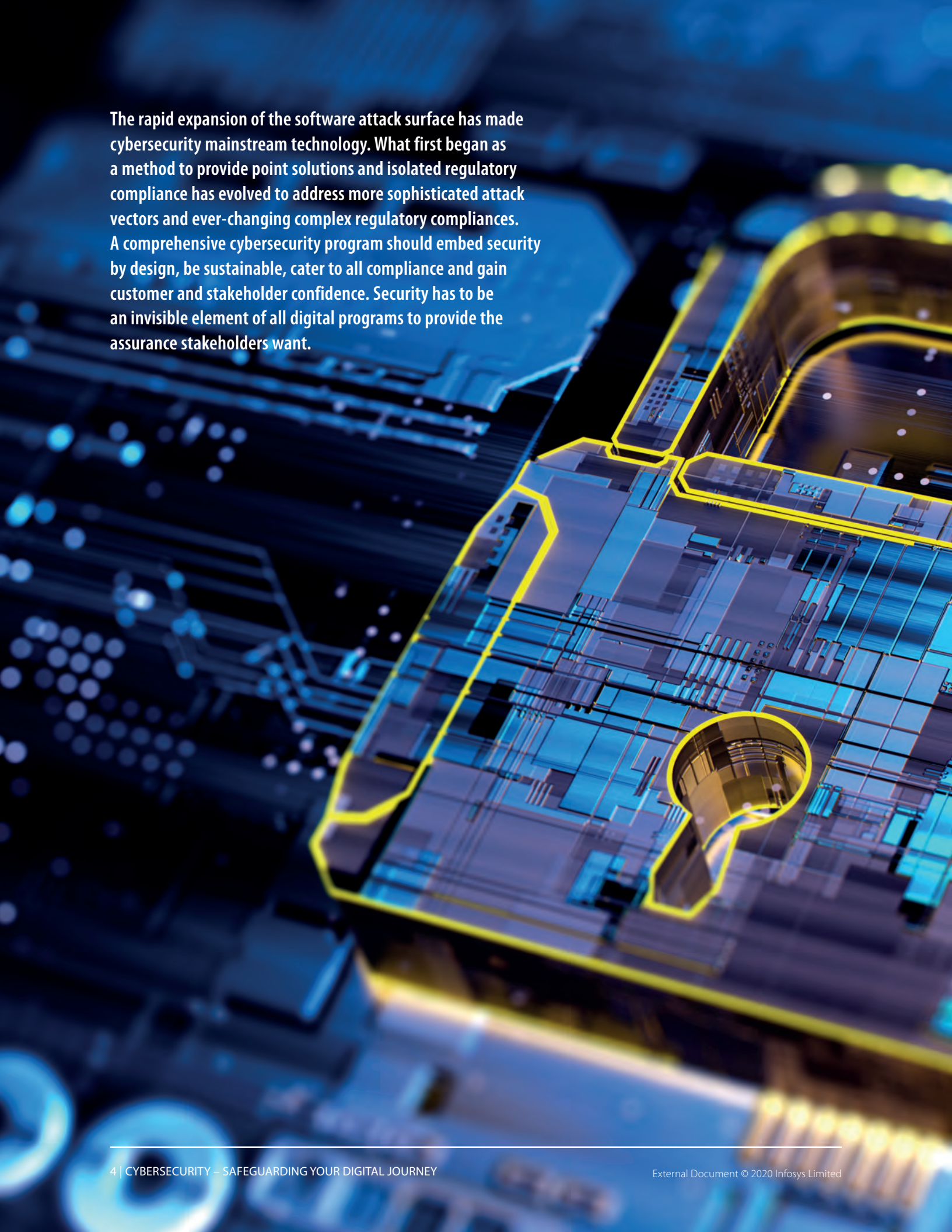


CYBER
SECURITY –
SAFEGUARDING
YOUR DIGITAL
JOURNEY



Contents

Cybersecurity's evolution to counter attacks	5
Infrastructure security	8
Identity and access management	10
Data security	12
Governance, risk management and compliance	14
Vulnerability management	16
Managed security services and threat detection and response	18
Internet of things, operational technology and 5G	20
Cloud security	22
A triple helix solution for ever-evolving threats	24
Advisory council and contributors	25



The rapid expansion of the software attack surface has made cybersecurity mainstream technology. What first began as a method to provide point solutions and isolated regulatory compliance has evolved to address more sophisticated attack vectors and ever-changing complex regulatory compliances. A comprehensive cybersecurity program should embed security by design, be sustainable, cater to all compliance and gain customer and stakeholder confidence. Security has to be an invisible element of all digital programs to provide the assurance stakeholders want.

Cybersecurity threats have advanced dramatically in the last 20 years. The cybersecurity industry has responded with a wide range of regulations, frameworks and controls, as well as tools and platforms to counter them. Regulatory compliance like BS-7799/ ISO 27001 was developed between 2000 and 2008 – an era dominated by antivirus, firewall and VPN solutions. Between 2009 and 2014, these technologies evolved further to give rise to application-aware firewalls, unified threat management, deep packet inspection, malware analysis and more. It also brought forth the NIST framework and ISF standards of good practices. More recently, from 2015 until 2018, technology, as well as the regulatory and privacy compliance landscape saw rapid growth. It brought the inception of big data analytics, DevSecOps, MITRE ATT&CK framework, web application firewalls, threat intelligence and threat hunting, to name a few. From 2019 to today, we see zero-trust frameworks, blockchain technology and the Internet of Things gain traction, as well as container security, breach attack simulation and NDR/CDR solutions.

