Endpoint Security (EPDR Solution)

Perfect for small business

Secure your devices from malware and ransomware

CyberCision Endpoint Security EPDR uses WatchGuard, an innovative cybersecurity solution for computers, laptops and servers, delivered from the Cloud. It automates the prevention, detection, containment and response to any advanced threat, zero day malware, ransomware, phishing, in-memory exploits, and fileless and malwareless attacks, inside and outside the corporate network.

Unlike other solutions, it combines the widest range of endpoint protection technologies (EPP) with automated detection and response (EDR) capabilities. It also has two services, managed by WatchGuard experts, that are delivered as a feature of the solution:

- Zero-Trust Application Service: 100% classification of the applications
- Threat Hunting Service: detecting hackers and insiders

Simplifies & Maximizes Security

Easy to Use and Easy to Manage

Automated EDR Features

Integrates traditional endpoint technologies with innovative, adaptive protection, detection and response technologies in a single solution.

Powered by world's leading solutions for small business

WatchGuard

CyberCision

Endpoint Security (EPDR Solution)

Perfect for small business

ZERO-TRUST MODEL: A LAYERED PROTECTION

WatchGuard's Endpoint Security platform doesn't rely on just one single technology; we implement several together to reduce the opportunity for a threat actor to have success. Working in concert, these technologies utilize resources at the endpoint to minimize the risk of a breach.

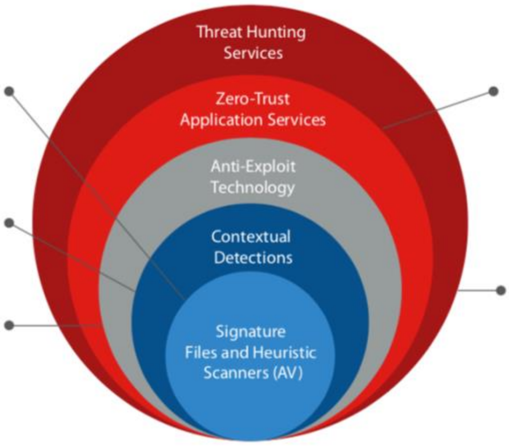
Zero-Trust Model: A layered protection

ENDPOINT LAYERS:

Layer 1/ Signature Files and Heuristic Technologies
Effective, optimized technology to detect known attacks

Layer 2 / Contextual Detections
They enable us to detect malwareless and fileless attacks

Layer 3 / Anti-Exploit Technology
It enables us to detect fileless attacks designed to exploit vulnerabilities


Threat Hunting Services
Zero-Trust Application Services
Anti-Exploit Technology
Contextual Detections
Signature Files and Heuristic Scanners (AV)

CLOUD-NATIVE LAYERS

Layer 4 / Zero-Trust Application Service
Provides detection if a previous layer is a breach, stops attacks on already infected computers and stops lateral movement attacks inside the network

Layer 5 / Threat Hunting Service
It enables us to detect compromised endpoints, early stage attacks, suspicious activities, and detection of IoAs

Signature files and heuristic technologies, known as traditional endpoint protection (EPP), make up a next-generation antivirus technology layer that is proven effective against many common, low-level threats. It's optimized to detect known attacks, based on specific signatures, generic and heuristic detection, and malicious URL blocking.

Contextual detection is key for detecting malwareless and fileless attacks as it looks for abnormal resource and application utilization. It is very effective against script-based attacks, attacks using goodware OS tools such as PowerShell, WMI, etc., web browser vulnerabilities and other commonly targeted applications such as Java, Adobe, and more.

Anti-exploit technology detects fileless attacks that are designed to exploit vulnerabilities. It searches for and detects anomalous behavior – a surefire signal of exploited processes. Anti-exploit technology is mission-critical on unpatched/waiting-to-be-patched endpoints, and on endpoints with operating systems that are no longer supported.

Our Zero-Trust Application Service classifies 100% of processes, monitors endpoint activity, and blocks the execution of applications and malicious processes. For each execution, it sends out a real-time classification verdict, malicious or legitimate, with no uncertainty and without delegating decisions to the user, avoiding manual processes.

Benefits

Simplifies & Maximizes Security

- Its automated services reduce the costs of expert personnel. There are no false alerts to manage, no time wasted on manual settings, and no responsibility is delegated.
- No management infrastructure to install, configure or maintain.
- Endpoint performance is not impacted since it is based on a lightweight agent and Cloud-native architecture.

Easy to Use and Easy to Manage

- Endpoint Security portfolio handles all needs of your endpoint protection in a remarkably simple way from a single web console.
- Easy to set up. Cross-platform endpoint management from a single pane of glass.
- It provides a clean and obvious user interface design that can be quickly mastered.

Automated EDR Features

- Detects and blocks hacking techniques, tactics and procedures, and malicious in-memory activity (exploits) before it can cause damage.
- Resolution and response: forensic information to thoroughly investigate each attack attempt, and tools to mitigate its effects (disinfection).
- Traceability of each action: actionable visibility into the attacker and their activity, facilitating forensic investigation.