CYBERSECURITY: WHY IT'S TIME TO PARTNER UP

FIS MANAGED EXTENDED DETECTION AND RESPONSE (XDR)

How managed cybersecurity services are the most effective way to protect financial institutions and merchant businesses from modern cyber threats.

Greater Opportunities, Greater Threats

The past few years have seen organizations accelerate their digital transformation plans to meet the increased global demand for online services and solutions, leading to boosted profit margins and supercharged expansion plans.

However, as digital operations scale at speed, many risk being left relying on outdated security technologies not built to cope with today's complex, fast-moving threatscape. Driven by cyberattacks, data breaches, and IP theft, we've subsequently witnessed a rapid increase in attack volumes.

The increasing complexity and sophistication of security threats means organizations often have difficulty keeping up with the installation, management, and configuration of the security solutions needed to prevent threats and comply with industry regulations.

Additionally, due to cyber talent shortages and overloaded internal Security Operations Center teams, many lack access to the human resources and tools needed to adequately protect themselves. That's worrying news as cybercrime is costing companies $1.79 million per minute.[1]

[1] Forbes, 2022

Scaling up your security

Organizations looking to minimize risk and move forward with confidence require a more holistic approach to threat detection and response – one that encompasses all endpoints as well as covers the increased attack surface created by expanding networks and new cloud environments.

This guide unpacks how you can achieve this, illustrating why rolling out a modernized end-to-end cyber strategy in partnership with a trusted cyber provider can be a vital component in securing your future success.

925
CYBER-ATTACK ATTEMPTS

per organization in 2021, plus 50% more attacks per week from Q2 in 2021 vs. 2020

Source: Checkpoint, 2022

Financial Institutions:

Cyberthreat Challenges Mapped

As vital allies for businesses and their transactions across the globe, banks, credit unions, and capital markets in particular face serious threats from multiple sources.

Keeping up with security threats as bad actors develop new methods and novel vectors to breach your security measures isn't easy. While an attacker only needs to find and exploit a single vulnerability, those in charge of defending against attacks have to keep on top of all possible attack vectors.

This is compounded when top-notch security tools are expensive and require the right specialist staff to implement them. Plus, the cybersecurity skills shortage doesn't seem to be disappearing anytime soon with one in ten in-house cyber specialists exiting the industry in 2022 due to burnout.[2]

[2] Forrester, 2021 [3] Gartner, 2021

Talent gap

The 'cybersecurity talent drought' is worsening; the number of unfilled cybersecurity jobs grew by 350% – from one million positions in 2013 to 3.5 million in 2021.

Source: Business Wire, 2021

Growing fears

This combination of challenges often keeps internal security teams at financial institutions awake at night, knowing they probably don't have the necessary resources in place to deflect the risks, nor successfully manage the ever-growing number of vulnerabilities discovered every year.

Even if you can field a fully-equipped cybersecurity posture, the costs associated with managing everything internally are high. According to Gartner, global security and risk management spending was expected to exceed $150 billion in 2021; a 12.4% rise from 2020.[3]

Even companies with high-grade security firepower at their disposal aren't meeting their security objectives.

The average financial services organization has over 19 security tools at its disposal but research shows these tools tend to harm an institution's overall security stance more than help it.

Having a disparate portfolio of security tools reduces overall visibility, opening up an organization to a greater threat of attack. Only 17% of financial services organizations are able to respond to incidents more effectively while 60% experience more difficulty in determining the source of a security incident.[4]

20-30%

Projected increase in cybersecurity budgets for financial institutions this year, with XDR being a top priority.

Source: VMware, 2022

[4] IDG, 2021

81%

OF ORGANIZATIONS

were unable to integrate their security tools while 95% said that using their tools increased their level of risk.

Source: IDG, 2021

The way forward

This is why it has become increasingly important to find a partner who understands how to defend against modern cyberattacks in today's volatile threat environment. The ideal cybersecurity partner will have a cohesive spread of tools, innovative processes, and expert staff to greatly reduce the risk to your organization as well as alleviate any regulatory burdens.

