Be in it to Win it: Why you should be selling WatchGuard Endpoint Security Solutions

Agenda for today

- Our evolution as Endpoint Security vendor
- What makes us different?
- EDR? Why do organizations need it?
- Product offer and the Value Proposition
- From “trust everything” to Zero-Trust and Threat Hunting
- How YOU win

Our evolution as an Endpoint Security Vendor

2020

WatchGuard acquired Panda Security
Partners and customers can now benefit from advanced endpoint threat detection and response fueled by modern AI capabilities, behavior profiling techniques and cutting-edge security event correlation, as well as additional operational benefits such as centralized management across network and endpoint security.

2007

First in cloud-based scanning

Released the first 100% cloud-based malware analysis tool

2012

100% Cloud Security

First vendor to move the entire portfolio to the cloud

2015

EPP + EDR released

First vendor to release a fully integrated single agent EPP and EDR

2016

Market Guide for EDR

Panda Security was included in the Gartner Market Guide for EDR

2017

EPP + EDR over MSS

Panda Security released the Threat Hunting Service completely embedded in EDR

2019

Customer Choice 2019

Panda Security was named Customer Choice 2019 by Gartner Peer Insights for EDR solutions

What makes us different?

- We have developed a Zero-Trust Application Service to **reduce the UNKNOWN**
- Our mission is to reduce the number of security incidents to **ZERO**
- We provide our customers **endpoint data** that competitors are not even collecting
- Our complementary SOC model enables larger organizations to introduce **Forensic Tools**
- We transformed the traditional Threat Detection approach into a **Threat Hunting Service**


WatchGuard

What is Endpoint Detection and Response (EDR)?

- Endpoint Detection and Response (EDR) platforms are a category of endpoint security tools, built to provide endpoint visibility and used to detect and respond to cyber threats and exploits.

- Gartner's Senior Analyst Anton Chuvakin defined the term in 2013 as "tools that are **primarily focused on detecting and investigating suspicious activities (and traces of such) on hosts/endpoints**".

Why do organizations need an EDR?

- They provide an accurate firsthand view of a hacking operation as it unfolds (and traces of such)
- Critical forensics information, including process actions, file access, network events and configuration changes are collected from managed endpoints
- EDR solutions were built to provide complete visibility to endpoints and servers, monitor and spot abnormal behaviors that indicate malicious activity.

What are the essential elements of an EDR?

