# WATCHGUARD ADVANCED EPDR

## CYBERSECURITY CHALLENGES

Endpoints are the primary target for most cyberattacks. As the technology infrastructure becomes more complex, organizations struggle to find the expertise necessary to monitor and manage endpoint security risks. So, what types of challenges are security teams facing when adopting endpoint security solutions?

- **Ever-evolving sophisticated threats:** Efficient, proactive security practices can mean distinguishing between a minor security operation or being a victim. These practices range from reducing the attack surface to uncovering emerging threats before an actual compromise.
- **Alert fatigue, lack of efficiency:** Security teams receive thousands of weekly alerts, of which only 19% are considered trustworthy, and only 4% are investigated. Two-thirds of security teams' time is dedicated to managing alerts and classifying suspicious files manually.
- **Poor performance:** Frequently, endpoint security solutions require installation and management of multiple agents on each monitored computer, server, and laptop, causing serious errors, poor performance and high resource consumption.

As defenders, security teams need autonomous prevention, detection, and response solutions and weapons to easily hunt, investigate, and respond to threats lurking in the environments, taking the security stack to the next level to minimize adversaries' dwell time.

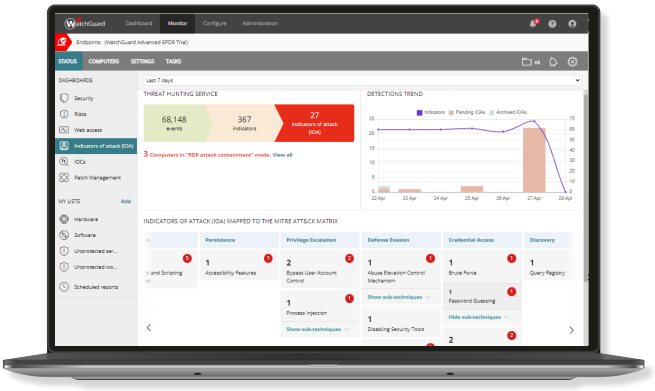
## LEVEL UP YOUR CYBERSECURITY SERVICES

WatchGuard Advanced EPDR is a cutting-edge cybersecurity solution delivered from the Cloud for computers, laptops, and servers. It automates the prevention, detection, containment, and response to any advanced threat, inside and outside the corporate network.

It combines preventive and EDR technologies with two security services:

- **Zero-Trust Application Service:** Cloud-based machine learning automatically classifies all files
- **Threat Hunting Service:** behavioral analytics to uncover threat actors utilizing living-off-the-land (LotL) techniques.

WatchGuard Advanced EPDR extends WatchGuard EPDR by adding to your technology stack hunting and investigation tools, such as IoCs search engine, advanced IoAs detections, access to enriched endpoint telemetry, and behavioral file analytics mapped to the MITRE ATT&CK framework. It also provides remote access to Windows, macOS, and Linux endpoints for rapid investigation and response.



Supported operating systems: Windows (Intel & ARM), macOS (Intel & ARM), Linux, iOS and Android.

WatchGuard Advanced EPDR integrates preventive endpoint technologies with EDR technologies in a single solution, allowing security teams to deal with advanced cyber threats.

### Attack Surface Reduction

- Centralized endpoint Security Risk detection and scoring
- Unmanaged endpoint proactive detection
- OS and hundreds of Applications vulnerability assessment

### Prevention

- Personal or managed firewall (IDS)
- Device control
- Application Control: Deny list / Allow list
- Permanent multi-vector anti-malware & on-demand scan
- Pre-execution heuristics
- URL filtering – web browsing
- Anti-phishing and Anti-tampering
- Attacks detected through network traffic analysis
- Endpoint Access Enforcement and Connections denial

### Hunting and Detection Technologies

- Continuous endpoint monitoring with EDR
- Zero Trust Application and Threat Hunting Services
- Sandboxing in real environments
- Anti-exploit protection
- Automated detection and containment of RDP attacks
- STIX indicators of attack (IoCs) and YARA rules searches
- Execution monitoring or denial of common LotL applications
- Access to the enriched telemetry
- Events and indicators of attack (IoAs) mapped to MITRE ATT&CK
- CAPA tool information for files (behaviors, strings, imports, exports)

### Containment and Remediation

- Computer isolation and reboot of systems
- Remote shell from the Cloud to endpoints
- Automatic remediation and ability to rollback
- Recover encrypted files with shadow copies

## BENEFITS

**Cost-Effective Operations - No More Wasted Time on Suspicious Files**
Like WatchGuard EPDR, the Zero-Trust Application Service gives your team back all that time dedicated to reverse engineering suspicious files that other solutions alert on without closing the loop and delegating the last verdict to you.

**Comprehensive Endpoint Security to Tailor to Your Services**
WatchGuard Advanced EPDR provides a comprehensive range of capabilities to strengthen endpoint security programs, including attack surface reduction, threat prevention, detection, and response, proactive hunting tools and remote endpoint connection for prompt response.