The evolution of cybersecurity is business-driven. With the increase in the threat landscape due to ransomware, phishing attacks and other cybercrimes, expectations from stakeholders have increased to adopt cybersecurity as an early lifecycle of any technology. COVID-19 amplified the situation. When many in the global workforce had to work remotely, the attack surface increased. And, with the increased threat landscape, adversary capabilities also grew to orchestrate cyber-attacks and breaches. To counter this, cybersecurity now focuses on the efficiency of controls, predictability of costs and constant innovation and evolution. Security by design, cyber hardening, reduced risks and assured quality, managed services, as well as innovation and automation, are expectations from stakeholders in any cybersecurity program.

Today, workspace transformation, cloud adoption, digital transformation and borderless architecture are the focus of cyber defense programs. Digital technologies like 5G, software-defined networking, artificial intelligence (AI)/machine learning (ML), blockchain, big data and open source are also rising.

A strong cybersecurity program also demands compliance with existing and new regulations. Regulatory laws like general data protection regulation (GDPR), the California Consumer Privacy Act of

2018 (CCPA) and the Health Insurance Portability and Accountability Act (HIPAA) are driving global baselines on data protection and privacy practices. The focus now is on an all-round cybersecurity program governing, not only for technology but also for compliance, which is sustainable, reduces risks and enhances customer confidence.

Cybersecurity's evolution to counter attacks

During cybersecurity's evolution, the most advancements have been made across the following cybersecurity domains: Infrastructure Security; 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); Internet of Things (IoT), Operational Technology (OT) and 5G; and Cloud Security.

Infosys cybersecurity experts focused this analytical study on the three horizons of cybersecurity's evolution.

Horizon (H1): In the initial decade of cybersecurity transformation, periodic business workload monitoring helped organizations evaluate security controls implementation effectiveness, their configuration and operations and their technical security metrics. While in the software development lifecycle (SDLC) phase, their source code assurance approach subverted their adversaries' attempts to exploit the flaws in the application code and affect the end systems.

Horizon (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 managed security operations lifecycle with scalability and agility. This requirement-specific approach allows customers to benefit from both cloud-native and external security solutions while providing context-rich visibility, security governance and compliance in a multi-cloud environment.

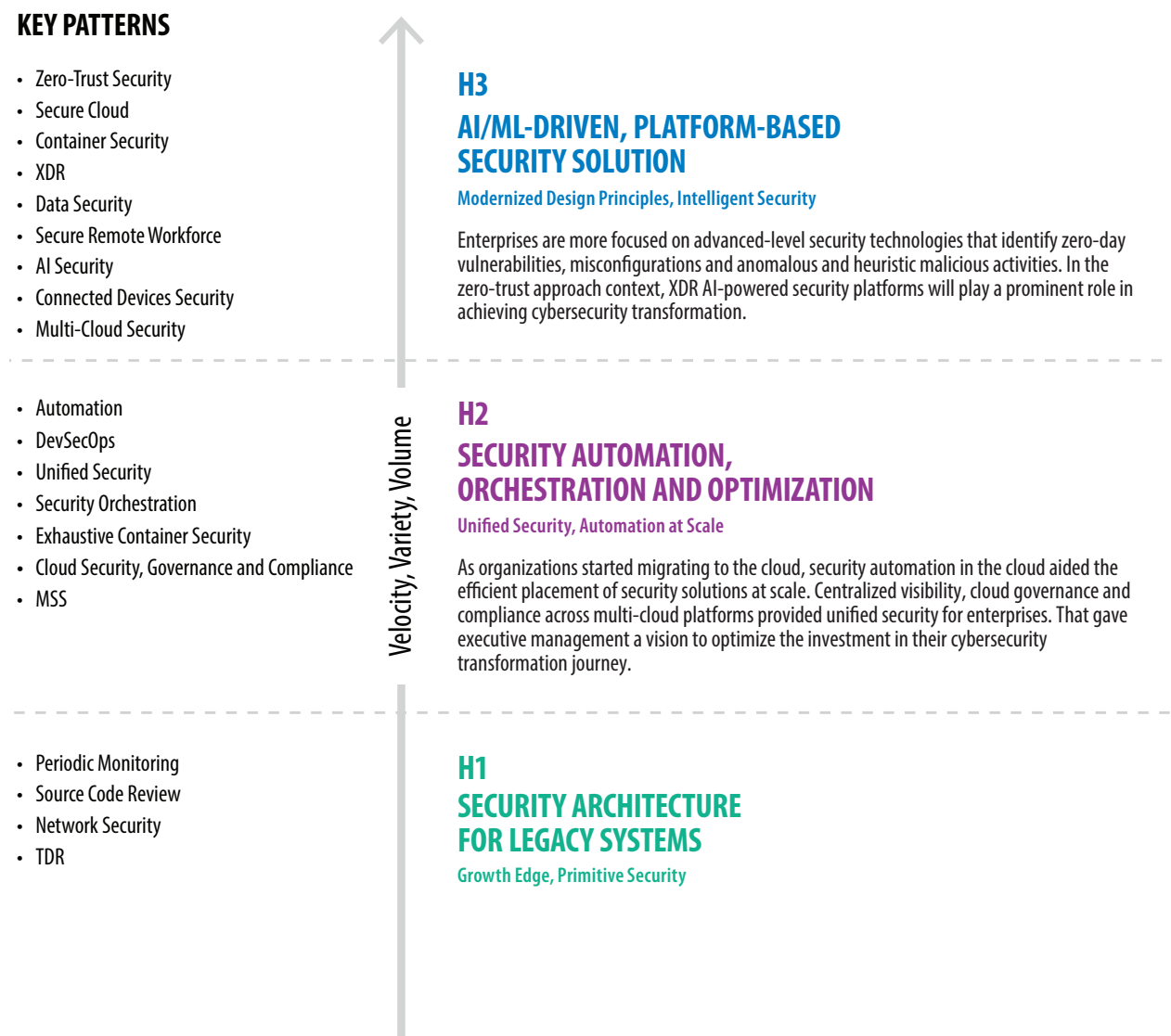
H2 offers unified security for containers, serverless computing, CI/CD integrations in DevSecOps, security

orchestration, integrated governance and underlying cloud platform ecosystems.

