Next generation security services as the new paradigm.

Lampros Katsonis
Regional Presales Manager

panda

pandasecurity.com

Panda Security Worldwide

Since its inception in 1990, Panda Security has become a leading European multinational in the development of **advanced cybersecurity** solutions and management and monitoring tools.

Distribution in **+180** countries

Presence in **55** countries

1st Company to introduce daily signatures

Products in **23** different languages

We protect **+200M** devices

We care for **+30M** corporations

1st Company to introduce cloud AV solutions

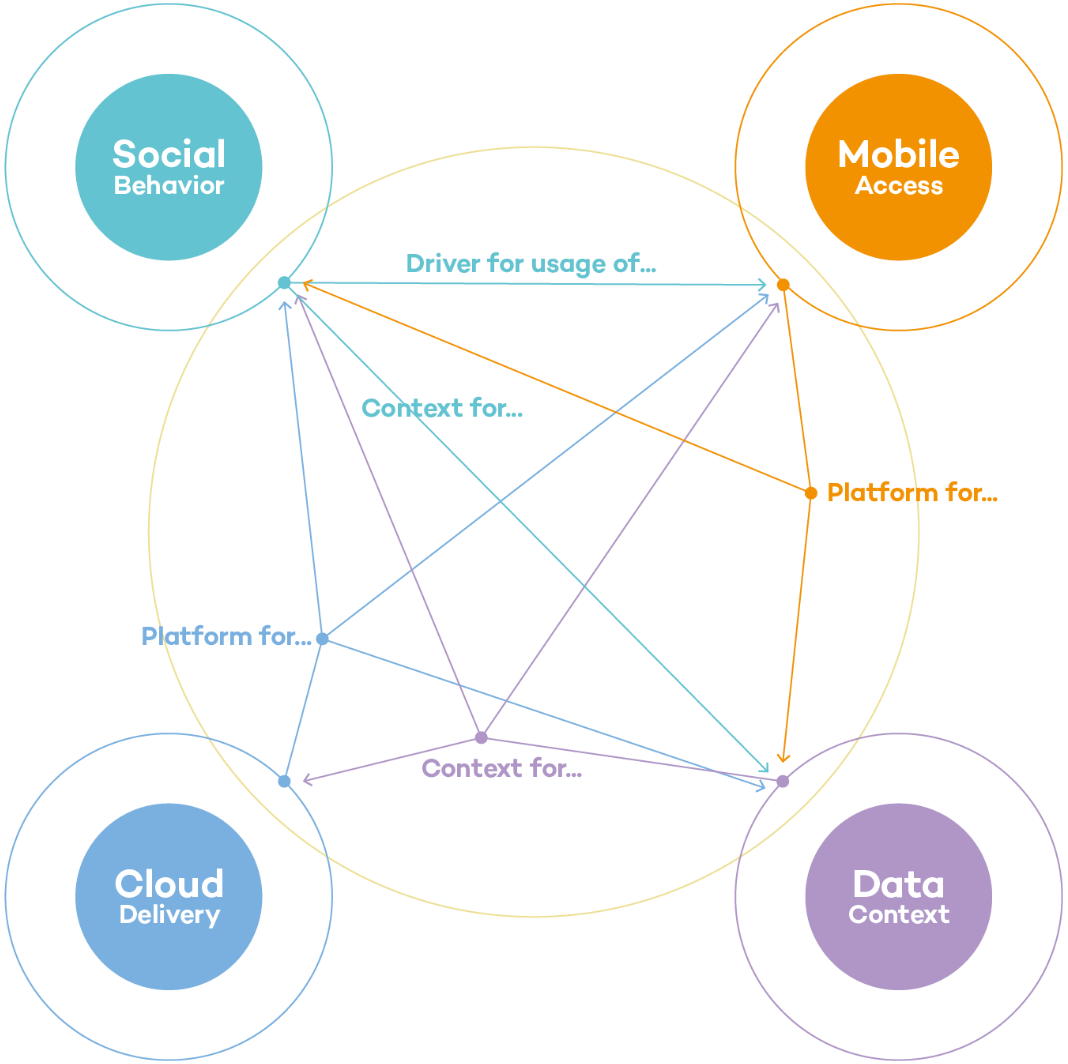
Innovating for **27** years

Dynamics of digital life. "Nexus of forces"

Our current digital behavior means a **complex, interconnected, and hyper-dynamic environment.**

Now, **the perimeter is where the user is**.

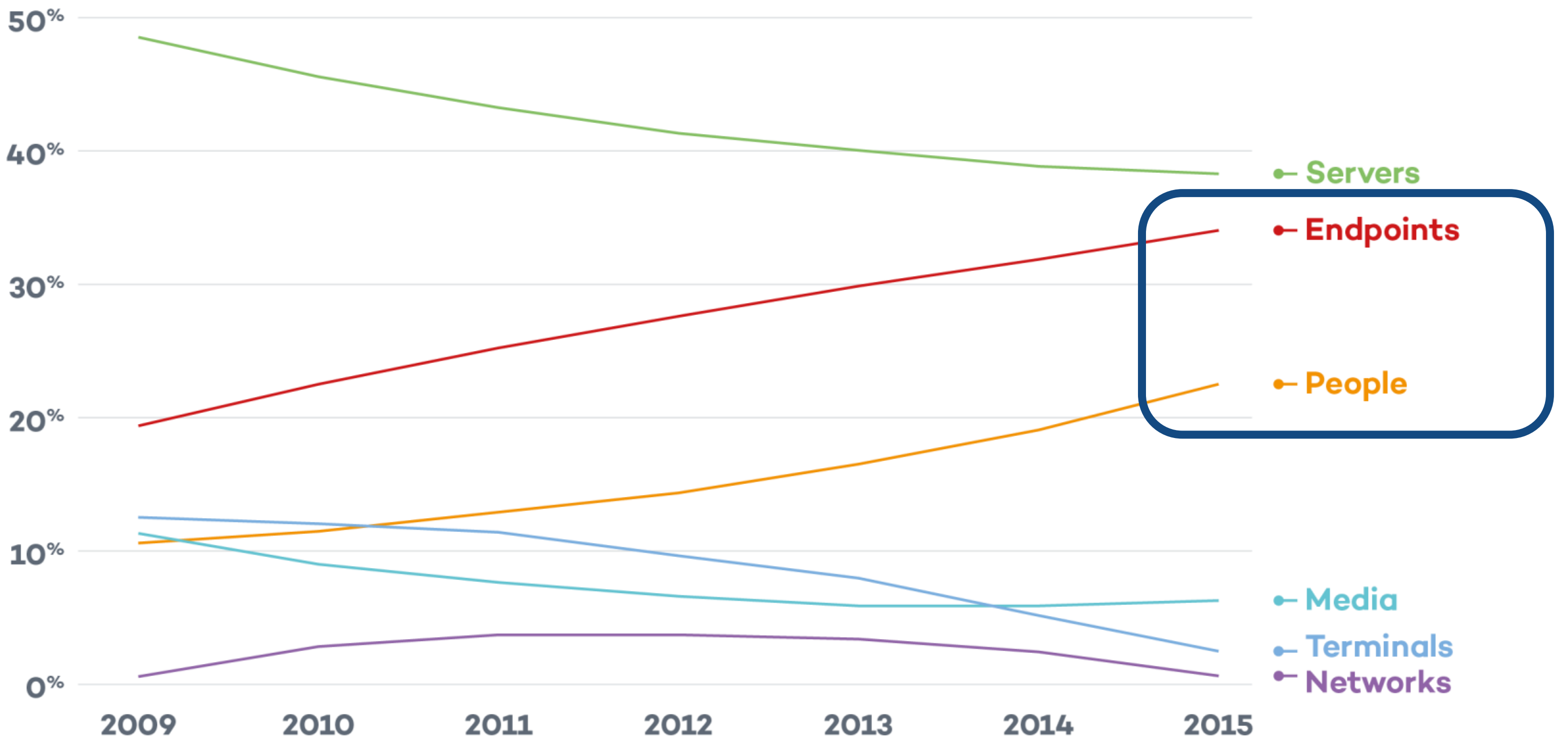
The complexity of IT systems increases **vulnerability in the face of cyber-threats**.



