STAY ONE STEP AHEAD OF RISING THREATS

Cybercriminals won't rest. Neither should you.

The threats posed by malicious actors are becoming more complex and their attacks more sophisticated. It's no surprise businesses are finding it hard to manage all the security solutions needed to repel them and stay compliant.

But internal security teams don't have to carry the whole burden. Partnering with a managed XDR provider can greatly enhance your security posture at a far lower cost, while providing holistic threat management across your entire technology stack.

68%

The year-on-year increase of reported data breaches in 2021

Source: ITRC, 2022

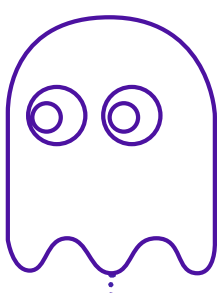
$4.24 MILLION

Average cost of a data breach in 2021, the highest on record

Source: IBM, 2021

The old ways don't cut it

The security approaches of the past were not built to cope with today's fast-moving threatscape. As the volume of cyberattacks and the number of potential vectors increases, more and more attacks are successful despite the presence of traditional security solutions.



70%

IT security teams that say their lives are being emotionally impacted by IT threat alerts

Source: Help Net Security, 2021

61%

Proportion of cybersecurity teams that are understaffed

Source: ISACA, 2021

Not only are the tools on hand often no longer sufficient, but internal Security Operations Center (SOC) teams are dealing with staffing shortfalls and alert overload, leading to gaps in your security perimeter and lapses in data protection.

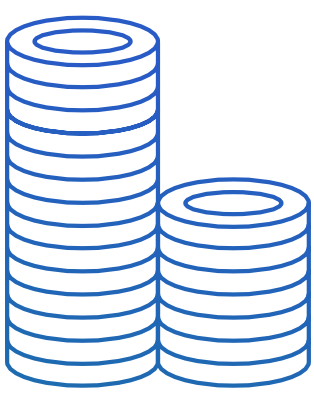
$265 BILLION

Amount that global ransomware damage is predicted to cost by 2031

Source: Cybersecurity ventures, 2021

The stakes are getting higher

Consumers are also becoming increasingly concerned with how businesses handle their personal data and how it can expose them to risk. Data breaches are reported widely and not only drive away potential new customers, but cause defection to competitors – highlighting the risks of failing to act.



206 DAYS

The average time to identify a data breach inside an organization

Source: IBM, 2021

45%

IT leaders considering outsourcing their cybersecurity due to inefficiency of existing tools

Source: Security Magazine, 2021

Attacks aren't going away. So, businesses need a more holistic approach to managing their IT security. One of the key ways this can be done is through an Extended Detection & Response (XDR) solution that encompasses traditional endpoints and your entire network and cloud ecosystem.

20-30%

Expected increase for most financial institution security budgets this year, with XDR named as the highest security priority

Source: VMware, 2022

85%

Consumers who would stop engaging with an organization if their data was compromised

Source: Business Today In, 2021

How FIS can help

Our FIS Managed XDR service offers maximum protection across your entire network with tools that rapidly detect, analyze, investigate, and respond to threats with mitigation and containment protocols. Plus, our security operations center monitors and remains up to date with the ever-changing threat environment 24/7, 365 days a year – so you don't have to.

FIS Cyber Fusion Center

Gives you access to 24/7 security monitoring and response capabilities.

Cloud-Native SIEM Solution

Delivers intelligent security analytics and threat intelligence across the enterprise.

Cybersecurity Advisor

Offers a dedicated Cybersecurity Advisor as your team's point-of-contact for technical and day-to-day service delivery.

FIS Grade Security

Provides peace of mind by extending the same ironclad protection used to secure FIS systems to your business.

FIS Managed XDR: Our four security pillars

Prevent

Next-generation antivirus fully protects from malware-free and fileless 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.

Ready to feel like your data security is back under control?

Find out how