Courtesy of
Wheeler & Taylor Insurance

CYBERRISKS&LIABILITIES

# Endpoint Detection and Response Explained

Endpoint detection and response (EDR) is a cybersecurity solution that continuously monitors security-related threat information and endpoint data to detect and respond to ransomware and other kinds of malware. It provides visibility into security incidents occurring on endpoints—such as mobile devices, desktop computers, laptops, embedded devices and servers—to prevent damage and future attacks. This article discusses the importance of EDR solutions, how they work and the types of threats they can detect.

### The Importance of EDR Solutions

According to the Identity Theft Resource Center, nearly 294 million people were impacted by 1,682 data breaches at U.S. corporations in 2021. As cyber threats grow more sophisticated and frequent, and remote work more common, these advanced attacks have become more difficult to identify in real time. Therefore, it's important for organizations to prioritize cybersecurity measures that can deflect, analyze and respond to the constant barrage of cyberattacks. EDR solutions can provide a number of features that improve an organization's cybersecurity risk management, including:

- **Improved visibility**—EDR solutions continuously collect data and analytics before compiling them into a single, centralized system. These insights can give security teams full visibility into the state of a network's endpoints from a single console.
- **Rapid investigations**—Since EDR solutions automate data collection and processing, security teams can gain rapid context regarding incidents and take steps to quickly remediate them.
- **Remediation automation**—Security teams can allow EDR solutions to automatically perform certain incident response activities based on predefined rules, enabling them to block or rapidly remediate incidents.
- **Contextualized threat hunting**—The continuous data collection and analysis provided by EDR solutions can allow threat hunters to identify and investigate potential signs of an existing issue.

### How Do EDR Solutions Work?

EDR solutions offer advanced threat detection, investigation and response capabilities—including incident data search and investigation triage, suspicious activity validation, threat hunting, and malicious activity detection and containment—by constantly analyzing events from endpoints to identify suspicious activity. These tools provide continuous and comprehensive visibility into what is happening in real time by recording activities and events taking place on endpoints and all workloads. By generating alerts, security teams can uncover, investigate and remediate issues. The primary functions of an EDR security system include:

- Monitoring endpoints and collecting activity data
- Analyzing data to identify threat patterns
- Using behavioral analysis to detect anomalies
- Removing or containing identified threats
- Notifying security personnel
- Researching identified threats and searching for suspicious activities

Overall, EDR solutions can be used to shorten response times for incident response teams and eliminate threats before damage is done.

WT | Celebrating 150 Years
SINCE 1871

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.

### What Types of Threats Do EDR Solutions Detect?

EDR is an integral part of an organization’s complete information security posture. It can detect the following threats to a network:

- Malware, including spyware, ransomware, viruses and bots
- Misuse of legitimate applications
- Stolen user credentials
- Suspicious user activity and behavior
- Fileless attacks during which malicious software is not installed and therefore more likely to be missed by anti-virus tools

### Conclusion

EDR solutions are helpful in protecting both the enterprise and the user while also adding value to a company’s integrated approach to cybersecurity.Furthermore, they are frequently required by insurance underwriters in order to obtain cyber insurance. For more risk management guidance, contact us today.