Horizon (H3): In H3, cloud-native, external vendor security solutions supporting a zero-trust approach will be the mainstream focus for organizations. Unlike endpoint detection and response (EDR), extended detection and response (XDR) carries cross-layer threat detection and response capabilities to provide data visibility across networks, device endpoints, analytics and more to address sophisticated threats. Passive and

agentless IoT platforms will empower the connected devices ecosystem, provide real-time visibility and offer AI/ML-based analytics to deliver actionable insights and reduce infrastructure risk with zero impact. Cloud customers need to rethink their strategy with cloud security posture management (CSPM), a cloud workload protection platform (CWPP) and cloud access security broker (CASB) solutions to address the future of cloud security and eliminate reliance on traditional, on-premise security approaches.

Figure 1: Adapting to market dynamics: the three horizons



Source: Infosys

Let us explore the key trends across each domain:

1. **Infrastructure Security**
2. **Identity and Access Management**
3. **Data Security**
4. **Governance, Risk Management and Compliance**
5. **Vulnerability Management**
6. **Managed Security Services and Threat Detection and Response**
7. **Internet of Things, Operational Technology and 5G**
8. **Cloud Security**

Figure 2. Key trends across cybersecurity subdomains



Source: Infosys

INFRASTRUCTURE SECURITY



With increased cloud adoption and off-premise hosting, the exposure of information assets for enterprises has widened. Enterprises have begun implementing security controls to provide a holistic view of the threat landscape. These controls have also given them the ability to detect real-time threats and fine-tune their security control configurations to isolate, remediate and prevent threats.

Since 2017, there has been a drastic increase in ransomware attacks. These attacks have impacted many enterprises with significant business outages, productivity losses, data and system recovery costs, as well as monetary losses from fulfilling ransom demands. Traditional antivirus tools failed to prevent many ransomware attacks because they lacked functionality and were too complex for remote workforce use. Organizations began mandating the adoption of advanced AI- and 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 – Legacy security controls are transformed with a secure access services edge framework

Software-defined wide-area network adoption is already at high speed with many of our customers. By replacing legacy multi-protocol, label-switching, wide-area networks, the secure access services edge (SASE) framework transforms the security controls toward the edge. Our analysts predict that 80% of organizations will be SASE framework compliant by 2024. This journey entails shifting to an “as-a-service” model with the SASE framework to yield better ROI, robust security and reduced complexity. The SASE framework also

gives chief experience officers (CXOs) a single-pane view as all the technologies within SASE will have full integration.

In the past, enterprises used to acquire, deploy, configure and build the security controls in their data centers, public cloud and private cloud as needed within limited pre-defined data center locations. Users then consumed these security controls irrespective of their geographical location. This traditional model

required high dependency on the hosted sites of the security controls, which resulted in network latencies and, in turn, a poor user experience.

Almost every security control technology provider has started investing and building their capabilities to have either all the SASE security controls in their offerings or have them in their list as a partnered offering. They are also committing roadmaps to bring them into a single management pane with tighter integration to meet the defined SASE framework. Many enterprises have started adopting the SASE framework, choosing security-as-a-service while adopting the latest security controls such as zero-trust access networks, CASB solutions and others.

Infosys provides consulting and advisory services to enterprises to transform their legacy network and security controls to a SASE framework. They have started this transformation for a few customers, including a major healthcare service provider in North America, an energy customer in Germany and a consumer goods organization in the United Kingdom.

Trend 2 – Extended detection and response provides cross-layer security across the enterprise

XDR tools allow a security incident detection and response platform to consume the data from endpoints, network devices and security devices. This cross-layer security supports automated AI and

ML actions that protect multiple vectors – from apps and data to end users – from security attacks.

In the past, security incident and event management (SIEM) tools were used to correlate security logs from sources like endpoints, antivirus agents, network devices, security devices and applications to detect and identify security incidents. Security orchestration, automation and response (SOAR) tools were used to automate responses to the incidents utilizing user-defined playbooks.

XDR tools support SIEM and SOAR tools by utilizing AI and ML to build context-based correlation rules around threat intelligence and execute the appropriate remediation actions without intervention from a security analyst.

However, an XDR toolset is limited to single-technology provider tools. This poses a challenge for enterprises with multi-vendor security tools, which is why XDR technology providers have started expanding their interoperability to provide wider coverage soon.

Architects recommend the adoption of cloud platform-based XDR tools to reduce the overhead that comes with traditional deploy, configure, and manage approaches.

Infosys has helped several enterprises transform their security controls to XDR, including an energy and utilities enterprise in Europe, and a healthcare provider and packaged food company in North America.

IDENTITY AND ACCESS MANAGEMENT



Identity is a crucial business function and there has always been a need for managing access to information (data) to the identities. The core objectives to manage identities were fulfilled by installing processes to ensure the right users have access to the right set of information at the right times. Mapping to the technology standards for accelerated user provisioning enabled authentication and authorization for the accessed information (applications/systems). The functional blocks in IDAM were implemented as point solutions to cater to disparate policies of federated business units within an enterprise and focused on managing access for enterprise workforce users.

