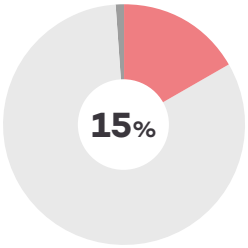
Panda Adaptive Defense 360 for MSPs/MSSPs

Reinventing your cybersecurity services

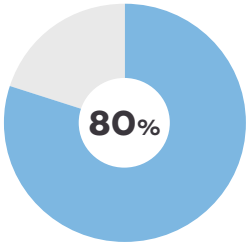
GARTNER[1] PREDICTION FOR 2020:



15% of all **medium to large companies** will be using **detection and response services managed by providers.**

15% by 2020

>1% today



80% of **security service providers globally** will be offering **managed detection and response services.**

80% by 2020

SEIZE THE OPPORTUNITY

MSPs and MSSPs have a great opportunity to expand their service portfolio and now is the time for them to act and help their customers adopt an advanced and adaptive endpoint security. EDR solutions with **automated detection and response, and managed services** are the fastest and most cost-effective way, as no investment is required in proprietary technologies or expert support, rapidly generating value.

Panda Adaptive Defense 360 is the cloud-based, cybersecurity solution for workstations, laptops and servers that automates the prevention, detection, containment and response against any present or future advanced threats, zero-day malware, ransomware, phishing, memory exploits and malwareless attacks.

It is different from other solutions in that it combines the widest suite of **protection technologies (EPP)** with **automated EDR capabilities**, thanks to one service **managed by the experts** at **Panda Security:**

- Service for classifying **100% of applications.**

This service ensures that cyberthreats are identified before they can run or generate massive damage across the organization.

ADVANCED AND ADAPTIVE SECURITY ON ENDPOINTS

Traditional security, based on detecting known malicious processes, is insufficient. Gartner has encouraged businesses to move from "response to incidents" to "continuous response", meaning that an organization is continuously committed to security, as endpoints are continually under threat from attackers.

Panda Adaptive Defense 360, reinforces the four phases of Gartner's[2] adaptive security architecture:

- **Prevent:** The model stops unknown processes from running until they are classified as trusted by Machine Learning technologies, supervised by data analysts and malware experts.
- **Detect:** ML (Machine Learning) and behavior monitoring of processes identify attacks that successfully evade preventive measures.
- **Respond and forensic analysis:** Contain the attack, prevent its lateral movements, remedy the effects, and identify what, how and why, among other points.
- **Predict attacks:** Anticipate them, analyze trends, and switch from a reactive to a proactive approach with actions to reduce the attack surface.

THE OPPORTUNITY

Endpoints are the new perimeter

Mobility, processing and cloud storage have revolutionized corporate environments. **Endpoints are the new perimeter**. Security solutions on endpoints must be **advanced, adaptive and automatic**, with the highest levels of prevention and detection of attackers, who will sooner or later manage to evade preventive measures. Such solutions must also offer agile tools to respond quickly, minimizing damage and reducing the attack surface

The professionalization of hackers

Enemies are increasingly sophisticated and growing in number, the result of their professionalization, the democratization of technologies and the continuous leaks of cyberintelligence.

Next-generation **cyberthreats** are **designed to slip past traditional solutions completely undetected**, using different **hacking techniques**, such as the use of legitimate software for malicious purposes.

Problems for organizations

EDR solutions, far from being the solution, increase **workloads**, demanding specialized cybersecurity resources to correlate millions of events and analyze the multitude of alerts generated, which in many cases are false. Such expert help is scarce and expensive.

Businesses are looking for their suppliers to deliver products, technologies and managed, comprehensive services that make advanced and adaptive security viable.

OBSTACLES FOR MSPS AND MSSPS

Most MSPs and many MSSPs suffer the effects of the **commoditization of the sector, with decreasing margins**. They experience the continuous flight of customers to other MSSPs and SoCs that offer advanced security services in the perimeter, network and on endpoints themselves, based on economies of scale, proprietary technologies and specialized resources, all which require a large initial investment.

They also lack **visibility** and experience in **endpoint** monitoring.

[1] **Gartner Market Guide for Managed Detection and Response Services**. Toby Bussa, Craig Lawson, Kelly M. Kavanagh, Sid Deshpande May 31, 2017
[2] **Designing an Adaptive Security Architecture for Protection from Advanced Attacks**. Neil MacDonald and Peter Firstbrook, 12 February 2014, refreshed 28 January 2016, ID G00259490,

Panda Adaptive Defense 360 for MSPs/MSSPs

Implementing an advanced and adaptive security model requires the perfect synchronization of technologies and experts in Big Data, machine learning, cybersecurity intelligence and automated response and remediation tools, among many other things.

