
FIS
Microsoft
WHITE PAPER
CYBERSECURITY IN THE CLOUD
How to secure your entire cloud journey

EXECUTIVE SUMMARY

Cloud services have changed the face of business, offering scalability, efficiency and cost savings not available with on-premises IT infrastructure. The cloud makes it easier for organizations to manage the ever-increasing amount of data passing through their systems, helping teams communicate and collaborate across different locations. By enhancing the ability to access and manage information, the cloud has introduced a new way of approaching productivity and security – and has transformed how we work.

In the past decade, we've seen organizations transition from an onsite IT model to moving some services to the cloud, to transferring all services to the cloud. A hybrid IT environment spanning on-premises and cloud infrastructure is not uncommon. Almost every organization today has some presence in the cloud, from using email in the cloud to using a business application as an SaaS service. In fact, Gartner predicts that 95% of new digital workloads will be deployed in cloud-native environments by 2025. Businesses that haven't adopted cloud in some shape or form are lagging behind and spending significantly more in IT expenses compared to their peers.

The proliferation and adoption of cloud-based services has not only increased efficiencies, but also reshaped the landscape of cybersecurity. Managed service providers (MSP) offering extended detection and response (XDR) services have emerged as a critical component of business operations both as core and supplementary providers of cybersecurity services.

In this paper, we'll discuss the cloud cybersecurity challenges facing today's businesses, the trends FIS® and Microsoft® have observed through providing, managing and securing one of the world's largest cloud platforms, Azure, and the solutions we offer to combat rising threats.

Cybersecurity risks and challenges

As demand for cloud services has increased in recent years, so has the risk of unauthorized access to data. **Phishing attacks and social engineering tactics** are common, granting cyberthieves multiple points of entry to sensitive data in the cloud. With the average cost of a data breach in the U.S. at $9.44 million, organizations cannot afford to cut corners on cybersecurity.

Misconfigured cloud settings and unpatched vulnerabilities top the list of factors that weaken the security of cloud solutions, leading to unauthorized access, account hijacking and data breaches. Organizations that fail to properly configure their cloud solutions are at a greater risk of a breach; 27% of organizations have experienced a security incident in their public cloud infrastructure within the last 12 months. Of these, nearly a quarter (23%) were caused by security misconfigurations in cloud infrastructure.

Yet many organizations don't have the resources or expertise to properly configure and manage cloud solutions. A survey of IT professionals revealed that only 37% track and detect resource misconfigurations in their infrastructure as a service (IaaS) framework, and fewer than half (47%) routinely scan IaaS resources for software vulnerabilities.

A **lack of people and processes** is often the greatest impediment to successfully securing cloud environments. Many organizations face resource constraints in implementing, managing and monitoring cybersecurity tools. In fact, 61% of cybersecurity professionals say it's challenging to have the right employee skillsets to deploy and manage a complete solution across cloud environments, and 53% cite ensuring data protection and privacy for each environment as a top challenge.

That said, the challenges of protecting your business go far beyond the aforementioned and include a host of other factors. Many businesses use a **fragmented cybersecurity toolkit,** which adds to the complexity of cybersecurity.

A recent survey by IBM found that organizations typically use more than 50 different security solutions and deploy 20+ different tools when responding to a cybersecurity incident. While there's a sentiment toward cybersecurity that "more is better," a piecemeal approach has many downsides, including higher costs for hardware and software licenses and decreased productivity with so many tools to manage.

Dealing with multiple solutions also makes it more **difficult to achieve satisfactory ratings on operational controls audits and regulatory examinations.** Manual tracking of data from various sources is time consuming and prone to errors. It also requires experienced and knowledgeable staff, which brings up another challenge: **lack of resources to hire, train and maintain key staff** to monitor and manage cloud solutions and cybersecurity efforts. Without knowledgeable and experienced professionals dedicated to managing the solutions, even the most thought-out cybersecurity strategy won't have the support it needs to be successful.

Many institutions also grapple with other **resource constraints** in cybersecurity management. From the inability to access solutions due to costs, to challenges with implementing and managing the technology, limitations on dedicated resources create a gap in cybersecurity management which leads to bigger issues.

Additional challenges for institutions pursuing a comprehensive cybersecurity strategy for their cloud activities include the **inability to effectively layer cybersecurity within their operations and not having back-end protection** in the event of a data breach or cybersecurity event. Cybersecurity requires multiple layers of defense to protect systems, networks, applications and data transmission. The aftermath of a data compromise is costly and time consuming and can lead to long-term damage to an institution's brand and reputation.

Seven cybersecurity trends

If ever there was a race with no ending, cybersecurity would be it. As quickly as technology advances, so do the vulnerabilities. Cybersecurity controls that are effective today are often defenseless against tomorrow's threats. To help organizations get a better grasp of their standing in the evolving cybersecurity landscape, we've outlined seven prominent trends below.

1. The cloud is a growing target for cyberattacks.

When remote work became the norm during the pandemic, adoption of cloud-based services grew exponentially – and so did the risks of a breach. A 2022 survey of IT professionals in small- and mid-sized organizations revealed how large a target the cloud has become. **More than half** reported an increase in the volume and complexity of attacks on their organization, as well as an increase in the impact of those attacks. Ransomware posed a significant threat with **67% experiencing** that type of attack.

