
FIS MANAGED SECURITY SERVICES (MSS)

INTRODUCTION

With the rise in cyber attacks over the past few years, cybersecurity must be given even greater priority in the financial services market and beyond.

However, many organizations are struggling to keep pace with rapidly evolving threats and compliance issues, leaving them exposed to potentially extreme financial and reputational damage.

THE CHALLENGE FOR US FINANCIAL INSTITUTIONS

1. Increased security breaches

62%

Of all FIs experienced an increase in financial crime in 2022

Source: PMNTS, 2022

$9.44M

Average cost of a data breach in the U.S.

Source: IBM, 2022

THE CHALLENGE FOR US FINANCIAL INSTITUTIONS

2. Increased regulatory/compliance requirements

$4M

In avg. revenue lost due to a single non-compliance event

Source: Secureframe, 2022

170%

More is spent on non-compliance vs compliance

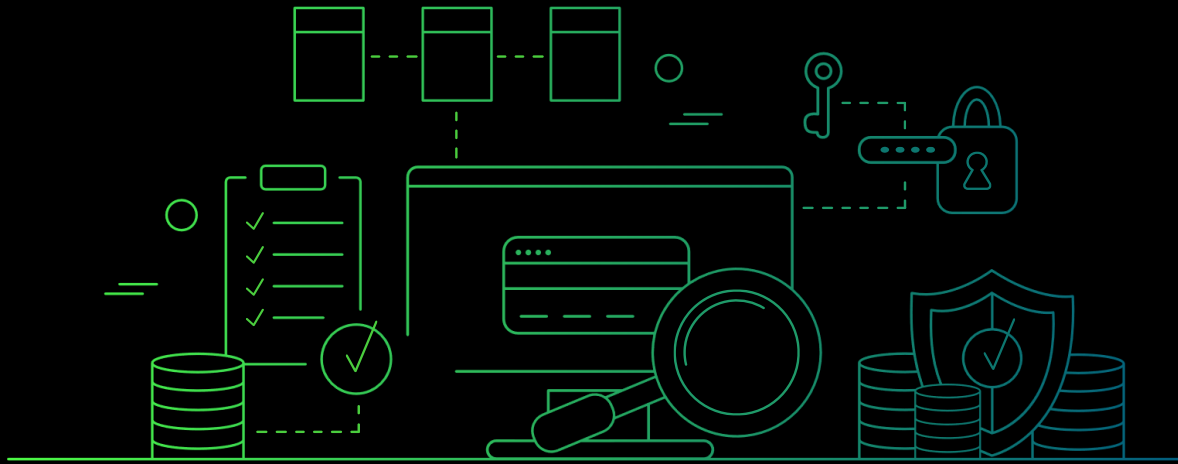
Source: Secureframe, 2022

THE SOLUTION:
FIS MANAGED SECURITY SERVICES (MSS)

FIS MANAGED RISK AND SECURITY SERVICES (MSS)

FIS' fully managed cybersecurity solution suite brings together a range of powerful, coordinated services that undergo rigorous, consistent testing to ensure our offerings remain current with regulatory requirements while featuring exceptional security capabilities.

Our service involves continuously auditing and comparing the applications we use against industry benchmarks and best practices to ensure we deliver unified, best-in-breed solutions to our clients.



WHAT MAKES FIS' MANAGED SECURITY SERVICES UNIQUE

Designed for financial institutions at their request, our solution stands out in the market due to our people, processes, and tools:

Our people

Because our solution is designed and led by a team of former bankers, we have a unique perspective into how financial organizations operate and what their key needs are.

WHAT MAKES FIS' MANAGED SECURITY SERVICES UNIQUE

Designed for financial institutions at their request, our Managed Risk and Security Services stand out in the market because of our people and processes:

Our processes

We constantly monitor for changes in the regulatory environment and collaborate with our clients' auditors and examiners to stay ahead of trends and deliver up-to-date compliance and best practice guidance to customers.

WHAT MAKES FIS' MANAGED SECURITY SERVICES UNIQUE

Designed for financial institutions at their request, our solution stands out in the market due to our people, processes, and tools:

Our tools

We offer you the same cutting-edge risk management and assessment toolset that we use to protect ourselves – ensuring you have a successful risk, information security, and compliance program at your fingertips.

FIS MANAGED SECURITY SERVICES (MSS)

FIS MANAGED SECURITY SERVICES

Access FIS Grade security with the same premium tools we use to protect ourselves to detect, analyze, investigate, and respond to threats to your business with mitigation and containment protocols.

