watchguard.com/endpoint

WatchGuard Advanced
Endpoint Security

Unlock Your Managed Security Services Growth

panda
a WatchGuard brand

Index :

1. Introduction

It's no secret that most small and midsize organizations lack the financial and personnel resources to manage vital cyber security functions.

This is a problem in part because the threat of a significant cyber attack for midsize organizations is no less than the threat to larger enterprises. Due to automated attacks, these organizations are even more likely to be targeted and compromised by threat actors.

Cyber criminals do not discriminate based on the size of the organization, they simply look for vulnerabilities. Midsize businesses are often easier to target due to their lack of dedicated cybersecurity resources and personnel.

On the other hand, governments worldwide continue to impose strict regulations that enforce cybersecurity protections/controls within all companies, regardless of size because, as said before, threats have moved beyond large organizations to also target their smaller counterparts.

According to the Verizon's 2020 Data Breach Investigations Report, 28% of the breaches in 2019 involved small and medium business, 74% of them executed by external threat actors, which means that more than 25% of them involved insider threats, and the 83% of data breaches were financially motivated.[1] But using endpoint managed security services can – and should – prevent these events and their outcomes.

Endpoint managed security services take the best of enterprise-grade services, technologies, and people to create customizable, affordable, and reliable packages for small and midsize businesses.

26%

of the breaches in 2019 involved SMB victims

74%

of SMB data breaches involve external threat actors

83%

of data breaches against SMBs are financially motivated

1. Verizon's 2020 Data Breach Investigations Report (DBIR)

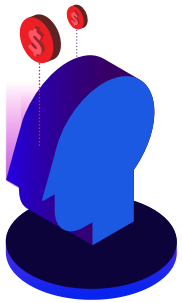
2.Opportunity

Managed Security Providers (MSPs) and Managed Security Service Providers (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, along with managed services, are the fastest and most cost-effective way, as no investment is required in proprietary technologies or expert support.

Perimeters Increase in Number

Endpoints, applications, and services are operating outside the traditional network perimeter.

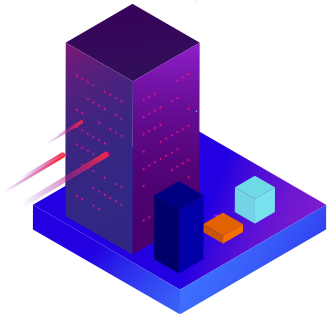
This expands the surface area for attackers to target, increasing the number of real perimeters that become more granular and closer to the logical entities they protect — the network, the users, devices, applications, and data, placing more emphasis on a "zero trust" security model.



The Professionalization of Hackers

Cyber enemies are increasingly sophisticated and growing in number as the result of their professionalization, the democratization of technologies, and the continuous leaks of cyber intelligence.

Next-generation cyber threats 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 products, 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.

3.Obstacles for MSPs and MSSPs

Most midsize MSPs and many MSSPs suffer the effects of the commoditization and the aggressive merger and acquisition (M&A) activity among providers in the sector, with decreasing margins, experiencing the continuous flight of customers to other MSSPs and SOCs.

These competitors 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. 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
a WatchGuard brand

