WatchGuard Endpoint Security
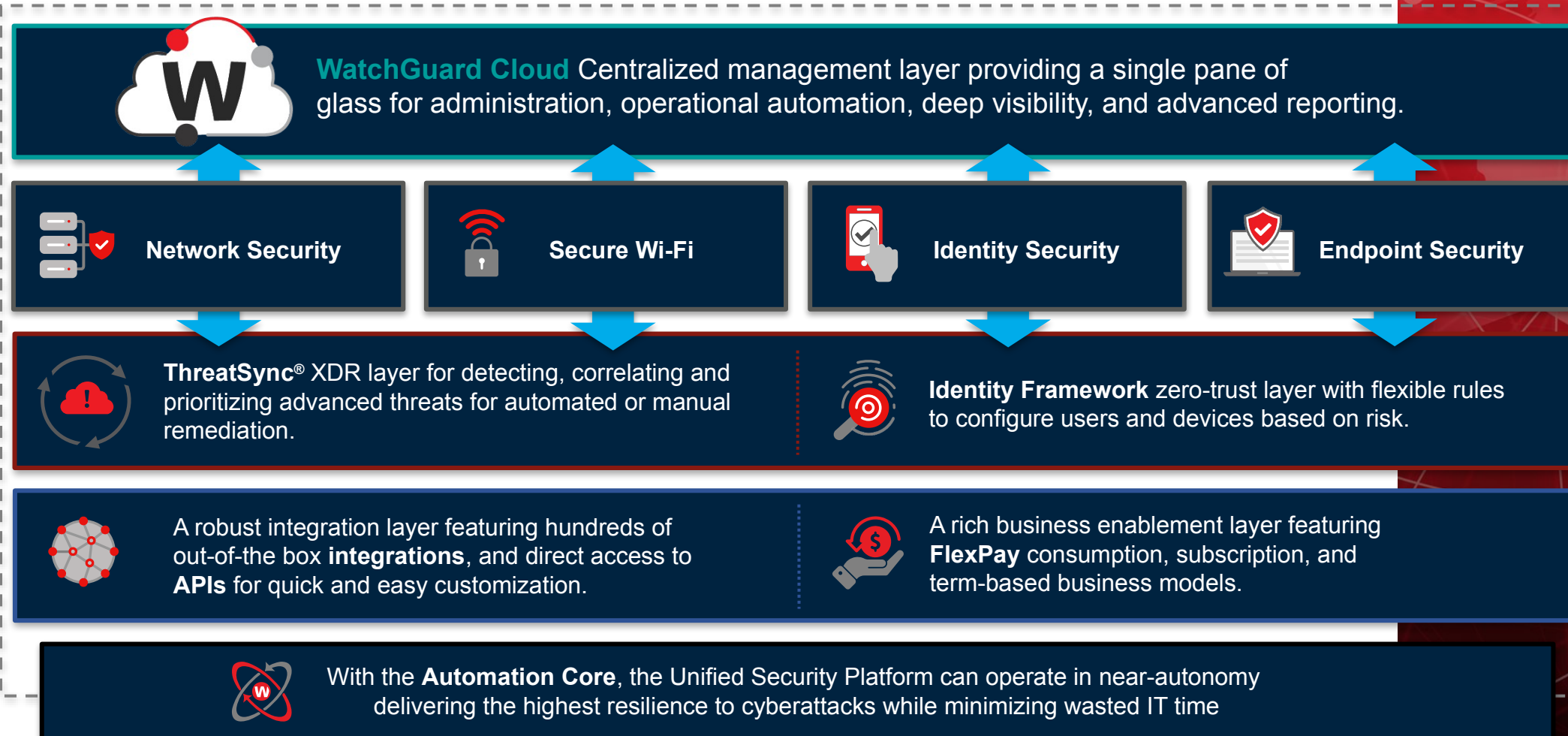
Powerful and trusted solutions to simplify centralized management and maximize protection of endpoint security

Nagy Gábor
SafeSoft Kft.
www.safesoft.hu
info@safesoft.hu

WatchGuard's Unified Security Platform® Architecture

Leap to Advanced, User-Centric Security

WatchGuard Cloud Centralized management layer providing a single pane of glass for administration, operational automation, deep visibility, and advanced reporting.

