HORST
INSURANCE

Protecting
What Matters
To You®

Extended Detection and Response Explained

Extended detection and response (XDR) is a security solution that offers organizations end-to-end visibility, detection, investigation and response across multiple security layers. Unlike endpoint detection and response (EDR), XDR provides a holistic view of threats across the entire technology landscape rather than only those within managed endpoints. This article explains what XDR is and how it works, outlines the benefits of XDR and discusses how it compares to EDR.

What Is XDR and How Does It Work?

XDR uses data collected across multiple security layers to provide IT and security teams with real-time, actionable threat information. By utilizing extended visibility, analysis and response across endpoints, workloads, users and networks, XDR can help organizations reduce blind spots, detect threats faster and jump-start threat remediation. Essentially, XDR helps security teams:

- Recognize advanced and hidden threats
- Detect and follow threats in and across various systems
- Improve the time it takes to detect and respond to threats
- Improve the threat investigation process

There are several components of XDR that provide organizations with a wider grasp of threats via the following:

- **An analysis of internal and external traffic**—XDR can identify cybersecurity threats even after they've bypassed system perimeters.
- **Integrated threat intelligence**—XDR learns from attacks on other systems to detect similar events in its own environment.
- **Machine learning-based detection**—XDR can detect zero-day and nontraditional threats that bypass signature-based methods.

The Benefits of XDR

XDR adds value to organizations by combining multiple security offerings into one incident detection and response product. Benefits of XDR include:

- **Greater visibility and context**—Threats that utilize legitimate software, ports and protocols can often slip past system defenses undetected. With XDR, security analysts can see threats on any security layer. It can also offer insights into how an attack happened, who was affected and how it spread.
- **Improved prioritization**—As cyberthreats become increasingly frequent, it can be difficult for IT and security teams to keep up with security alerts. XDR can help prioritize threats by grouping related alerts across the framework and presenting the most important ones.
- **Enhanced automation**—XDR's automation abilities allow IT teams to handle a large volume of data and consistently execute complex processes.
- **Faster detection and response**—Since XDR is continuously monitoring the technology landscape, it enables organizations to detect and respond to threats faster than before.
- **More sophisticated responses**—XDR can tailor specific systematic responses and leverage other control points to minimize the overall impact of the affected endpoint.

How Does XDR Compare to EDR?

XDR is an evolution of EDR—a cybersecurity solution that continuously monitors security-related threat information and endpoint data to detect and respond to ransomware and other types of malware. However, EDR can only detect and respond to threats inside managed endpoints, which limits the scope of threats that can be detected. In contrast, XDR goes beyond the capabilities of EDR by analyzing all security layers and offering organizations a more holistic view of threats.

Conclusion

In an increasingly complex threat landscape, XDR solutions can provide organizations with flexible and efficient security enforcement and remediation. For more risk management guidance, contact us today.

This Cyber Risks & Liabilities document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice.