Zero-Trust Application Service

Sophistication of cyber attacks

Cyber Defense Against Advanced Threats

State-of-the-art cyber attacks are designed to get around the protection provided by traditional security solutions. These attacks are becoming more frequent and more sophisticated as hackers become more professionalized. It is also a result of a lack of focus on correcting security vulnerabilities. Because of this, traditional protection platforms (EPPs) are not enough. This is because they do not provide detailed enough visibility into the processes and applications running on corporate networks. What's more, some EDR solutions, far from solving anything, create greater stress and increase security admin workloads by delegating the responsibility for managing alerts and forcing them to manually classify threats.

AI as disruptive innovation in security

The Zero-Trust Application Service is a managed service included as part of the WatchGuard EPDR and WatchGuard EDR solutions. This service classifies applications as either malware or as trusted, and then only lets trusted applications execute on each endpoint. Since it is a fully automated service, it does not require any input or decision from the end user or from the security analysts or IT teams.

The service classifies 100% of running processes in real time, monitors endpoint activity, and blocks the execution of applications and malicious processes (pre-execution, in-execution and post-execution).

The Zero-Trust Application Service has three key components:

1. Continuous monitoring of endpoint activity from a Cloud-native platform.

   The activity of every application at the endpoint, regardless of its nature, is monitored and sent to the Cloud for continuous classification. This way, malware executions, and even sophisticated threats such as supply chain attacks, can be prevented.

   The Zero-Trust Application Service enables a deny-by-default position to any process running on the endpoint, avoiding the execution of potential damaging applications and malicious processes. For each execution, it sends out a real-time classification verdict, malicious or legitimate, with no uncertainty and without delegating any manual process to the client. This classification process allows the execution of applications classified as legitimate, but what happens if a legitimate application turns into malware over time?

   In many cases, legitimate software is co-opted into performing malicious actions for financial gain, including some from prestigious software firms.

   These anomalous behaviors of seemingly legitimate software are reclassified thanks to the continuous monitoring and reassessment that is carried out in our Big Data platform.

2. Automated, AI-based classification.

   Automated classifications are made in a Cloud-based AI system, where an array of multiple machine-learning (ML) algorithms process hundreds of static, behavioral and context attributes are processed in real time. Attributes are extracted from the telemetry of the protected environment and from a set of physical sandboxes in which executable files are detonated.

   Today, the rate of automated classification is 99.98%, so that only 0.02% of the processes need intervention from our experts. The AI classification system is therefore self-sufficient, scalable to large volumes of files, working in real time and without relying on any input from the end user.

3. Risk-based application control.

Refers to the modes of operation of the protection agent running at the endpoints.

There are two levels of protection:

- **Hardening mode:** default-deny for any unknown application or binary coming the outside (web downloads, email, removable media, remote locations, etc.).
- **Lock mode:** default-deny for any unknown application or binary, regardless of its origin (from the network, from within the endpoint itself, or from the outside). It ensures that all running processes are trusted.

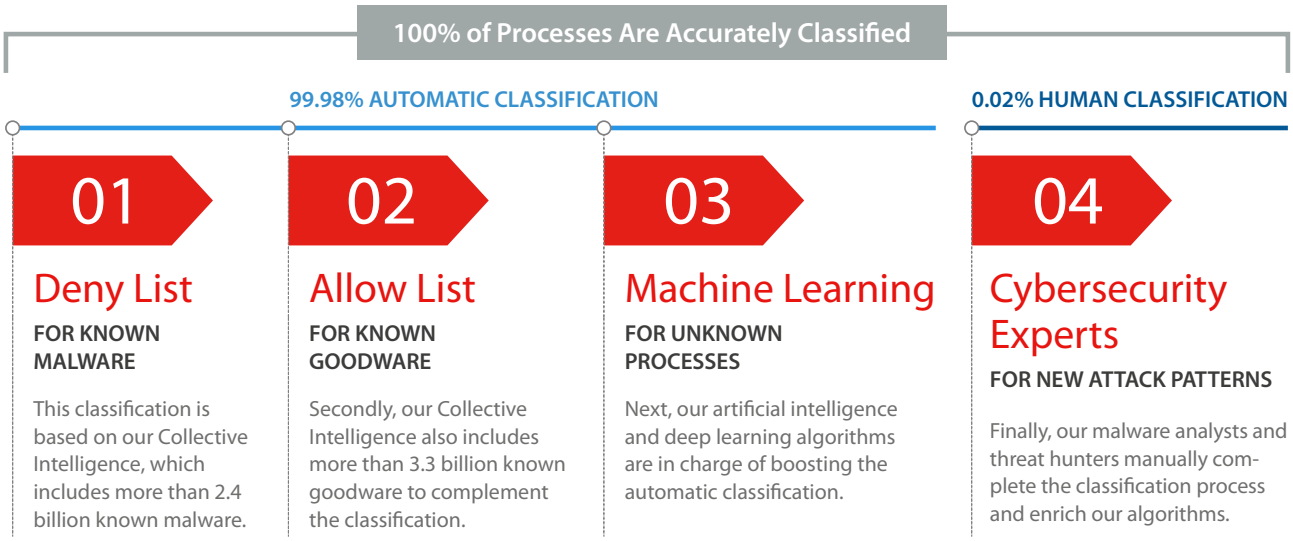
WatchGuard Endpoint Security Collective Intelligence

This is another key component hosted in the Cloud that increases the efficiency of the Zero-Trust Application Service.

Collective Intelligence represents the consolidated and incremental knowledge repository of all applications, binaries and other files containing interpreted code, both trusted and malicious.

This repository in the Cloud is continuously fed by the AI system and by expert analysts, and at the same time is continuously being queried by the solutions and services of WatchGuard Endpoint Security prior to any execution.

How the Zero-Trust Application Service works:



The graphic above shows how the technologies in the stack seamlessly work together, enabling the classification of all applications, binaries and files with interpreted code, in real time.

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.

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com