The Target is the Endpoint…

…but only 11% of the security budgets is allocated to protect them

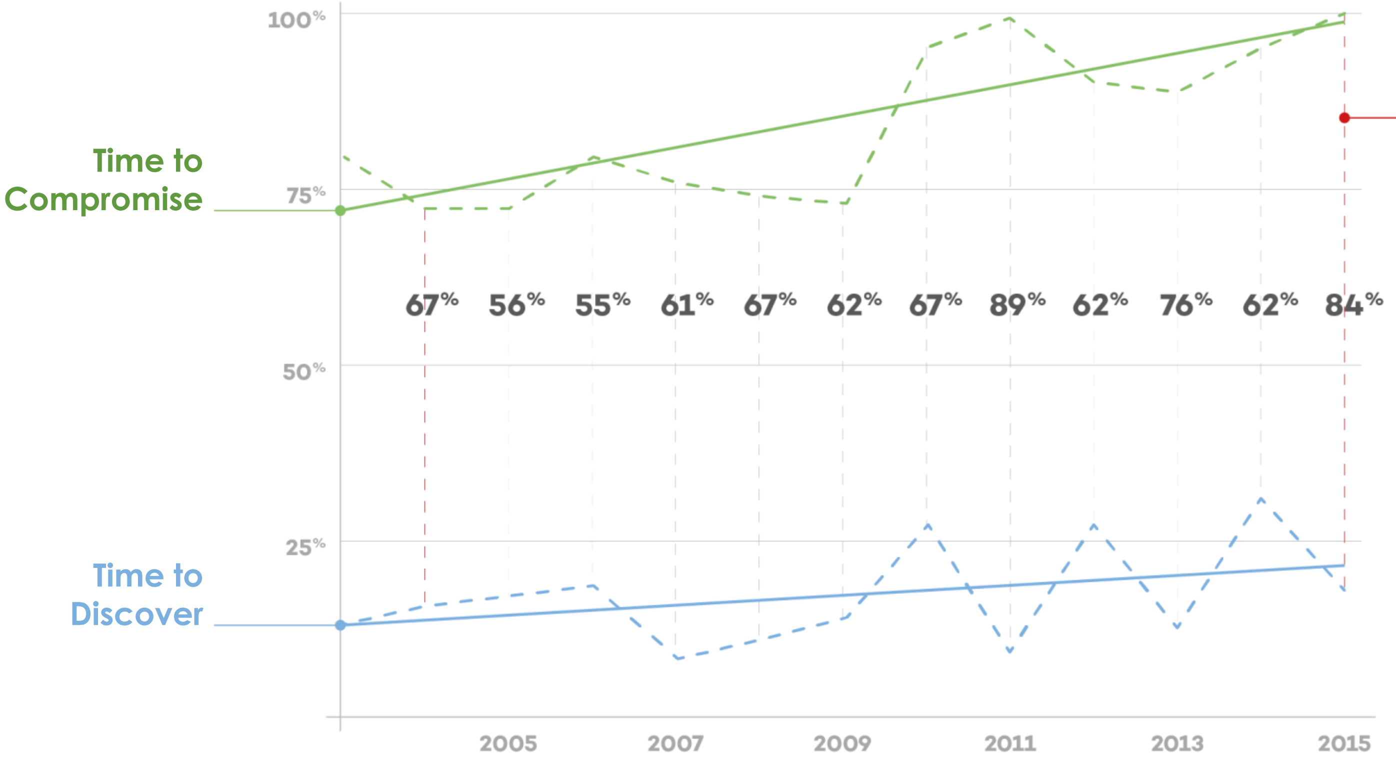
% Incidents by Target



Source: Verizon Data Breach Investigations Report 2016.

The Gap is Getting Wider.

The figure shows how the **percent of breaches** where time to compromise/time to discovery was **days or less is increasing**.



