EPDR Minimizes the Need for MDR Services

Today's organizations face an increasingly sophisticated and diverse threat landscape. Managed Detection and Response (MDR) capabilities provide detection and response to cyberattacks as a service, normally including a Service Level Agreement (SLA). A team of security experts are constantly monitoring the company's systems, detecting any anomalous behavior and helping to provide an immediate response in case of an incident. However, adopting an MDR service can be costly for many companies.

WatchGuard's EPDR managed services, Zero-Trust Application Service and Threat Hunting Service are crucial elements to minimize the need for hiring a traditional MDR service. Zero-Trust Application detects and classify every single application only allowing to run processes classified as Goodware. Artificial Intelligence technologies and cybersecurity experts analysis allow us to classify 99.9% of the applications within four hours[1]. Additionally, the automated Threat Hunting Service help us detecting hackers and insiders.

Core Services Today: Zero-Trust Application Service

The Zero-Trust Application Service is a managed security service (MSS) included as part of the WatchGuard EPDR and WatchGuard EDR endpoint security solutions. This service classifies all running system applications as either trusted or malicious, only allowing trusted applications to execute on each endpoint. Since it is a fully automated service, it does not require any input, decision or manual interaction from the end user or from the IT security teams.

The service classifies 100% of running processes in real time, monitors endpoint activity, and suspends the execution of yet unknown applications and malicious processes.

The Zero-Trust Application Service has three key components:

- Continuous monitoring of endpoint activity from a Cloud-native platform.
- Automated, AI-based classification for 99.98% of the programs run on endpoints.
- Cybersecurity experts to classify the remaining 0.02% of the applications.

100% of Processes Are Accurately Classified

99.98% AUTOMATIC CLASSIFICATION | **0.02% HUMAN CLASSIFICATION**

01 Deny List

FOR KNOWN MALWARE

This classification is based on our Collective Intelligence, which includes more than 2.4 billion known malware.

02 Allow List

FOR KNOWN GOODWARE

Secondly, our Collective Intelligence also includes more than 3.3 billion known goodware to complement the classification.

03 Machine Learning

FOR UNKNOWN PROCESSES

Next, our artificial intelligence and deep learning algorithms are in charge of boosting the automatic classification.

04 Cybersecurity Experts

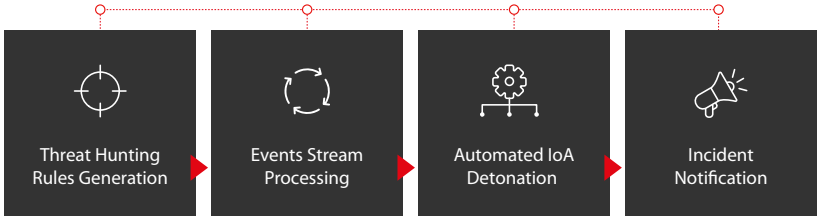
FOR NEW ATTACK PATTERNS

Finally, our malware analysts and threat hunters manually complete the classification process and enrich our algorithms.

[1] WatchGuard Endpoint Security Zero-Trust Application Service - Service Level Agreement: https://www.watchguard.com/es/wgrd-trust-center/watchguard-technologies-cloud-hosted-products-service-level-agreement

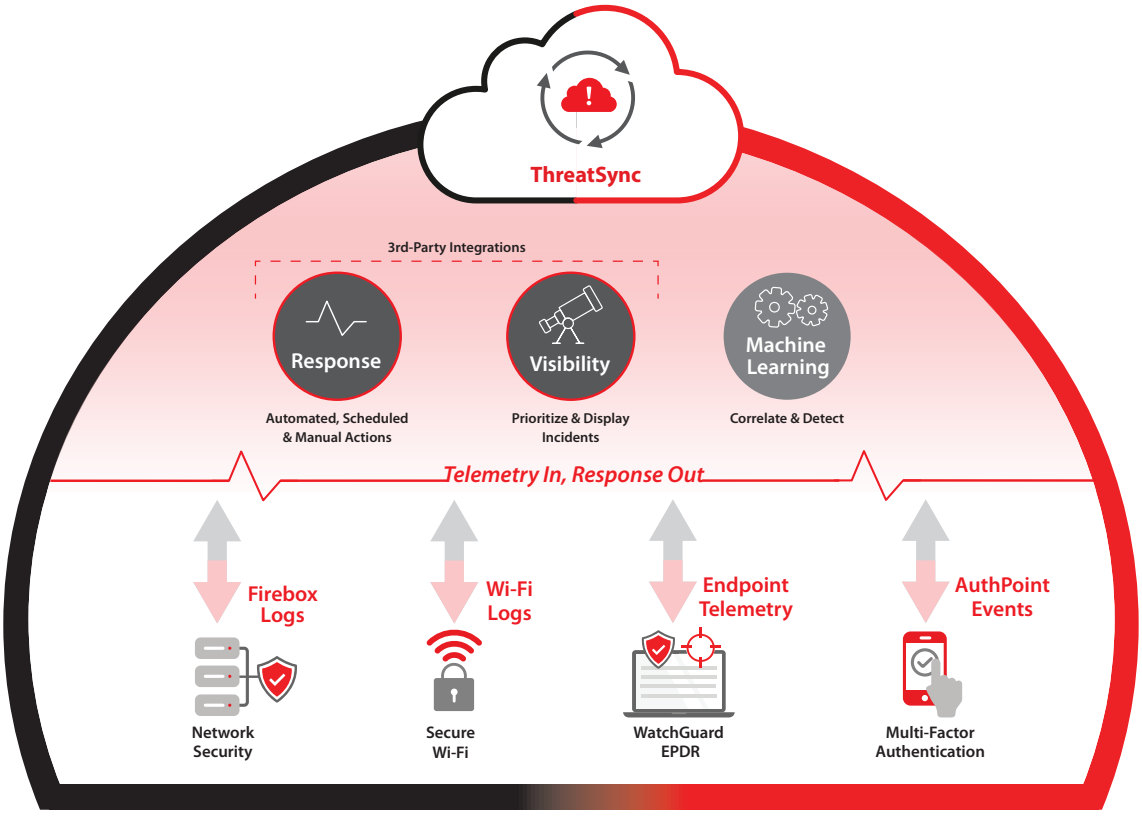
Core Services Today: Threat Hunting Services

Our Threat Hunting Service is based on an ever-evolving set of threat hunting rules developed by WatchGuard 's threat specialists. These are automatically processed against all endpoint telemetry data, indicators of attack (IoAs) producing triggered IoAs of high confidence with a low rate of false positives to minimize mean time to detect and mean time to respond (MTTD and MTTR). These IoAs are the result of a continuous process to discover threat actors, using advanced data analytics, our proprietary threat intelligence, and the expertise of our analysts. The service inherits all the cyber intelligence that we have perfected thanks to our 30+ years of experience in threat research and the historical visibility offered by a registry of application behaviors that ingests more than 10 billion events per day.



Extended Detection and Response (XDR)

Connect the detections classified by the Zero-Trust Application Service and the anomalous behaviors detected by the Threat Hunting Service across your ecosystem, with ThreatSync and enable your team to determine and automate multiple response actions to prevent threats from spreading into the whole organization. ThreatSync provides extended detection capabilities by consuming and correlating indicators of compromise (IoCs) from all WatchGuard security products.



About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, endpoint security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by more than18,000 security resellers and service providers to protect more than 250,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for midmarket businesses and distributed enterprises. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America.

To learn more, visit WatchGuard.com.

Questions: david.rufer@watchguard.com