WatchGuard Endpoint Security

Extensible Protection to Prevent, Detect and Respond to Advanced Threats

The endpoint is a favorite target for cyber criminals, with plenty of known vulnerabilities to be exploited, and software versions that are often out of date. These devices are frequently on the Internet without protection from corporate perimeter security, and worse yet, employees can unwittingly enable hackers to make their way onto corporate endpoints and networks. It's past the time when businesses of all sizes need to implement powerful endpoint security that includes endpoint protection (EPP) integrated with advanced endpoint detection and response (EDR) technologies.

WatchGuard's endpoint security platform delivers maximum protection with minimal complexity to take the guesswork out of endpoint security. Our user-centric security products and services offer advanced EPP and EDR approaches with a full suite of security and operations tools for protecting people, devices, and the networks they connect to from malicious websites, malware, spam, and other targeted attacks. Tools to manage patches, remote monitoring encryption and more use the same console to further enhance security. Uniquely powered by automated, AI-driven processes and security analyst-led investigation services, our Panda Adaptive Defense products provide 100% classification, certifying the legitimacy and safety of all running applications – a critical need for any company implementing a zero-trust security model.

Good or Bad – Know with 100% Confidence

Most endpoint security products block what is known to be bad, investigate what is suspicious, and allow what is not known – enabling malware that rapidly morphs to bypass defenses with other unknown traffic. By contrast, the Panda Adaptive Defense products feature a Zero-Trust Application Service that classifies 100% of executables by analyzing all suspicious and unknown processes and applications using special machine-learning algorithms in our Cloud platform, and even verifying with our lab technicians when needed. As a result, all executables are known to be goodware or malware, so that customers receive only confirmed alerts and enjoy the ultimate protection that comes from the default-deny position of a zero-trust model.

Extend Security, Visibility and Operations Capabilities

Panda Adaptive Defense 360 (AD360) is a comprehensive solution, combining next-generation antivirus protection and endpoint detection and response (EDR) as well as the option to add visualization tools, patch management, content filtering, email security, full encryption, and more. Many of these products are also available with other base security offerings, including Panda Endpoint Protection, Endpoint Protection Plus, and Adaptive Defense – allowing customers to create a custom solution that best fits their distinct needs.

Find Lurking Threats Without Adding Staff

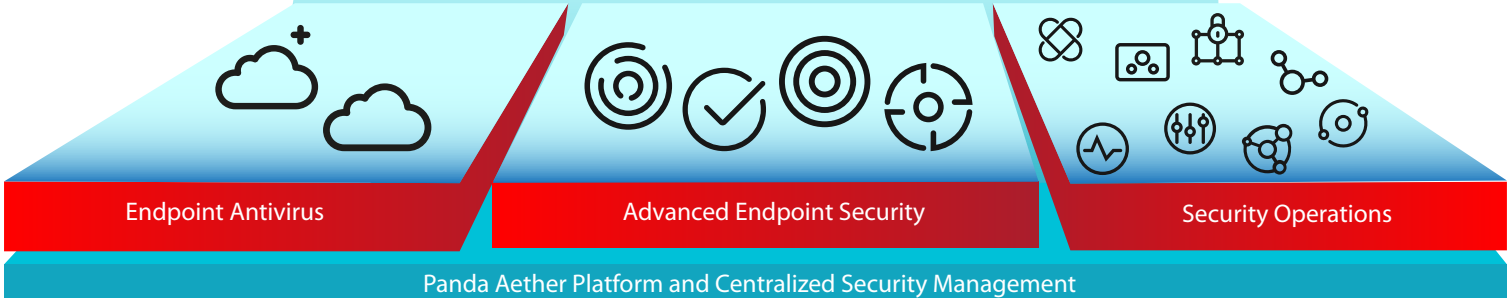
Threat hunting usually requires a highly skilled resource and consumes many hours before they detect threats and return the insights that make it clear how to remediate them. Our advanced EDR solutions offer a Threat Hunting service where our security analysts monitor the customer endpoint environment and provide information about potential ongoing attacks including root cause analysis, anomalies detected, relevant IT insights and potential attack surface reduction plans. This is a standard feature that comes with our Adaptive Defense and AD360 products and saves companies from having to allocate IT staff time and energy on investigating infected endpoints themselves.

Enjoy Intuitive, Cloud-based Management

Companies with limited IT staff and security expertise benefit from multi-factor authentication protection that's easy to deploy and manage from the Cloud. AuthPoint runs on the WatchGuard Cloud platform and is available from wherever you are. There is no need to install software, schedule upgrades or manage patches. Moreover, the platform easily accommodates a single global account view or many independent accounts, so that distributed enterprises and managed service providers can display only the data relevant to a person's role.

