Panda Adaptive Defense 360

Endpoint Protection Platform, EDR and 100% Attestation Service.

Panda Adaptive Defense 360 is a cybersecurity suite that combines Endpoint Protection and Endpoint Detection and Response (EDR) solutions, with 100% attestation, all equipped in a unique, lightweight agent.

The value of this advanced cybersecurity service is based on four principles:

Prevention, Detection and response

for attacks with and without malware, in a single agent

Real time and Historical visibility

detailed information of all activity on endpoints

Classification of 100% of processes

99.98% via Machine Learning, 0.02% by expert Panda analysts

Forensic Analysis of Attacks

Actionable insights into attackers and their activity

The combination of these solutions and services provides a detailed overview of all activities on every endpoint, total control of running processes, and reduction of the attack surface.

> *"Panda Security was named a Visionary in the Gartner 2018 Magic Quadrant for Endpoint Protection Platforms[1]."*
>
> *Ian McShane, Eric Ouellet, Avivah Litan, Prateek Bhajanka.*
>
> **Gartner 2018 Magic Quadrant for Endpoint Protection Platforms January 2018**

> *"A necessary evolution against unknown threats. Panda Adaptive Defense has a compendium of tools that we have not seen in other solutions."*
>
> **Data and Analytics. Industry: Services 250M -500 M USD.North America December 2018**
>
> www.gartner.com/reviews/review/view/646718

Gartner peerinsights™

4.6 ★★★★★½
131 Verified reviews

92% Recommend

Panda Adaptive Defense 360
Limitless Visibility, Absolute Control

Reinventing Cybersecurity

The new security model that has all the answers.

Panda Security unveils a new security model that combines the latest technology in prevention, detection, response and remediation.

- **Continuous monitoring of all applications**
- **Classification of all processes on all endpoints**
- **Big Data and Machine Learning Technologies**
- **Behavioral analysis and IoAs detection**
- **Prevention against Known Malware**
- **Detection of Advanced Malware**
- **Dynamic Exploit Detection**
- **Behavior-Based Detection**

Find out everything Panda Adaptive Defense 360 and its modules can do for you:

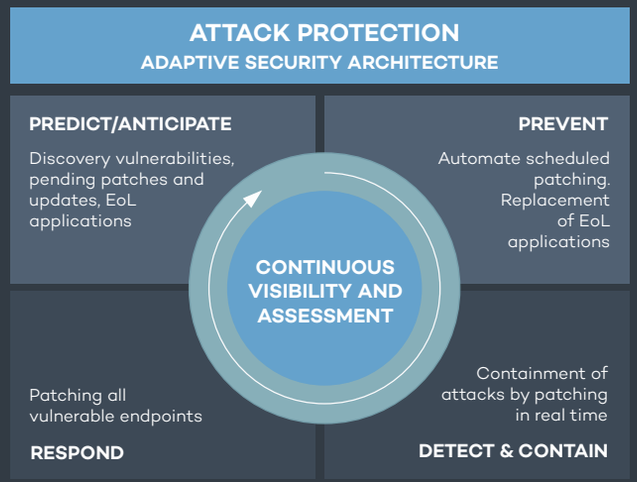
LIVE DEMO

Panda Patch Management

Panda Patch Management is a user-friendly solution for managing vulnerabilities of the operating systems and third-party applications on Windows workstations and servers. It reduces risk while strengthening the prevention, containment and attack surface reduction capabilities of your organization. The solution does not require the deployment of any new endpoint agents or management console as it is fully integrated in all of Panda Security's endpoint solutions.

Plus, it provides centralized, real-time visibility into the security status of software vulnerabilities, missing patches, updates and unsupported (EOL3) software, inside and outside the corporate network, as well as easy-to-use and real-time tools for the entire patch management cycle: from discovery and planning to installation and monitoring.

- Discovery: vulnerable computers, patches and pending updates
- Patch and update planning and installation tasks
- Endpoint and update status Monitoring
- Granular management based on groups and roles with different permissions

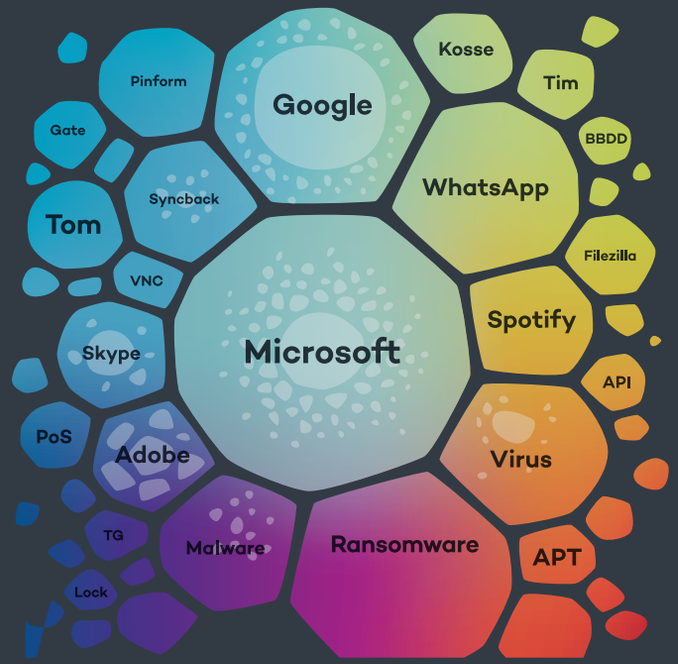


MORE INFORMATION

Advanced Reporting Tool

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. Advanced Reporting Tool automatically generates security intelligence and allows organizations to pinpoint attacks and unusual behaviors, as well as internal misuse, based on the monitored events gathered at the endpoints.

- Perform calculations and graphical visualization
- Receive alerts on Network Security Status Indicators and IT resources usage
- Determine threat origin and perform forensic analysis
- Gain visibility into endpoint vulnerability
- Monitor and control misuse of corporate resources



MORE INFORMATION

SIEM Feeder

This module generates added value and offers greater visibility into everything happening on your network by incorporating all the data gathered by Adaptive Defense into your own SIEM solution.

With this module, you can integrate a new source of critical information: the processes and programs run on every device in your company.

SIEM FEEDER MODULE WILL REVEAL

- Which new programs are being run and are not yet classified
- How these programs reached your network
- Any suspicious activity on users' devices
- Which software with vulnerabilities is being used
- Which processes are accessing user data and transmitting it outside the company
- How much network resources each process is consuming

MORE INFORMATION