STORMSHIELD

ENDPOINT SECURITY

STORMSHIELD

PROTECTION FOR WORKSTATIONS

Protection for workstations, servers, and terminal devices

Our Mission

Make the digital world a sustainable and trustworthy environment while ensuring business continuity and data protection for organizations, their employees, and their customers.

TRANSPARENTE SECURITY

Compatible with other antivirus solutions, Stormshield Endpoint Security and Panda Adaptive Defense offer **an additional level of security.**

PROACTIVE PROTECTION

With in-depth, proactive protection, Panda Adaptive Defense and Stormshield Endpoint Security solutions provide **next-generation armor** that is capable of protecting the assets of companies and organizations of all sizes.

COLLABORATIVE DEFENSE

Stormshield works with Panda Security to develop joint offers, **share information about threats**, and collectively improve our customers' defenses.

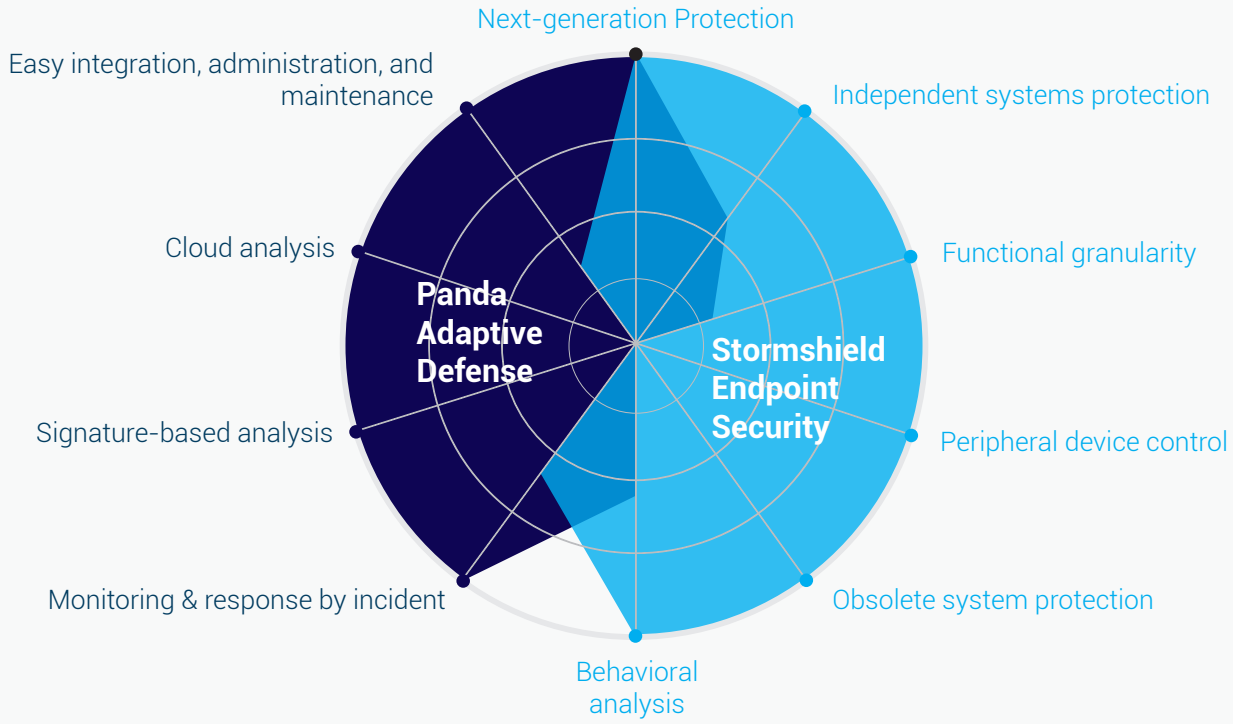
Take advantage of the best security

A layer of comprehensive protection

The Panda Adaptive Defense range is the first offering to combine the capabilities of EPP (Endpoint Protection Platform) and EDR (Endpoint Detection & Response) into a single solution.

