



Adaptive Defense 360

Product Description

Index

Index.....	2
1. Panda Security a WatchGuard Company.....	3
2. Features of the solution.....	4
2.1. Key features of Adaptive Defense 360.....	4
2.2. Adaptive Defense 360 Architecture.....	6
2.3. Panda Security Big Data.....	7
2.4. Administration of the web console.....	8
2.5. Computers protected through Adaptive Defense 360.....	8
2.6. Detection Logic through Machine Learning.....	9
2.6.1. Events Timeline Storage – Events timeline.....	10
2.6.2. Threat Hunting and Investigation Service.....	10
2.7. Panda Advanced Visualization Tool (AVT).....	12
2.9. Patch Management.....	15
2.9.1. Key Features.....	15
2.10. Full Encryption.....	17
2.10.1. Key Features.....	17
2.11. Data Control.....	18
2.11.1. Key Features.....	18
3. Adaptive Protection.....	19
3.1. The protection cycle.....	21
3.2. Phase 1, Protection.....	21
3.3. Phase 2, Detection and Monitoring.....	24
3.4. Phase 3, Response & Remediation.....	27
3.5. Phase 4, Adaptation.....	29
3.6. Main components.....	30
3.7. Status.....	30
3.8. Computers.....	33
3.9. Settings.....	35
3.10. Users.....	35
3.11. Computer Settings.....	35
3.12. Network settings.....	35
3.13. My alerts.....	37
3.14. Workstations and Servers.....	37
3.15. Tasks.....	38
4. Advantages.....	38

1. Panda Security a WatchGuard Company

However complex, we make it simple

WatchGuard Technologies, Inc. is a leading global provider of network security, secure Wi-Fi, multi-factor authentication, network intelligence, and endpoint protection. The company's award-winning products and services are trusted around the world by nearly 10,000 security resellers and service providers to protect more than 80,000 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, Asia Pacific, and Latin America. To learn more, visit [WatchGuard.com](https://www.watchguard.com).

WatchGuard Technologies, announced in 2020 that it has closed the acquisition of the advanced endpoint protection provider, Panda Security. Panda Security is now a wholly-owned subsidiary of WatchGuard, and the combined company enable its current and future customers and partners to consolidate their fundamental security services for protection from network to endpoint under a single company. Initially focused on the development of antivirus software, it has since expanded its line of business to advanced cyber-security services powered by cybercrime-preventing technology, combining EDR and EPP solutions as a market differentiator.

Its patented technology TruPrevent, a set of proactive capabilities aimed at blocking unknown viruses, along with its Collective Intelligence model, the first system to automatically detect, analyze, and classify malware in real time, have been the precursors to the new Adaptive Defense security model.

"Reinvent Cybersecurity"

The decline of traditional approaches to fighting malware, and the increasing complexity of new attacks are setting new standards in computer security. Traditional protection models are no longer able to handle these types of attacks. This is why Panda Security developed a unique new security model which is able to provide real time monitoring and classification of all running processes, forensic analysis, Threat Hunting, and Data Analytics.

2. Features of the solution

Adaptive Defense 360 is an endpoint security solution based on several different protection technologies, making it possible for companies to replace existing traditional Endpoint Protection products with a complete and reliable service.

Adaptive Defense 360 protects systems by allowing the execution of verified software only, using real-time monitoring and execution control to classify all processes through the analysis of both their nature and behavior.

Furthermore, it provides forensic analysis and remediation tools to investigate and mitigate both known malicious threats, and even proactively blocked unknown security threats.

Unlike traditional endpoint protection technologies, Adaptive Defense 360 uses a new concept of security, adapting itself to the environment of every single company. This is all possible thanks to the continuous assessment of actions taken by every single process.

Adaptive Defense 360 is a cross-platform service compatible with Windows, Linux, macOS and mobile devices. It also does not require an infrastructure, which reduces its TCO to a minimum.

2.1. Key features of Adaptive Defense 360

Adaptive Defense 360 is a managed service which strengthens a company's security posture against zero-day threats (e.g. ransomware), hacker attacks, and insider threats.

It is based on four main pillars:

- **Visibility:** traceability of each action taken by an executed process
- **Detection:** constant monitoring of executed processes, real-time blocking of zero-day threats, targeted attacks, and other advanced threats designed to bypass traditional antivirus solutions
- **Response:** forensic information and remediation tools for deep analysis and response
- **Prevention:** blocking of future attacks from unknown applications which have not yet been classified by Panda Security as malware, exploits or zero-days



