

Panda Security



[pandasecurity.com](https://www.pandasecurity.com)

Global Presence

Since its inception in Spain in 1990, Panda Security has been a leading developer of cybersecurity solutions and management and monitoring tools.

We are one of the main cybersecurity vendors, protecting individuals and enterprises.

We protect
+200M
devices

Offices in
55
countries

We have
+600
employees

Innovating for
28
years

29 Years of Innovation

Over the course of its history, Panda Security has introduced some of the most important advances in the world of cybersecurity

2019.

The leading European vendor of EDR systems, receiving the Gartner Peer Choice distinction

2018.

First EDR vendor to receive EAL2+ certification under common criteria recognized by 28 countries globally

2017.

The only vendor to include a managed threat hunting service in the base purchase of its EPP

2015.

First with a combined security model: Endpoint Protection Platform + Endpoint Detection & Response (EPP+EDR)



1994.

First network deployment and update tool

1998.

First daily signature

2007.

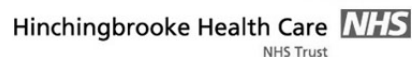
First product to use cloud based scanning

2012.

First security business with an entirely cloud-based product offering

Leading UK Clients Trust Panda

Public Sector



Industry



Charity / NFP



Independent Views



What others say



Best Endpoint Detection and Response Solutions of 2019 as Reviewed by Customers

Customers' Choice - Jan 2019



Gartner Peer Insights have collected more than 120,000 customer reviews across over 320 markets.

They recognize the most valued vendors with a

Vendors and Products	Reviews	Overall Rating	
		1 — 2 — 3 — 4 — 5	
Carbon Black	190	4.5	customers' choice 2019
SentinelOne	135	4.7	customers' choice 2019
Panda Security	129	4.6	customers' choice 2019
CrowdStrike	78	4.8	customers' choice 2019
Symantec	76	4.6	customers' choice 2019
Cybereason	75	4.4	customers' choice 2019

What reviews say

Panda Security are a founding member of AMSTO

We have an enviable record from numerous independent reviews and comparatives.

Our cloud-based security service combines
protection services and top value ensures it earns a
well-deserved reputation for reliability and performance.

Our cloud-based security service combines
genuine security and top value ensures it earns a
well-deserved reputation for reliability and performance.
PC Pro A-List

We ultimately recommend clients try our solution in their network to ensure it is right for them.



Common Criteria

Panda Adaptive Defense 360 is the first EDR to achieve EAL2+ under the Common Criteria.

EAL2+ requires the developer to consider the product on a holistic basis- design, development, customer usage, support and future considerations.

Reassures customers that developer's claims about the security features of their product are valid and have been independently tested.

Common Criteria is recognised by 28 countries across the globe.

In the UK this is overseen by NCSC.



Common Criteria certified solutions are required by governments and enterprises around the world to protect their mission-critical infrastructures.

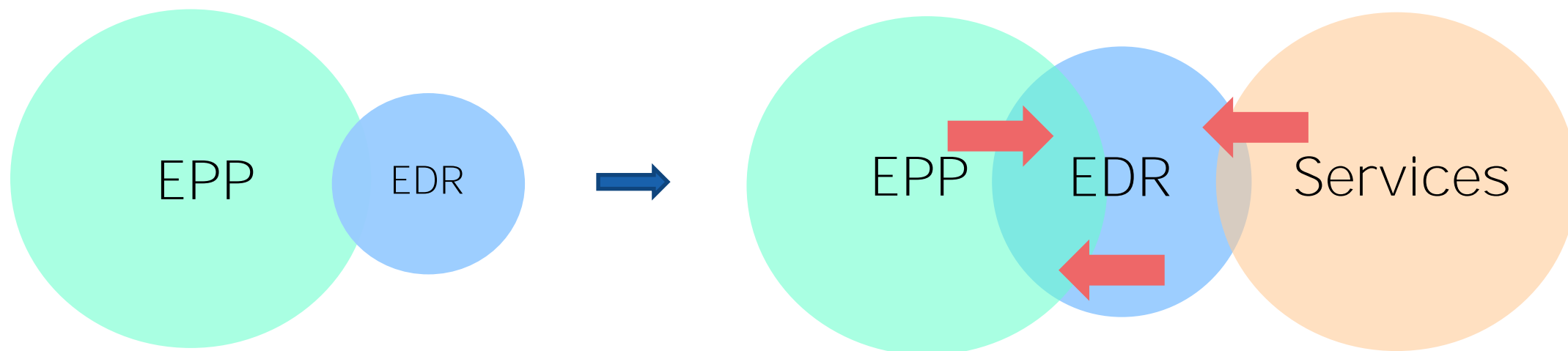
The Common Criteria standard provides an assurance on different aspect of the product security covering areas such as:

- “ Product Development - specification, design, security architecture and implementation
- “ User Guidance - for secure deployment and preparation of the product
- “ Independent Tests- The product and functional security requirements
- “ Vulnerability assessments

Panda Security Solutions

The simplest solution to the most complex digital challenges.

Endpoint protection trends

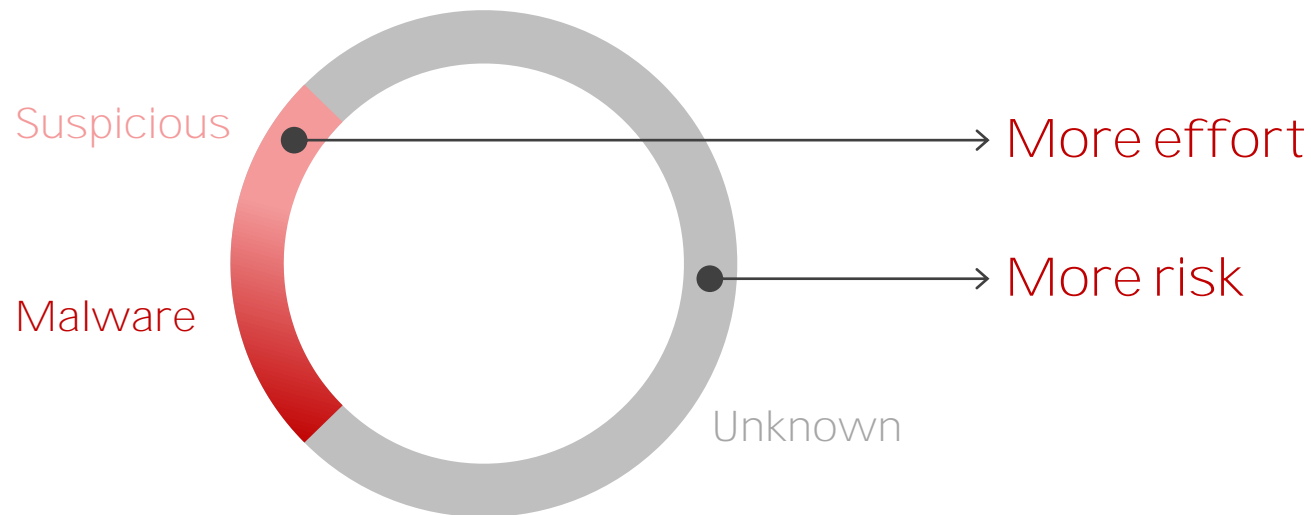


- “ Endpoint Protection Platforms consolidating EDR functions.
- “ Leading vendors offering managed Threat Hunting Services.