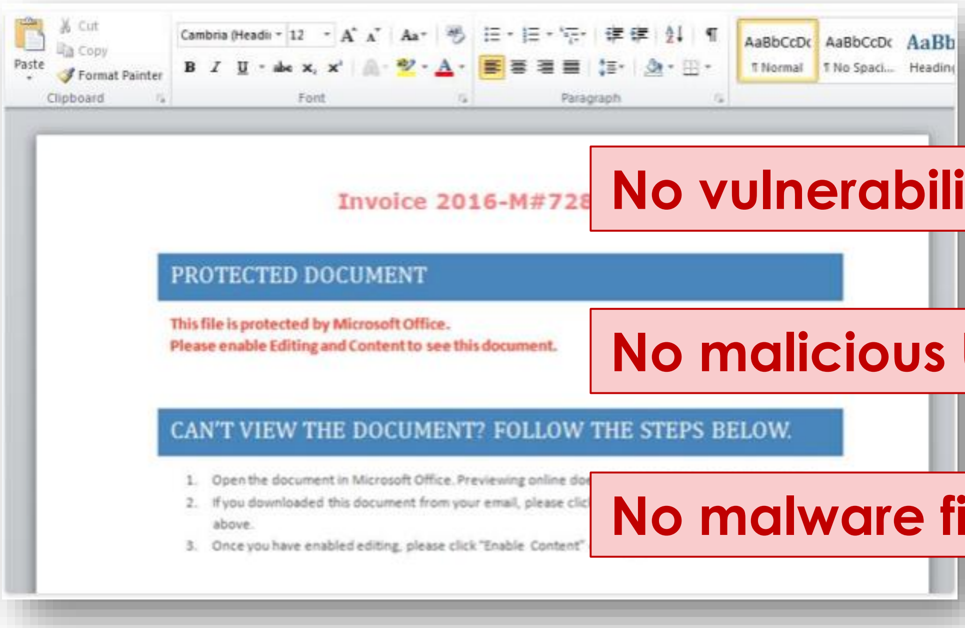
Attackers are more efficient now than ever before.

Source: Verizon Data Breach Investigations Report 2016.

Challenge #1: “Malwareless” attacks.

Attackers exploit social engineering and vulnerabilities in the design of security products.

“POWERWARE” attack



Invoice 2016-M#728

PROTECTED DOCUMENT

This file is protected by Microsoft Office.
Please enable Editing and Content to see this document.

CAN'T VIEW THE DOCUMENT? FOLLOW THE STEPS BELOW.

1. Open the document in Microsoft Office. Previewing online do
2. If you downloaded this document from your email, please clic above.
3. Once you have enabled editing, please click "Enable Content"

No vulnerabilities exploited.

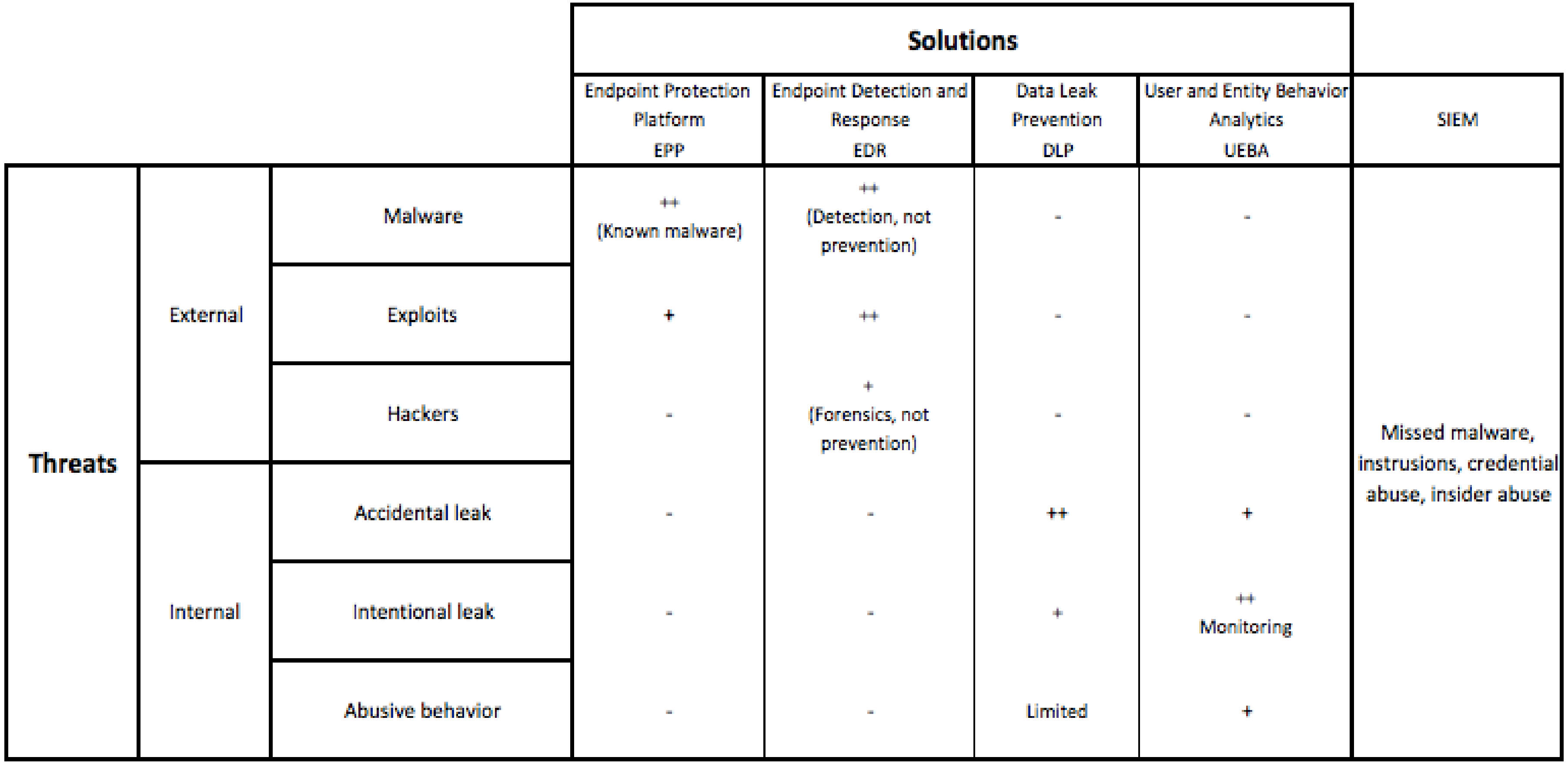
No malicious URL involved.

No malware file on disk.

POWERSHELL encrypts files. Conventional defences won’t work.

Challenge #2: Agent clutter prevents visibility.

Non-integrated solutions create complexity, performance issues, and lack of visibility.



			Solutions				
			Endpoint Protection Platform EPP	Endpoint Detection and Response EDR	Data Leak Prevention DLP	User and Entity Behavior Analytics UEBA	SIEM
Threats	External	Malware	++ (Known malware)	++ (Detection, not prevention)	-	-	Missed malware, instrusions, credential abuse, insider abuse
		Exploits	+	++	-	-	
		Hackers	-	+ (Forensics, not prevention)	-	-	
	Internal	Accidental leak	-	-	++	+	
		Intentional leak	-	-	+	++ Monitoring	
		Abusive behavior	-	-	Limited	+	

Top challenge: Alert noise

Only 4% of alerts are ever investigated.