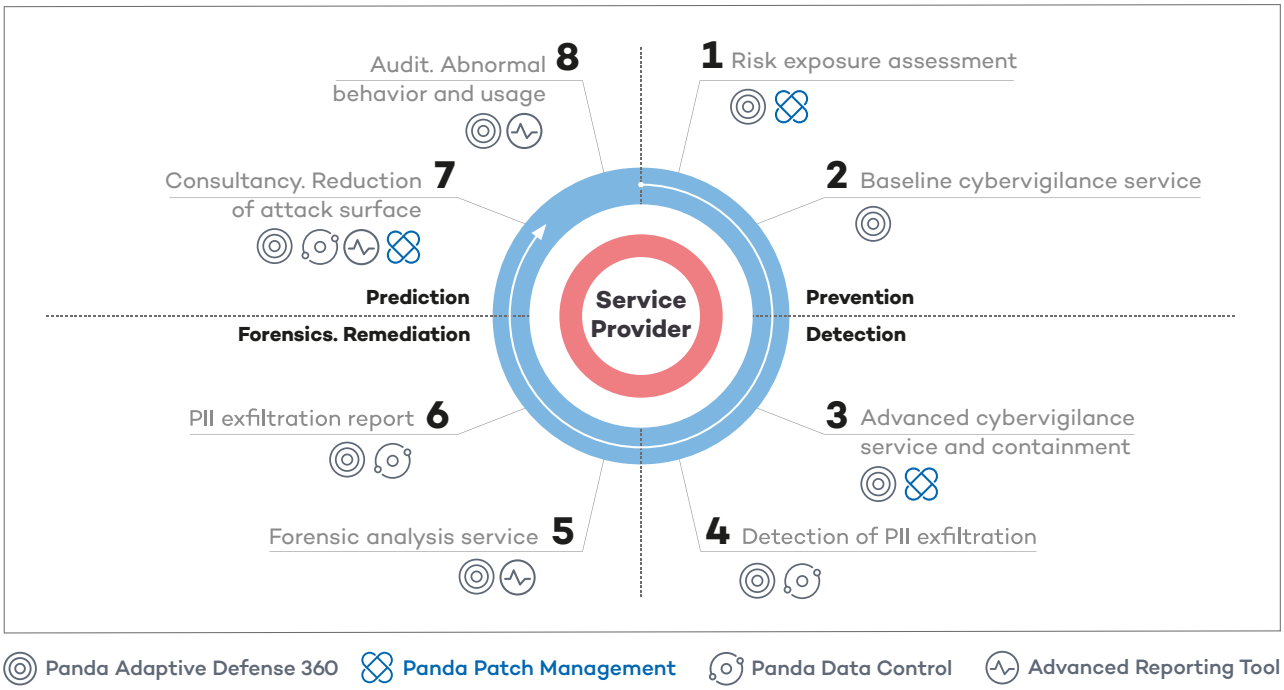
Panda Adaptive Defense 360 and its modules (Panda Patch Management, Advanced Reporting Tool, Panda Data Control and Panda Full Encryption) seamlessly deliver the means our Partners need to increase their services with advanced security on endpoints, without major investment.

Figure 1 below shows some of the Expanded Advanced and Adaptive Security Services that our Partners can offer customers thanks to Panda Adaptive Defense 360 and its modules.

BENEFITS FOR PARTNERS

- **Greater offer** of services, **competitive differentiation** for your business.
- **Upgrade and cross-sell** services, increasing **revenue per customer,** greater ARPU.
- **Better prevention, detection capabilities and immediate response**, reducing your **operating costs per incident**. Increased margins.
- **Better global service**, greater **customer loyalty**. **Recurring revenue**.
- Tools for Partners: **Panda Partner Center and Partners Program**.

Figure 1. Our partners' managed services with Panda Adaptive Defense 360 and its modules, in line with Gartner's adaptive security architecture.



PANDA SECURITY PARTNERS PROGRAM

Panda Security offers its Partners Program to a select group of service providers that want to join forces and include a branch of our organization in theirs, to offer global services and solutions for advanced and adaptive security. Our security solutions, acclaimed by customers and analysts alike, combined with aggressive margins and a comprehensive service portfolio, represent an attractive and unique business opportunity for our partners. Find out more at https://www.pandasecurity.com/business/partners/

Partners Program Benefits:

Technical and sales training

- Sales training
- Technician training
- Regular certification
- Unlimited licenses for PoCs
- Dedicated Channel Account Manager

Marketing

- Product and marketing collaterals
- Marketing campaigns
- Partners portal
- Join events
- The best solutions according to analysts and reviewers

Business and operation

- Wide range of products and services
- 3 levels: Business, Premier, Elite
- 24/7 Support in your language
- License pool. Margins according to volume
- Tools for improved service
- Free access to your Panda Partner Center
- NFR Licenses (Not for resale)

To find out more about Panda Adaptive Defense 360, Panda Partner Center, managed services, or Panda Security's Partner Program, visit our website at: https://www.pandasecurity.com/business/partners/ and contact us at https://www.pandasecurity.com/about/contact/

AWARDS AND CERTIFICATIONS

Panda Security regularly participates in and receives awards for protection and performance from Virus Bulletin, AV-Comparatives, AV-Test, NSSLabs.Panda Adaptive Defense achieved the EAL2+ certification in its evaluation for the Common Criteria standard.

Panda Security acknowledged as 'Visionary' in the Gartner Magic Quadrant for Endpoint Protection Platforms (EPP) 2018.