The current model Å

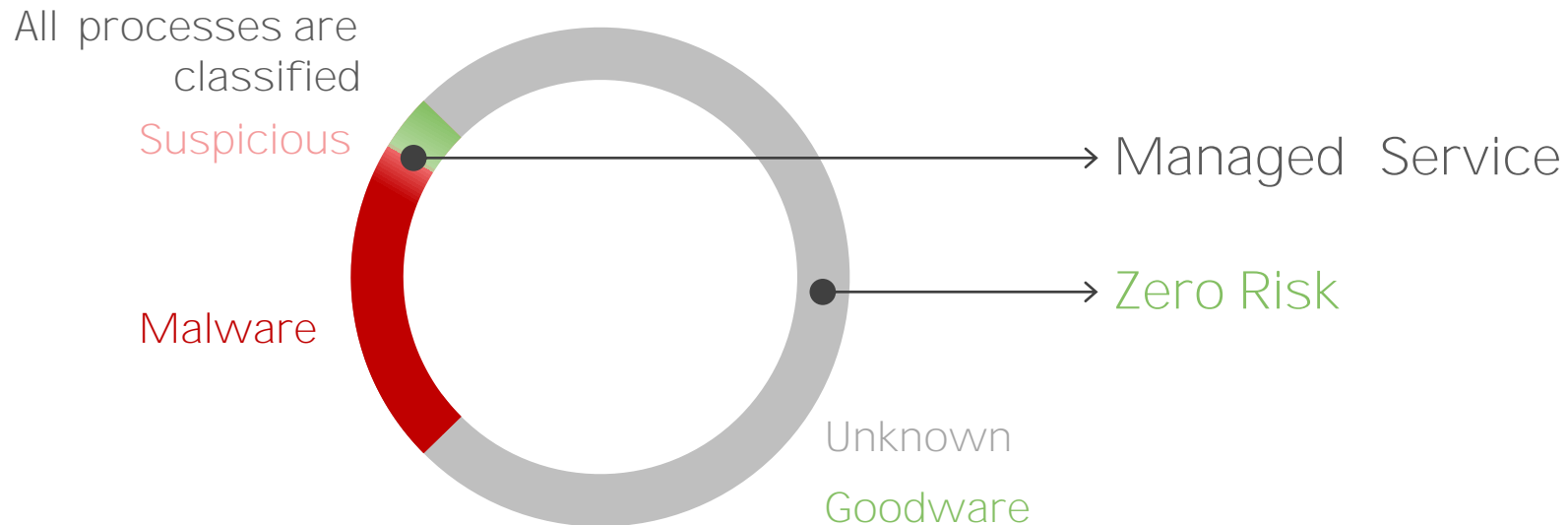
Å] g · V U g Y X isolated detection of known malicious processes which means:

- “ All suspicious activity must be investigated on a case-by-case basis.
- “ All malicious processes are allowed.
H \ U h Ñ g · k \ m · \ U W_ Y f g · WU b · k c f _ systems so easily and their success rate is so high.



A new model of cybersecurity is born

Service managed by
Real-time visibility and forensic analysis



Based on the classification of all running processes on your network

- “ Every d f c [f l a t i t y is monitored and analyzed in real time.
- “ All behavior is verified by the managed service. The administrator does not have to investigate anything.

Maximum level of protection, less effort and no risk.

Panda Adaptive Defense 360

Organisations still being compromised: Despite layers of next-gen security, hackers, zero-day and targeted attacks are still causing havoc.

Panda Adaptive Defense is a security suite that integrates Endpoint Protection and Endpoint Detection and Response (EDR) solutions, with 100% Attestation and Threat Hunting and Investigation Services, all delivered via a single lightweight agent.

The combination of these solutions and services provides a highly detailed visibility of all endpoint activity, an absolute control of all running processes, and the reduction of the attack surface.



- “ Prevention, Detection and Response for malware and malwareless attacks, under a single agent.
- “ Real time and Historical Visibility of all endpoint activity with highly detailed information.
- “ 100% Classification of Processes 99.98% by Machine Learning, \$ " \$ & i ' V m ' D U b X U Ñ g ' a U ` k U f Y ' Y I d Y f h g "
- “ Threat Hunting and Forensic Analysis led by Panda Security and A G G D Ñ g ' Y I d Y f h ' U b U ` m g h g "

Panda Advanced Reporting Tool

IT staff are overwhelmed: Increasing volumes of data causes vital details to be overlooked

This module aggregates all the data gathered, correlating and graphically presenting it in real time to offer granular visibility into any event that takes place on the network.

The Advanced Reporting Tool dashboards include key indicators, searches and preset alerts across three areas:

- “ Security incidents.
- “ Access to critical information.
- “ Network resources and applications used.