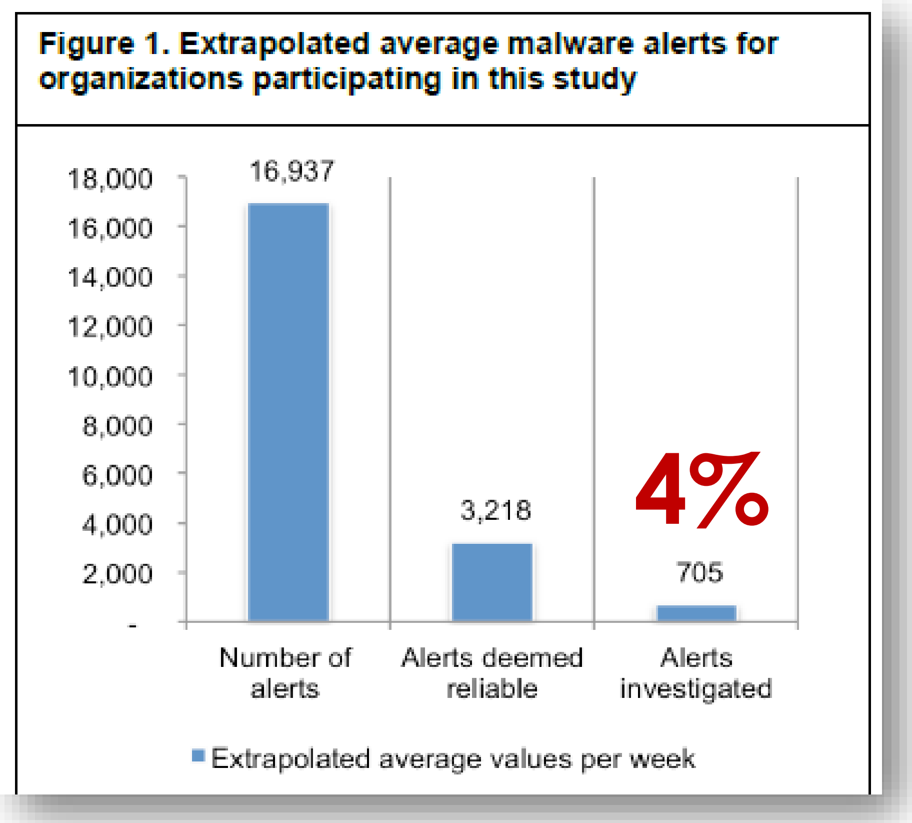


Figure 1. Extrapolated average malware alerts for organizations participating in this study

"Two-thirds of the time spent by security staff responding to malware alerts is wasted because of faulty intelligence"

"It costs organizations an average of $1.27 million annually in time wasted responding to erroneous or inaccurate malware alerts"

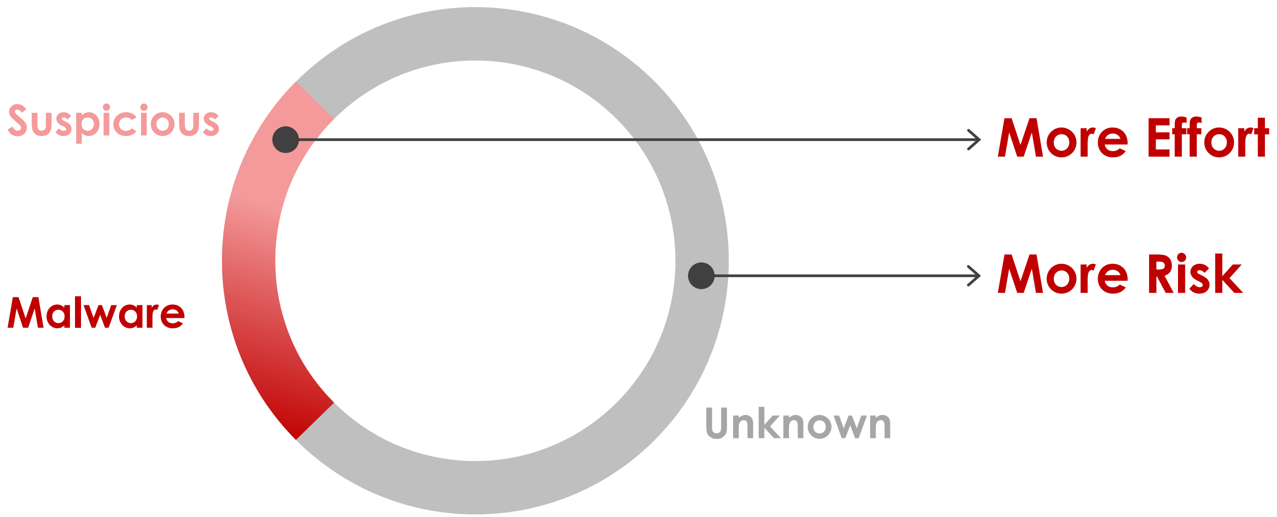
Source: Ponemon Institute. "The cost of malware containment". n=630.

A New Approach to Endpoint Security.

The Prevailing Paradigm…

… is based on **punctual detection** only of **known malicious processes**, this means that:

- All **suspicious activity** has to be **investigated case by case**.
- **All unknown malicious processes are allowed.** That's why attackers skirt around these systems so easily, and their **attacks' success rate is so high**.