Enabling detection

Cross-correlating data across multiple sources/environments

Combining whitelisting with behavioral analysis

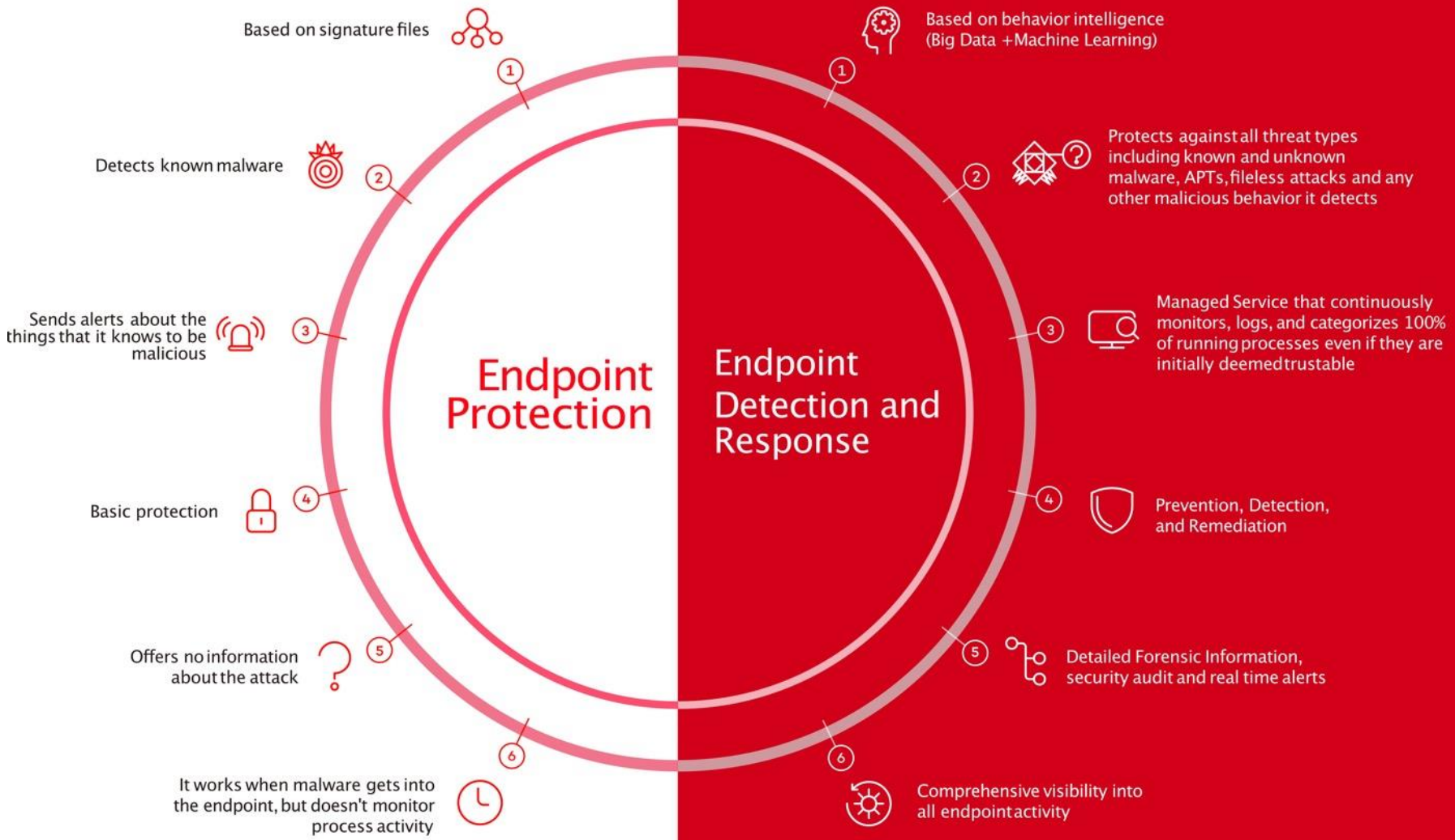
Observing endpoint activity without interfering

Empowering incident remediation and forensics investigation

Enabling effective cleanup and remediation

Working with your antivirus

Our proposition



WatchGuard Endpoint Security Solutions

- Workstations, laptops, servers and virtual instances
- Windows (Intel & ARM), Linux, macOS (Intel & ARM) and Android
- Inside/outside network, branch offices and remote workers

Next-Generation Antivirus (EPP)

WatchGuard EPP | EPP Capabilities

Advanced Endpoint Security (EDR)

WatchGuard EDR | EDR Capabilities | Zero-Trust Application & Threat Hunting Services

Advanced Endpoint Security (EPP+EDR)

WatchGuard EPDR | EPP + EDR Capabilities | Zero-Trust Application & Threat Hunting Services

WatchGuard Cloud

Endpoint Security Management | Visibility | License tracking

Single Lightweight Agent

Data Control
- Inventory and PII file classification
- Real-time PII monitoring
- Delete PII in files

Patch Management
- Microsoft and 3rd party applications patching
- End-of-Life application management
- Patch rollback and Windows Update service control
- On-demand or scheduled patching tasks

WatchGuard EPDR | Panda Adaptive Defense 360
- Protection against sophisticated targeted attacks
- Detection of unknown exploits
- Virtual patching for unsupported systems
- Machine Learning and Deep Learning
- Zero-Trust Application Service
- Containment and Remediation features
- Threat Hunting Service