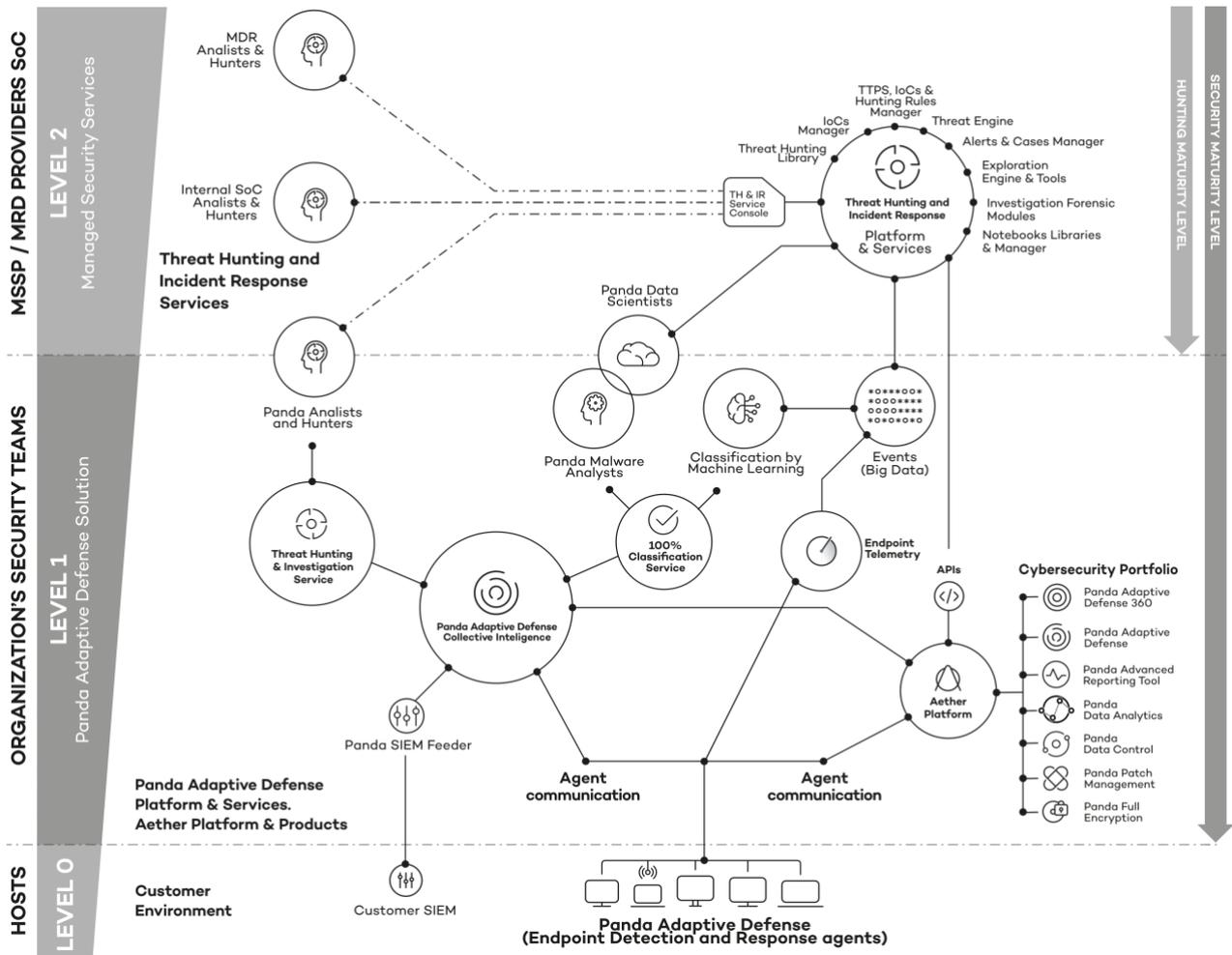
While Adaptive Defense 360 is a management service which offers security without requiring network administrator intervention, it also provides clear and detailed information on the activity of processes in use by all users of the network.

The information can be used by administrators to clearly and preventively evaluate potential impact on security policies.

All users who have deployed the Adaptive Defense 360 agent on their workstations or servers benefit from an innovative security service, blocking the execution of programs which could turn into threats the moment they execute.

