

## Endpoint Detection and Response (EDR)

This *CRL Cyber Circular* focuses on the second of the Top Cybersecurity Controls, Endpoint Detection and Response (EDR). EDR is rapidly becoming a foundational component of enterprise security architectures.

### Description

Endpoints – user laptops, desktops, and mobile phones, as well as functional hardware devices (often called Internet of Things or IOT technology) such as printers, sensors, controls systems, alarm systems, and countless others – are potential entry points for malicious actors to gain access to enterprise networks and resources.

EDR technology, with its origins in anti-virus, augments prevention measures by continuously monitoring endpoints for indications of cyber threat activity that has already penetrated boundary defenses and is active in the network. Essential features of EDR include: continuous monitoring of endpoints, detection and analysis of anomalies, the ability to take immediate remediation actions, and alerting security operations personnel of the threat events. Unlike antivirus, which is limited to its database of known malware signatures, EDR identifies cyber threats through behavior analysis and analysis of data from system logs, file changes, network traffic, and other sources.

EDR relies on software agents in each endpoint to feed data to the EDR platform and then to the Security Operations Center to form a full operational picture of the enterprise.

Two main variations of EDR solutions are found in the market: Extended Detection and Response (XDR) and Managed Detection and Response (MDR).

XDR expands the scope of EDR, capturing and analyzing more data sources to develop a better understanding of an ongoing attack, and the best response options.

MDR, in which the EDR or XDR platform is monitored and managed remotely by the provider, is offered by some EDR solution providers. This outsourcing of endpoint monitoring should be considered when examining the EDR solutions available because the

### Top Cybersecurity Controls

1. [Multifactor authentication for remote access and admin/privileges](#)
2. [Endpoint Detection and Response \(EDR\)](#)
3. [Secured, encrypted, and tested backups](#)
4. [Privileged Access Management \(PAM\)](#)
5. [Email filtering and web security](#)
6. Patch management and vulnerability management
7. Cyber incident response planning and testing
8. Cybersecurity awareness training and phishing testing
9. Hardening techniques, including Remote Desktop Protocol (RDP) mitigation
10. Logging and monitoring/network protections
11. End-of-life systems replaced or protected
12. Vendor/digital supply chain risk management

NOTE: Numbers 1 through 5 of the Top Cybersecurity Controls are viewed by cyber insurance carriers as most important in the underwriting process. Cyber insurance applicants that lack strong controls in the top five areas may be denied insurance, pay higher premiums, or have other conditions imposed on their coverage.






day-to-day tuning and management of an in-house EDR platform may require more specialized staff resources than the enterprise can provide.

### Application

The key to success with EDR is in the configuration and tuning of the solution for the specific operating environment. Default configurations will not deliver optimal performance in any given enterprise. Knowing this, hackers design their attacks to avoid detection by default EDR configurations. Tuning is a constant balance between minimizing false positives while not missing true positives.

### Implementation Suggestions

Some top EDR vendors and products are identified below, and there are many others. This list can serve as a starting point for organizations seeking to adopt an EDR solution. While EDR solutions offer many of the same capabilities, vendors differentiate their offerings to focus on specific enterprise needs and sizes. Organizations should research the available solutions and develop a deployment plan that will serve near-term needs and be scalable for the future.

Vendor	Solution	Description
 <b>CROWDSTRIKE</b>	CrowdStrike Falcon Pro Enterprise	<ul style="list-style-type: none"> <li>A unified set of security tools to provide a single source of truth: antivirus, EDR, XDR, managed threat hunting, and integrated threat intelligence.</li> <li>Attack path visibility, adversary context, and MITRE ATT&amp;CK mappings.</li> <li>Automated threat investigations accelerate alert, triage, and response.</li> </ul> <a href="https://www.crowdstrike.com/platform/endpoint-security/">https://www.crowdstrike.com/platform/endpoint-security/</a>
 <b>Microsoft</b>	Microsoft Defender for Endpoint	<ul style="list-style-type: none"> <li>Integrated into Windows platforms; no agents needed on Windows endpoints.</li> <li>Cloud-based and highly scalable for large enterprises.</li> <li>AI-based automation, Machine Learning, and behavioral detection algorithms.</li> <li>Detects and corrects software vulnerabilities and security configuration issues.</li> </ul> <a href="https://www.microsoft.com/en-us/security/business/endpoint-security/microsoft-defender-endpoint">https://www.microsoft.com/en-us/security/business/endpoint-security/microsoft-defender-endpoint</a>
 <b>Bitdefender</b>	GravityZone EDR	<ul style="list-style-type: none"> <li>Dedicated protection for datacenters, physical endpoints, mobile devices, and Exchange mailboxes.</li> <li>Visibility into the full lifecycle of an attack from the initial point of compromise.</li> <li>Detailed root cause analysis of threats that extend beyond the endpoint.</li> </ul> <a href="https://techzone.bitdefender.com">https://techzone.bitdefender.com</a>
 <b>TREND</b>	Trend Vision One	<ul style="list-style-type: none"> <li>Third-party security integrations, including Splunk, IBM QRadar, Cortex XSOAR.</li> <li>Comprehensive prevention, detection, and response capabilities powered by AI.</li> <li>Managed XDR service suited to smaller organizations without extensive IT teams.</li> </ul> <a href="https://www.trendmicro.com/en_us/business/products/one-platform.html">https://www.trendmicro.com/en_us/business/products/one-platform.html</a>
 <b>CORTEX</b>	Cortex by Palo Alto Networks	<ul style="list-style-type: none"> <li>Cloud-native XDR platform with software agents on endpoint devices.</li> <li>Blocks advanced malware, exploits, and fileless attacks; stops threats with Behavioral Threat Protection, AI and cloud-based analysis.</li> <li>Capabilities: Machine Learning threat detection; Root Cause Analysis; Deep Forensics; Flexible Response; Threat Hunting; Incident Management support.</li> </ul> <a href="https://www.paloaltonetworks.com/cortex">https://www.paloaltonetworks.com/cortex</a>