SIEMFeeder
- Integration with corporate SIEM platforms
- Details and context of all endpoint activity
- CEF, LEEF, Syslog and Kafka support

Full Encryption
- Managed Full Disk Encryption with BitLocker
- Centralized management of recovery keys
- Centralized encryption policies
- Encryption dashboards, widgets and reporting

Advanced Reporting Tool
- Preconfigured & customizable dashboards, reports and alerts
- Dashboards, widgets, and predefined queries for security KPIs
- KPIs for vulnerable applications, access data and files, shadow files
- Raw data from: endpoint operations, network connections, data access, processes
- Endpoint data retention: 12 months

WatchGuard EPP | Panda Endpoint Protection Plus
- Anti-malware and HIPS protection
- Managed Endpoint Firewall
- Device Control
- Hardware/software inventory
- Web browsing monitoring and filtering

WatchGuard Cloud

Simplify Every Aspect of Security Delivery

Value proposition

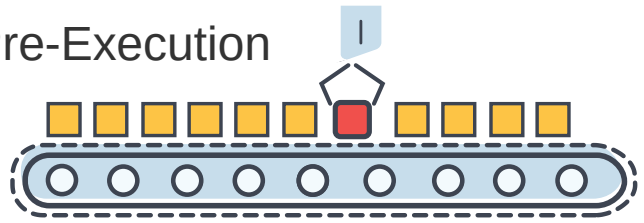
- WatchGuard empowers Partners to deliver exceptional customer value through a combination of innovative service-oriented products, enablement, and purchasing programs that complement more comprehensive IT solutions built to meet customer needs:
  - Complexity reduction,
  - Secured everywhere,
  - Analytics and visibility,
  - Monitoring internal security to understand external threats,
  - Protecting business-critical systems,
  - Defend endpoints from advanced threats,
  - Increase efficiency with deep-sight data analysis,
  - Lighten security administration footprint.

Matching your profile and the value proposition

Straightforward solutions for partners who focus on volume	Our more complex solutions for partners with a strong focus on service delivery	Solutions for partners who deliver managed security services to their customers
Endpoint Protection Next-Gen Endpoint Protection	**Endpoint Detection and Response**	**Managed Detection and Response**
Panda Endpoint Protection Plus WatchGuard EPP	Adaptive Defense / Adaptive Defense 360 WatchGuard EDR / WatchGuard EPDR	Managed EDR Services
Web Access Control	Patch Management	Endpoint Detection and Response
Full Disk Encryption	Advanced Reporting Tool	Threat Hunting
Patch Management	Systems Management	Systems Management
Mobile Device Protection	SIEMFeeder	Data Analytics
Device Control	Data Protection (GDPR-centric)	CyberSOC Services

“Trust everyone, run everything”

Pre-Execution

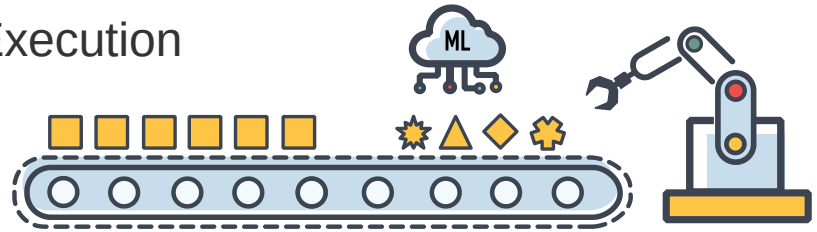


- Malware signatures
- URL Reputation
- Heuristics
- Deny-list rulesets

VENDOR KNOWLEDGE

Anomalous behavior detected

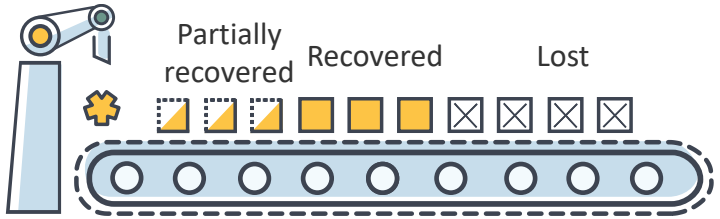
Execution



- Live or Sandbox execution
- Based on behavior (ML, AI, other technologies)
- Good vs. Bad