4. Advanced security on endpoints

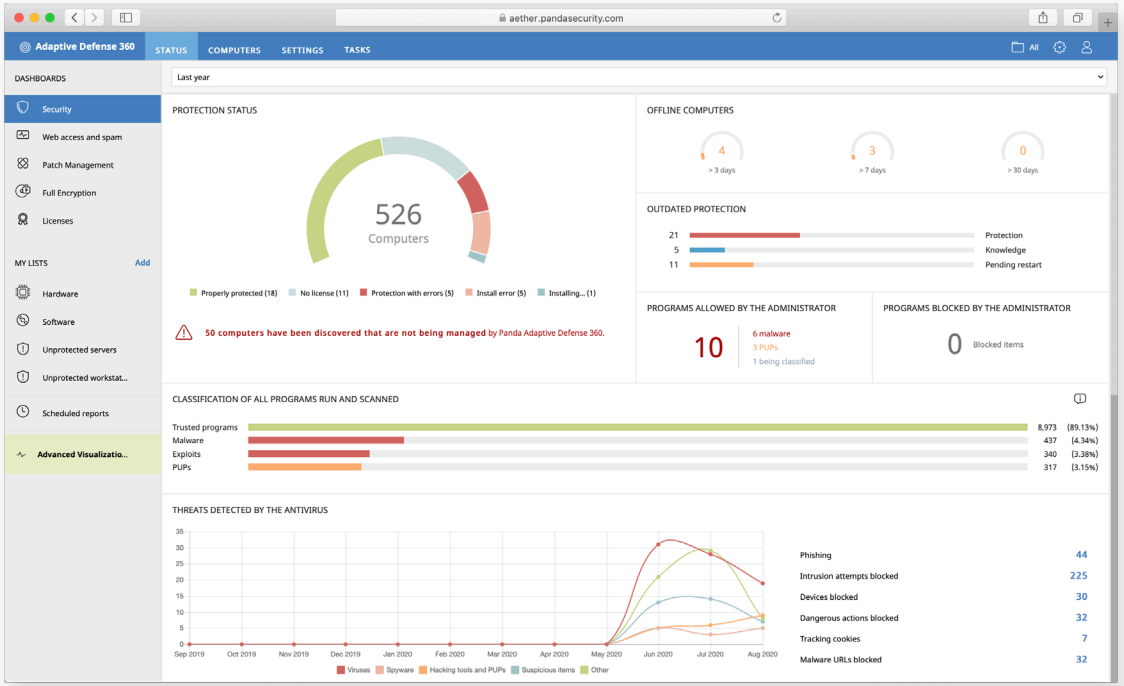
Traditional security, based on detecting known malicious processes, is insufficient. Businesses need to move from “response to incidents” to “continuous response,” meaning that an organization is continuously committed to security, as endpoints are continually under threat from attackers.

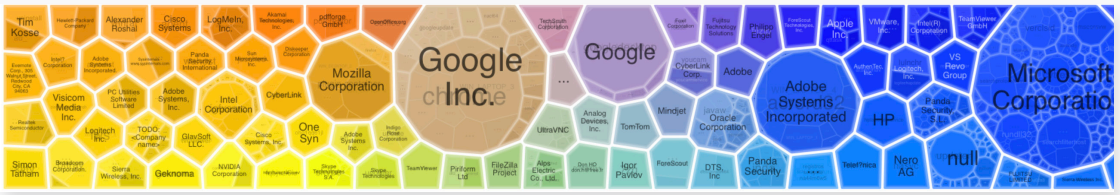
Panda Adaptive Defense 360 (AD360) is the Cloud-based, cybersecurity solution for workstations, laptops, and servers that automates the prevention, detection, containment, and response against any present or future advanced threats, zero day malware, ransomware, phishing, in-memory exploits, and malwareless attacks.

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

- **Zero-Trust Application Service**
- **Threat Hunting Service**

These services ensure that cyber threats are identified before they can run or generate massive damage across the organization.





panda
a WatchGuard brand

5.How the WatchGuard Endpoint Security portfolio helps overcome those obstacles

Prediction

8 Anomalous Usage Analysis Service

Consultancy service based on abnormal connections based on time, bandwidth usage, protocols, countries, endpoints, etc.

