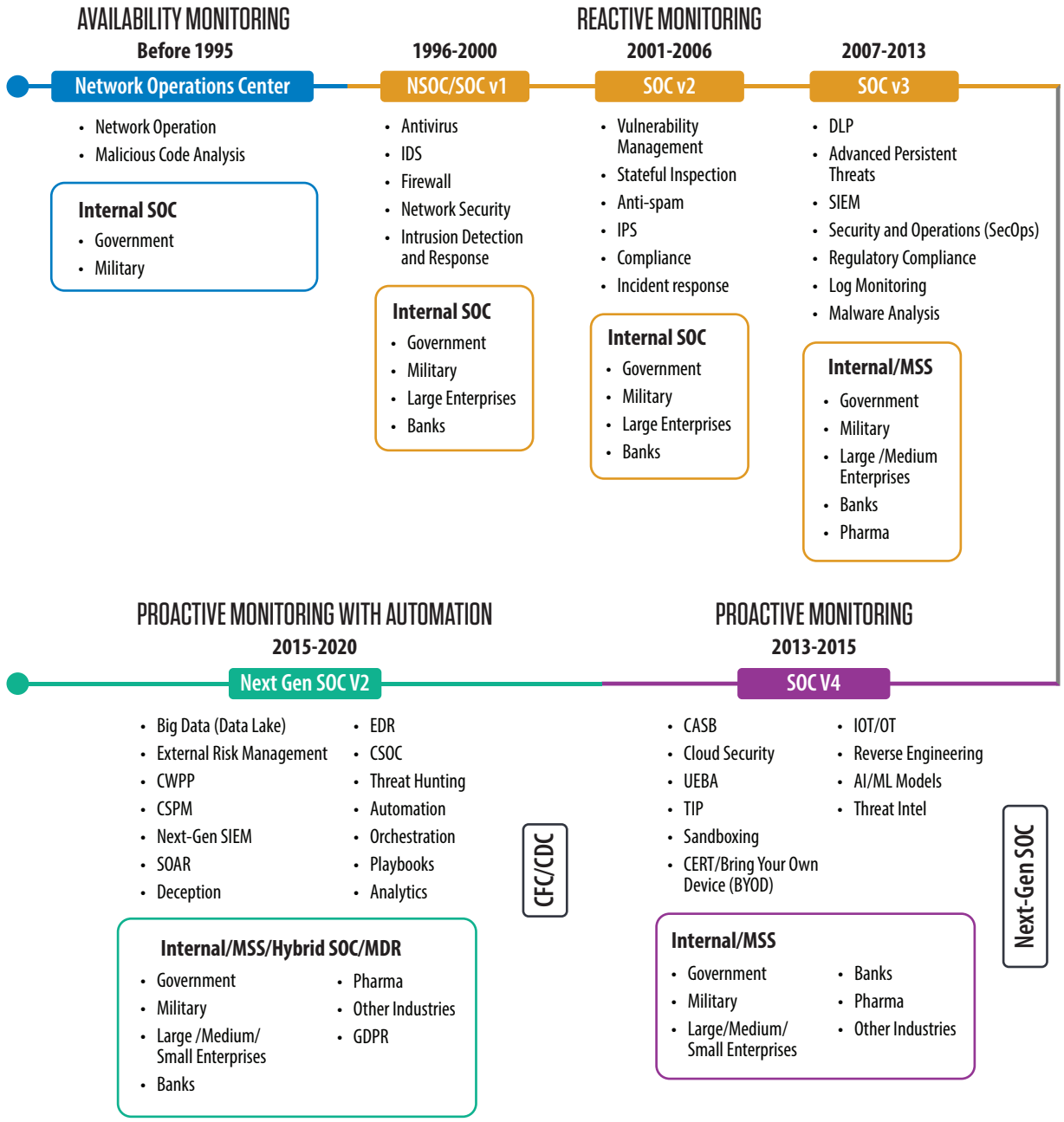
MANAGED SECURITY SERVICE - THREAT DETECTION AND RESPONSE

The cyber threat landscape is continually evolving, as the motives of threat actors shift from creating system damage to monetary benefits. Organizations have begun preparing a robust defensive strategy to protect their information assets. MSS and TDR have been in existence for a few years and are gaining momentum across all industries worldwide. Incident detection and response have become an integral part of an organization's cybersecurity program. Regulatory standards mandate the need for security operations to monitor threats.

Adopting cyber threat intelligence and hunting has bolstered security operations and enabled organizations to be proactive rather than reactive to incidents.