VENDOR TECHNOLOGY

Post Execution



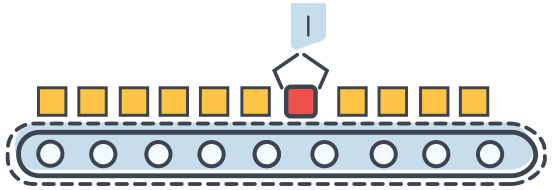
Machine Learning, AI o otras tecnologías pueden no decidir lo suficientemente rápido y es posible que se requiera una reversion (rollback)

VENDOR SERVICES

From “Trust Everyone” to “Trust No One”

VENDOR KNOWLEDGE

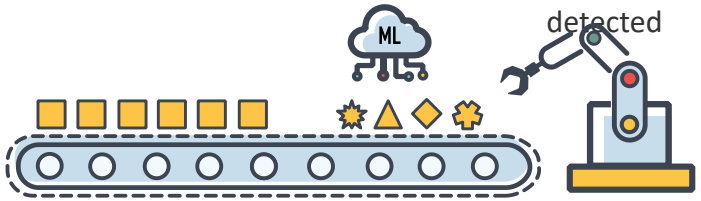
- Malware signatures
- URL Reputation
- Heuristics
- Deny-list rulesets



Pre-Execution

VENDOR TECHNOLOGY

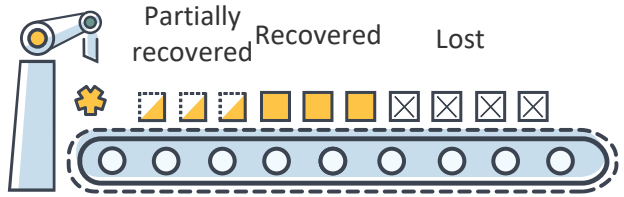
- Live or Sandbox execution
- Based on behavior (ML, AI, other technologies)
- Good vs. Bad



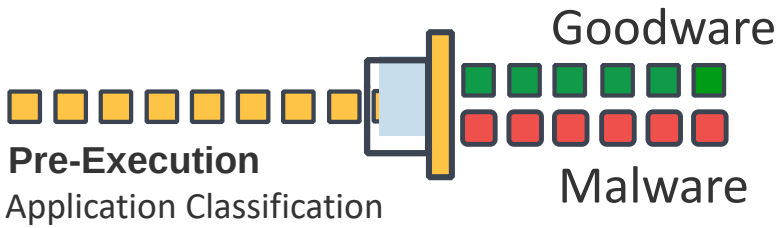
Execution

VENDOR SERVICES

Machine Learning, AI or other technologies may not decide fast enough, and rollback may be required