As businesses expand globally, IDAM has become more complex, while the pointed solutions (legacy/home-grown IDAM) have become less effective. The scope of identity personas has expanded to include enterprise workforce, vendors, partners, customers and non-human identities (e.g., bot identities). IDAM now focuses on five goals: establishing holistic governance across on-premise and cloud infrastructure, managing risk posture through automated provisions 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. In essence, the modernization in IDAM is reducing compliance risks and allowing users to manage identity controls.

Trend 3 – Strengthened access governance brings greater transparency

The modernized needs of digital transformation require strengthened identity and access governance solutions to establish transparent access across on-premise, hybrid and cloud-hosted applications and infrastructure assets. This strengthened governance framework provides:

- A single-pane view into who has access to what across on-premise and cloud infrastructures

- The ability to dynamically monitor and remediate access risks across the landscape
- Continuous compliance management aligned with regulatory requirements
- A defined, contextual access control framework and segregation of duties enforcement

As organizations modernize their IT landscape, they need to establish visibility across tiers of structured

and unstructured data, as well as on-premise and cloud infrastructure assets. Likewise, the advent of IoT/OT devices requires more modern processes for overseeing non-human identities that manage such devices. To do this, enterprises must converge intelligent application gateway (IAG) processes for IT and IoT/OT landscapes and establish a human-device relationship to enforce access authorization with appropriate visibility across such data sets.

The following principles must be established to cater to the needs of access governance for modernized enterprises:

- Implementation of a holistic, risk-aligned access control framework that is role- or policy-based
- Continuous user access review and risk remediation
- Interoperable identity standards for data interchange across federated access systems
- Processes for dynamic risk analysis and compliance with regulatory standards, leveraging user and entity behavior analytics capabilities within an enterprise

Such capabilities can be delivered through next-generation IAG-focused tools such as SailPoint Identity IQ, Saviynt SSM and Microsoft Azure AD.

Infosys has helped a major U.S.-based financial services company transform and strengthen their identity and access governance framework. We established a technology framework for the rapid onboarding of applications, setting up a privileged access management solution framework and providing holistic access governance across the enterprise landscape.

Trend 4 – A zero-trust security model maintains identity as a core component

A zero-trust model establishes that the legacy approach that involves inherently trusting services, individuals or devices within the corporate network is

flawed. Zero trust maintains that all users or devices, irrespective of their access location, be authenticated and authorized to access the requested applications or services.

Thus, the traditional, perimeter-bound security principle is modernizing to a foundational zero-trust security model, with identity at the core. The evolution of a zero-trust security model encompasses:

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

When designing a zero-trust model, the principles mentioned above – with identity at the core – should be considered for securing access to enterprise applications and services, whether they are set up on-premises or in the cloud.

Some of the industry-leading tools which can help deploy a zero-trust identity model include offerings from Microsoft Azure AD, PingID, Okta and CyberArk, to name a few.

Infosys has helped a major U.S.-based non-alcoholic beverages company achieve cloud transformation by migrating their identity controls to the Azure cloud, remediating their access management solution to allow Azure AD single sign-on and multi-factor identification, installing privileged access management through CyberArk and progressively improving their cybersecurity posture with the adoption of zero-trust security principles.

DATA SECURITY



At one time, data security focused on perimeter-based protection with limited encryption usage, especially for drives and application-level secure sockets layer (SSL)/transport layer security (TLS) protection. If any, database protection was limited to the native vendor-provided encryption capabilities such as SQL and Oracle TDE, often managed by the DBA group.

With the wide adoption of social media, mobile, analytics and the cloud came the concept of zero trust, which has led to data security technologies maturing both in depth and coverage. As data moved to these different landscapes, the focus shifted to data-centric protection (protecting the data where it resides) while both in transit and in use.

Advances in other technologies such as blockchain, ML, homomorphic encryption and multi-party computing are now used in data protection, merging the protection of data at rest, in transit and usage.

However, none of these technologies can provide transformational data protection capabilities for enterprises without a coordinated data governance process that ensures policies are applied uniformly. An infonomics focus on quantifying the value of data is expected to further drive data security governance investment decisions in the coming years.

Trend 5 – Integrated data protection and classification tools enhance security at all touchpoints

Data loss prevention (DLP) tools protect data on-premises on endpoints (when in use), during transit (network) or at rest (on storage). DLP can be integrated with a CASB to ensure the same DLP policies are applied to cloud-hosted data. User entity behavior

analysis (UEBA) capabilities in 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 like 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 SIEM tools for correlation and incident detection so that the central security operations team can act as needed.

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

Trend 6 – Data encryption with key management becomes a best practice in cloud protection

Encrypting all sensitive data in the cloud helps prevent inadvertent access to other tenants or CSPs. However, key control needs to be with the organization. Key management-as-a-service (KMAAS) is a best practice

wherein keys from vendors such as Thales can be used along with cloud-native encryption capabilities. There are three benefits KMAAS provides: local encryption key management in Thales, the segregation of duties for better data protection hosted in the cloud and, lastly, the ability to shred the keys, which destroys the data at the end of life. Currently, Microsoft Azure employs Thales e-Security HSM, while Amazon Web Services uses Cavium HSM.