The current trends seen in MSS/TDR include adopting AI/ML, deception, cloud security monitoring, orchestration, and automation for rapid incident response. Organizations must follow consistent incident response procedures during incident investigations to bring efficacy.

Figure 3. Evolution of security operations centers (SOCs)



Source: Infosys

Trend 12 — Orchestration, automation, and response technology ease incident management

Incident management has traditionally been executed with defined standard operating procedures or playbooks. However, security analysts who were given these playbooks during an investigation provided inconsistent outcomes and delayed responses.

The SOAR technology has revolutionized how security operations work by establishing playbook development standards. Playbooks are broken down into smaller incident response task pieces and defined systematically to automate the response wherever possible. It has created a granular way of looking at the incident to decide how it must be investigated. SOAR platform integration with other technology controls has elevated the maturity of an organization's security operations program and enabled a mean time to detect, respond, and resolve.

> A Europe-based manufacturer developed a SOAR solution to enhance its cybersecurity investigation quality and effectiveness. The solution helps the company reduce mean time to detect (MTTD) and mean time to respond (MTTR) by enabling security alerts that could be qualified and remediated in minutes.

Trend 13 — Advanced security monitoring through cloud-specific protection programs

As organizations move their data to the cloud, security becomes vulnerable. CASB solutions can help by shadowing data and IT.

A CWPP provides the following capabilities:

- Workload configuration and vulnerability management.
- Network segmentation, firewalling, and traffic visibility.
- Workload behavior monitors — essentially EDR for servers (also referred to as host-based intrusion detection systems).
- Anti-malware scanning.
- System integrity measurement, attestation, and monitoring.
- Application control.
- Log management and review.

CSPM platforms assess cloud workloads and provide a view of the risks involved in those tenants, such as security misconfigurations, vulnerabilities, lack of encryption, improper encryption key management, and extra account permissions. With CSPM's high value, organizations have started integrating it into their DevOps processes.

> A U.S.-based financial services company wanted to setup a basic SOC monitoring system. It partnered with Infosys to setup an incident response plan and integrate log sources to Oracle Cloud Infrastructure (OCI) log analytics. This enables the company to track events and respond to any anomalies identified by the system.

INTERNET OF THINGS, OPERATIONAL TECHNOLOGY, AND 5G

Security for OT systems was not a significant consideration, mainly due to the belief that OT was an "air gapped" stand-alone system. But then Stuxnet and other similar cyberattacks happened. With a rise in attacks and the inception of the fourth industrial revolution, organizations began to understand the importance of a security framework in the OT environment to reduce the cyber risks from IoT/OT integration. Moreover, the boundaries between the OT and IT environments are getting blurred, so it is the preferred attack surface for cybercriminals and insider attacks.

IoT and OT technologies understand security requirements, system challenges, and protocols that run in this environment. This ensures the security implementation does not affect availability requirements and people's safety. These security platforms are currently capable of looking inside OT protocols, understanding security vulnerabilities, and recommending any network segmentation requirements based on the Purdue model. They also offer secure remote access, aggregate OT environment logs, and detect threats. The aggregated logs can further correlate with cyber defense centers to provide security monitoring of the OT environment and incident response. Next-generation 5G wireless connectivity and AI/ML integration will further fuel IoT/OT growth, reliably improving the intelligent data analytics, data transfer rate, coverage, and connection stability for a critical connected ecosystem.

Trend 14 — IoT and OT tools enable complete network visibility

Enterprises were finding it difficult to track and manage their critical infrastructure due to the distributed nature of assets. However, increasing attacks necessitated the demand for monitoring operational and security events and implementing a proper incident management program. Organizations mainly required visibility on IoT and OT assets, traffic, and associated risks.

Innovative technologies enable organizations to understand security threats and anomalies in the network and provide complete network visibility through passive IoT and OT traffic monitoring. Tools from companies such as Claroty, Indegy, Cisco, Forescout, and Microsoft Defender for IoT (erstwhile CyberX) assist organizations in their digitization journey by understanding the risks associated with IoT and OT integration. In addition, they help achieve effective security reviews, cyber-physical use case

implementation, and integration with next-generation firewalls, VM tools, network access control, SIEM, SOAR, and CMDB.

With the growing maturity of these tools, organizations have become more comfortable with blended active and passive scanning tools for better asset visibility. Along with the AI-enhanced cyber-physical system and organization controls, these solutions help businesses with automated risk scores and compliance against the OT industry's standards and regulations.

> An Australian mining company partnered with Infosys to manage its OT security platform to ensure continuous security monitoring and operational availability at 50 OT plants spread across Australia, Americas, and other regions. The implementation of configuration changes helped the company streamline events and incident management.