A Complete Package with Flexible Options to Meet Every Need

- ✔ Fully Cloud-Native
- ✔ Lightweight Agent
- ✔ Machine Learning Scoring
- ✔ EPP, EDR, Threat Hunting, Zero-Trust Ready



Panda Adaptive Defense & Panda Adaptive Defense 360

- Provides powerful endpoint detection and response (EDR) protection from zero day attacks, ransomware, cryptojacking and other advanced targeted attacks using new and emerging machine-learning and deep-learning AI models.
- Choose from EDR-only (Panda Adaptive Defense) and EPP + EDR (Panda Adaptive Defense 360) options
- Get 100% classification with Zero-Trust Application Service – creating the kind of response required for deployment of a zero-trust model
- Increase staff utilization and efficiency with insights from the Threat Hunting Service
- Implement defense-in-depth endpoint security with Adaptive Defense 360, which includes all the benefits of our Adaptive Defense product and our Endpoint Protection product in one package

Panda Endpoint Protection & Panda Endpoint Protection Plus

- Protects endpoints from viruses, malware, spyware and phishing with signatures, local cache, and even our own proprietary intelligence feeds derived from the malware previously detected from Adaptive Defense products
- Choose from advanced anti-malware (Panda Endpoint Protection) and anti-malware with URL-filtering and MS Exchange anti-spam protection (Panda Endpoint Protection Plus) options
- Finds zero day exploits using behavioral heuristics and known indicators of attacks as "contextual rules"

panda
a WatchGuard brand

WatchGuard acquires Panda Security, June 1, 2020
Both companies have been leading innovators in their respective fields for decades and together deliver a powerful security platform that bridges the network and user perimeter.

Additional Security Operations Products

Add optional modules available with all EPP and EDR security products:

Panda Patch Management is a solution to centrally manage updates and patches for operating systems and for hundreds of third-party applications and unsupported (EOL) software programs.

Panda Full Encryption leverages Microsoft's BitLocker technology to encrypt and decrypt endpoint information with central management of the recovery keys from our Cloud-based management platform.

Extend with more optional modules available only with Adaptive Defense products:

Advanced Reporting Tool automatically generates security intelligence and provides tools to pinpoint attacks and unusual behaviors, and to detect internal misuse of the corporate network.

Panda Data Control* discovers, classifies, audits and monitors unstructured personal data stored on endpoints and servers throughout its lifecycle.

SIEM Feeder enables a new source of critical information to the security intelligence of all the processes run on your devices while being continuously monitored. (Available only with Adaptive Defense 360)

Layer on effective security with these additional products

Panda Systems Management is an RMM tool for our endpoint security products, for managing, monitoring and maintaining them no matter where they are in the world.

WatchGuard DNSWatchGO provides DNS-level protection and content filtering that keeps businesses safe from phishing, ransomware, and other attacks even when users are outside of the network, without requiring a VPN.

Aether Cloud Management

- Connect in real time to deploy tasks to thousands of devices in seconds
- Manage all Panda-branded products from a single console
- View devices across endpoint platforms including Windows, Linux, macOS and Android

**Not available in all regions*

Reasons to Upgrade Your Security

1. Add protection for a newly distributed workforce as company work-from-home policies expand.

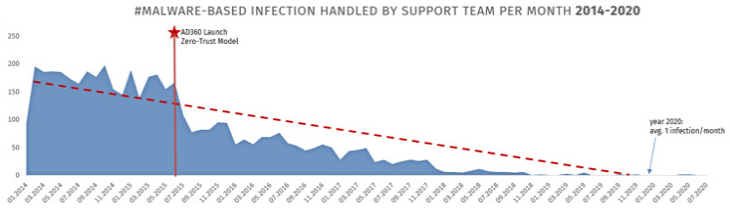
This package includes Panda AD360, WatchGuard DNSWatchGO, and WatchGuard AuthPoint product for multi-factor authentication. These solutions combine to protect users from the widest range of threats; and beyond endpoint security, it protects company resources from infiltration due to lost or stolen employee credentials – an attack vector used in some of the largest published breaches.

Recommended Solution: **WatchGuard Passport**

2. Recover after an attack, or after discovery of latent malware on endpoints or corporate networks when the malware originated on an endpoint.

Companies in this position know two things – first, that they are certainly of interest to cyber criminals and second, that their current level of protection is not adequate. As the advanced protection of AD360 has evolved with the Zero Trust Application Service and Threat Hunting Service the number of malware-based attacks that our support team has investigated/remediated has trended to nearly zero – meaning that our customers aren't experiencing them. Combine this with the visibility and management tools to increase the productivity of an over-burdened IT team, and it delivers what's needed to prevent repeated attacks and expensive remediations.