Network Security

Secure Wi-Fi

Identity Security

Endpoint Security

ThreatSync® XDR layer for detecting, correlating and prioritizing advanced threats for automated or manual remediation.

Identity Framework zero-trust layer with flexible rules to configure users and devices based on risk.

A robust integration layer featuring hundreds of out-of-the box **integrations**, and direct access to **APIs** for quick and easy customization.

A rich business enablement layer featuring **FlexPay** consumption, subscription, and term-based business models.

With the **Automation Core**, the Unified Security Platform can operate in near-autonomy delivering the highest resilience to cyberattacks while minimizing wasted IT time

Clarity & Control

Complete Security

Shared Knowledge

Operational Alignment

Automation

WatchGuard

XDR with ThreatSync®

WatchGuard Endpoint Security

WatchGuard Endpoint Security

|	Base Offering	
WatchGuard EPP	EPP Windows, macOS, Linux and Android	
WatchGuard EDR, EDR Core	EDR Services: Zero-Trust Application & Threat Hunting	
WatchGuard EPDR	EPP + EDR Services: Zero-Trust Application & Threat Hunting	
WatchGuard Cloud	Single management platform for all of our endpoint security solutions. It is based on 3 pillars: Real-Time communication with endpoints, cross-endpoint Platform, multi-product/module	
Additional Products	DNSWatchGO – Cloud-based, domain-level protection, content filtering, keep users safe outside the network	
	Passport –	Cloud-delivered security for remote employees to work freely from the office, at home or on the go. With Passport You can Authenticate, Protect users and Prevent, detect and respond to known and unknown threats.

WatchGuard EPP

Endpoint Protection Platform

WatchGuard EPP

- It includes a full range of endpoint protection features, such as antivirus, firewall, device control, and URL filtering

- Centrally management of all endpoints, both inside and outside the corporate network.

- Real-time Lookups to WatchGuard Threat Intelligence.

- No need to maintain hardware and software.

- Its lightweight agent has no impact on endpoint performance, simplifying security management and increasing operational efficiency.

- Host firewall and device control

- Web browsing category-based monitoring and filtering
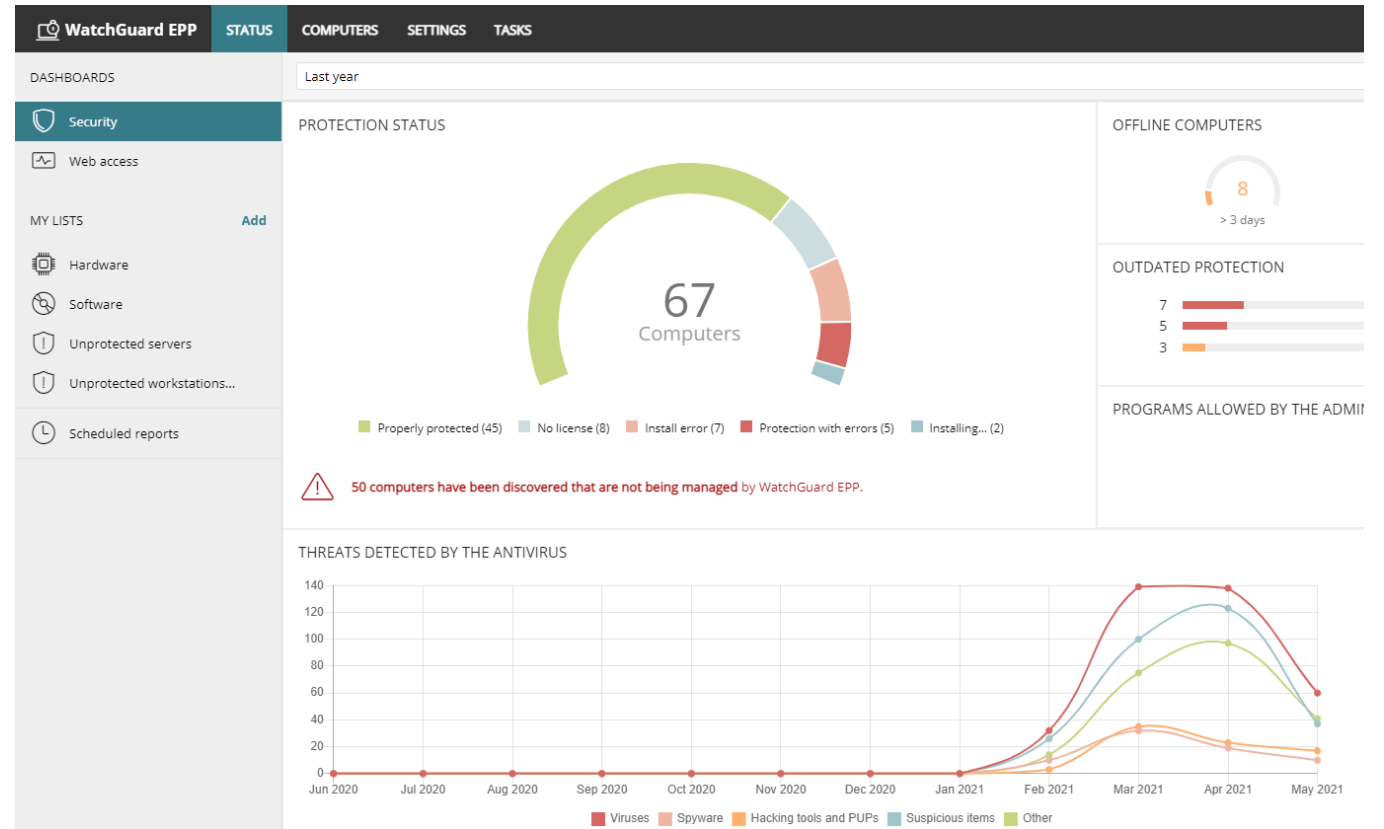
A Single Lightweight Agent With Maximum Workload in the Cloud