Ultimately, the right partner will instill confidence that your business can overcome all current and future threats.

Merchants:

Cyberthreat Challenges Mapped

Fraud is becoming more complex with increasingly creative and sophisticated malicious actors targeting merchants in the process of digitizing.

For many merchants, the risk of payment fraud and data breaches has increased in parallel with the sharp rise in eCommerce transaction volumes and value during the pandemic. However, traditional fraud detection and prevention strategies are failing to keep up with modern threats.

For instance, there are a growing number of organizations that franchise their ransomware-as-a-service (RaaS) capabilities to attackers. This RaaS model permits more criminals to use sophisticated and 'proven' tactics, techniques and procedures to perpetrate their attacks.

Card threats

Card transactions are flourishing with the burgeoning popularity of eCommerce and online banking. Consequently, payment fraud is on the rise as well. To combat this growing menace, regulatory agencies are continuously developing and refining stricter rules and compliance protocols for you to comply with, including the Payment Card Industry Data Security Standard (PCI DSS).

However, it can be difficult to know which parts of your environment are required to be compliant, and how best to secure them. And, without proper and consistent testing processes in place, you may fall out of compliance with even realizing it.

Protecting data

Data protection is not just about using encryption, firewalls, and antivirus software. It's also about ongoing scoping, configuration, maintenance, monitoring, testing, and more. However, you may find it difficult to manage the wide-ranging security mechanisms needed to prevent fraud as well as comply with industry regulations.

This lack of expertise can lead to an over-reliance on implementing cyber tools while failing to monitor and manage them correctly to ensure they remain optimized. This represents a serious problem as automated cyberattacks — unlike IT staff members — do not need rest. Also, because it often takes just minutes for a cyberattack to infiltrate IT systems, you must now monitor your systems 24/7/365.

Huge hike

In 2020, there was an estimated **150%** increase in ransomware attacks; 2021 has seen this activity continue to spike upward.

Source: Harvard Business Review, 2021

Fresh threats

Merchants experienced more fraud in 2021 than 2020, with new types of fraud affecting **62%** of merchants.

Source: Telemedia, 2022

As a merchant, you bear the burden of protecting the private information you collect from consumers, whether you are storing or transmitting it.

This responsibility could have serious consequences if you mishandle information. And the costs of payment fraud or data breaches aren't simply financial. Customers are unforgiving of merchants who are perceived to be responsible for data breaches and hacks. Even a single instance of fraud or data theft after a transaction can make consumers defect to other merchants.

Expanding threats

With the number of cybersecurity attacks skyrocketing, it's time to get serious about clamping down on payment fraud and PCI compliance. This will ensure you have all the information and solutions you need to become more aware of the emerging risks you face, and to meet the necessary regulatory requirements.

Big losses

Over 1/3 of online merchants lose 6% or more of their turnover to payment fraud, with many also seeing increased operational expenses and customer churn as a result.

Source: Worldpay, 2021

65% OF SHOPPERS

are likely to terminate their relationships with merchants after experiencing even a single instance of data theft or payment fraud.

Source: PYMNTS, 2021

Introducing the Solution:

FIS Managed Extended Detection and Response (XDR)

At FIS, we know what it takes to protect businesses, acknowledging how hard it is to create the right processes, find the right people, and engineer the right tools.

Deploying our Managed XDR solution means you can rely on the comprehensive security expertise of FIS to control and secure your technology ecosystem, providing you with peace of mind and proactive protection. Our global team of cybersecurity professionals utilizes cutting-edge solutions to process trillions of raw security logs. This generates billions of complex events and millions of automated actions to protect you and your customers.

Thousands of organizations already trust FIS to secure their transactions and banking solutions. What if we could bring that same grade of security to your organization to keep it safe?