**Enhanced Hunting and Response at Your Fingertips**
Thanks to centralized IoC searches, WatchGuard Advanced EPDR enables security teams to discover threats without dealing with complex queries. The Threat Hunting Service delivers IoAs contextualized with telemetry. IoAs and events are enriched with MITRE tactics and techniques for swift correlation and response.

**Scalable Managed Security Services to Grow at Your Pace**
WatchGuard's Unified Security Platform Architecture brings comprehensive security from network to endpoint, Wi-Fi, and identity, with unparallel platform features, at no additional cost. The more services you adopt, the greater your operational and business benefits.

## 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 succeed. Working in concert, these technologies utilize resources at the endpoint to minimize the risk of a breach.

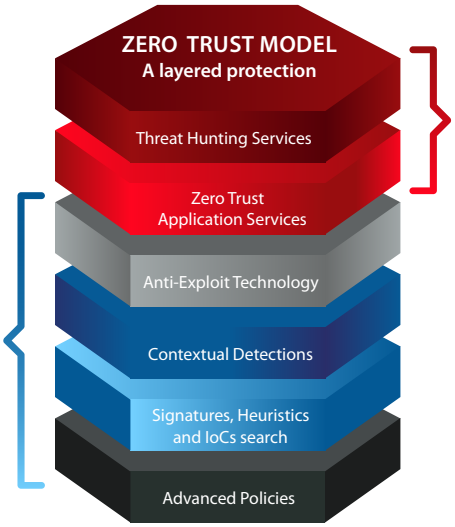
### ENDPOINT LAYERS:

**Layer 1/ / Enhanced Security Policies**
Detect or block the execution of common attack techniques

**Layer 2 / Signature Files, Heuristic Technologies and STIX IoCs Search Engine** enables security teams to hunt for recently disclosed attacks by hash, filename, path, C2 domain, IP, and YARA Rules

**Layer 3 / Contextual Detections** of malwareless attacks using OS tools such as PowerShell, WMI, web browsers, and other commonly targeted applications such as Java, Adobe, and more.

**Layer 4 / Anti-Exploit Technology**
It enables us to detect fileless attacks designed to exploit vulnerabilities




### CLOUD-NATIVE LAYERS

**Layer 5 / Zero-Trust Application Service**
Classifies 100% of processes before they run, denying any execution until it is certified as trusted

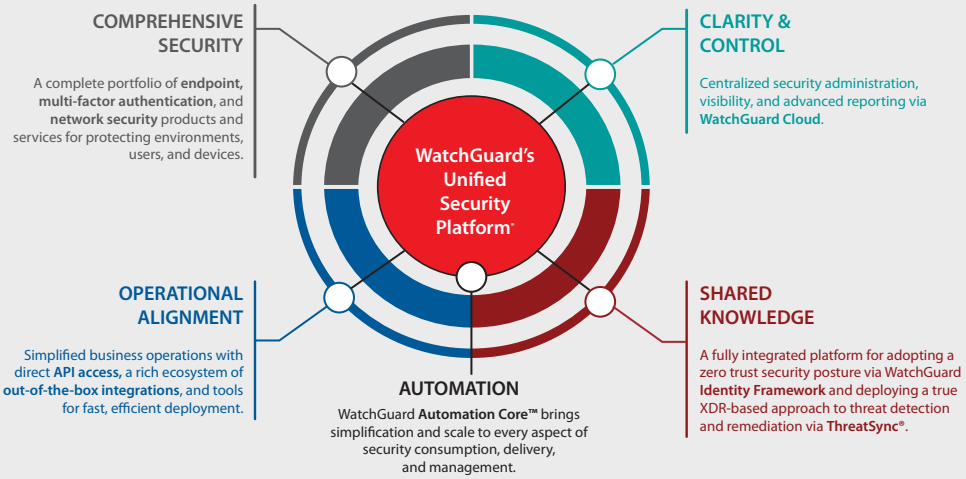
**Layer 6 / Threat Hunting Service**
It enables us to detect compromised endpoints, early stage attacks, suspicious activities, and detection of IoAs. Non-deterministic IoAs are contextualized in the Cloud-based console with the associated telemetry, enabling security analysts to investigate potential attack attempts.

## IMPLEMENT POWERFUL, SIMPLIFIED SECURITY WITH WATCHGUARD'S UNIFIED SECURITY PLATFORM

WatchGuard Unified Security Platform architecture is a single platform for elevating modern security delivery.

Our platform approach helps you deliver powerful security services for every threat vector with increased scale and velocity while supporting operational efficiencies and greater profitability. Learn more here.

### A single, scalable platform for elevating modern security delivery.




U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 WEB www.watchguard.com
WatchGuard Technologies, Inc.

No express or implied warranties are provided for herein. All specifications are subject to change and expected future products, features or functionality will be provided on an if and when available basis. ©2024 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, Unified Security Platform, WatchGuard Automation Core, ThreatSync, and the WatchGuard logo are registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other tradenames are the property of their respective owners. Part No. WGCE67589_092524