2.2. Adaptive Defense 360 Architecture

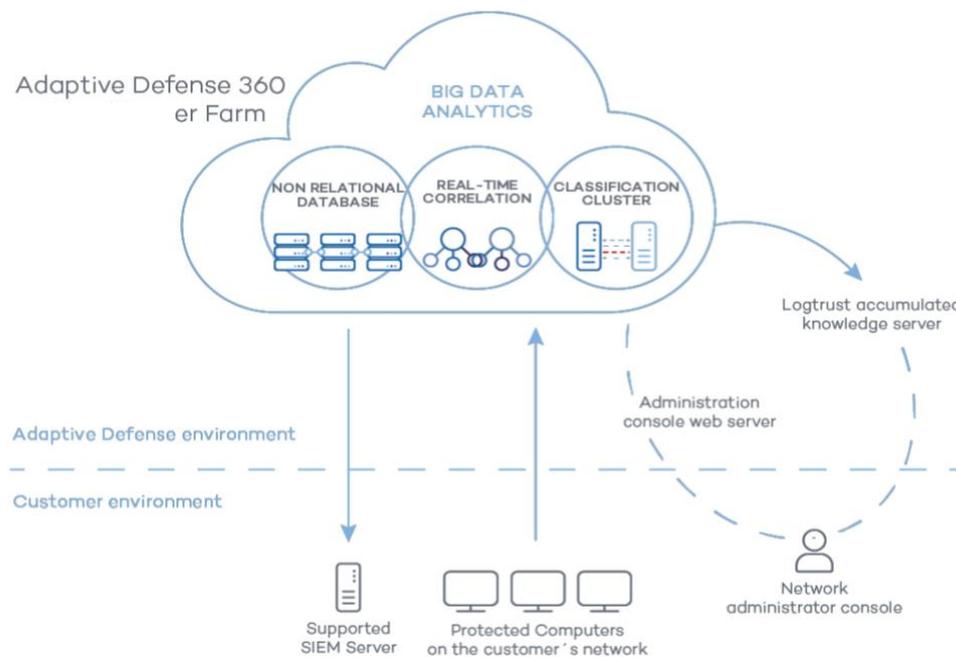
Adaptive Defense 360 is an advanced security service based on the behavioral analysis of all processes executed on each host in the network. The analysis of these processes is performed by using Machine Learning techniques in Panda Security's Big Data infrastructure. This makes it possible to avoid the installation of hardware or additional resources inside the local customer environments. The architecture of Adaptive Defense 360 and its components is illustrated below:



2.3. Panda Security Big Data

Adaptive Defense 360 uses both Machine Learning and Big Data technologies by way of different elements:

- Panda Security's Collective Intelligence (Big Data Analytics)
- Web administration console
- Endpoint protection agent
- Advanced Search modules (Advanced Visualization Tool, Data Control, Data Analytics platform). These are optional and allow access in "native/raw" format to relevant telemetry generated by the solution



The classification of the processes on computers is performed automatically, without added overhead for the IT and Security teams.

The endpoint agent installed on the client provides the Panda Security platform with data concerning the nature of the processes being assessed, which influences the corresponding decision on whether to allow or block a specific application. This new model of analysis and classification is called **Zero-Trust Application Service**, and offers many advantages over traditional detection techniques that are based on submitting possible malware samples for subsequent analysis (typically a manual process), and the later issuance of a detection "signature":

- Each process that tries to execute on computers protected by Adaptive Defense 360 is first classified, removing the uncertainty inherent in traditional Endpoint Protection solutions which are able to identify known elements only, as a result permitting all unknown processes to run.
- The "window of opportunity" for malware (time between the identification of a new threat and the issuance of a traditional signature) is virtually eliminated. The submission of unknown files has no impact on network performance: unknown files are sent only once, and through bandwidth management every single agent or group of agents can be set up to communicate in an optimized way. No sensitive information is ever sent to Panda Security, only binary files.
- The continuous monitoring of all processes allows Adaptive Defense 360 to reclassify as malware items which at an earlier point in time might have been showing goodware characteristics. This is a

typical trait of targeted attacks and other threats designed to remain invisible to traditional Endpoint Protection solutions.

- Not requiring any local infrastructure means no need to implement and maintain on-premise components, databases, remote servers, centralized distribution points or install dedicated software on physical/virtual hardware.

2.4. Administration of the web console

Adaptive Defense 360 is fully managed through a web-based console.

This web console is compatible with most browsers, includes responsive design and it is always up - wherever you are and whichever device you are using, including tablets and smartphones.