Panda Adaptive Defense 360 | Panda Advanced Reporting Tool

7 Attack Surface Reduction Service

Consultancy service based on health and configuration checks, protection coverage, patch statuses, etc

Panda Adaptive Defense 360 | Panda Advanced Reporting Tool
Panda Patch Management | Panda Data Control

6 Proactive Sensitive Data Control Service

Review of potential risk of sensitive data exfiltration. Advanced sensitive data search recommendations

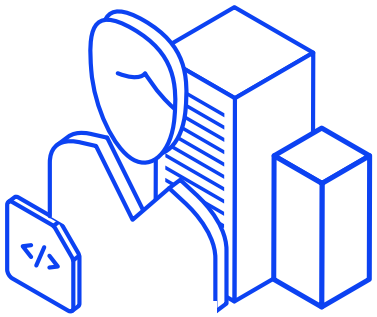
Panda Adaptive Defense 360 | Panda Data Control

Attack investigation and response

5 Forensic Analysis Service

Forensic analysis in case of a confirmed or potential incident, breach, or data exfiltration

Panda Adaptive Defense 360 | Panda Advanced Reporting Tool



Prevention

1 Basic Security Posture Assessment Service

Health checks: installation errors, basic configuration, connectivity, product updates

Panda Adaptive Defense 360 | Panda Patch Management

2 Standard Security Posture Assessment Service

Unprotected discovered devices, plus configurations, missing critical patches, etc.

Panda Adaptive Defense 360

3 Advanced Security Posture Assessment Service

Review of detections, per type, per machine. Identification of “risky users” and root causes

Panda Adaptive Defense 360 | Panda Patch Management

4 Sensitive Data Monitoring Service

Monitoring of volume, location, and movements of PII and other sensitive data

Panda Adaptive Defense 360 | Panda Data Control

Proactive monitoring, detection, and hunting

Figure 1. Shows some of the expanded advanced services that our partners can offer customers thanks to Panda Adaptive Defense 360 and its add-on modules.

Panda Adaptive Defense 360 and its add-on 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.

WATCHGUARD ENDPOINT SECURITY

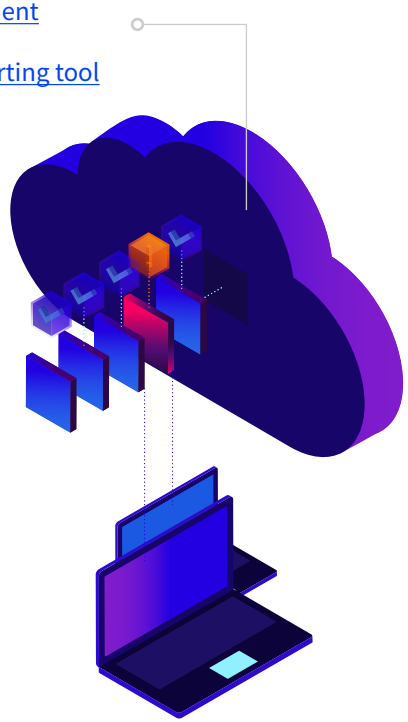
Adaptive Defense 360

Patch Management

Advanced Reporting tool

Data Control

Full Encryption



panda
a WatchGuard brand

Threat prevention and vulnerability exploitation

The Zero-Trust Application Service of **Panda Adaptive Defense 360** stops unknown processes from running until they are classified as trusted by machine-learning technologies, supervised by data analysts and malware experts. Our partners can supervise the classification process on behalf of their clients.

Panda Patch Management allows partners to manage their clients' vulnerabilities in operating systems and third-party applications. It provides centralized, real-time visibility into the security status of software vulnerabilities, missing patches, updates, and end-of-life software of all client endpoints. Partners can easily prevent their clients from being victims by simple patching on a regular basis, on-demand from the Cloud-based console.

Proactive monitoring and detection

In this type of service, the managed security services vendor protects against common threats and sophisticated attacks and alerts clients when there is suspicious activity in the network and endpoints.

Panda Adaptive Defense 360 incorporates a series of advanced technologies, such as machine learning and behavior-based detection, to block the execution of unknown malware and malware specially crafted to go unnoticed on corporate workstations and servers. These technologies collect huge amounts of information about actions taken on customer computers thanks to the continuous monitoring of all running processes.

Advanced Reporting Tool automatically generates security intelligence and provides managed service providers with the tools to pinpoint attacks, unusual behaviors, and detect internal misuse of the corporate network. It delivers real-time, deep insight into the day-to-day behavior of their customers' applications, networks, and users.