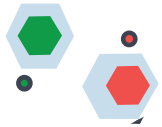


Post Execution



Pre-Execution
Application Classification

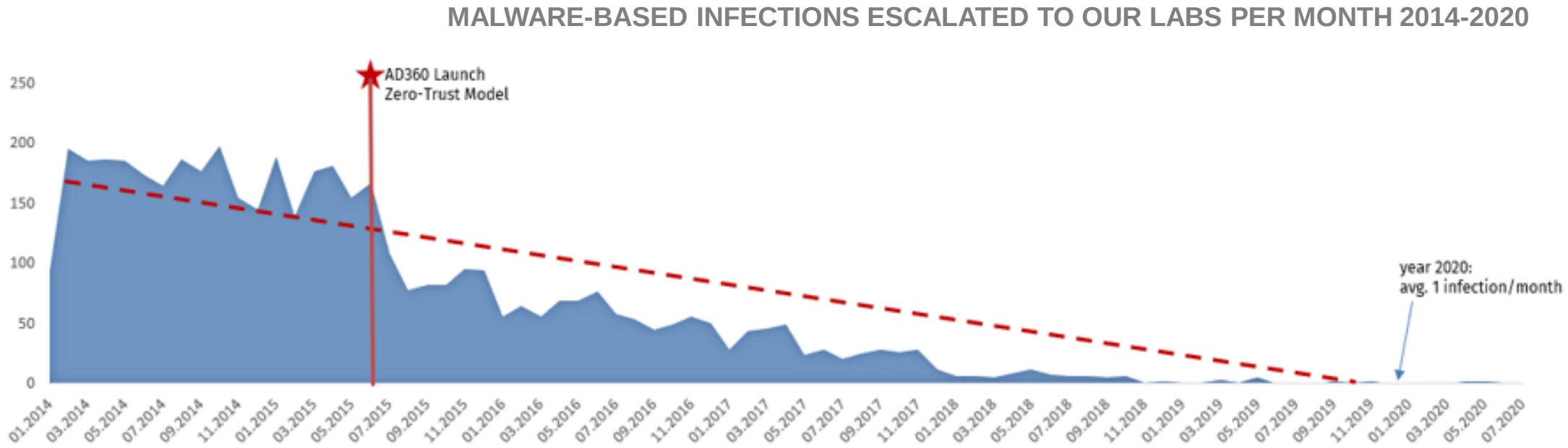
ZERO-TRUST APPLICATION SERVICE



Threat Hunting

Execution monitoring

Our unique protection model. Results



Analysts move from reactively responding to compromised customers to proactively notifying them about suspicious activity in their endpoints

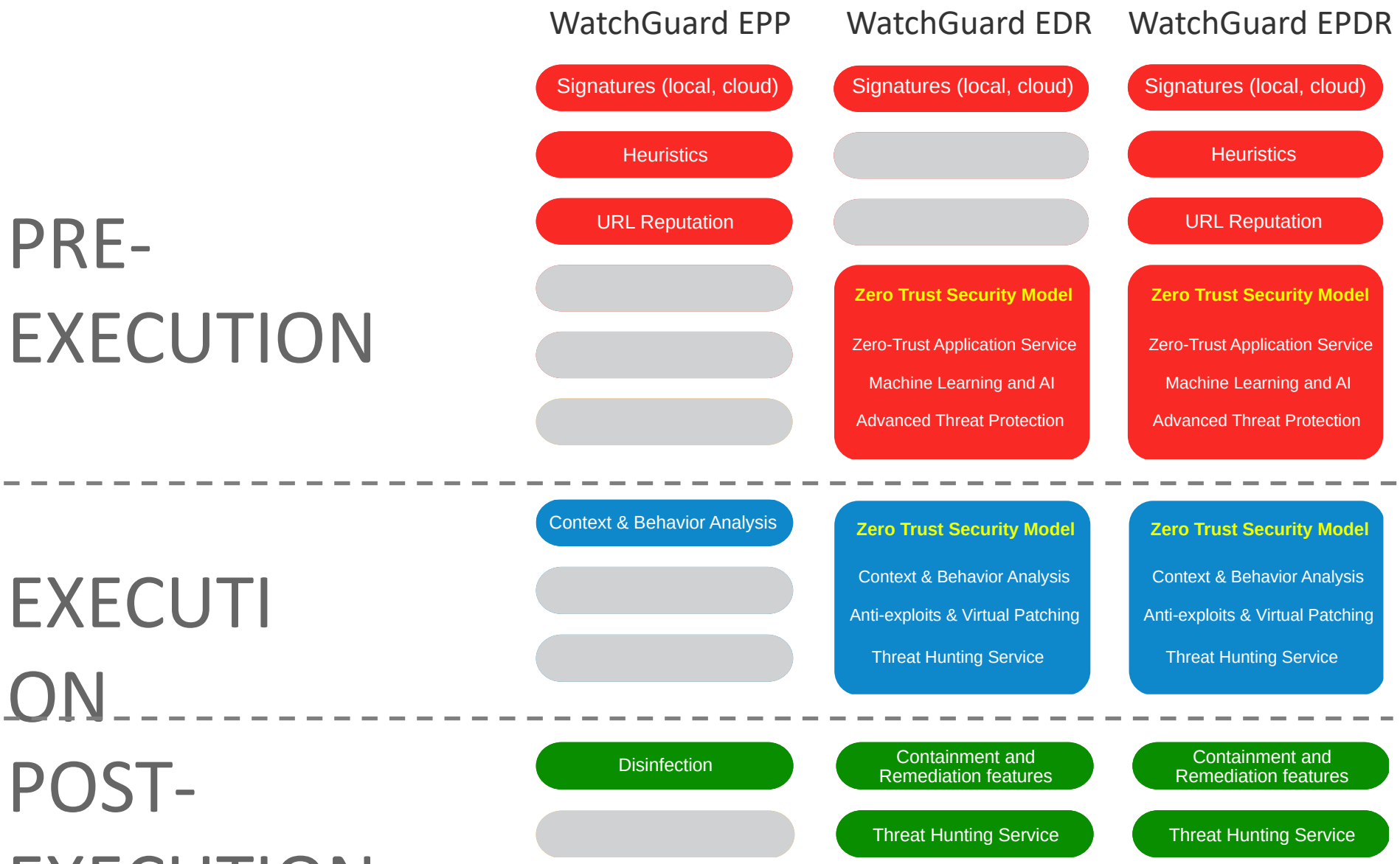
"The Zero-Trust Application Service can drastically reduce the threat surface of endpoints."
Gartner Magic Quadrant for EPP, 2018.

