Adaptive Defense 360

Limitless Visibility, Absolute Control

Adaptive Defense 360

Next-Gen Endpoint Protection & Machine Learning

The new security model that has all the answers

Adaptive Defense

Adaptive Defense is an advanced cyber-security managed service based on three principles: Continuous Monitoring of all applications, Automatic Classification of endpoint processes using Big Data and Machine Learning techniques, and Depth Behavior analytics by expert technicians.

This Cyber-Intelligence Platform analyzes, categorizes and correlates all the data obtained about cyber-threats in order to initiate prevention, detection, response and remediation routines.

Next-Generation Endpoint Protection

Advanced cyber-security to counter malware, with prevention, detection and remediation capabilities.

Endpoint Detection and Response

Monitoring, collecting and categorization of 100% the active processes on all the organization's endpoints.

Malware Intelligence Platform

The correlation of data on cyber-threats configures a security intelligence system to uncover patterns of malicious behavior.

www.pandasecurity.com/intelligence-platform/

Numbers don't lie

Not a single device in 'lock' mode has been infected — **0%**

It has detected malware in **100%** of the environments in which it has been installed, regardless of the protection solutions in place — **100%**

It keeps more than **12,000** corporate customers safe around the world — **12K**

We have blocked more than **2.3 million** security breaches in 2016 alone — **2.3M** (2016)

This new security model protects more than **1 million** endpoints & servers — **1M**

Every day it correlates more than **2.5B events** — **2.5B**

End users are not impacted in any way — **0**

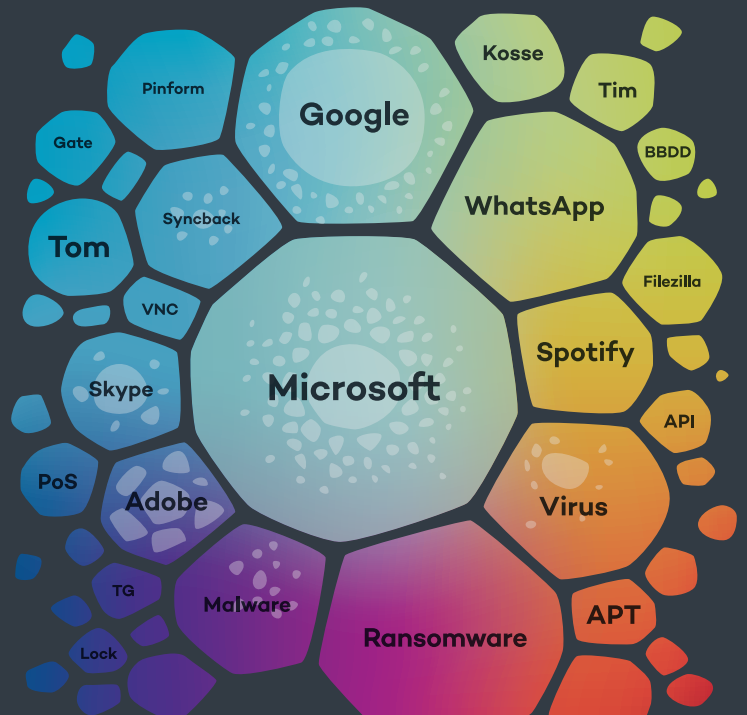
It has categorized over **3.5 million** applications to date — **3.5M**

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



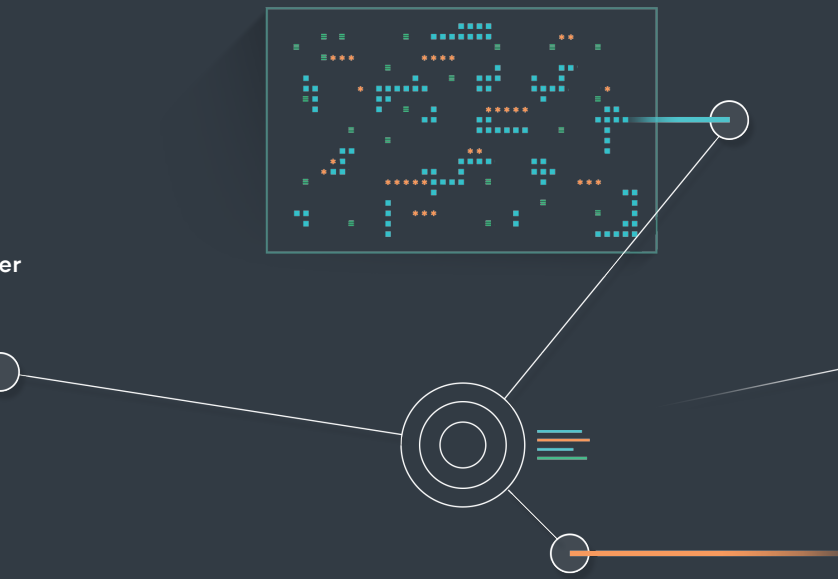
SIEM Feeder

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



"Panda uses a differentiated approach where every executable file on the system is categorized. Providing prevention and advanced remediation and malware removal capabilities to its EDR."

Gartner. Nov 2015

"As this solution classifies all executed processes, it cannot fail to record any malware."

AV Comparatives. Jan 2017

"The automated classification process using machine learning provides real-time or near-real-time analysis of all running executables for suspicious activity. It also provides detailed forensics."

Gartner. Jan 2017

panda