2.5. Computers protected through Adaptive Defense 360

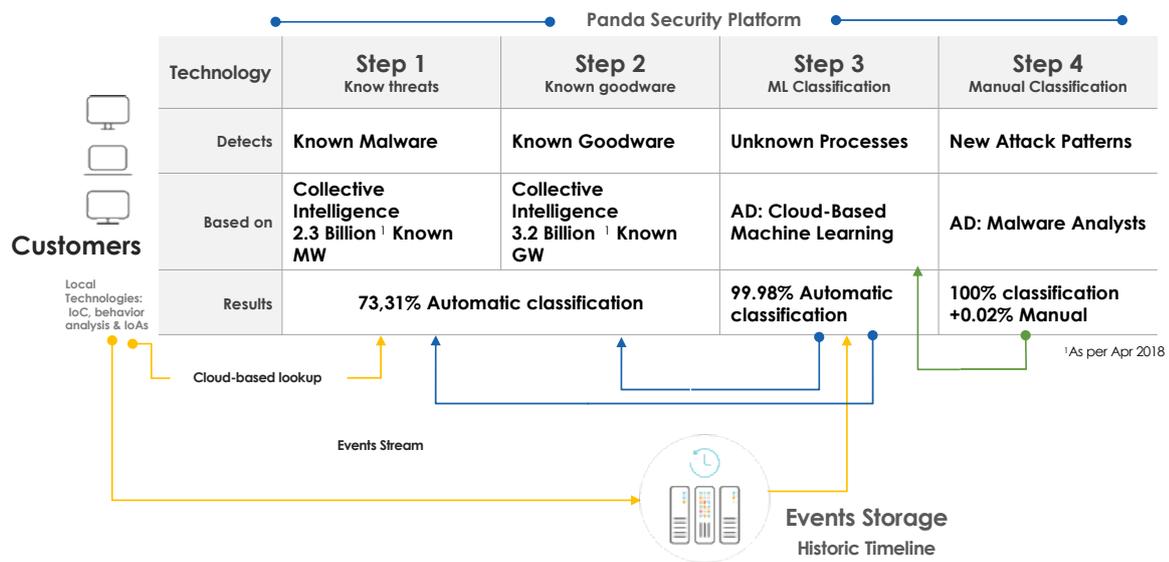
Adaptive Defense 360 requires the deployment of a software component (agent), installed on all company endpoint devices. This component includes two modules: the communications agent and the protection.

The communications agent manages data flows between the endpoint and the Panda Security backend. It also establishes P2P (peer-to-peer) communication between computers in the same company network, thus coordinating local updates amongst all agents deployed. The peer-to-peer allows an agent to centrally download new signature files (for the traditional security components) or protection upgrades and make them available for computers connected in the same network. This model becomes even more efficient in complex or geographically distributed networks, making its scalability virtually unlimited.

2.6. Detection Logic through Machine Learning

Panda Security's unique protection model combines a few fundamental factors:

- What has already been determined as malicious, i.e. a known threat (**step 1**)
- What has already been determined as Goodware, i.e. known and reliable (**step 2**)
- What is automatically analyzed and classified as either Goodware or new Malware, through Machine Learning algorithms (**step 3**)
- What is manually classified by Panda Security analysts (**step 4**)
- What is being used to deliver the Threat Hunting & Investigation Service (Events Timeline Storage)



The Machine Learning algorithms implemented by Panda Security are based on the “Ranker on ensemble of models” model. Each of these is designed to return the classification verdict for each unknown process and host/user attempting to execute it. Each of these gets a rating, defined as a “score”. The final verdict is weighed on the partial results elaborated with predictive algorithm models and the model used (ensemble) to guarantee maximum accuracy, the certainty of the outcome and a number of false positives that equals zero.



Data lake

1.2 PB per million endpoints of data collected in 2020;
762 million binaries processed in 2020



Collective Intelligence

It represents the consolidated and incremental knowledge repository of all applications, and binaries, continuously fed by the AI system and by the expert analysts.



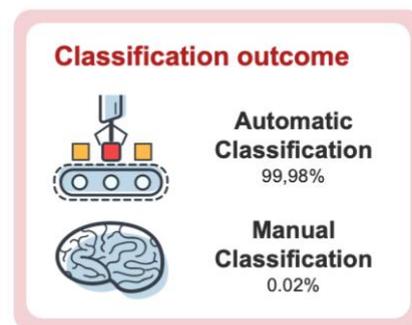
Algorithm

RANKER is an ensemble of models designed to predict the classification of each process, with multiple algorithms working with a set of flags.



Classification score

The classification score of each process is recalculated based on the dynamic behavior of the process and recalculated based on the new evidence received (Retrospective Analysis).



2.6.1. Events Timeline Storage – Events timeline

The events timeline is automatically created based on analyzed telemetry events. The telemetry events are not considered incidents, malicious objects or anomalies in themselves. They also represent information linked to a specific object, e.g.:

- **Processes:** creation of a process, execution of a process, injection of a process in another event (child), etc.
- **File:** Creation of a new file by an event/process, editing of a file, deletion of a file, opening of a file, etc.
- **Communications:** opening of a communication socket, use of a communication protocol, communication direction, the origin of the communication, etc.
- **Registry:** creation, edit and deletion of a registry key, etc.
- **Administration:** use of administrative credentials, login/logout events, installation of processes, service activity, etc.

2.6.2. Threat Hunting and Investigation Service

In addition to the Adaptive Defense 360 security solution, the Threat Hunting & Investigation Service provides an unparalleled level of protection without additional charges.

Based on Gartner's definition of the difference between the Threat Detection and Threat Hunting, Panda Security decided to implement a management service that singles out what can be identified as a hacker attack, defined as lateral movement which follows a malicious attack or malicious behavior through the use of legitimate software (without the presence of malicious code).