Like the rest of the WatchGuard Endpoint Security solutions, it is a Cloud-based service, which means MSPs and MSSPs can add it on a project basis without either big up-front costs or the time and effort associated with traditional IT infrastructure.

Finally, **Panda Data Control** discovers, classifies, audits, and monitors unstructured personal data stored on endpoints and servers. It's designed to help organizations and their MSSPs to comply with data protection regulations, as well as to discover and protect personal and sensitive data, both in real time and throughout its lifecycle on endpoints and servers.

Hunt

Next, the managed security services provider proactively (and continuously) searches for malicious threats, indicators, and zero day vulnerabilities.

Panda Adaptive Defense 360 includes the Threat Hunting Service in addition to its EPP and EDR capabilities and the Zero-Trust Application Service, allowing for early detection of new and sophisticated threats in the endpoint using malwareless techniques. It is its proactive nature and continuous searching for anomalies that distinguishes threat hunting from the other protection methods.

Attack investigation

Here, the managed security services vendor validates and prioritizes threats on behalf of clients, analyzing all security alerts using the latest intelligence.

Panda Adaptive Defense 360 technologies collect huge amounts of information about the actions taken on customer computers thanks to the continuous monitoring of all running processes. With this information, the solution is capable of determining the extent to which a customer's network has been compromised, helping administrators take appropriate measures. The web console makes all this information available to managed security providers through various resources, each of which provides different levels of detail, such as the execution graphs displaying actions taken by threat actors detected by any of the advanced detection technologies it incorporates.

Respond

Panda Adaptive Defense 360 provides several remediation tools that help resolve security issues. Some of these tools are automatic and don't require intervention, whereas other tools require certain actions through the web console.

For example, malware detected in the file system or in any attack vector is automatically disinfected. Sometimes eradicating threats requires a forced restart to apply updates, finish manual disinfection tasks, or fix protection errors. In other cases, the computer may need to be isolated from the network, preventing confidential data exfiltration and propagation of threats to other computers.

Managed security service providers can combine automatic remediations and manual intervention to eliminate and avoid threats expanding in the network.

Predict

Some MSSPs will further develop plans and recommendations to minimize breach impact. The attack execution graph, shown in AD360 for each detection, reveals how the threat actor was able to enter the endpoint, and this information can be used to predict future attacks.

Panda Patch Management shows all updates and patches that are missing in each endpoint, which are an open door for threat actors. It also provides mechanisms to immediately update patches from the Cloud-based console.

All of these capabilities allow partners to easily provide service to reduce the attack surface of a client's infrastructure.

Panda Adaptive Defense 360 includes the Threat Hunting Service in addition to its EPP and EDR capabilities and the Zero-Trust Application Service, allowing for early detection of new and sophisticated threats in the endpoint using malwareless techniques.