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 Endpoint Protection Model

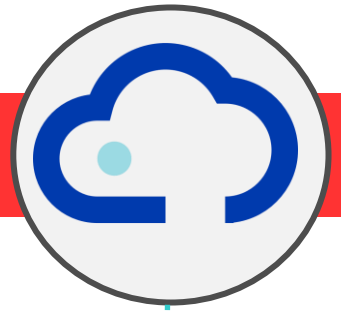


How you win

- Stop ransomware TODAY with a high security posture
- Get an “endpoint security team” with Service-as-a-Feature
- Identify and automate incident remediation
- Mitigate time spent on vulnerability and threat research to prioritize patches
- Reduce the number of agents deployed (including EPP, EDR, SW/HW inventory, full disk encryption, patching)
- Deliver real-time insights into day-to-day application, user and network activity

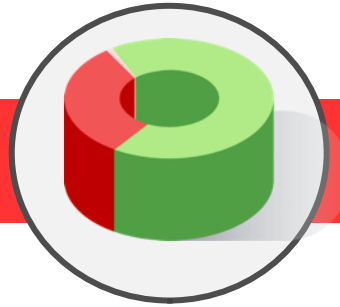
The differentiation

Unified Security Platform



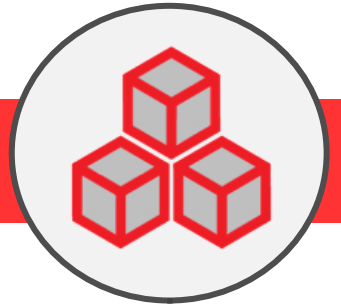
A single pane of glass for security delivery & lightweight endpoint agent

Zero-Trust App Service



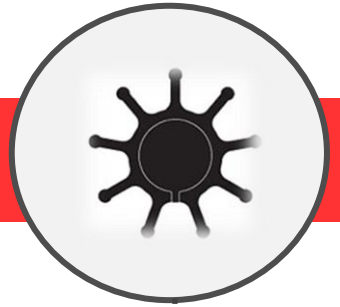
Prevent, detect and respond to known and unknown advanced threats without added cost or complexity

Simplicity



Easy and straightforward to configure, deploy, and centrally manage

Flexibility and Extensibility



A single agent for a complete range of products/modules that allow scaling as partners and customers grow


Q&A


Thank you