The Threat Hunting & Investigation Service (THIS) aims at alerting on attack traces, which could have been left in the past (IOC) or as a result of an ongoing attack (IOA).

The detection of an attacker's presence can be accomplished through:

- **Threat Detection:** a known attack vector has been discovered in real-time (real-time streaming)
- **Threat Hunting:** once an attack hypothesis deriving from an anomalous behavior (IOA) has been generated and validated.

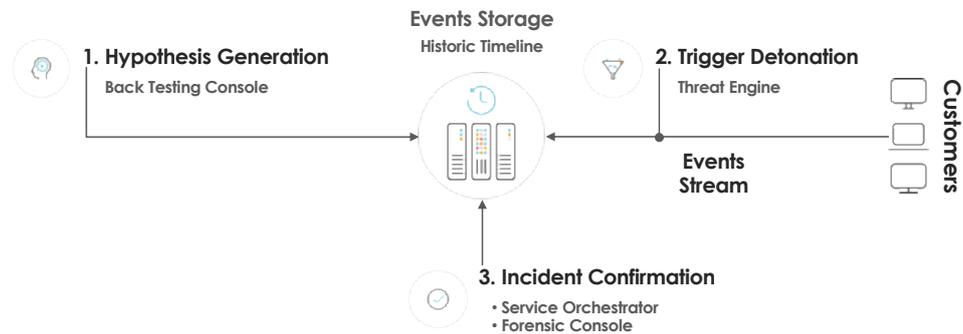
As opposed to Threat Detection, which verifies and identifies known attack techniques, Threat Hunting is characterized by the proactive and continuous search for attacks which are yet unknown and non-identifiable by traditional security technologies.

Panda Security Threat Hunting & Investigation Service differs from traditional Threat Detection in the following:

- **It is proactive:** Threat hunters at Panda Security don't wait for an alert to be generated by an Indicator of Compromise (IOC).
- **It is based on hypothesis formulation:** Threat hunters at Panda Security constantly searching for traces and clues of possible attacks, typically those which are non-verifiable by traditional Endpoint Protection technologies, in order to generate new confirmable hypothesis and create new Detection rules.

The hypothesis generated by this continuous and constant research are edited, validated and run against the Panda Security Event Storage Timeline which collects events globally from all hosts protected by Panda Security in the last 12 months. When a formulated hypothesis has been validated, the verification is then

extended to the Event Storage Timeline, after which it becomes a new rule in the traditional Threat Detection Service, so that all Panda Security clients can benefit from it worldwide.