For protecting data on SaaS applications, CASBs are used. This technology provides a combination of data protection in transit with proxy integration and data at rest with API integration. CASB audit capabilities help discover a shadow IT environment to support standard governance policies implementation. Most industry-leading CASB solutions can be integrated with on-premise DLP solutions to extend current protection policies to the cloud. This combination extends the enterprise's own IT governance policies and government regulations to third-party software and storage in the cloud between the cloud service consumers and cloud service providers.

A global investment company headquartered in Singapore began a cloud-first strategy that included public cloud, private cloud and multiple SaaS applications. Infosys designed and implemented their end-to-end data protection using a Symantec DLP for on-premises and integrated it with a CASB solution to extend similar protection to SaaS and IaaS. A CASB audit helped discover a shadow IT environment, while an AI-based UEBA helped identify access anomalies and prevent security incidents.

GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE



GRC for information security relies on the definition of frameworks, policy design and ongoing governance to protect the enterprise as technologies are introduced and as business and external threats change. Most GRC tools focus on providing integrated risk management across the enterprise and automating processes. There are still multiple white spaces in the market and Infosys, in partnership with Cybernext and Living Labs has developed multiple tools in this area. Infosys' Cyber Gaze, for example, is a cyber metrics management platform filling a gap in the current market.

GRC technology innovations offer real-time dashboards for better visibility supporting governance, supply chain risk management, enterprise-wide risk quantification and trend analysis. Tools such as RSA Archer, MetricStream, ServiceNow GRC and IBM OpenPages provide support for automated compliance assessments, while platforms like CyberCompass help integrate the process and technology controls for enterprise-wide visibility.

Trend 7 – Greater focus is placed on supply chain security and vendor risk management

As organizations increasingly collaborate with partners and outsource work, the risk of compromise also increases in the supply chain. A single weak link can impact an organization's security and reputation. Multiple high-profile third parties have experienced breaches, including consumer retailer Target, showing any business could be at risk.

VRM is a comprehensive approach to identify the different vendors an organization has relationships with and the cyber risks they are exposed to. VRM tiers the risk of each vendor and then tracks and mitigates

these risks. VRM also vets potential suppliers before they are approved as vendors.

Multiple regulations, including GDPR, put the onus of VRM on the organization, holding them responsible for any breaches or data loss.

GRC automation platforms such as RSA Archer, MetricStream and ServiceNow provide integrated VRM capabilities. Most solutions are now available in the cloud and 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. Others, like BitSight and RiskLens, provide continuous vendor assessments using publicly exposed assets and information on the dark web. We expect to see more integration across tools and automation through AI and bots to reduce the efforts and costs of VRM.

For a leading packaged food retailer in the U.S., Infosys defined their VRM process and the vendor tiering criteria to create tier-specific security assessments that met the organization's 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 – Cyber metrics lead security governance enabling enterprise-wide stakeholder collaboration

As cyber threats increase and organizations deploy multiple security tools, chief information security officers (CISOs) struggle to understand the impact of their security posture and track the effectiveness of their initiatives. Transaction systems such as SIEMs provide only a snapshot of their current 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 requires understanding and input from multiple groups and stakeholders beyond the IS or IT teams. This is possible with well-defined cyber metrics that support data-driven governance and provide specific improvement inputs to each team. The ability to drill down to specific periods and business units/geographies also helps executives measure and track the effectiveness of the control implementations across the organization.

Most organizations use manual spreadsheets and PowerPoint slides to track cyber metrics, making the process cumbersome and unreliable. Similarly, it takes time and resources to develop a cyber metrics management tool using reporting and analytics platforms. To combat this challenge, Infosys developed Cyber Gaze.

A leading U.S.-based healthcare service organization was using traditional spreadsheets to manage metrics, so Infosys implemented the Cyber Gaze platform to help the CISO, CIO and IT leadership track and perform trend analysis of more than 160 cyber metrics. The flexible platform allows for quick implementation of new metrics as new cyber controls are implemented, allowing agility that was not available before. This platform can be used to collaborate across the CISO 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 when implemented and effectively managed. VM technology and processes handle the identification, prioritization, governance and treatment of weaknesses throughout the infrastructure, network and application layer threat surfaces.

A large number of vulnerabilities make it difficult for enterprises to prioritize the most critical fixes. Timely remediation requires support from business and IT teams with conflicting priorities, which creates effectiveness challenges for VM teams.

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

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. With ERP solutions now exposed to the internet and the cloud, there is an increase in hacker activities. While ERP vendors have native solutions, there are niche solutions from vendors like Onapsis that provide end-to-end protection of business-critical ERP solutions.

Trend 9 – Secure by design adoption embeds security early and ensures digital trust

Secure by design is the concept of identifying security requirements upfront and during the architecture definition and design phases, and then ensuring that security is verified during the build and test phases before go-live. Similarly, regulations for privacy such as GDPR mandate the concept of privacy by design,

which ensures consent is captured and managed via data collection. The personally identifiable information (PII) data captured requires protection from breaches and unauthorized access or usage and must be destroyed when no longer needed.

Organizations are developing enterprise-level security policies, design frameworks, guidelines and checklists, along with approved tools and components for usage across the organization. Established gating criteria and governance processes ensure that security is built into every technology initiative with any exceptions tracked for closure.

Secure architecture reviews and threat modeling helps to identify design and architecture flaws. DevSecOps adoption enables the identification and closure of weaknesses during the development and operation phases to improve product quality and reduce time to market. Organizations need a central team in place to provide white-listed components, as well as vet and approve any new open-source components teams wish to use.

Vendors like MS 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 secure by design and secure SDLC.

A global software platform and services provider looked to strengthen their product security implementation processes. Infosys partnered with them to enable secure by design via an SDLC implementation for their product development lifecycle. DevSecOps was implemented for automated scans with continuous monitoring and support to reduce the cost of security inclusion and enable developer self-help.