A dedicated team of experts

Unknown threats are analyzed via the Cloud. Machine learning algorithms expedite human analysis, which alone is capable of identifying complex behaviors.



For unconnected environments

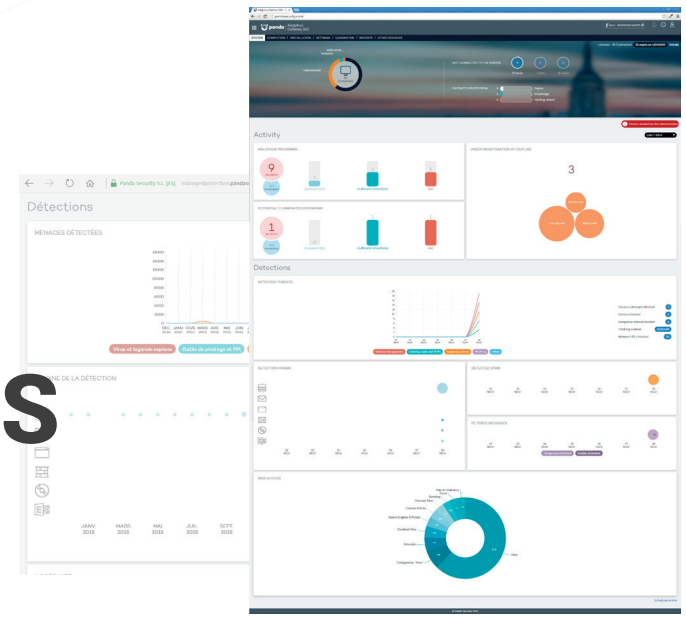
Stormshield Endpoint Security immediately blocks attacks, even unknown attacks, by detecting abnormal behavior (exploiting vulnerabilities, corrupting memory, attempted keylogging, etc.) regardless of the infection vector.

Contextual Protection

Stormshield Endpoint Security reacts automatically based on its environment. This unique adaptability means it can immediately react and strengthen the level of protection in the event the context changes, whether or not the workstation is connected to the Internet.

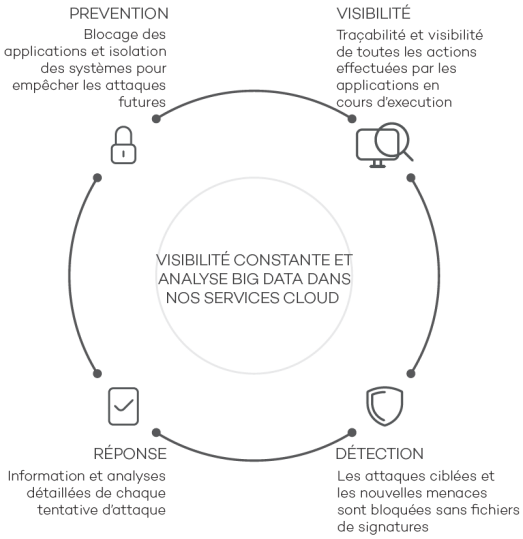
PROTECT
YOUR IT SYSTEMS

Keep advanced threats at bay



Proactive protection for workstations

Panda Security's Adaptive Defense is a new cybersecurity model that ensures comprehensive protection of terminal devices and servers. It classifies 100% of services and processes carried out on each computer of the entire organization's IT system and monitors and analyzes their behaviors contextually. More than 2 billion applications have already been classified.



Adaptive Defense

Panda Adaptive Defense is able to precisely classify each application that is started in your company while only authorizing legitimate programs to run. This new security model operates on three principles: constant monitoring of applications on computers and servers, automatic classification by machine learning using the Cloud's Big Data platform, and analysis by technical experts of applications not automatically classified so as to determine with certainty the behavior of everything running on the company's systems.

Adaptive Defense **360**

Panda Adaptive Defense 360 is the first offering to combine the capabilities of EPP (Endpoint Protection Platform) and EDR (Endpoint Detection & Response) into a single solution. First and foremost, Adaptive Defense 360 integrates Panda's most comprehensive EPP with real-time monitoring and security reports, corrective tools, protection based on user profile, centralized control of connected mobile devices, and web filtering and monitoring.