Trend 15 — Real-time security monitors help detect vulnerabilities and violations in 5G

The evolution of 5G opens opportunities for emerging technologies such as IoT-based smart meters, connected cars, augmented and virtual reality, and telemedicine with lower latency, higher capacity, low energy, high throughput, and increased bandwidth capabilities. But 5G infrastructure virtualization, network resource sharing, dynamic network topologies, and slicing introduce novel security challenges such as isolation flaws in 5G infrastructure virtualization. Adding or removing software and hardware elements in dynamic network topologies will introduce unknown attack vectors, causing network security violations. Organizations are looking for innovative and secure technology solutions to manage these security challenges and obtain real-time visibility, among other benefits.

In 5G, security monitors help detect vulnerabilities, security policy violations, and abnormal behavior, and they provide security metric stats. Tools such as Trend Micro, Nokia's NetGuard Adaptive Security Operations, Palo Alto's K2-Series next-generation firewall, and Mobileum's signaling firewall ensure the security and protection of 5G networks, services, and subscribers. To secure 5G networks, solutions must protect the fronthaul, backhaul, and data center from complex network attacks such as DDoS and brute force.

> A U.S.-based telecommunications company wanted to secure communication in a 5G ecosystem. Infosys helped the company manage security services to continuously detect, monitor, and manage the associated risks in 5G telecom devices, data, and integrations.

CLOUD SECURITY

Lack of confidence in the cloud's ability to provide security delayed its adoption. However, the continuous, innovative, and dedicated efforts of cloud and security solution providers effectively addressed the concern.

Initially, the cloud environment employed few controls to address security risks. The approach was simplistic and included extending the controls and tools from the data center with legacy monitoring tools. These tools were modified to monitor and manage in the cloud environment. Now, cloud-compatible security tools and guardrail policies are available from cloud-native and third-party OEM-based solutions. Native solutions are highly integrated into cloud platforms, and third-party security solutions provide niche and advanced security functionalities. The right balance of both has brought the SBD principle to the forefront, providing the right confidence to enterprises. Cloud platforms are based on application programming interfaces that provide great flexibility to embed security, not only in the build phase but also in a codified manner.

Trend 16 — Secure landing zones gain prominence for cyber resilience and security as a built-in culture

Enterprises are increasingly adopting public cloud platforms such as Amazon Web Services (AWS), Azure, and Google Cloud Platform (GCP). However, distributed models of these cloud environments have become a newer security issue for enterprises. Multiple accounts or subscriptions are created based on departments (e.g., marketing, sales, HR, IT) or criticality (e.g., production, nonproduction, sandbox, test). Full authorization and administration are provided at the resource, resource group, or subscription/account level.

The enforcement of standardized security across multiple environments (e.g., subscriptions, accounts, projects) through guardrails and centralized security controls ensures cyber resilience across distributed enterprise clouds and creates security as a built-in culture. Centralized security controls include identity

and access management, logging, encryption, network security, etc. Secure landing zone architecture and approach provide these functionalities from the foundation to operations.

> A leading American food manufacturing company partnered with Infosys to design and build a foundational cloud on GCP, following the secure landing zone approach. The provisioning of GCP organizational policies to native and third-party security controls was done through codification based on HashiCorp's Terraform, ensuring faster delivery of the environment and secure cloud from day one.

Trend 17 — Cloud security as code ensures continuous compliance in production

A wide range of security solutions is natively available from cloud service and cloud security-focused providers. However, these providers need to employ the latest advancements and strengthen the implementation framework to empower developers to use cloud services without compromising security controls.

Now, it is a mainstream practice to codify the security of cloud services and policies and embed them into DevSecOps and rugged DevOps. These practices emphasize the shift-left approach of cloud security to codify it in the software engineering and provisioning life cycles. Provisioning and configuration management tools from cloud service providers and open tools such as Ansible and Terraform codify security policies and controls such as cloud IDAM, Key Vault firewalls, etc. Tools such as HashiCorp's Sentinel and Pulumi help codify organizational security policies. These codified security controls should be part of the CI/CD pipeline to ensure security misconfiguration is avoided early and validated with security-testing DAST solutions that ensure continuous compliance in production.

> A leading American automotive company wanted to automate its infrastructure setup and security configuration "as code." It involved meeting software requirements, establishing necessary cloud security controls, and integrating SailPoint Identity IQ into its DevOps pipeline. Following the implementation, the company achieved fully compliant resources on AWS in under 30 minutes.