Trend 10 – ERP on cloud adoption leads to a greater focus on business-critical ERP application security

ERP systems have been fundamental enablers and the epicenter of business. For decades, SAP and Oracle have been the largest ERP players. With enterprise assets and data collected, processed, analyzed and reported through ERP systems, they have been the target of frequent breaches. These threats have only increased with ERP applications moving to the cloud.

Given the nature of these applications, it is critical to detect and prevent unauthorized changes and configurations that expose an ERP's vulnerabilities. Hence, holistic business-critical application security or ERP security is now a priority for CXOs.

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

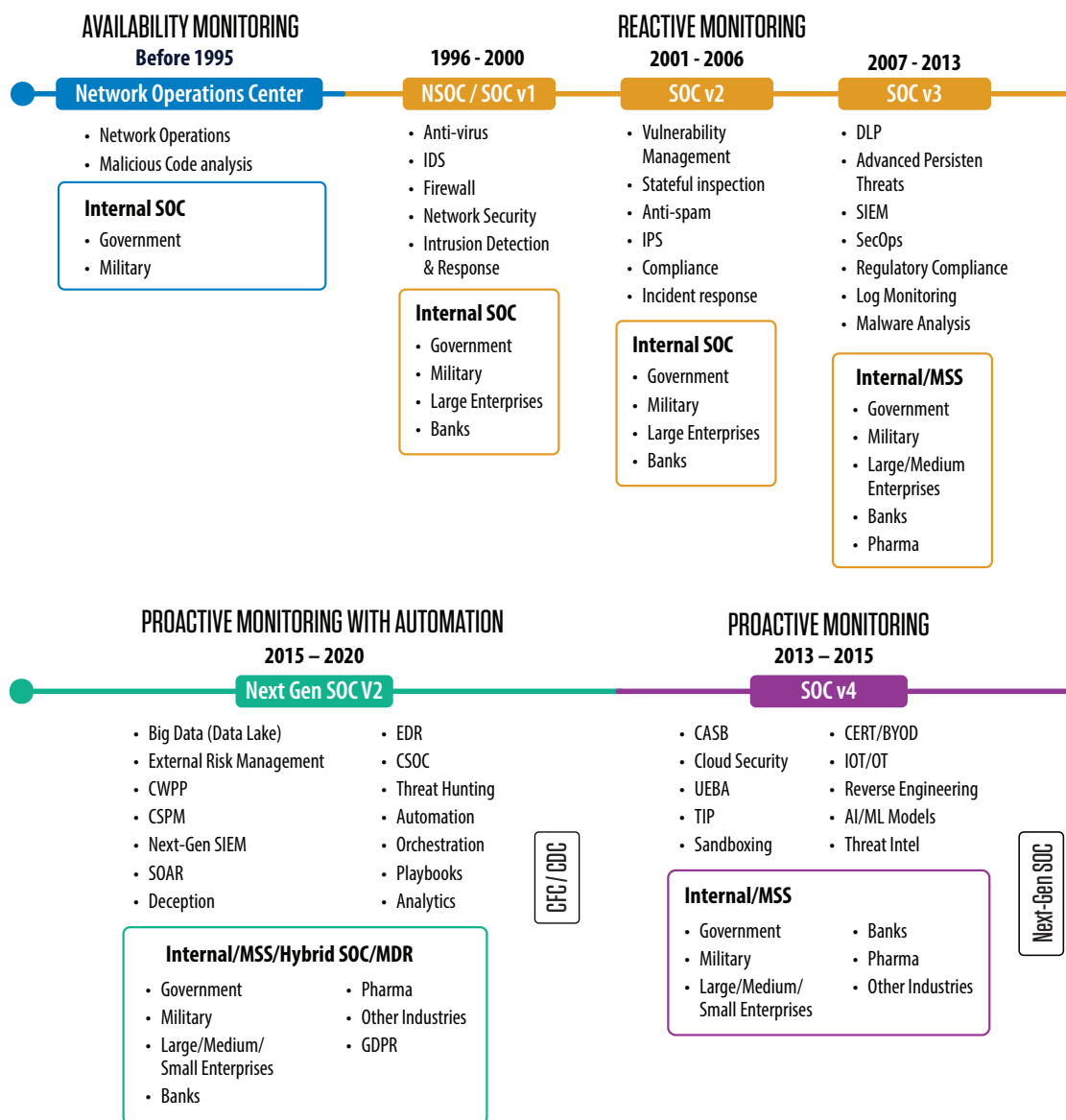
Infosys helped a leading U.S.-based pharmaceutical company improve their SAP ERP security posture and reduce the cost of compliance by implementing the Onapsis platform and integrating an ITSM tool. Resulting benefits include continuous vulnerability scanning and alerts, improved workflows and compensating controls to maintain compliance between audits.

MANAGED SECURITY SERVICES AND THREAT DETECTION AND RESPONSE

The cyber threat landscape is continually evolving as the threat actors' motives shift from creating system damage to monetary benefit. As such, organizations have begun preparing a robust defensive strategy to protect their information assets. MSS and TDR have been in existence for a few years but are gaining momentum across all industries worldwide. Incident detection and response has 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 threat hunting has bolstered security operations and enabled an organization to be proactive rather than reactive to an incident.

Figure 3. Evolution of Security Operations Center



Source: Infosys

The current trends seen in the MSS/TDR include adopting AI/ML, deception, cloud security monitoring, orchestration and automation for rapid incident response. There must be a consistent incident response procedure followed across the incident investigation to bring efficacy.