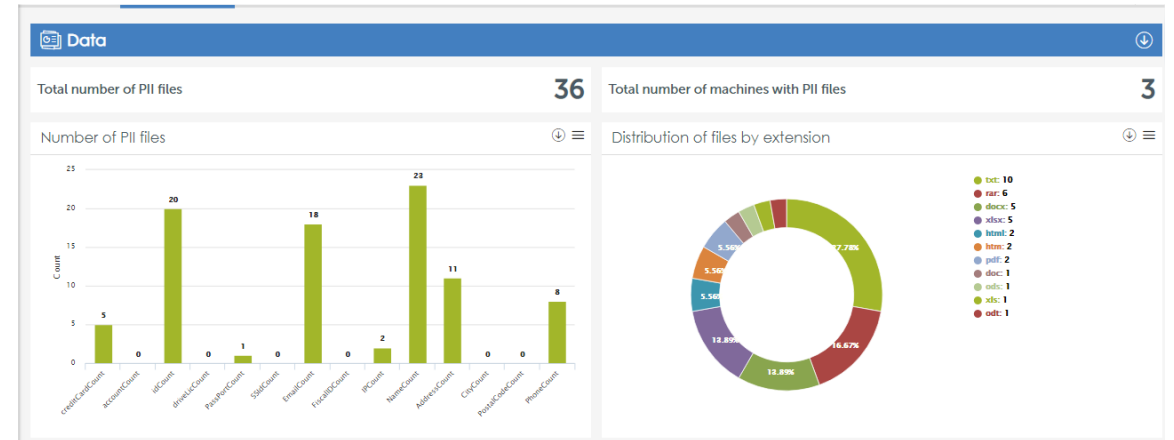
- “ Threat control: Determining the origin of security threats and applying security measures to prevent future attacks.
- “ Manage access: Implementing more restrictive policies to access critical business information.
- “ Monitor and detect: misuse of corporate resources that may have an impact on business and employee performance.
- “ Correcting employee behavior that is not in line with the usage policies defined.

Panda Data Control

Massive data breaches occur too often: Uncontrolled access to company personal (PII) & sensitive (IP) data is an everyday threat leading to serious financial loss & reputational damage.

This module is designed to assist organizations in complying with data protection regulations, as well as discovering and protecting personal and sensitive data both in real time and throughout its lifecycle on endpoints and servers.

Panda Data Control discovers, audits and monitors unstructured personal data on endpoints: from data at rest to data in use and data in motion.

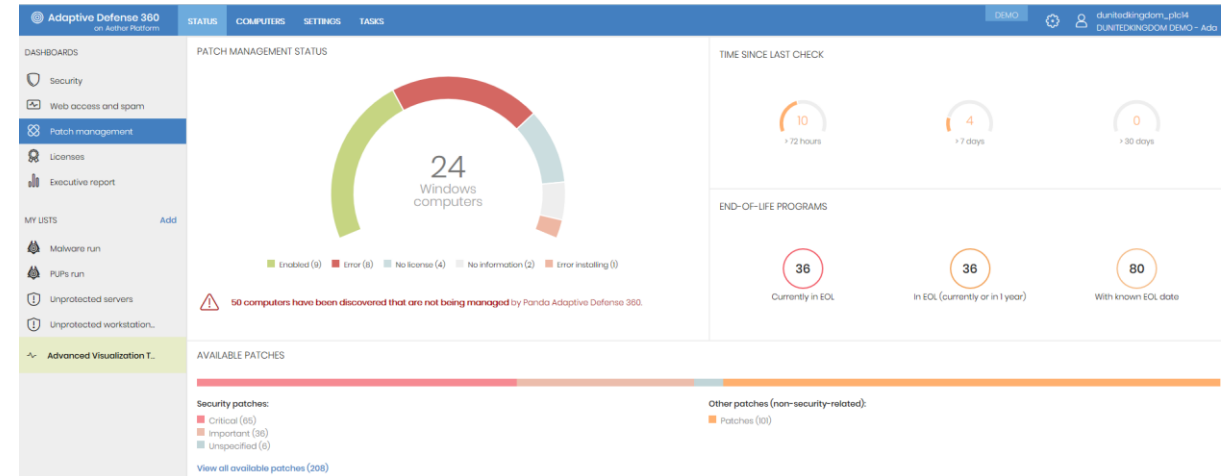


- “ Discover and audit: Identifies users, devices, or servers in your company with access to Personally Identifiable Information (PII).
- “ Monitor and detect: Alerts, in real time, on leaks, use, and suspicious unauthorized transit.
- “ Simplify management: Its activation is immediate and managed directly from the same Cloud platform.
- “ Control of Data: Demonstrate that the company has complete control over the PII located on its devices.

Panda Patch Management

Vulnerabilities are constantly being exploited: Unpatched software leaves the doors to your network wide open to hackers.

The single most effective method of blocking malware and hackers from entering your network is to patch known vulnerabilities.



- “ Scan all computers, from anywhere, any time.
- “ No additional deployments - single agent)
- “ Update all versions of third party apps.
- “ Apply patches on test computers before pushing out.
- “ Generate rules for automatic patching with exceptions.
- “ Update hundreds or thousands of computers in real time.
- “ Automatic management of patch interdependencies .

Reinventing Cybersecurity

