VIEW POINT

HOW TO MODERNIZE 3 CRITICAL CYBERSECURITY FUNCTIONS

Strengthen protection for access, endpoints, applications, and data with Infosys expert managed services and Microsoft security technologies

Gold
Microsoft Partner
Azure Expert MSP
Microsoft

Infosys®
Navigate your next

Modernizing Security for Digital Business

Maintaining a strong cybersecurity program is a growing and continual challenge for any business that strives to become more digital. No longer is IT simply focused on perimeter-based security where all access is tightly governed from inside the firewall.

The IT environment is spread across a mix of on-premise and cloud solutions. Users and their multiple devices need to access business applications and data from their home offices. And SaaS and mobile applications are as equally woven into business data and workflows as IT-managed Windows applications.

With these factors driving your move to digital business, traditional approaches to security leave you vulnerable to untraditional threats. The security technology behind a digital business is a particular challenge. Many last-generation tools—such as for security information and event management (SIEM) or mobile device management (MDM)— cannot deliver the security visibility and response measures needed now.

Worse, it's becoming harder and more expensive for most IT organizations to maintain their own tools, staff, and operations for security management. Top security talent is in high demand, making it particularly difficult to hire and retain experienced staff.

Instead of lagging behind, your business can benefit from outsourcing all or parts of the security program.

By choosing to work with an experienced partner like Infosys, your business can realize:

Stronger security measures based on the latest Microsoft technologies

Hard-to-find expertise for security solution design

Higher efficiencies for security management

Cost savings difficult to achieve on your own

As a Microsoft global system integrator partner, Infosys offers expertise through consulting, managed services, and technology solutions in three critical areas of a strong security program.

Identity and Access Management solutions verify every identity to protect access to your networks, applications, and data

Data Security solutions support robust, end-to-end threat detection and response management

Endpoint Management solutions protect corporate data while simplifying employee mobility and supporting intelligent devices

89% of IT heads say they increasingly need to rely on trusted advisors to help navigate new technologies, processes, and methodologies.[1]

Identity and Access Management

Managing Access When Your Network Is Everywhere

Infosys Managed Security Services and Microsoft Azure keep application and data access in control.

Today, employees, contractors, suppliers, business partners and even customers are accessing the network from many places and devices, over countless types of connections. Once inside, those users need to access sensitive data and tools that are spread across multiple servers, applications, and cloud platforms.

Together, these factors make it vital to safeguard user identities and their associated access privileges from the theft and misuse that can lead to data leakage.

Yet how can you be confident that users are who they say they are, devices are safe, and that all application and data access attempts are authorized? How can you get the right users the access they need without inadvertently opening a door for a malicious attack?

These are the core questions behind a critical framework for cybersecurity: Identity access and management (IAM). With the goal of verifying identities and privileges for every access, a robust IAM framework combines technology with monitoring and management services to protect networks, applications, and data.

A Framework for Identity and Access Management

At Infosys, we plan and design an IAM framework through a structured process that encompasses:

- Assessing the readiness and implementing security controls at each layer of the Azure platform
- Configuring processes, policies, and rules for identity lifecycle management across on-premise and cloud resources
- Automatically provisioning appropriate access for all users and devices, including privileged access
- Setting up processes for fine-grained, multi-factor authorization and delivering single sign-on and role-based access control capabilities across different channels
- Establishing a governance framework for compliance with enterprise security and regulatory requirements
- Establishing privileged access governance to manage access for the most critical and sensitive systems
- Continuously monitoring and assessing risks for on-premise and cloud resources

This IAM framework is based on the strengths of Microsoft Azure technology and Infosys services for ongoing management.

Technology:

Azure Active Directory

Active Directory is an enterprise identity service for managing access by internal and external users to a company's resources in Azure. Features for single sign-on and multi-factor authentication grant access to applications while helping to protect and govern access to IT resources.

40 percent of IT leaders say cybersecurity jobs are the most difficult to fill.[1]

Services:

Identity and Access Monitoring and Management

An ever-changing threat landscape creates high demand on any cybersecurity operation. And given the challenges of hiring and retaining security staff, your IT organization may not have the in-house knowledge and capabilities needed to keep up. For this reason, many companies look for an outsourcing solution that can strengthen key security elements such as identity management.

By working with Infosys as a managed services partner, our clients gain these essential IAM management capabilities and expertise.

Infosys services are offered through multiple security defense centers and more than 600 consultants who have the skills and experience to design and implement an IAM framework.

Infosys IAM Consulting and Managed Services

- IAM advisory consulting
- Identity governance and administration
- Access and privileged access management
- Consumer authentication and governance
- Managed services for identity and access management
- Risk analytics

Data Security

Keeping Up with Cybersecurity Threats

Infosys Managed Security Services and Microsoft Azure Sentinel deliver timely alerts to support effective response.

As more of your business activity becomes digital, cybersecurity becomes even more critical to protecting revenues, reputation, and customer trust. Are your security systems and operations keeping up?

A traditional system for security information and event management (SIEM) may not easily scale or adapt to meet today's security demands. And if you have an in-house Security Operations Center (SOC), you know how hard it can be to find and retain expert staff.

Overcoming these challenges will take a new approach to threat detection and monitoring. It's an approach that combines the best technology for logging and analyzing threats with expert managed services for your security operations.

A New Solution for Threat Detection and Monitoring

The strategic Infosys and Microsoft collaboration combines the strength of the Microsoft product portfolio and Infosys services to help enterprises effectively profile cybersecurity risks and manage threats comprehensively.