WatchGuard Endpoint Security agent is extremely light from a performance perspective with most of the processing done in the cloud.

- Initial Bandwidth:
  - 13MB Installer and communications agent
  - 89MB Endpoint protection package
  - Bandwidth consumption can be minimized using the CACHE
- Communication with the server:
  - Download – 3.2MB/day*
  - Upload – 1MB/day*
- Real-time on-access protection:
  - 500 KB: Bandwidth used on the first day, when the cache is empty
  - 35-100 KB: Bandwidth used after the first day, once the information is cached
- Compatible with other security vendor solutions
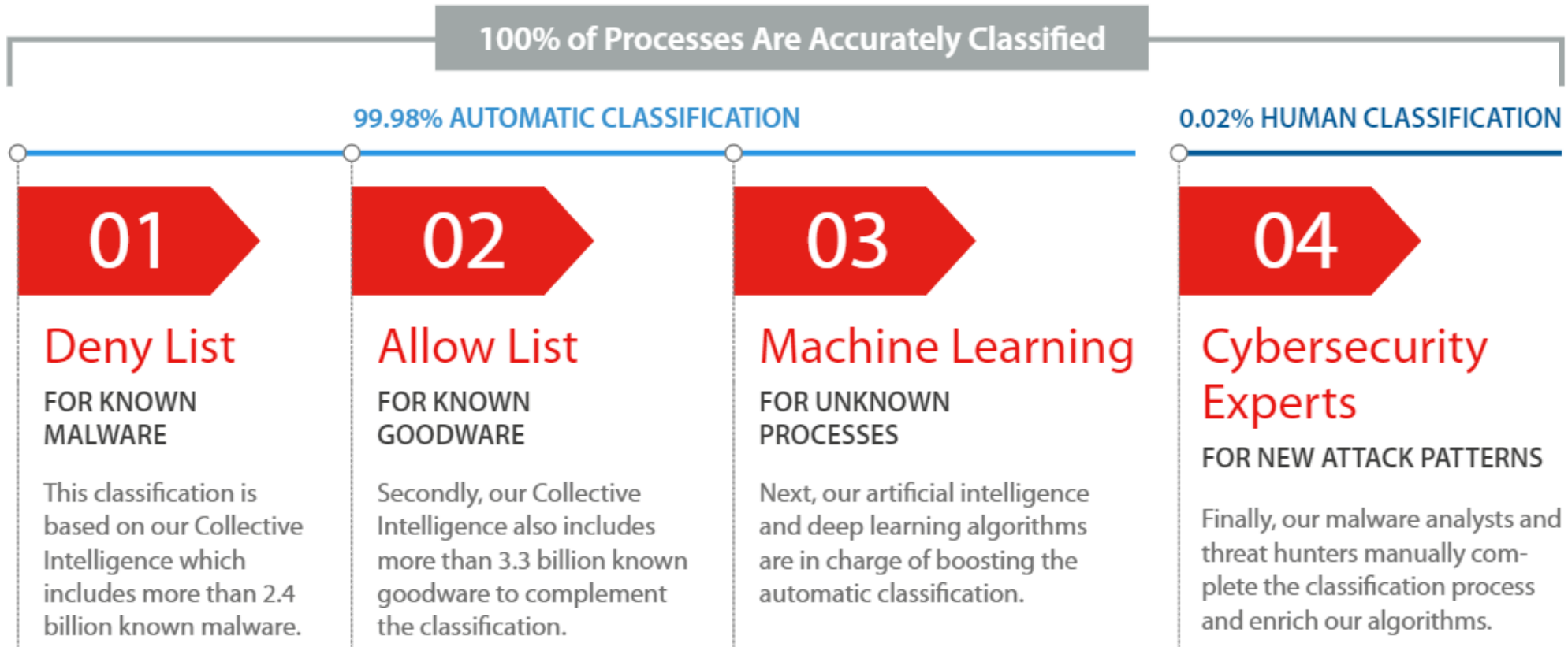 - Using the standards recommended by the manufacturer