300+

Financial institutions secured

$252B

U.S. assets secured

1 TRILLION+

Logs analyzed each year

300,000+

Devices secured and monitored

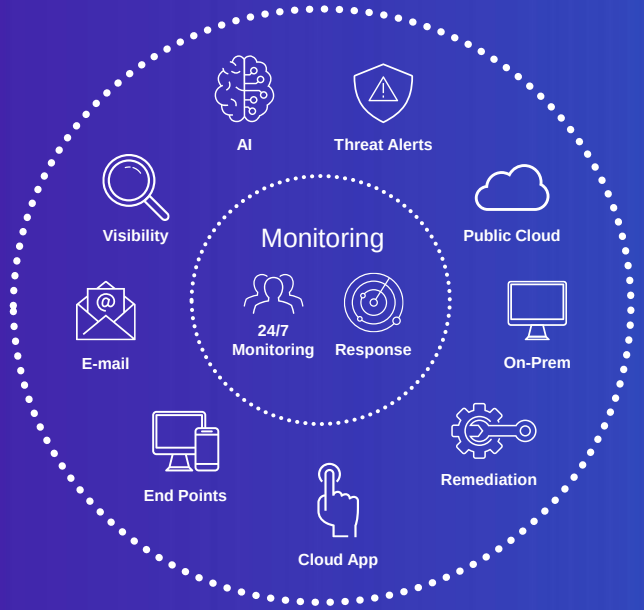
~7,200,000

Annual vulnerabilities remediated

~14.3B

Malicious emails blocked annually

FIS MANAGED SECURITY SERVICES MAPPED

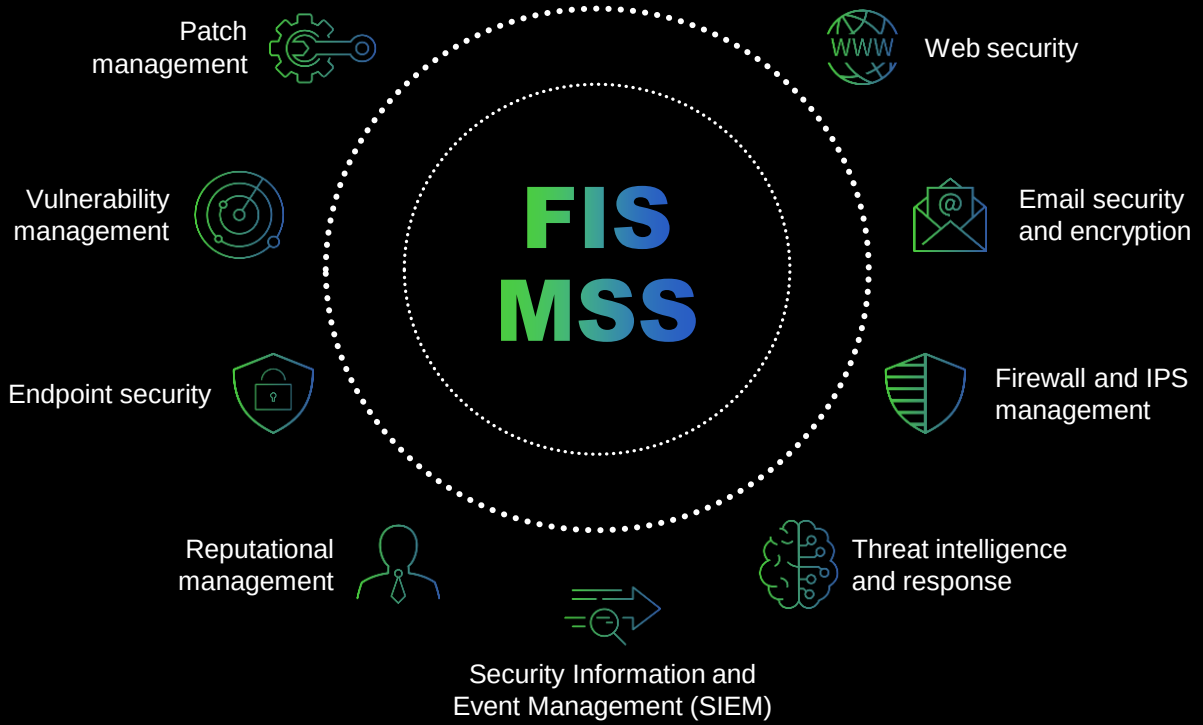


- Collect telemetry and respond to threats across systems, environments, and tools, using FIS' integrated solution
- 24/7 security monitoring and response capabilities, delivered out of FIS' Cyber Fusion Centers
- Vulnerability identification and FIS facilitated remediation keeps your services hardened
- Real-time visibility for the client to vulnerabilities, logs, and alerts via our MSSP portal and direct SIEM access

MANAGED SECURITY SERVICES (MSS)

FIS MSS comes as a comprehensive package that provides cybersecurity capabilities to clients of all sizes, and comprises:

MANAGED SECURITY SERVICES (MSS)



PATCH MANAGEMENT

Key features

Threats managed

Enables proactive threat management by automating the collection and delivery of patches throughout your enterprise with FIS agents checking for missing patches daily

Patches automated

Automated deployment of critical and security-related Microsoft Windows patches, as well as approved updates to in-scope client devices

VULNERABILITY MANAGEMENT

Key features

Scans conducted

Internal and external scans conducted for vulnerabilities, misconfigurations, and various security risks on all network devices

