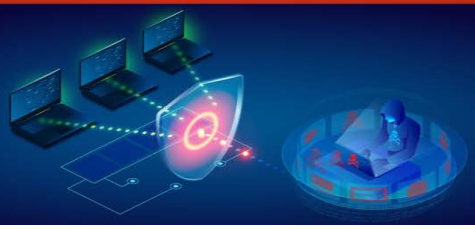
Endpoint Detection and Response (EDR)



Complete Your Endpoint Security Solution with EDR

WatchGuard EDR responds to known and unknown threats by providing visibility and controlling applications running on the network. While antivirus and endpoint protection platform products are important for scanning endpoints to look for known threats, their benefits are limited without continuous monitoring to spot advanced attacks such as APTs, exploits and fileless attacks. Adding WatchGuard EDR on top of an endpoint antivirus solution fills the gaps for comprehensive, effective endpoint security. Or deploy the full set of capabilities with WatchGuard EPDR, including our EPP and EDR solutions, for complete coverage in one centralized solution.

Key Features

- Continuously monitor endpoints
- Classify 100% of processes (pre-execution, running and post-execution) using the Zero-Trust Application Service
- Sandbox in real environments
- Automatically detect and respond to targeted attacks and in-memory exploits
- Prevent unknown processes from executing
- Find malicious actors, attack attempts and use tools to mitigate its effects with the Threat Hunting Service

Stay Ahead of Cyber Attacks

WatchGuard EDR provides powerful endpoint detection and response (EDR) protection from zero day attacks, ransomware, cryptojacking and other advanced targeted attacks using new and emerging machine-learning and deep-learning AI models. With complete visibility to endpoints and servers, it monitors and spots malicious activity that can bypass most traditional antivirus solutions.

Easily Add to Antivirus-Only Deployments

WatchGuard EDR installs on top of existing endpoint AV solutions to add a full stack of EDR capabilities to automate the detection, containment, and response to any advanced threat and includes our unique Zero-Trust Application Service and Threat Hunting Service.

Enable a Zero Trust Architecture With 100% Classification

The Zero-Trust Application Service that comes with WatchGuard EDR classifies processes as either malware or as trusted, prior to letting only the trusted execute on each endpoint. It enables a continuous endpoint monitoring, detection and classification of all activity to reveal and block anomalous behaviors of users, machines and processes.

Our AI system automatically classifies 99.98% of all running processes. The remaining percentage is manually classified by our malware experts. This approach allows us to classify 100% of all binaries without creating false positives or false negatives.

Increase Staff Utilization and Efficiency

The Threat Hunting Service in WatchGuard EDR delivers insights directly from our team of cybersecurity experts to help our customers reduce the time to detect and respond to the latest attacks. Our analysts study suspicious activity and investigate the indicators of attack to find evasion and compromise techniques, and then create new rules that can be delivered to endpoints to rapidly protect them against new attacks. Our hunters also proactively search for patterns of anomalous behavior not previously identified on the network, and provide recommendations on how to mitigate an ongoing attack and reduce the attack service of potential future attacks.

Uncover Your Vulnerability Risks

Why start patching when it's already too late? Identify potential vulnerabilities and take proactive measures to mitigate them before attackers exploit them. The vulnerability assessment tool helps businesses to evaluate and prioritize security weaknesses and vulnerabilities in applications and systems, so you improve your security posture and ensure your organization stays ahead of the latest threats.