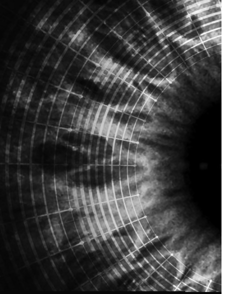
Enterprise Strategy Group by TechTarget



XDR: More Than Just Another SecOps Tool

The extended detection and response (XDR) megatrend has influenced virtually every security solution provider to participate in some way in the XDR movement, as security strategies require more comprehensive visibility and speed to shut down threats before they cause damage. Beyond better detection and response, XDR is helping IT and security leaders consolidate tools; improve team skills, efficiency, and effectiveness; and support business growth and IT transformation initiatives.

This Enterprise Strategy Group Infographic was commissioned by Cisco and is distributed under license from TechTarget, Inc.

Security Operations: More Difficult Than Two Years Ago

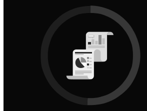
The rapid adoption of cloud and SaaS-based applications, together with a more diverse and distributed device operating environment, has expanded the attack surface, challenging even the most mature security solutions to keep up. Further exacerbating this situation is the growing number of fragmented security tools in use and the ongoing cybersecurity skills shortage, resulting in visibility challenges and an increase in the number of reactive and firefighting activities.

» Top Reasons Security Operations Are More Difficult Than They Were Two Years Ago

- The threat landscape is evolving and changing rapidly
- The attack surface has grown (i.e., more devices, applications, network traffic, etc.)
- The volume and complexity of security alerts have increased

Current Strategies Are Inadequate and SOC Modernization Is Desired

Since these security operations challenges will only accelerate in the future, many CISOs realize that current SOC strategies are inadequate. To cope with the increasing threat volume and IT scale and sprawl, organizations have several opinions about SOC modernization. **For example:**



51%

strongly agree that their **organization would benefit from greater data collection, processing, and analysis.**

SOC teams are expected to **increase** their consumption of threat intelligence information, gather more cloud telemetry, and integrate security and observability data over time.

45%

strongly agree that their **organization is actively integrating individual security tools into a more cohesive architecture.**

SOC teams need **greater** interoperability and improved operational efficiency via technology integration.

XDR

CISOs want XDR tools that can improve security efficacy, especially regarding advanced threat detection. Additionally, they want XDR to streamline security operations and bolster staff productivity. XDR tools integrate security products spanning hybrid IT architectures designed to interoperate and coordinate on threat prevention, detection, and response. XDR unifies control points, security telemetry, analytics, and operations into one enterprise system.

52%

of organizations believe **XDR will supplement** current security operations technologies.

44%

XDR will help to consolidate current security operations technologies into a common platform.

XDR Is Contributing in Many Ways to the Improvement of Security Program Objectives

According to research from TechTarget's Enterprise Strategy Group, when asked what are or likely would be the highest priorities for organizations when considering use cases for XDR, respondents most commonly reported that their organizations were prioritizing an XDR solution that could:

- Help prioritize alerts **based on risk.**
- Improve the detection of **advanced threats.**
- Offer more efficient **threat or forensics investigations.**
- **Act as a layered addition** to existing threat detection tools in order to identify advanced or more complex threats.
- Reinforce security controls and **prevent future similar attacks.**
- **Consolidate disparate tools** into a common, simplified threat detection and response architecture, streamlining incident response workflows.

> “**More than just a detection and response operational tool,** XDR solutions are helping organizations gain new levels of visibility into risk and threats, detect and mitigate advance threats, and improve operational efficiency and analyst retention, resulting in improved overall security posture and program scalability."
>
> **- Dave Gruber,** *Principal Analyst, Enterprise Strategy Group*

XDR solution investments are contributing to multiple security program objectives, including:

- Earlier detection, mitigation, and remediation of advance threats.
- Increased visibility into program gaps and areas of risk, aligned with the evolving threat landscape.
- Exposure and risk-based threat prioritization.
- Staffing efficiency, increased throughput, and employee retention enabled by automation, AI, and refined user experience.
- Improved data and tools integration, consolidation, and collaboration.
- Incident response readiness and effectiveness.

Conclusion

XDR investments are contributing to critical business outcomes and strengthening overall security posture while increasing team throughput. Enterprise Strategy Group recommends that security leaders take the time to explore how and why XDR solutions from security platform providers such as Cisco Systems can strengthen security outcomes, improve the scalability of security investments, and help consolidate security tools reducing cost and complexity.

LEARN MORE

CISCO

Source: Enterprise Strategy Group Research Report, *SOC Modernization and the Role of XDR*, October 2022.