Trend 11 – Orchestration, automation and response technology revolutionizes 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.

SOAR technology has revolutionized the way security operations work by bringing a standard to playbook development. Playbooks are broken down into smaller incident response task pieces and are 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, mean time to respond and mean time to resolve in a matter of minutes.

Infosys has helped one of its customers deploy and manage its security operations with SOAR, which has benefited the organization with increased investigation quality and effectiveness. The systemic implementation has led to significant manual workload reductions.

Trend 12 – Cloud-specific protection programs provide advanced security monitoring

Traditionally, an organization's data resided in its physical data center, where security controls were deployed and monitored. Now, as they move their data to reside in the cloud, its security is in question regarding who is accessing the data, how it is accessed and who is sharing the data. CASB solutions can help by shadowing data and IT.

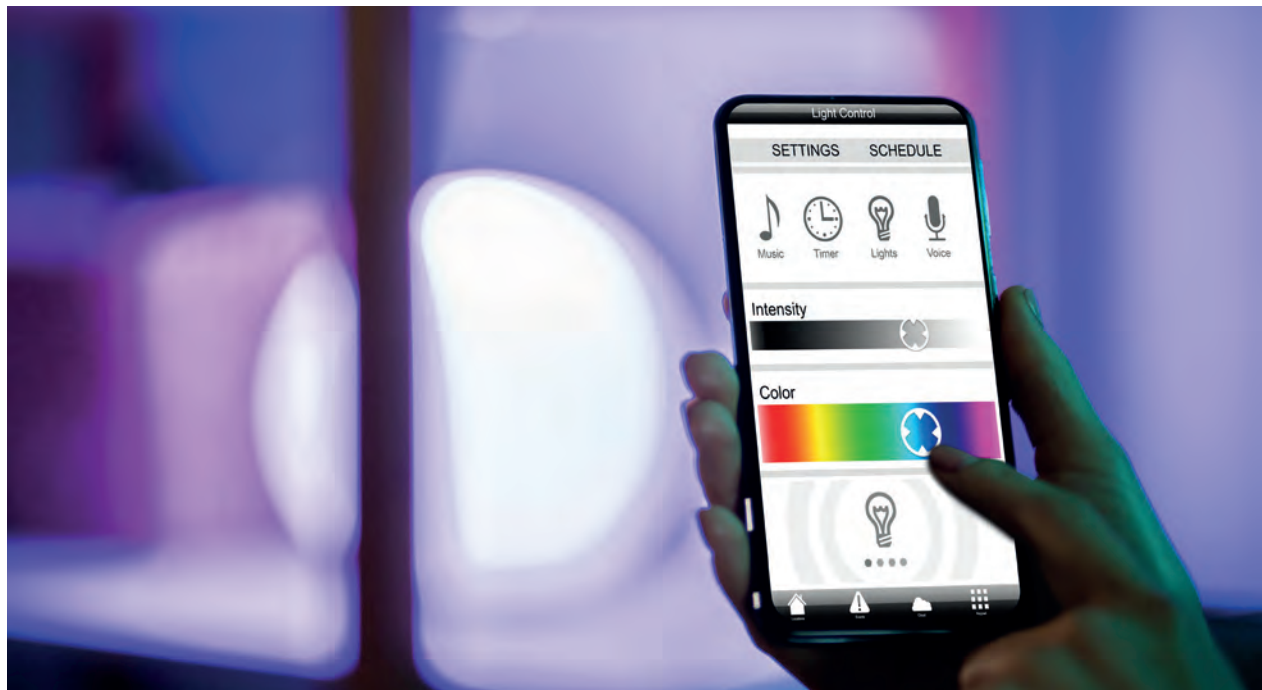
A CWPP provides multiple capabilities, including:

- 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 risk involved in those tenants, such as security misconfigurations, vulnerabilities, lack of encryption, improper encryption key management, extra account permissions and more. With CSPM's high value, organizations have started integrating it into their DevOps processes.

Infosys helped one of its customers with CWPP implementation and monitoring, which has strengthened the cloud instances and lessened threats. We enabled comprehensive hybrid cloud reviews and threat detection and integrated CWPP with a SIEM platform for incident response.

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” standalone system. But then Stuxnet and other similar cyber-attacks happened. With an increase in attacks and the inception of the fourth industrial revolution, organizations began to understand the importance of adopting a security framework in the OT environment to reduce the cyber risk from IoT/OT integration.

In the initial stages, most organizations started performing security assessments to identify the risks in their IoT and OT environment. They implemented physical security measures to restrict access, such as endpoint security using antivirus, secure communication of IoT sensors to platforms using SSL/TLS and basic device authentication and authorization of IoT devices. Now, we see tools and technologies designed for the IoT and OT environment that understand the 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 and improves an organization’s overall security maturity. 5G wireless connectivity and AI/ML integration will fuel IoT growth, reliably improving the intelligent data analytics, data transfer rate, coverage and connection stability for a critical-connected ecosystem.

Trend 13 – Complete network visibility is enabled with tools that track operational technology

Main requirements from organizations included the visibility of IoT and OT assets, traffic and associated risk. The distributed nature of the assets made it difficult for enterprises to track and manage their critical infrastructure. The increasing attacks against their infrastructure necessitated the demand for monitoring

operational and security events and implementing a proper incident management program.

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

like Claroty, Indegy and 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, CMDB and more.

With these tools' growing maturity, organizations 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 OT industry standards and regulations.