This alliance is focused on building robust systems, platforms, and solutions for end-to-end threat detection and response management across hybrid infrastructures. The goal is to help our enterprise clients remain secure, compliant, and trusted.

One-third of surveyed CIOs indicated that security and risk management are the top driver of their IT spending.[1]

Infosys threat monitoring solutions deliver several essential capabilities.

- Microsoft Azure Sentinel as the SIEM system to improve logging and processing for security alerts and data streams
- User and entity behavior analytics (UEBA) to detect threats that may not be recognized by simple monitors and alerts
- Integration of threat intelligence and automated analytics to provide actionable information on easy-to-understand dashboards
- Architecture and design to improve threat detection logging as well as cloud security monitoring
- An effectively structured and staffed SOC for 24x7 threat monitoring, analysis, and trending, as well as incident logging, management, and response

Technology:

Microsoft Azure Sentinel

Microsoft Azure Sentinel is a powerful, cloud-native SIEM solution to detect, prevent, and respond to data threats across the enterprise. An Infosys solution uses Azure Sentinel to collect data across on-premise systems and multiple clouds, apply Microsoft threat intelligence, and respond to incidents rapidly with built-in automation of common tasks. Azure Sentinel also offers advanced artificial intelligence (AI) and security analytics for smarter threat detection and investigation at scale.

Infosys was named winner in the Managed Security Services Provider/Threat Detection and Response Disruptor Category at the Microsoft Security 20/20 Partner Awards.

Services:

Infosys Cyber Next Platform

The Infosys Cyber Next Platform delivers comprehensive managed security services to our clients from global Cyber Defense Centers.

These centers are staffed by more than 100 expert consultants in threat management services and more than 200 consultants skilled in SOC implementation and managed services.

Infosys managed security services are coupled with the real-time threat intelligence that enhances Azure Sentinel SIEM data. Our threat intelligence labs contribute research on new threat-detection technologies as well as zero-day vulnerabilities and attack frameworks.

Additionally, Infosys consulting services offer advice on architecture and best practices for a threat monitoring solution, as well as planning and implementation for migration from an existing SIEM system.

Infosys Threat Detection and Management Services

- Consulting to design, build, and manage a Microsoft Azure Sentinel implementation
- Outsourced SOC for incident response and management
- Managed security across a public or hybrid cloud

Endpoint Management

Managing Security On Every Device

Infosys Managed Security Services for Microsoft 365 and Microsoft Endpoint Manager strengthen security on mobile devices, IoT sensors, and more.

The devices accessing your network are no longer limited to corporate-issued laptops and mobile devices, safely under IT's control. Today, there are employee-owned smartphones and tablets, IoT sensors, and other edge nodes. Mobile devices are critical for enabling employees to work productively anywhere by accessing data and applications in the cloud. And IoT devices are increasingly important for improving operations and opening opportunities for digital business.

If your IT team is like most, you struggle with securing mobility and managing endpoints in order to protect data and there are and maintaining regulatory compliance.

Modern Security for a Modern Workplace

The modern workplace needs a security solution that protects corporate data while also simplifying employee mobility and supporting intelligent devices. A solution that will protect access to corporate applications and data, whether they are stored on-premise, in the cloud, or on a mobile device. A solution that designs and implements security technologies carefully to achieve the right balance of protection and simplicity for the user experience.

Technology:

Microsoft Endpoint Manager

Use Microsoft Endpoint Manager (which includes Microsoft Intune) to securely manage iOS, Android, Windows, and Mac OS devices.

This cloud-based endpoint management solution streamlines and automates device deployment, provisioning, policy management, updates, and data wipes when needed. You'll control access to sensitive business applications and data even without requiring manual device enrollment by employees or partners.

Services:

Infosys Endpoint Security

Managing endpoint security requires advanced capabilities that can be deployed across a diverse and complex device ecosystem. Infosys offers consulting, implementation, and managed operations that strengthen your security program end to end.

Service features include:

Workplace security consulting, definition of a technology roadmap and rollout strategy, and change management support

Implementation and migration of a new endpoint security solution

Ongoing operations for endpoint management, software updates, help desk services, and security governance

Also important is assuring that software-as-a-service tools are properly secured for use by mobile devices. Infosys security services for Microsoft 365 manage access and protections for these core business applications as well as files stored on Microsoft OneDrive.

Infosys Consultingand Managed Servicesfor Endpoints

- Microsoft Endpoint Manager and Intune design, implementation, and managed operations
- Microsoft 365 implementation and security

The Infosys and Microsoft Partnership

Infosys and Microsoft have a rich legacy of partnership spanning over 15 years. As partners, our goal is to bring together our complementary strengths to deliver specialized capabilities, industry solutions, and services that will help our customers and empower every person and every organization to achieve more. We want to not only enhance the value that our customers realize from their technology investments, but help identify business opportunities in a forward-looking, proactive manner.

Infosys achievements include:

- Among the top three Global System Integrator partners for Azure
- Microsoft Azure Expert Managed Services Provider for native and hybrid cloud environments
- More than 1000 certified Azure consultants
- Awarded 2019 Microsoft Global Alliance SI Partner of the Year for exceptional Microsoft-based solutions

Multiple Fortune 500 clients have already benefited from the advantages of our services and solutions for managing cybersecurity.

Visit www.infosys.com to see how outsourcing to Infosys can modernize security management in your business.

For more information, contact askus@infosys.com

Navigate your next