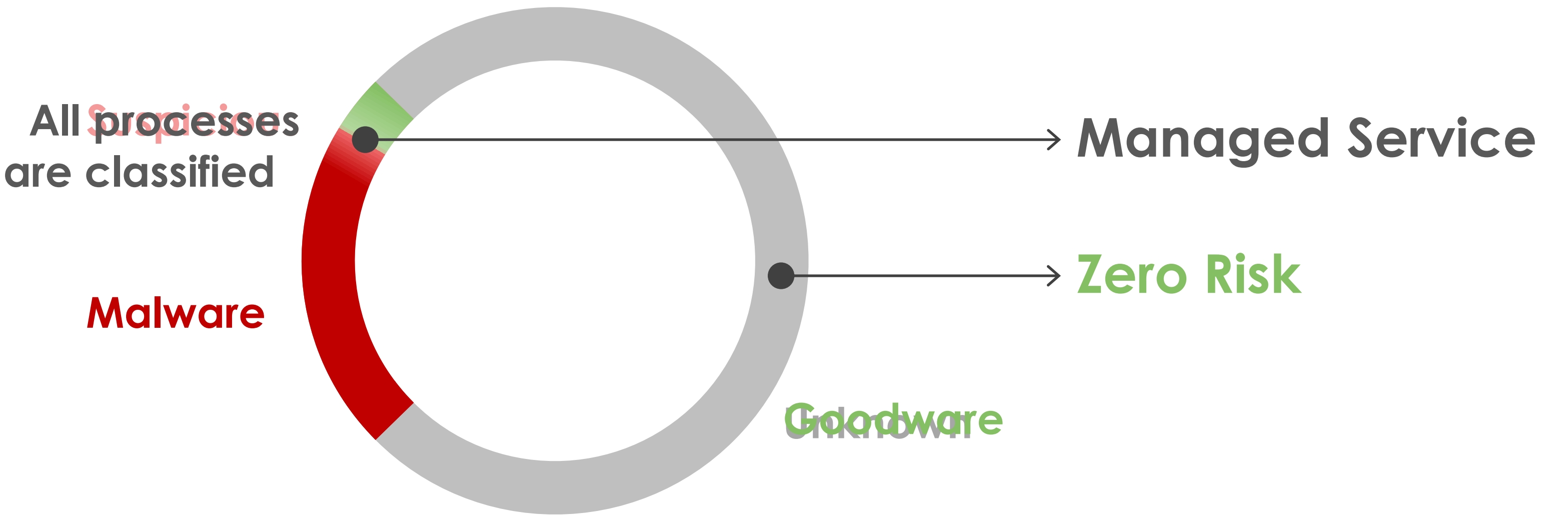


A New Cybersecurity Paradigm.

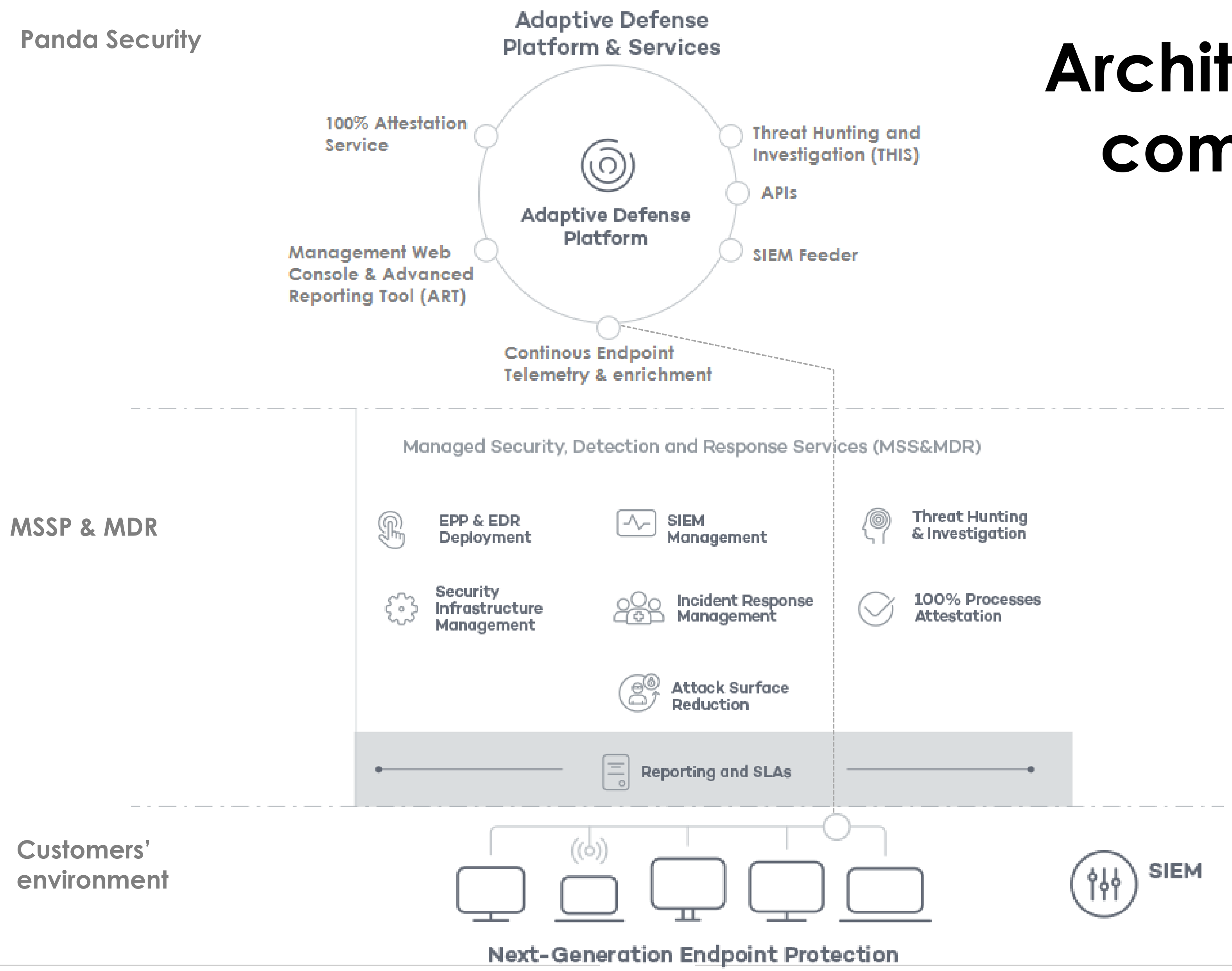
It is based on the **classification of absolutely all running processes** on your network.