2. False positives are a challenge in cybersecurity management.

Threat detection is crucial to identifying and mitigating compromises, yet false positives continue to be a significant distraction for cybersecurity teams that are already stretched thin. Only **33% of organizations** have the resources to detect and respond to threats, while even fewer (25%) have processes in place to respond to security threats around the clock.

3. Cloud Security Posture Management (CSPM) is critical.

Due to the dynamic nature of cloud operations connecting various networks and users, traditional security practices offer insufficient protection. By providing a single view into risk monitoring across multiple cloud environments, CSPM automates and streamlines threat detection. With centralized visibility into and control over all cloud resources, CSPM prevents misconfigurations and reduces the complexity of cybersecurity management.

4. Consumer protection efforts are influencing cybersecurity activities.

Industry mandates like the GDPR are highlighting the misuse of data and the need to secure sensitive information. This is prompting organizations to focus on protecting data against bad actors operating both within and outside their systems. It's good for business, since consumers are more aware of threats and are accustomed to cybersecurity processes like CAPTCHA tests and two-step authentication.

5. Security operations centers (SOCs) play a significant role in combatting cybersecurity threats.

As cybersecurity threats become more frequent, complex and persistent, organizations cannot rely on technology alone for protection – they need the human touch. By combining and centralizing an organization's cybersecurity resources and personnel into a single team, SOCs enable organizations to more quickly and effectively monitor, prevent, detect, investigate and respond to security incidents 24/7/365.

6. Cybersecurity is transitioning to a proactive approach.

Another reaction to the breadth and complexity of cloud security is the transition from reactive cybersecurity management to proactive threat hunting. More organizations are implementing a **zero trust** strategy that requires all users to be authenticated, authorized and continuously validated when accessing applications and data. **Honeypots** are being used to lure cybercriminals away from legitimate targets and gather information about their methods and motivations. Organizations are also employing **kill chain analysis** to identify cyber vulnerabilities and ensure sufficient controls are in place to ward off attacks.

7. Organizations are seeking a consolidated cybersecurity solution.

Due to the costs and complexities of managing multiple technologies, more organizations are seeking a centrally managed solution that consolidates, prioritizes and streamlines their cybersecurity efforts. Security vendor consolidation addresses many of the operational inefficiencies and lack of integration associated with multiple security solutions, and **three out of four (75%) organizations are pursuing vendor consolidation, up from 29% in 2020**.

Layers of protection

All these trends are pushing businesses to move toward an embedded cybersecurity solution offering **layered protection** that addresses the full spectrum of exposure. This includes misconfigurations, common vulnerabilities and exposures (CVEs), privileges and configuration drift and compliance across a multi-cloud or hybrid environment.

XDR services provide a simplified, proactive and faster approach to threat detection and response by collecting, correlating and analyzing data across multiple security layers (email, endpoint, server, cloud workload and network). Consolidating cybersecurity efforts with XDR services eases technology complexity, implementation and management and optimizes costs by reducing the number of necessary products, features and licenses.

There are two primary scenarios for layered protection. The first, organizations that have some cybersecurity services and want an additional layer of security. The second, organizations that have insufficient (or no) cybersecurity services and want an MSP to manage everything. **Microsoft estimates that half of their customers will need XDR services by 2024.**

Microsoft Azure's embedded security and the power of FIS Grade Security

With a focus on fintech and the highly-secure financial industry, FIS sees what's happening across the cybersecurity landscape before anyone else. In partnership with Microsoft, we bring "FIS Grade Security" capabilities to our clients' assets with access to the same premier tools, best practice processes and expert staff that we use to protect our own assets that help power the world's economy. All tools and services undergo regular regulatory scrutiny, and our comprehensive cyber insurance benefit offers additional protection in the event of a cyberattack.

FIS Managed XDR and the FIS Managed Security Services (MSS) suite integrate with the **Microsoft Azure** cloud platform to offer a unified, end-to-end cybersecurity solution that brings new efficiencies and capabilities to our clients' cybersecurity and cloud adoption efforts. By providing the security strategy used to guide our own cloud security initiatives, FIS and Microsoft offer the strongest counter measures to protect against cyberthreats.

An advanced managed security service, **FIS Managed XDR** provides threat intelligence, threat hunting, 24/7 security monitoring, incident analysis and incident response. It is a quick-to-implement, infrastructure-less, cloud-native, fully managed (by FIS) security solution that helps organizations of all types proactively detect and defend against cyber threats, protecting all workloads regardless of their location.

The **FIS MSS suite** is our most comprehensive cybersecurity offering, providing a broad range of cybersecurity solutions designed to protect every aspect of a business from cyberthreats. MSS includes the 24/7/365 protection provided by FIS Managed XDR, firewall and IPS management, email security and encryption, website protection and monitoring services, and much more.