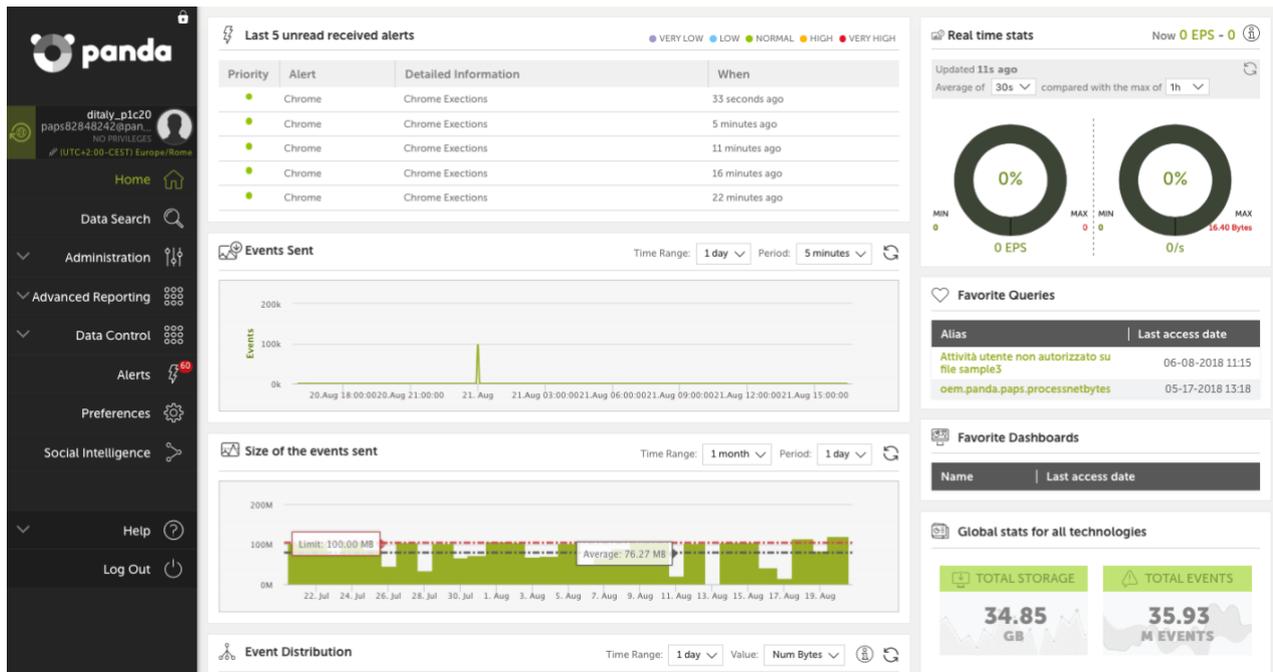


Only specialized Threat Hunters can provide this kind of service. As opposed to Threat Detection, mostly based on automated verification systems, Panda Security's Threat Hunters continuously use their knowledge and skills to compete in the same league as the most capable hackers and cyber-criminals of today. Without additional charges, Panda Security leverages their creativity and their commitment to detect every possible hacker attack on protected environments. **The Service is entirely managed by Panda Security, and it does not require the client to own any Cybersecurity specialized resources - those are already part of Adaptive Defense.**

2.7. Panda Advanced Visualization Tool (AVT)

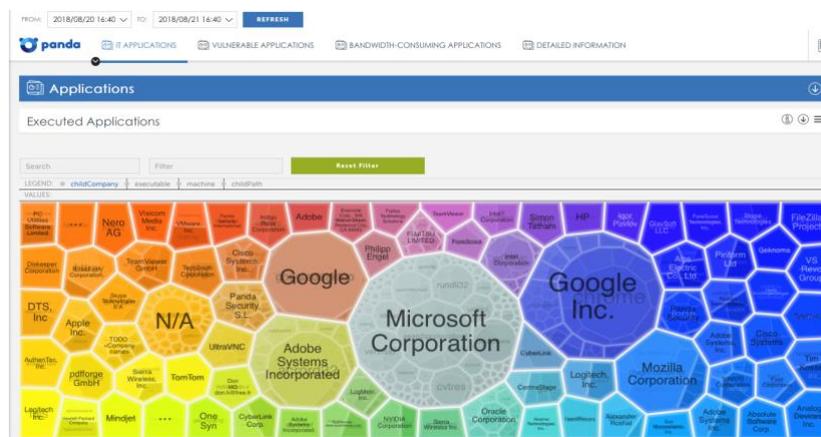
Adaptive Defense 360 offers optional modules able to add maximum visibility to endpoint security management, verify compliance in the use of corporate applications, analyze bandwidth usage, provide advanced analysis tools and much more.

AVT is accessible through single sign-on directly from the management interface of Adaptive Defense. The initial Dashboard is simple, intuitive and rich in relevant statistical information.



Panda Security's DNA is ease of use, whichever solution you are looking for. Through the pre-configured dashboard our clients can immediately start to analyze data in real-time.

For example, in order to obtain immediate visibility of all applications and processes in execution on protected hosts, you will just have to select the Application Control dashboard and the time period to monitor. Moreover, ART is able to visualize any information in real-time at the moment it is collected.



It is also possible to edit the visualization of the various pre-configured Dashboards by modifying their appearance, the selection of data to visualize and customize the query source which serves as the data set for the Dashboard.



AVT offers a query editing feature, no matter if you want to edit an existing Dashboard or if you want to create a new one from scratch. These functionalities are available in both “script” format and in graphic format.

QUERY EDITOR

```

1 from oem.panda.paps.ops where user /= "<unknown>\<unknown>", user /= "NT
AUTHORITY\SYSTEM", user /= "NT AUTHORITY\SERVICIO LOCAL", user /= "NT AUTHORITY\Servicio
de red" select lower(childPath) as lowerPath select subs(lowerPath, re(".*\\\\"),
template(" ")) as Path2, split(Path2, ".exe", 0) as OfficeApplications where
OfficeApplications = "winword" or OfficeApplications = "excel" or OfficeApplications =
"devenv" or OfficeApplications = "mspub" or OfficeApplications = "outlook" or
OfficeApplications = "onenote" or OfficeApplications = "powerpnt" group every 30m by
OfficeApplications, user every 0 select 1 as Max