WatchGuard EDR

Endpoint Detection and Response

How the Zero-Trust Application Service Works

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.

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.

Threat Hunting Service

- **LotL (Living-off-the-Land) and fileless attacks** are a growing concern: they are more difficult to detect and make it easier for cybercriminals to attack stealthily
- **Hacker detection**
  - Find attackers using Living-off-the-Land techniques
  - Lateral movements
  - Compromised credentials
- **Identification of malicious employees**
  - User behavior modeling
- New or improved IoAs produced to block before damage

- Our Cybersecurity Team continuously monitors endpoint activity in real time in the form of **event telemetry (12 months).**

- In case of a validated breach, the Cybersecurity Team notifies the customer

- WatchGuard EDR can coexist with traditional security solutions

WatchGuard EDR Vs WatchGuard EPP
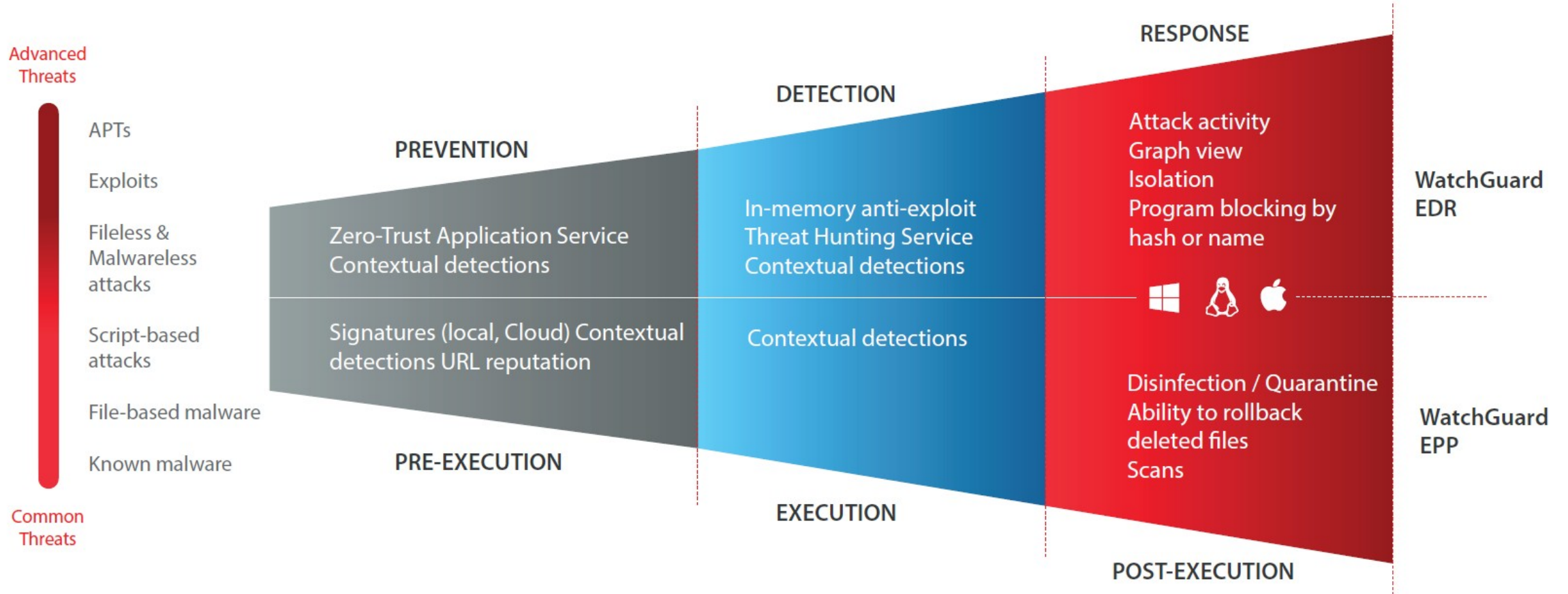
WatchGuard EDR Core