Adaptive Defense

to ensure that all applications are running securely

Comprehensive, reliable protection guaranteed

Panda Adaptive Defense can run two ways:

- **Standard mode** authorizes – after being audited – all applications classified as harmless as well as automated systems to run.
- **Extended mode** only allows software to run once it has been classified as harmless after a long learning phase.

Protection for vulnerable applications and operating systems

Adaptive Defense's vulnerability protection module uses behavioral and contextual rules to enable companies to work in a secure environment, even with systems that have not been updated.

Real-time information on the network's status

Take advantage of immediate alerts as soon as malware is identified in the network, with a comprehensive report detailing the location, infected computers, and action undertaken by the malware. You can also receive reports via e-mail on the service's daily activity.

Fully-managed service

You no longer have to invest in technical personnel to handle suspicious or quarantined files or even to disinfect and restore infected computers. Adaptive Defense automatically classifies all applications using machine learning in Big Data environments under the constant supervision of PandaLabs experts.

EPP/EDR Solution

Corrective actions

Centralized control of terminal devices

Web filtering and monitoring

Firewall for terminal devices (personal or company-issued)

Protection against sophisticated, unknown threats

Analysis Tools

Real-time virus alerts

Detailed malware report

Graphics of connections and performance events

Reports of known vulnerabilities of software

Compatible SIEM solutions

Easy Installation

3 modes of deployment

Security installation tailored to your needs

Comprehensive, user-friendly interface

Transparent security within everyone's reach

Compatibility

Workstation and server protection

Mac & Windows

Web console for monitoring

A custom solution

An ideal solution for your business needs

MSSPs and Other Service Providers
• Manage the solution from your offices (packaged solution) • Cloud-as-a-Service solution • Endpoint protection (Container)

Datacenters
• Endpoint protection (Antivirus) • Secure servers • Effectively fight against viruses or data leaks and losses

Education and Academia
• Secure workstations • Manage user behavior • Easy integration into the infrastructure • Effective protection against viruses or data leaks and losses

Banking and Finance
• Fully-supported compliance • Risk management and evaluation • Transparency and responsibility • Reduce operating costs

Public Administrations
• Secure workstations • Easily deployed • Fast learning curve • Effectively fight against viruses or data leaks and losses

Health and Healthcare Facilities
• Protect medical records • Secure workstations • Manage user behavior • Protect against viruses or data leaks and losses

STRENGTHEN **SENSITIVE OR CRITICAL ENVIRONMENTS**

Proactive protection against sophisticated and unknown attacks

Unconnected technology

The result of years of research and development, Stormshield Endpoint Security is used to recognize sophisticated and unknown attacks without requiring product updates or a connection to an external system.

It is the perfect solution to fulfill the protection requirements of off-line environments and is suitable for protecting obsolete environments, such as Windows XP (which no longer gets security patches).

Unique, proactive protection

Based on a unique technology that analyzes interactions between processes and the system of a workstation or server, Stormshield Endpoint Security provides proven protection against these sophisticated attacks, complementing your conventional protection tools. A series of security layers effectively prevents the system from being compromised and ensures its integrity.

A comprehensive workstation control solution

Stormshield Endpoint Security allows you to control various workstation behaviors and determine which are considered legitimate and which are prohibited. Our solution is essential for fighting against data leaks and losses, protecting against external viruses, and blocking the malicious usage of IT equipment provided by the company.

Endpoint Security has one of the highest levels of certification on the market (CC EAL3+ and FIPS 140-2). These signs of security are the reason we are trusted by organizations that have the most critical security needs: defense agencies, sensitive sectors, government and public administrations, financial institutions, and more.

COMMON CRITERIA CERTIFIED EAL3+

COMMON CRITERIA

FIPS

FIPS 140-2

Proactive response to modern threats

on workstations, servers, and terminal devices

Independent protection

Stormshield Endpoint Security is an independent protection solution that is not signature-based and, consequently, does not require updates. Its proactive and generic security mechanisms block zero-day threats, without the software needing to be updated or adapted.