Infosys helped an Australian mining company manage its OT security platform to ensure continuous security monitoring and operational availability at 50 OT plants spread across Australia, America and other regions. Infosys helped implement configuration changes that streamlined the events and incident management. Infosys ensured the overall performance and availability of their OT security platform.

dynamic network topologies and slicing introduce novel security challenges like isolation flaws in 5G infrastructure virtualization. In dynamic network topologies, the addition or removal of software and hardware elements 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 to detect vulnerabilities, security policy violations and abnormal behavior and provide security metric stats. Tools like Nokia's NetGuard Adaptive Security Operations, Palo Alto's K2-Series next-generation firewall and Mobileum's signaling firewall ensure security and protection of 5G networks, services and subscribers.

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

Trend 14 – Real-time security monitors detect vulnerabilities and violations in 5G

The evolution of 5G opens exciting doors for emerging technologies like IoT-based smart meters, connected cars and telehealth with lower latency, higher capacity, low energy, high throughput and increased bandwidth capabilities. But 5G infrastructure virtualization, network resource sharing,

CLOUD SECURITY



It took time for the cloud to become prevalent, and a primary reason for the delay was a lack of confidence in the cloud's ability to provide security. This concern has been addressed through continuous innovative and dedicated efforts from cloud and security solution providers.

In the initial stages, 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 that were modified to monitor and manage for the cloud environment. Now, cloud-specific security tools are available that are more efficient and intelligent, enforcing policy and compliance-based deployment for resources to ensure "secure by design" adherence at the first stage.

Trend 15 – Cloud security as code

A wide range of solutions for security are available from cloud service providers and cloud security-focused providers that employ advanced technology. However, a dramatic change in implementation is needed if they want to empower developers to consume cloud services without compromising the implementation of security controls.

Today, it is 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" of cloud security to codify it

in the software engineering and provisioning life cycle. Provisioning and configuration management tools from cloud service providers and open tools such as Ansible and Terraform, codify security controls such as firewall rules and subnet. Tools such as HashiCorp's Sentinel and Pulumi help in codifying 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.

Infosys partnered with a leading American automotive company to automate the infrastructure setup and security configuration “as code” with pre-requisite software installation, necessary cloud security controls, SailPoint Identity IQ integrated into DevOps pipeline. This provision the fully compliant resources on AWS in under 30 minutes. SailPoint IIQ builds, validation and deployment on different environments is easy with full automation “as code” and upgrade of IIQ is achieved in 20 minutes.

and policies for almost all known frameworks. In addition, effective security operations, automation and technologies such as EDR, next-gen firewall, SIEM and SOAR solutions provide effective security incident management and response handling.

With a lack of defined boundaries, a “context-aware zero trust” model will form the basis of identity and access management of cloud resources. As such, providers are rolling out monitoring solutions to provide AI- and ML-based threat detection and protection capability.

Infosys partnered with a major telecom company in the APAC region to launch new capabilities to its customers. The capabilities were built on Azure Cloud and the security operations were built on Azure Sentinel to monitor the security events from Azure Cloud and on-premised systems. Infosys ensured smooth security events monitoring and response with dashboards and AI and ML capabilities to address every use case.

Trend 16 – Context-aware and intelligent security technology emerges

Compliance and regulatory requirements are a big challenge in hybrid clouds. Today, these requirements are addressed through advanced and intelligent platforms from CSPs and specialized third-parties like Prisma Cloud that provide ready-to-use templates





A triple helix solution for ever-evolving threats

We see the threat landscape continually evolving. Every stakeholder's demand for comprehensive security stems from their customers' desire for safe and secure business operations. A strong cybersecurity program helps businesses meet their regulatory requirements depending on the industry sector, data sensitivity and location of the business operations. With the right mix of people, processes and technology, a well-designed cybersecurity program ensures that sensitive data will be appropriately handled and any breaches or attacks will be responded to quickly – all without interruption of services. Hence, the onus to deliver such a strong cybersecurity program lies with businesses and requires a long-term, futuristic approach for all cybersecurity domains. Infosys is committed to providing their customers thought leadership and a strategic view for all the cybersecurity towers so that businesses can focus on their respective domains and maintain customer confidence.

Advisory Council

Vishal Salvi

SVP – CISO & Head of Cyber Security

Mohammed Rafee Tarafdar

SVP and Unit Technology Officer

Prasad Joshi

SVP, Emerging Technology Solutions

Lakshmi Narayanan Kaliyaperumal

VP – Group Manager, Information Security

Kumar M. S. S. R. R.

AVP, Cyber Security

Shambhulingayya Aralelemath

AVP, Cyber Security

Contributors

Abhishek Hegde

Amit Gulati

Dinesh Matta

Jagadamba Krovvidi

James Zhen

Karthik Andhiyur Nagarajan

Kishore Susarla

Lakshminarayana Indraganti

M Sujatha

Manoj Kuruvanthody

Mohit Jain

Naresh Choudhary

Neel Kuruvemula

Nilby Jose

Nisha K P

Nitin Ainath Tagalpallewar

Nitin Bajpai

Rajeshwar Shende

Ramakrishna GR

Sangamesh Shivaputrappa

Sanjay Krishnan

Sanjay Mohan

Sesha Turimella

Shahidhussian Sayyed

Shrikrishna Manjarekar

Soumitri Mishra

Srinivasa Kumar L

Suresh Selvaraj

Venkatesh Sampath

Vijay

Vijayakumar V V Kudaka

Yogesh Shelke

Producer

Ramesh N

Infosys Knowledge Institute
ramesh_n03@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.



For more information, contact askus@infosys.com



© 2020 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/or any named intellectual property rights holders under this document.