- All **activity of all programs is monitored and analyzed in real-time**.
- All **behaviors are verified by a managed service**, the admins don’t have to investigate anything.
- **Higher level of protection with fewer effort.**

Managed Service with
Real Time Visibility & Forensic Analysis



Architecture & components



Panda Security

Adaptive Defense Platform & Services

Adaptive Defense Platform

100% Attestation Service

Management Web Console & Advanced Reporting Tool (ART)

Threat Hunting and Investigation (THIS)

APIs

SIEM Feeder

Continous Endpoint Telemetry & enrichment

MSSP & MDR

Managed Security, Detection and Response Services (MSS&MDR)

EPP & EDR Deployment

SIEM Management

Threat Hunting & Investigation

Security Infrastructure Management

Incident Response Management

100% Processes Attestation

Attack Surface Reduction

Reporting and SLAs

Customers' environment

SIEM

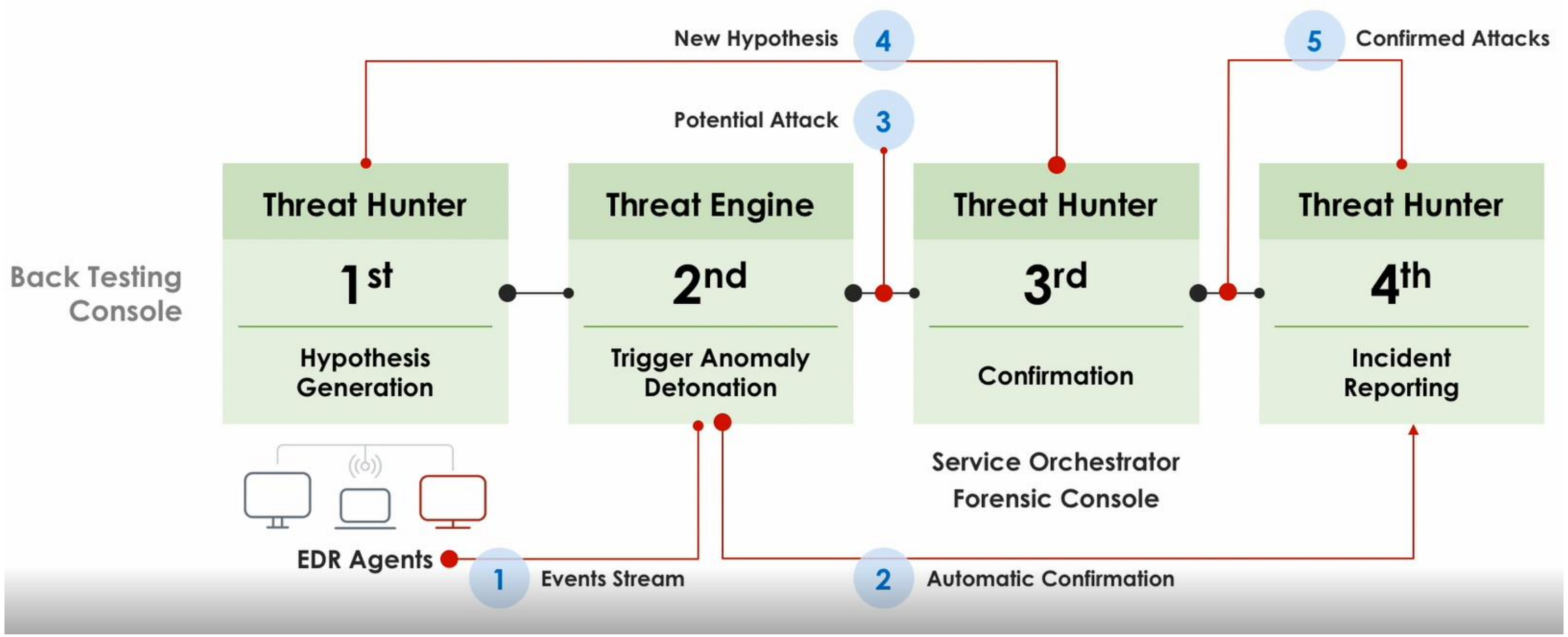
Next-Generation Endpoint Protection

How Adaptive Defense Works.

Sequence of filters.

Technology	Filter 1 Black Listing	Filter 2 White Listing	Filter 3 Auto Classification	Filter 4 Manual Classification
Detects	Known Malware	Known Goodware	Unknown Processes	New Attack Patterns
Based on	Competition: Hash AD: Behavior	Competition: Hash AD: Behavior	AD: Machine Learning	AD: Malware Analyst
Results	1.2 Billion	2.5 Billion	99.985% Automatic	0.015% Manual 1 Analyst: 250K endpoints

Threat Hunting process



Differentiation of Adaptive Defense.

Aplication Trustability

- **Trusted** applications
- **Eliminates detection gap**

Full traceability

- **Real monitoring** (no sandboxing)
- **Forensic Aid**
- **SIEM integration**

Management

- **Compatible** with other security products
- **Simple and immediate installation**

Service

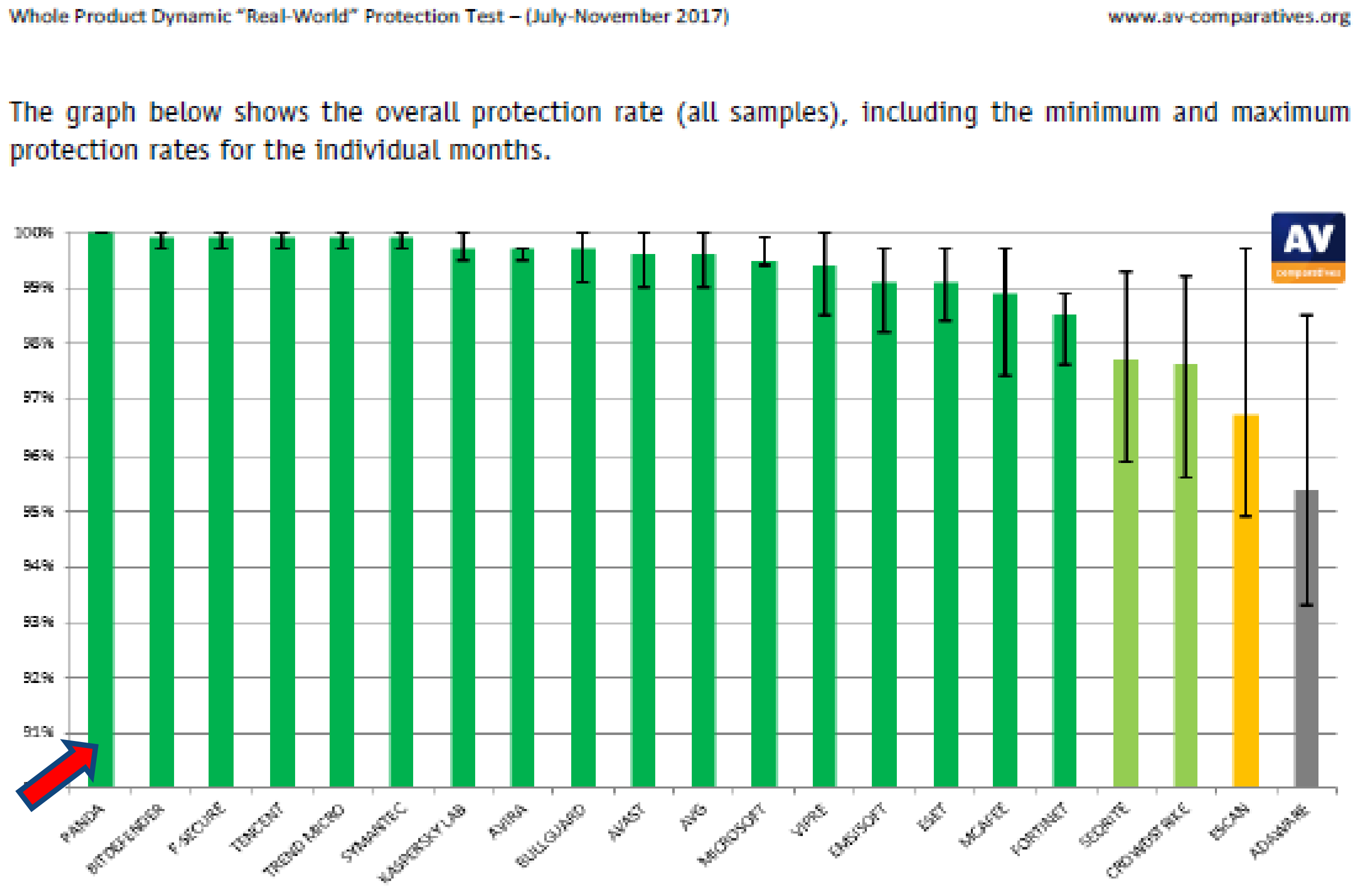
- **Unattended:** dedicated Panda's analysts
- All alerts are **confirmed**