Limited system footprint

The advantage of proactive technology is that it has a limited system footprint. Stormshield Endpoint Security technology monitors critical areas of the operating system for abnormal behavior.

Security policy granularity

Stormshield Endpoint Security offers great flexibility in how the security policy is configured so as to meet the specific needs of each company. This means that protection is adapted to your company's needs.

For critical infrastructures

Stormshield Endpoint Security offers software partitioning, peripheral device control (including USBs), and administration workstation hardening – features enabling you to be in compliance with the security measures required by the LPM (Loi de Programmation Militaire, or Military Programming Act).

Protection against unknown threats

Protection against exploiting operating system vulnerabilities

Protection against exploiting third-party application vulnerabilities

System memory integrity control

Intrusion prevention

Firewall

Network intrusion detection

Workstation protection

Malware detection by behavioral analysis

Operating system hardening

Application control (white list and black list)

Granular control of user rights

Granular control of sensitive data exfiltration

Peripheral device control and audits

Authorize or block peripheral devices by type or serial number

Block or restrict various operations

Protect against infection by an external storage device

Track files loaded on a particular peripheral device and/or by a particular user

Evaluate file transfers (appropriate or not)

Communications control

Firewall

Quarantine infected computers

Authorize subcontractors' workstations only if the company's VPN is used

White list of the company's WiFi access points

Restrict WiFi in ad-hoc mode

A custom solution

An ideal solution for your business needs

Defense and Military Organizations
• Choose trusted products • Operating system hardening • Proactive protection • Decontamination lock chambers • Peripheral device control

Industry
• Protect operator workstations • Non-signature protection • Peripheral device control • Monitor network use • Operating system hardening

Retail and e-Commerce
• Secure points of sale • Control access • Operating system hardening • Proactive protection

Banking and Finance
• Control access • Protect ATMs • Choose trusted products • Operating system hardening • Peripheral device control

Public Administrations
• Choose trusted products • Non-signature protection • Operating system hardening • Peripheral device control • Monitor network use

Health and Healthcare Facilities
• Effective protection against viruses or data leaks and losses (medical records) • Protect medical device workstations • Operating system hardening

Stormshield Endpoint Security

in a few key points

A SOVEREIGN SOLUTION

As a French cybersecurity provider, we have been providing solutions that meet European legal requirements for the last 15 years.

CERTIFICATIONS

Our Stormshield Endpoint Security solution is certified at the highest European level, guaranteeing customized protection for your organization's most sensitive and strategic information.

ÉCOSYSTÈME

We work with Panda Security to develop joint offers, share information about threats, and collectively improve our customers' defenses.

A CLEAR OFFER

With two solutions tailored to your needs, choose whichever product suits you best.

PROACTIVE PROTECTION

With in-depth, proactive protection, our solutions provide next-generation armor that is able to protect the assets of companies and organizations of all sizes.

A THREAT, A RESPONSE

You are protected against remote vulnerability exploitation, against the threat of a malicious internal user, against data leaks, and against attacks specific to certain sensitive environments (SCADA, point of sale, etc.).

EASY INTEGRATION

Compatible with other antivirus protection solutions, Stormshield Endpoint Security and Adaptive Defense offer an additional level of security.

EASY SUPERVISION

Stormshield simplifies your security with Stormshield Visibility Center. Stormshield Endpoint Security and Adaptive Defense events are collected in a single supervision tool that is indispensable for decision-making.

TECHNICAL SUPPORT

Our technical support works closely with our R&D teams to provide you with our software company's expertise.

STORMSHIELD

Stormshield is a wholly-owned subsidiary of Airbus CyberSecurity that provides innovative end-to-end security solutions for protecting networks (Stormshield Network Security), workstations (Stormshield Endpoint Security), and data (Stormshield Data Security).

www.stormshield.com

Version 4.0 - Copyright Stormshield 2018