```

OPERATIONS OVER COLUMNS

CREATE COLUMN | FILTER DATA | **AGGREGATE FUNCTION** | OR

Column Name: machinelip

Aggregation: Count

Arguments: Count machinelip (NEW ARGUMENT), op

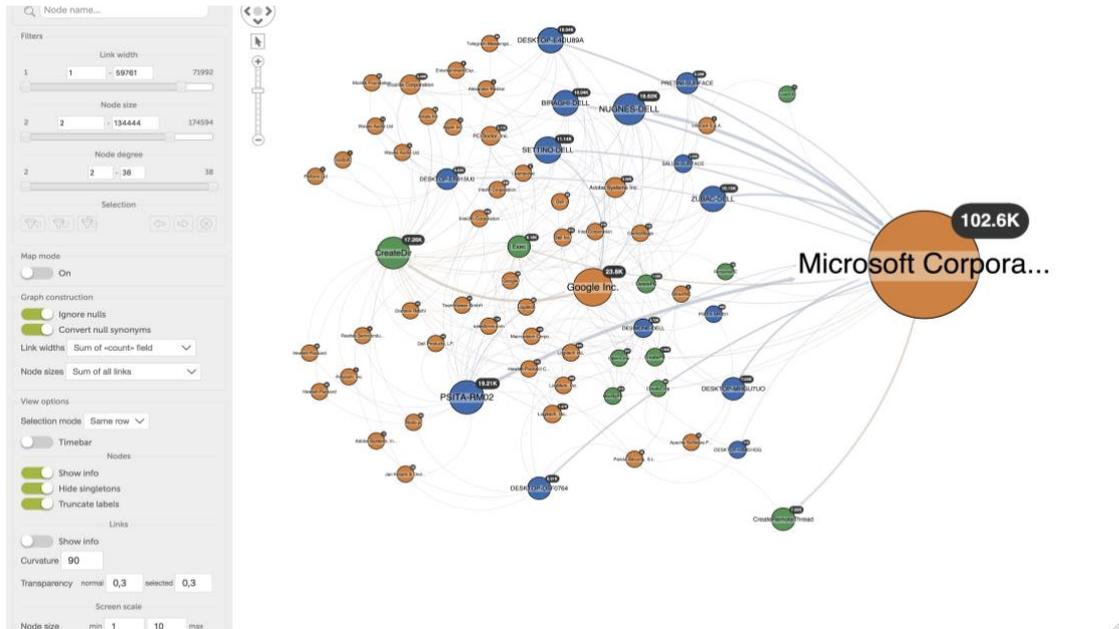
CANCEL | AGGREGATE FUNCTION

Some of the pre-configured dashboards include:

- Executed applications,
- Microsoft licenses in use,
- Vulnerable applications installed,
- Vulnerable applications executed,
- Data volume received per application,
- Data volume sent per application,
- Top 10 executed applications,
- Top 10 vulnerable applications executed,
- Malware detection,
- Detected accidents by type,
- Accidents per status,
- Hosts identified as sources or infection vessels,
- Outbound traffic per geographic region,
- Geo-synched outwards traffic,
- Login users (per host, per user, etc)
- Bandwidth use per application,
- File access.

For companies wanting to monitor application behavior or investigate a security incident, Panda Advanced Visualization Tool is the ideal tool. Its flexibility, granularity, and ease of use of the collected information allow full insight into what really happens inside the infrastructure.

With just a couple of mouse clicks it is possible to create customized Dashboards like the one below. Each Dashboard can be used in real-time and you can navigate through the collected data. This is a real-time monitoring tool rather than a simple static report.



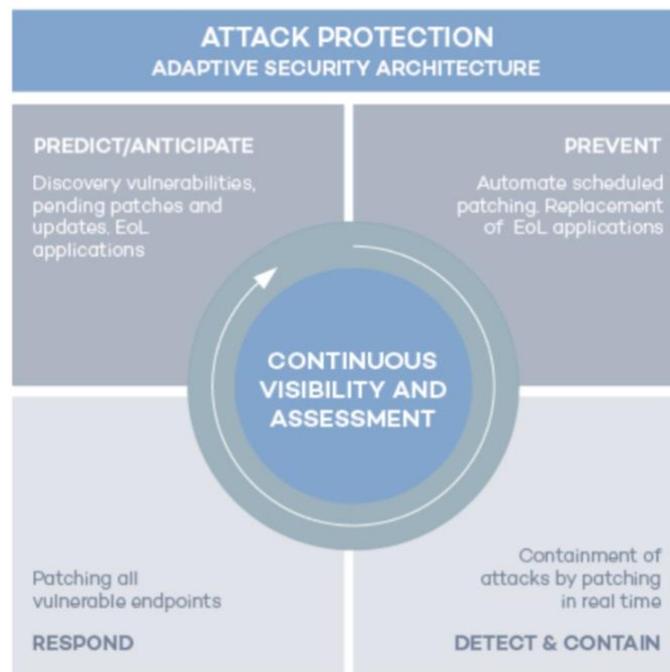
In the example above, an analysis of the interaction between hosts, users and application events takes place, allowing us to know:

- which application is used more often (indicated by the orange bubbles and by the size of the bubble including a counter),
- which hosts use which applications (indicated by the blue bubbles),
- which application-related actions are carried out by users (i.e. directory creation, file deletion, processes execution)

2.9 Patch Management

Today, 99.96% of active vulnerabilities in corporate endpoints are related to missing updates which, if installed, would greatly prevent the security risk. Additionally, 86% of vulnerabilities are due to unpatched third-party applications such as Java, Adobe, Mozilla, Firefox, Chrome, Flash, and OpenOffice, among others. If this trend continues, by 2020, 99% of the vulnerabilities causing security incidents will be known exploits that could be easily avoided by being patched before the incident.