DATA PRIVACY

Technological advancements risk the data privacy of individuals. Organizations enact new privacy laws and strengthen existing ones to address associated risks. They are implementing integrated privacy frameworks that comprise global and local privacy laws.

Earlier, compliance requirements primarily focused on local privacy laws and manually conducting assessments and privacy operations. Later, organizations started implementing renowned standards that included BS10012, ISO27701, the NIST privacy framework, and comprehensive privacy laws such as GDPR and CCPA.

Trend 18 — Integrated frameworks and privacy technologies enable effective data protection

Automated privacy assessments use privacy-enabled technologies to efficiently assess cloud, IoT, OT, AI, big data, and surveillance systems. Organizations should establish a PbD policy to embed privacy throughout the life cycles of technologies, from the early design stage through deployment, use, and ultimate disposal or disposition. Organizations are increasingly using quantum cryptography, differential privacy, and homomorphic encryption to protect data in a complex IT and cloud environment.

> An engineering, procurement, consulting, and construction company wanted to build a universal policy framework that could comply with all major laws and regulations across geographies. Infosys helped the company prepare a universal privacy framework, accommodating all the unique requirements under identified laws and the NIST privacy framework.

Glossary

Abbreviation/Acronym	Full Form
AI	Artificial intelligence
AWS	Amazon Web Services
BYOD	Bring your own device
CASB	Cloud access security broker
CCPA	California Consumer Privacy Act
CDR	Cloud detection and response
CERT	Computer emergency response team
CI/CD	Continuous integration/continuous delivery
CIO	Chief information officer
CISO	Chief information security officer
CMDB	Configuration management database
CSOC	Cyber security operations center
CSPM	Cloud security posture management
CWPP	Cloud workload protection platform
CXO	Chief experience officer
DAST	Dynamic application security testing
DevOps	Development and operations
DevSecOps	Development, security, and operations
DDoS	Distributed denial of service
DLP	Data loss prevention
EDR	Endpoint detection and response
ERP	Enterprise resource planning
GCP	Google Cloud Platform
GDPR	General Data Protection Regulation
GRC	Governance, risk, and compliance
HIPAA	Health Insurance Portability and Accountability Act
IDaaS	Identity as a service
IDAM	Identity and access management
IDS	Intrusion detection system
IoT	Internet of things
IPS	Intrusion prevention system
IRM	Information rights management
IS	Infrastructure security
ISF	Information Security Forum
IT	Information technology
MFA	Multifactor authentication
MITRE ATT&CK	MITRE Adversarial Tactics, Techniques, and Common Knowledge
ML	Machine learning
MSS	Managed security service
MTTD	Mean time to detect
MTTR	Mean time to respond
MXDR	Managed extended detection and response
NDR	Network detection and response
NIST	National Institute of Standards and Technology
OCI	Oracle Cloud Infrastructure
OT	Operational technology
PbD	Privacy by design
SaaS	Security as a service
SAST	Static application security testing
SBD	Secure by design
SDLC	Software development life cycle
SecOps	Security and operations
SIEM	Security information and event management
SOAR	Security orchestration, automation, and response
SOC	Security operations center
SSL	Secure socket layer
TDR	Threat detection and response
TIP	Threat intelligence platform
TLS	Transport layer security
VM	Vulnerability management
VPN	Virtual private network
VRM	Vendor risk management
XDR	Extended detection and response
ZTNA	Zero-trust network access

Advisory Council

Vishal Salvi
SVP, CISO, and Head of Cybersecurity

Mohammed Rafee Tarafdar
SVP and Chief Technology Officer

Prasad Joshi
SVP, Emerging Technology Solutions

Lakshmi Narayanan Kaliyaperumal
VP, Head of Information Security

Kumar M. S. S. R. R.
AVP, Cybersecurity

Shambhulingayya Aralelemath
AVP, Cybersecurity

Contributors

Abhishek Hegde

Amit Gulati

Amit Kadam

Darshan Singh

Kishore Susarla

M Sujatha

Mohit Jain

Nakul Sawant

Naresh Choudhary

Nitin Bajpai

Ramakrishna GR

Sangamesh Shivaputrappa

Sanjay Krishnan

Sanjay Mohan

Santosh Neelakantan

Sesha Turimella

Shahidhussian Sayyed

Shrikrishna Manjarekar

Surendra Nemani

Suresh Selvaraj

Varun Jain

Vijayakumar Kudaka

Producers

Ramesh N
Infosys Knowledge Institute
ramesh_n03@infosys.com

Abhinav Shrivastava
Infosys Knowledge Institute
abhinav.s08@infosys.com

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