ESG a division of TechTarget | Enterprise Strategy Group | Getting to the bigger truth.™

Deploying Extended Detection and Response (XDR) Platforms for Threat Management

Examining Potential Options

Cyber-risks are Increasing

According to ESG research, 82% of organizations believe that cyber-risk has increased over the past 2 years. This increase is due to factors like an increase in cyber-threats, greater dependence on IT for fulfilling business mission, and an increase in the amount of assets on the attack surface.

82%
believe cyber-risk has **increased** over the past 2 years.

Corporate Boards Are Becoming More Engaged with Cybersecurity

Aside from spending trends, board members want to be updated about the status of cybersecurity projects and any specific attack campaigns aimed at their industry or organization.

85%
of security and business professionals claim that **their board of directors is more engaged in cybersecurity** status, decisions, and strategy than it was 2 years ago.

Threat Detection and Response Challenges

Improving cyber-risk management demands that organizations make progress with threat detection and response. Unfortunately, there's a lot of work to be done as organizations have lots of challenges in this area. This data indicates that processes and technology changes are needed.

31%
We spend most of our time addressing high priority/ emergency threats

29%
We have "blind spots" on our network due to inability to deploy agents

23%
It's difficult to correlate and combine data from different security controls

22%
It is difficult to track/measure progress throughout the lifecycle of security incidents

'Platform' Adoption

To alleviate threat detection and response technology complexity, many organizations are contemplating replacing standalone security point tools with integrated multi-product "platforms." This raises the question, however, just what is a cybersecurity technology platform.

67%
of security professionals say that a cybersecurity "platform" is offered **as an agreed-upon, standard architecture provided as an OPEN suite of products integrated through standard APIs and development tools.**

PLATFORM PROLIFERATION IS ALREADY HAPPENING.

70%
of organizations have deployed, are planning to deploy, or are considering **deploying an extended detection and response (XDR) platform for threat management.**

Important Attributes of a Threat Detection & Response Platform

As organizations eschew threat management point tools, they have a list of specific requirements for threat detection and response platforms.

42%
Coverage across the entire attack surface

35%
Central management and reporting across all products and services

30%
Security analytics (i.e., collective analysis of product data)

21%
Extensible and open architecture (i.e. provide incremental value to existing security technologies like EDR, SIEM, etc.)

XDR Priorities

42%
Simplified visualization of complex attacks and understanding of how they progress

38%
Advanced analytics that can detect and identify modern, sophisticated attacks

31%
Automated response capabilities that can help block attacks in progress

Read more about Open XDR and SIEMs

GET THE REPORT

STELLAR CYBER®
We are Open XDR

Sources:
ESG Research Report, *Cybersecurity in the C-Suite and Boardroom*, February 2021.
ESG Master Survey Results, *The Impact of XDR in the Modern SOC*, February 2021.
ESG Research Report, *General Cybersecurity Process and Technology Trends*, to be published.