FIS Managed XDR:

Features

Managed Extended Detection and Response is an advanced managed security service that provides threat intelligence, threat hunting, security monitoring, incident analysis, and incident response.

Features include:

FIS Cyber Fusion Center

24/7/365 security monitoring and response capabilities

Cloud-Native SIEM Solution

Intelligent security analytics and threat intelligence across your enterprise

Cybersecurity Advisor

A dedicated cybersecurity advisor as your team's point-of-contact for technical and day-to-day service delivery

Prevent

Next generation anti-virus processes that fully protect you online and offline as well as stop malware-free and file-less attacks

Detect

Managed threat hunting, alert monitoring, triage, and protection

Investigate

Advanced investigation support to identify risk areas

Respond

Threat remediation through system isolation, persistence elimination, artifact removal, and policy tuning

What Makes FIS Managed XDR Solution Unique

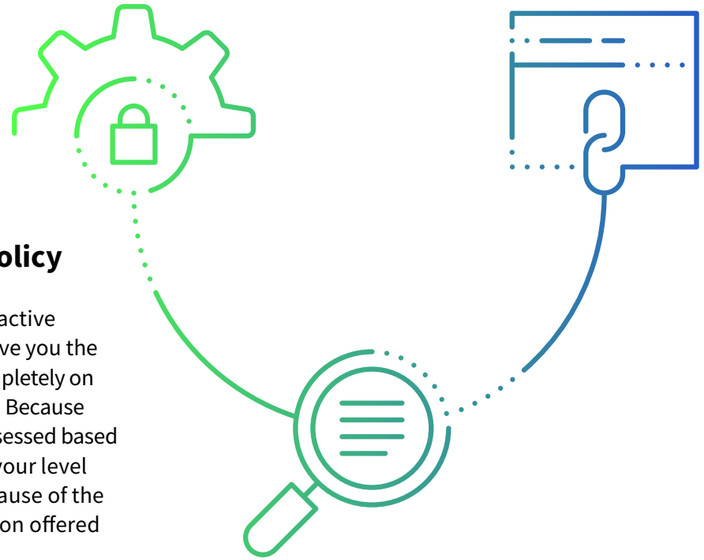
Three key reasons why our acclaimed solution stands out in a saturated marketplace:

1. FIS grade security

FIS Managed XDR represents the best-in-class prevention, detection, and response security solution for all areas of your network, endpoints, and cloud environment. Able to respond to the ever-changing threat environment with our 24/7/365 security operation, our solution stops breaches using its ability to rapidly detect, analyze, and remove threats that have bypassed defenses.

2. Heavily regulated environment

All of our services go through a rolling program of constant scrutiny coupled with regular examinations to give our clients peace of mind that their business will remain as safe as possible. Other competitors in this space are very unlikely to match our compliance expertise and level of scrutiny.



3. Cyber-insurance policy

Our cyber-insurance offers a proactive layer of protection designed to give you the confidence you need to focus completely on your business without distraction. Because cyber-insurance premiums are assessed based on the policyholder's risk level, your level will be reduced significantly because of the exceptional, recognized protection offered by FIS Managed XDR.

Key Takeaways

With FIS Managed XDR, you gain access to leading performance, trusted innovation, and flexible architecture. With our solution, you can:

- **Take advantage of a turnkey experience, using our predefined technology stack to secure all business areas from your network and cloud environment to each and every endpoint**
- **Benefit from proactive protection that enables you to always stay one step ahead of bad actors and cyber threats**
- **Easily implement our XDR tools and leverage FIS' human expertise and top-notch processes**
- **Ensure your infrastructure remains compliant and regularly tested to massively reduce vulnerability**
- **Feel safe in the knowledge that you're protected 24/7/365 by industry-best expertise, leadership, and services**

Visit our website to learn more about how we can help you stay ahead of the threats of today and tomorrow.

www.fisglobal.com/en/products/fis-managed-xdr / Email: getinfo@fisglobal.com