- WatchGuard EDR Core is included in the Firebox Total Security Suite license.

- EDR Core includes a subset of WatchGuard EDR features and supports XDR capabilities through ThreatSync.

- These basic features are available with EDR Core and you can assign them to your endpoints through security settings profiles:

  - Anti-tampering protection
  - Visibility into the hardware and software on an endpoint
  - Remote restart and reinstallation of the endpoint agent and protection software on the endpoint
  - Isolation of an endpoint
  - Discovery of unprotected endpoints
  - Tracking of user actions in the Endpoint Security management UI

WatchGuard EDR Core

These security features are not available with EDR Core:

- Web access control
- Firewall
- Antivirus
- Shadow copies
- Device control
- Zero-Trust Application Service (EDR Core does not classify unknown applications.)
- Scan tasks
- Program blocking
- Authorized software

WatchGuard EPDR

Endpoint Protection, Detection and Response

WatchGuard EPDR: Our EPP and EDR in a Single Solution

Unique combination of best-of-breed EPP and EDR capabilities

Automated prevention

Block non-goodware applications and exploits to prevent future attacks

Automated detection

Targeted and zero-day attacks blocked in real-time without signature files

Automated forensics

Forensic information for in-depth analysis of every attempted attack

Automated remediation

Automated malware removal to reduce burden on administrators

Key differentiators

Continuous monitoring and analysis of all running applications

✓ Fills the detection gap of AV products

✓ Minimizes risk of unknown malware

Extremely lightweight agent

✓ Virtually zero performance impact

✓ Cloud-based malware database

Cross-platform security

✓ Covers all infection vectors in Windows, Linux, Mac OS X and Android computers

✓ Browsing, email and file system protection

Easy to manage

✓ No maintenance or infrastructure required

✓ Each endpoint communicates with the Cloud
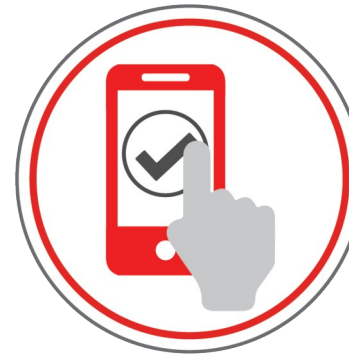
Highly automated solution minimizing cybersecurity risks

Passport

Protect Remote Employees

Passport – A Bundle of User-based Security Services

Prevent Phishing attacks with DNSWatchGO on and off the network

Protect against compromised credentials with AuthPoint MFA

Protect endpoints from malware with WatchGuard EPDR

Each service provides persistent, always-on protection that travels with your user.

Thank You