Controls approved

FIS' Enhanced Vulnerability Management directly and continuously addresses the evolving mandates and key controls set out by the financial industry's regulatory bodies

Best practices followed

The Center for Internet Security lists continuous vulnerability management as number three in its top 20 security controls

ENDPOINT SECURITY

Key features

Threats hunted

FIS Endpoint Threat Detection (ETD) quickly pinpoints compromised endpoints, investigates threats, and speeds response times to cyber incidents. Our experts perform advanced analysis of anomalous patterns to detect malicious activity that standard prevention solutions do not detect

Exploits mitigated

FIS Endpoint Threat Prevention uses AI-powered Next-Generation Antivirus (NGAV) to anticipate and prevent known and unknown threats. Being cloud-based, it can deploy in hours rather than months and the burden of managing infrastructure, software and signature databases is vastly reduced.

Data loss prevented

FIS Managed Endpoint DLP Service is a solution for the oversight and protection of confidential bank data. Best-practice driven, the program mitigates the risk of lost, misplaced, misused or stolen financial data through real-time monitoring of all confidential data elements

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Key features

All angles covered

FIS monitors all security solutions in our MSS suite of products for cybersecurity events every hour of every day

Events scrutinized

Security analysts review events for anything that may constitute a cybersecurity incident including suspicious activity, persistent attack attempts, indicators of compromise, and malware

Logs monitored

FIS monitors security logs from all Active Directory Domain Controllers by default and is alerted to suspicious events. These include generic accounts being added to domain admins, brute force login attempts, administrative changes within Active Directory, and suspicious logon failures

THREAT INTELLIGENCE AND RESPONSE

Key features

Solutions combined

Our Security Operations Center incorporates FIS Threat Intelligence by combining the advanced functionality of our Cyber Threat Intelligence, Cyber Fusion Center, and MSS Security Operations Center

Security updated

FIS has the most up-to-date intelligence, allowing us to scrutinize every aspect of security throughout our MSS suite of products

Visibility enhanced

Because we are the world's largest technology provider for financial institutions, we have an unrivalled line of sight across the industry and the ability to gather insights from hundreds of sources and organizations across the sector

FIREWALL AND IPS MANAGEMENT

Key features

Threats identified

Our Network Intrusion Prevention System inspects network traffic for suspicious activity and prevents malicious attacks such as viruses, denial of service attacks, spoofing attacks, vulnerability exploits, and more

Comms clarified

We monitor firewall logs for suspicious activity 24/7 to detect and respond to threats; any activity is correlated across our clients' networks and analyzed by our security analysts

Actions executed

As soon as a threat is detected, our analysts deploy countermeasures to protect the client from damage

EMAIL SECURITY AND ENCRYPTION

Key features

FIS provides a gateway email solution that protects against email-transported threats such as spam, phishing, and malware by using multi-layer malware analysis. We also issue updates addressing the latest threat signatures every 3-5 minutes.

To ensure your organization's safety, we analyze:

- Sender reputations of all inbound email; if poor, the email is dropped
- Attachments for malware, which are blocked if binary files such as .exe are attached
- Web links contained within emails to verify the integrity of the source
- Compressed files by opening them and looking for executable content; if found, the message is quarantined

WEB SECURITY

Key features

Our web security solution protects against advanced and targeted malware threats, combining multi-layer malware analysis from top Gartner rated anti-virus companies and heuristics that analyze webpage components in real time to block threats.

To provide comprehensive website safety, we:

- Block harmful sites based on signature, web reputation, and content analysis
- Analyze domain owner, host server, and other parameters to provide reputation scores upon request
- Deny DNS traffic to known malware destinations by configuring outbound DNS to only use secure servers

REPUTATIONAL MANAGEMENT

Key features

Brands protected

FIS proactively scans domains and websites seen for misuse of customer brands, logos, and webpages. If used for phishing or brand misrepresentation, we can initiate a "takedown" to stop this activity and add them to phishing filters for major web browsers to block public access

DNS changes monitored

FIS actively monitors customer public domains for IP address changes to check for hijacking or pharming. If there is ever an IP address different than what is expected, an alarm is generated, and an incident response is initiated

Website integrity secured

FIS tracks our clients' webpages for content changes and possible defacement. When detected, a ticket is opened to inform the client that changes have occurred. In the event of malicious content or defacement, the MSS incident response team works with the client and the web host to revert the changes or temporarily block access

SAFEGUARD AGAINST INTERNAL AND EXTERNAL RISKS WITH FIS' MANAGED RISK AND SECURITY SERVICES.

Learn more about how we can help you stay ahead of the risks of today and tomorrow.

Start Now

ALTERNATIVELY, CONTACT YOUR RELATIONSHIP MANAGER TO DISCUSS YOUR SECURITY AND RISK REQUIREMENTS:

Contact: https://www.fisglobal.com/en/contact-us / Email: getinfo@fis.com