100% Malware Prevention & Protection

TCO Drastically Improved

Third party validation

AV-Comparatives Benchmark



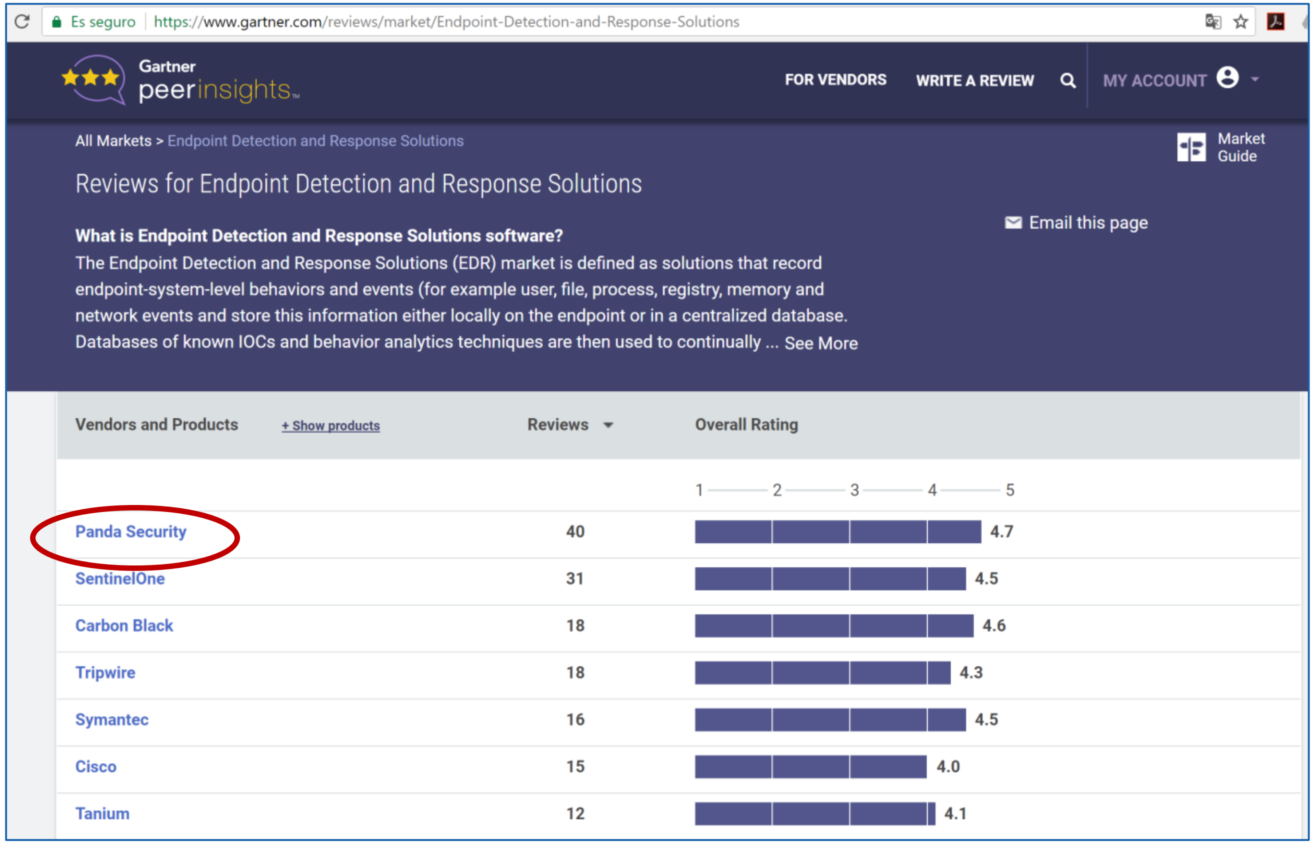
Whole Product Dynamic "Real-World" Protection Test – (July-November 2017) www.av-comparatives.org

The graph below shows the overall protection rate (all samples), including the minimum and maximum protection rates for the individual months.

100% detection rate in the last 6 months in a row. Real-world test.