Recommended Solution:
Adaptive Defense 360
Advanced Reporting Tool
Patch Management
Systems Management



3. Add EDR to an existing AV solution as a planned security investment.

These companies understand the security risks on the endpoint and have deployed an AV product, but they realize that they need an EDR solution in order to stay ahead of hackers. There's no need to wait for AV contract renewal; our Adaptive Defense EDR solution layers on top of an existing AV deployment so that customers can quickly benefit from our advanced, differentiated approach.

Recommended Solution: **Adaptive Defense 360**

4. Upgrade from a free or consumer-grade endpoint AV product.

Sometimes, small companies or those that have few devices that cross the network perimeter are banking on a reduced risk profile, and so they've put off making investments in security. However, the world is changing, and as businesses become more exposed and need to meet stricter data security and privacy regulations, they move to a business-grade solution like the Panda Endpoint Protection Plus product. With strong signature-based prevention, including signatures from malware seen in our installed base, as well as behavioral analysis, web content filtering and anti-spam products, EPP Plus is a smart choice that's future-proofed since the platform scales with business growth.

Recommended Solution: **Panda Endpoint Protection Plus**

AV comparatives APPROVED Business Security DEC 2019 · CITRIX Ready · CYBER THREAT ALLIANCE · ITPro. EDITOR'S CHOICE ★★★★★ · NSS LABS RECOMMENDED · OPSWAT. Access Control Certification Anti-Malware GOLD

"The proactive approach to fighting malicious software gives me peace of mind. It's easy to configure, manage, and remediate issues quickly through its simple web interface."

Jeff Smith
Technology Systems Administrator,
Sacred Heart Schools

Customer Highlight: BDO

BDO, an auditing and risk advisory firm with a footprint in 162 countries, is one of the fastest-growing professional services firms globally, specializing in accounting, auditing, tax and advisory services. Nico Fourie (BDO National IT director) views information security as a key pillar of any organization. "Organizations should be careful of becoming complacent or being lured into a false sense of security; even when you think you have your affairs in order," says Fourie. "In assessing our situation it's imperative that we have visibility into endpoints…and regulatory compliance in line with GDPR and POPIA also requires increased visibility and control of data," continues Fourie.

To address these challenges, BDO implemented Panda Adaptive Defense 360 (AD360) and the Advanced Reporting Tool (ART) and Panda Patch Management modules. "This multi-tool approach provides increased visibility and holistic reporting, allowing us to identify gaps in our security," says Fourie. Before deploying AD360, BDO had a signature-based solution in place that was unable to detect and block advanced and zero day threats. BDO is now protected against the kind of evasive malware and fileless attacks we see today. "AD360 has allowed us to implement a zero-trust approach, significantly reducing cybersecurity risk," says Fourie.

Name of organization
BDO South Africa

Country
South Africa

Solution
Adaptive Defense 360

Licenses
1,000

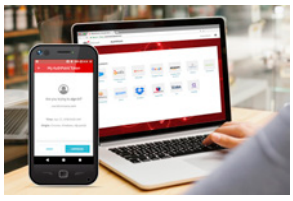
WatchGuard Unified Security Platform™

Network Security

WatchGuard Network Security solutions are designed from the ground up to be easy to deploy, use, and manage – in addition to providing the strongest security possible. Our unique approach to network security focuses on bringing best-in-class, enterprise-grade security to any organization, regardless of size or technical expertise.

Secure Wi-Fi

WatchGuard's Secure Wi-Fi Solution, a true game-changer in today's market, is engineered to provide a safe, protected airspace for Wi-Fi environments, while eliminating administrative headaches and greatly reducing costs. With expansive engagement tools and visibility into business analytics, it delivers the competitive advantage businesses need to succeed.



Multi-Factor Authentication

WatchGuard AuthPoint® is the right solution to address the password-driven security gap with multi-factor authentication on an easy-to-use Cloud platform. WatchGuard's unique approach adds the "mobile phone DNA" as an identifying factor to ensure that only the correct individual is granted access to sensitive networks and Cloud applications.

Endpoint Security

WatchGuard Endpoint Security is a Cloud-native, advanced endpoint security portfolio that protects businesses of any kind from present and future cyber attacks. Its flagship solution, Panda Adaptive Defense 360, powered by artificial intelligence, immediately improves the security posture of organizations. It combines endpoint protection (EPP) and detection and response (EDR) capabilities with zero-trust application and threat hunting services.

Find out more

For additional details, talk to an authorized WatchGuard reseller or visit **https://www.watchguard.com.**

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, endpoint security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by over 16,000 security resellers and service providers to protect more than 250,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for midmarket businesses and distributed enterprises. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Pacific, and Latin America. To learn more, visit WatchGuard.com.