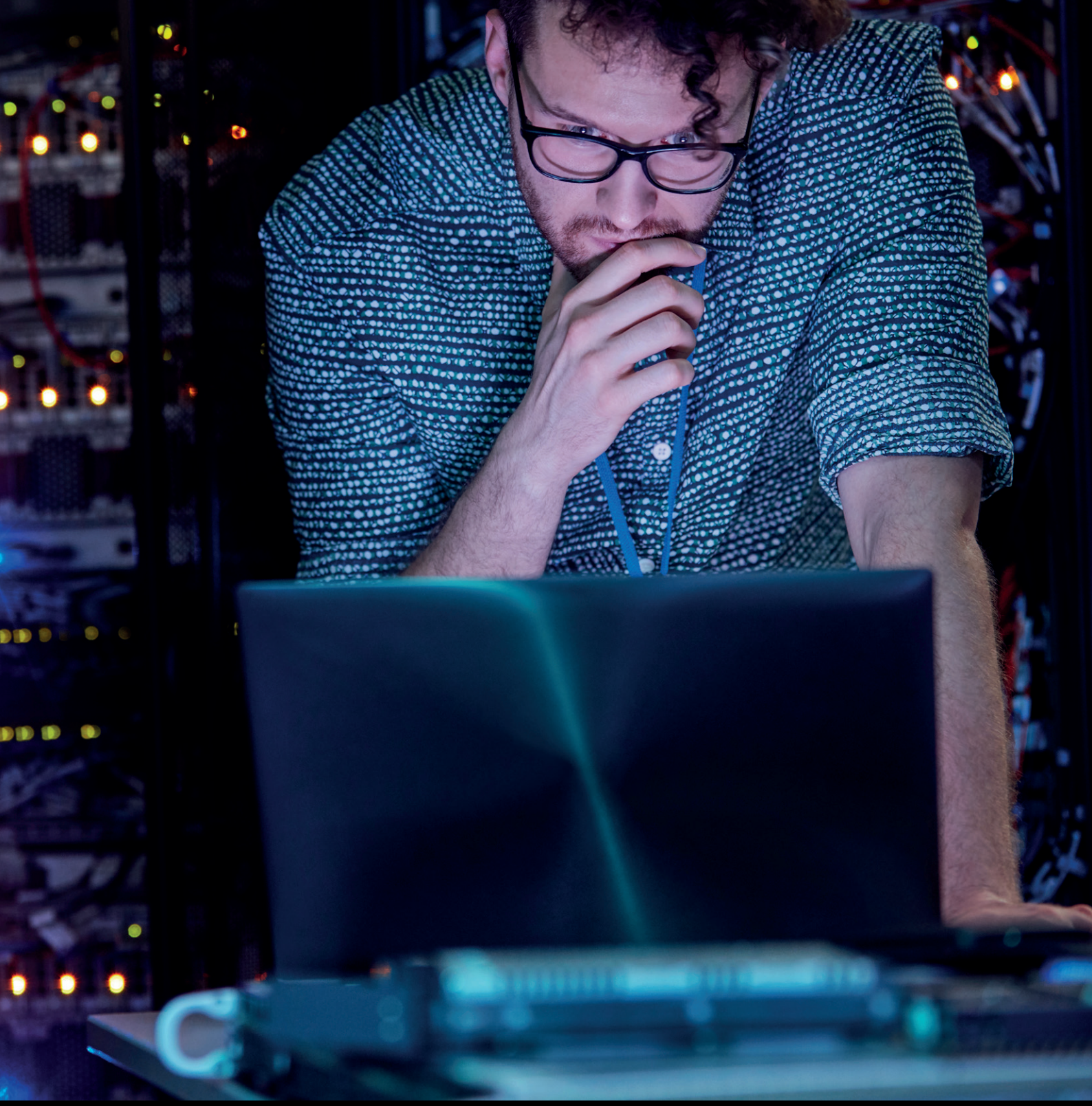
FIS Managed Cloud Services helps reduce costs, improve efficiencies and remove the burden of ongoing cloud management for clients at any point in their cloud journey. In partnership with leading cloud providers like Microsoft, we deliver an integrated, managed hosting service offering a flexible, compliant, always-on environment. We have extensive experience working with public, private and hybrid cloud environments and offer consultation services, implementation/migration services and ongoing managed support services.

Learn more about **FIS Managed Cybersecurity, FIS Managed XDR, and FIS Managed Cloud Services,** and how we can help you combat cyber threats in the cloud and beyond, here:

FIS Managed Cybersecurity Services →

FIS Managed XDR →

FIS Managed Cloud Services →



About FIS

FIS is a leading provider of technology solutions for financial institutions and businesses of all sizes and across any industry globally. We enable the movement of commerce by unlocking the financial technology that powers the world's economy. Our employees are dedicated to advancing the way the world pays, banks and invests through our trusted innovation, system performance and flexible architecture. We help our clients use technology in innovative ways to solve business-critical challenges and deliver superior experiences for their customers. Headquartered in Jacksonville, Florida, FIS is a member of the Fortune 500® and the Standard & Poor's 500® Index.

www.fisglobal.com

getinfo@fisglobal.com

twitter.com/fisglobal

linkedin.com/company/fis

FIS | ADVANCING THE WAY THE WORLD PAYS, BANKS AND INVESTS™