6. Benefits of WatchGuard Endpoint Security portfolio for our partners

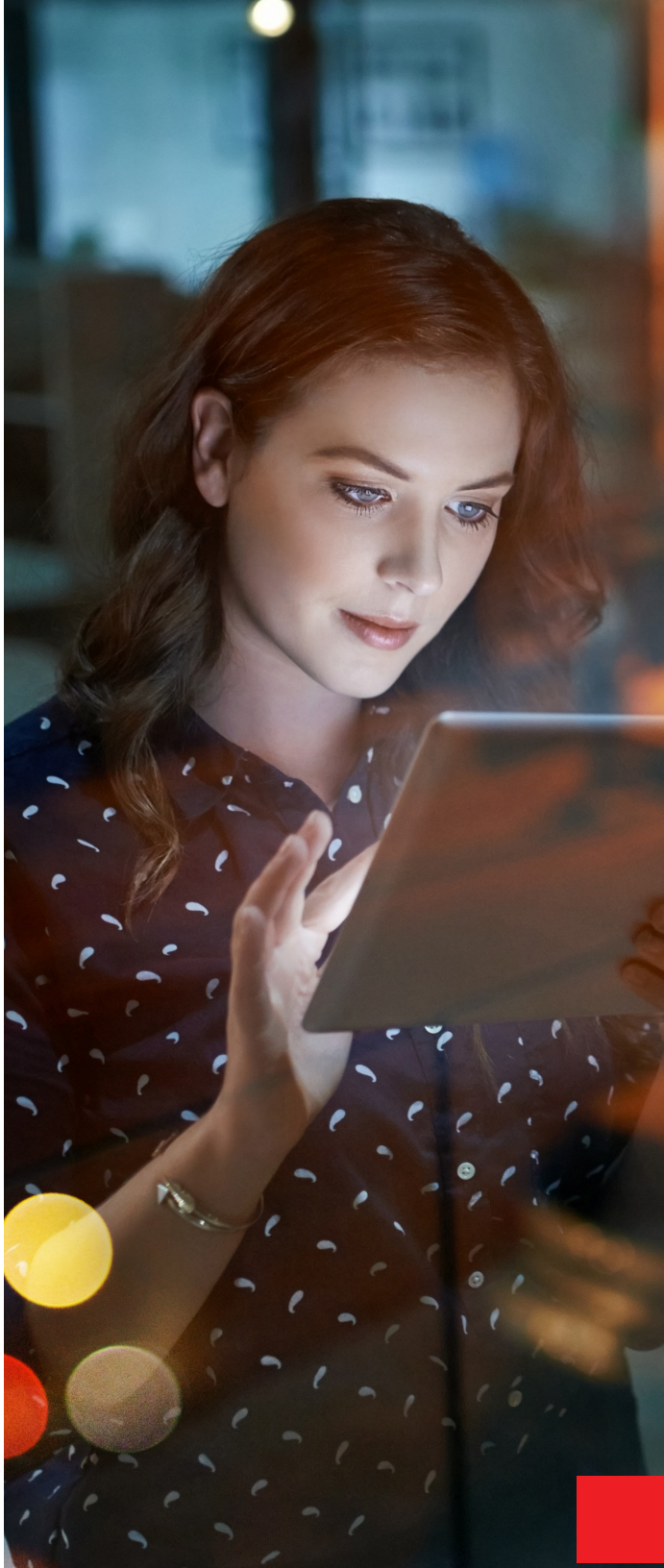
Greater service offerings: a competitive differentiation for your business

Better global service: greater customer loyalty for recurring revenue

Tools for partners: Panda Partner Center and WatchGuardONE Partner Program

Services can be upgraded and cross-sold: increasing revenue per customer for greater ARPU

Better prevention, detection capabilities, and immediate response: reducing your operating costs per incident for increased margins



panda
a WatchGuard brand

7. WatchGuardONE Partner Program

At WatchGuard, we have built a channel program unlike any other. WatchGuardONE is all about your profitability, and it's achieved through unsurpassed sales, marketing, and technical support, in addition to the most channel-savvy management team in the industry. The more you invest in learning about WatchGuard and the solutions we offer together, the more we invest in you.

This value-based principle continues to pay off for the tens of thousands of WatchGuard channel partners worldwide. But don't just take our word for it. **WatchGuard is consistently recognized year after year for pushing the envelope and leading innovation in partner enablement.**

WatchGuardONE Program Benefits:

- 24x7 Priority Technical Support
- Channel Account Management Team
- Field Marketing Team
- Assigned Sales Engineer
- Corporate WatchGuard Support
- Access to Threat Research Team
- Leads and Opportunities
- Business Tracker
- Renewals Management
- Partnership Management
- Profile Builder
- Deal Registration
- Marketing Campaign Kits
- Marketing Funds Management
- Marketing Automation
- On-Demand & Live Training
- Latest Company News
- Personalized Notifications
- Resource Center
- Competitive Intelligence

panda
a WatchGuard brand

WatchGuard

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com | pandasecurity.com

For more information visit our website