Third party validation

Gartner’s Peer-Insights program



All Markets > Endpoint Detection and Response Solutions

Reviews for Endpoint Detection and Response Solutions

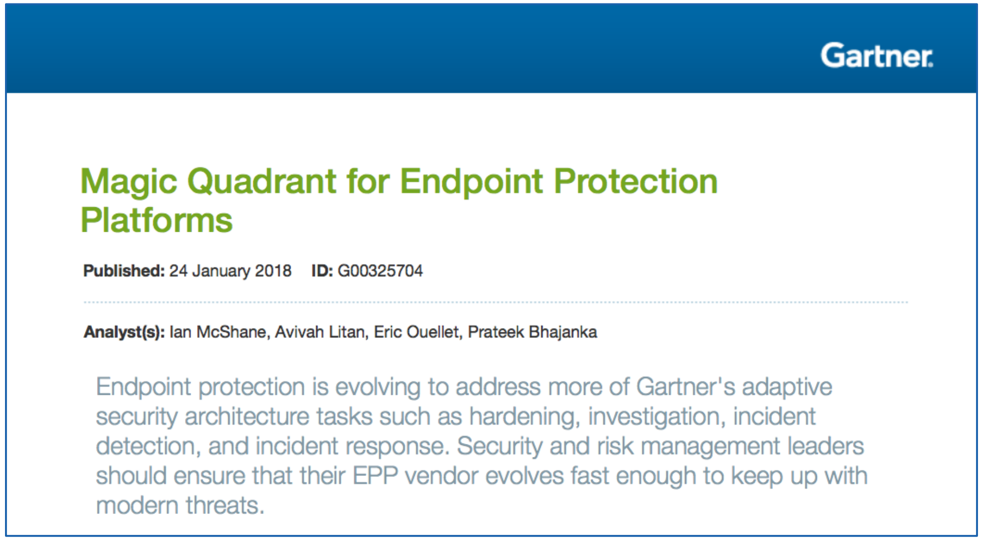
What is Endpoint Detection and Response Solutions software?

The Endpoint Detection and Response Solutions (EDR) market is defined as solutions that record endpoint-system-level behaviors and events (for example user, file, process, registry, memory and network events and store this information either locally on the endpoint or in a centralized database. Databases of known IOCs and behavior analytics techniques are then used to continually ... See More

Vendors and Products	Reviews	Overall Rating
Panda Security	40	4.7
SentinelOne	31	4.5
Carbon Black	18	4.6
Tripwire	18	4.3
Symantec	16	4.5
Cisco	15	4.0
Tanium	12	4.1

Ranked first in class for EDR Market with an overall rating of 4,7/5

Third party validation



Gartner.

Magic Quadrant for Endpoint Protection Platforms

Published: 24 January 2018 **ID:** G00325704

Analyst(s): Ian McShane, Avivah Litan, Eric Ouellet, Prateek Bhajanka

Endpoint protection is evolving to address more of Gartner's adaptive security architecture tasks such as hardening, investigation, incident detection, and incident response. Security and risk management leaders should ensure that their EPP vendor evolves fast enough to keep up with modern threats.

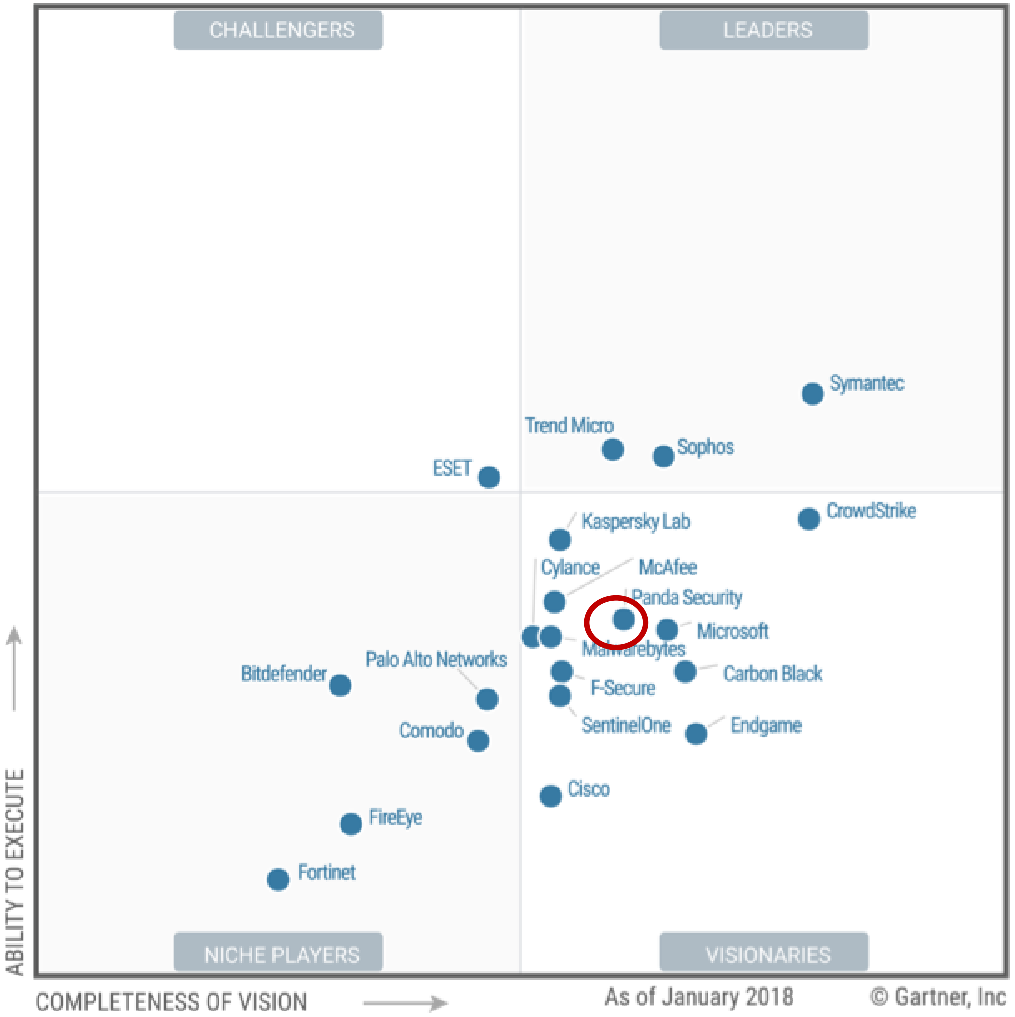
"…it is the only vendor to include a managed threat hunting service in the base purchase"

"The 100% attestation service can drastically reduce the threat surface of endpoints"

"…organizations will have a much better deployment success rate..:"

Magic Quadrant

Figure 1. Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (January 2018)

Adaptive Defense

Differentiating values.

100% Attestation Service

By Panda.

Continuous Monitoring and Threat Hunting

Total Visibility of endpoint activity.

Seamless Deployment and Management

Not a single malware infection allowed by Adaptive Defense in lock mode

Reinventing Cybersecurity.