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.

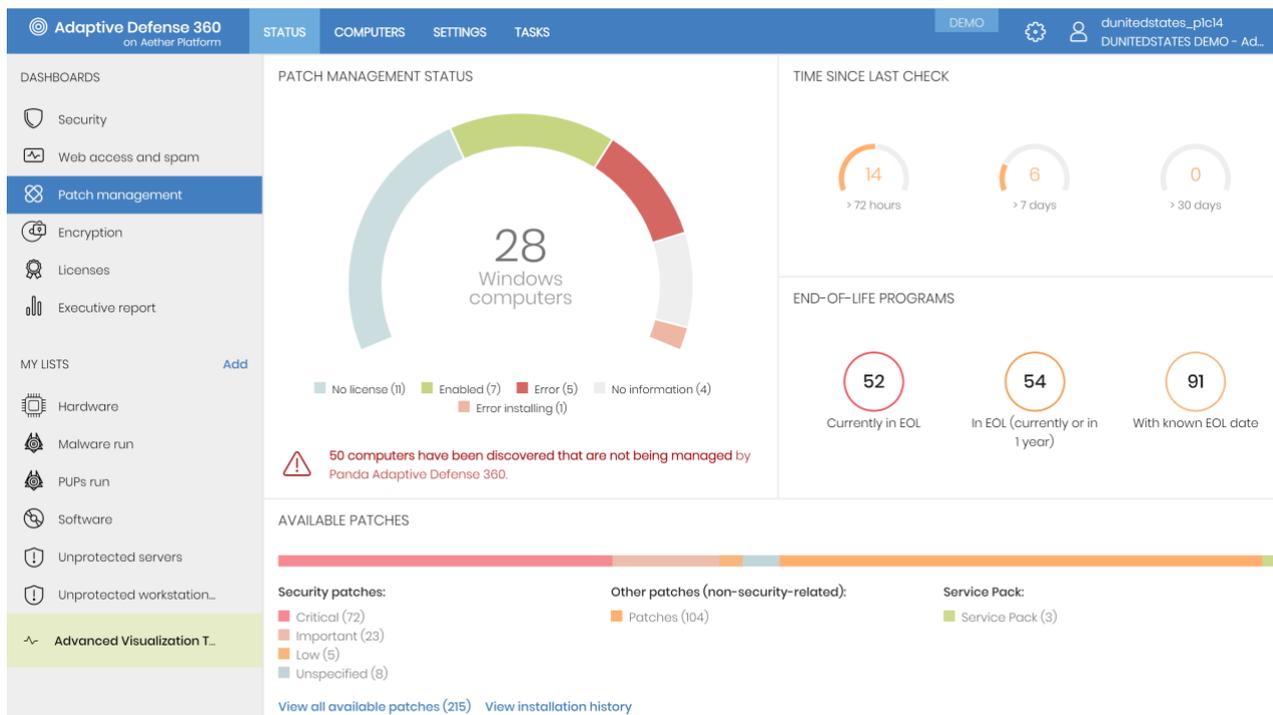


The solution does not require the deployment of any new endpoint agents or management console as it is fully integrated in all of Panda Security's endpoint solutions. Plus, it provides centralized, real-time visibility into the security status of software vulnerabilities, missing patches, updates and 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.

2.9.1 Key Features

Discovery:





Single-panel view with real-time information of all vulnerable computers, pending patches and unsupported (EOL3) software, with their remediation status.

- Detailed information about patches and pending updates, details of the relevant security bulletin, as well as computer and computer group information, and more.

Available actions:

- Filter and search for patches based on criticality, computer, group, application, patch, CVE ID and status.
- Ability to take actions directly on computers: restart, install now or schedule.
- Unattended scanning for pending updates, in real time or at periodic intervals (3, 6, 12 or 24 hours).
- In exploit detections, notification of pending patches. Ability to launch installations immediately or scheduled from the console, isolating the computer if required.

Patch and update planning and installation tasks:

- Configurable by criticality.
- Can be performed on specific endpoints and groups.
- Immediate, scheduled for one-time execution or for repeated execution at regular intervals (date/time).
- Ability to control computer restarts and set exceptions.
- Rollback to uninstall a patch that may cause an unexpected conflict with an existing configuration.

Endpoint and update status monitoring, via:

- Dashboard and actionable lists.
- High-level and detailed reports.
- Lists of updated computers, computers with pending updates with errors.

Granular management based on groups and roles with different permissions:

- Role-based visibility into vulnerable computers, patches and Service Packs.

2.10 Full Encryption

According to Gartner, **a laptop is stolen every 53 seconds**, and it seems clear that the growing amount of data stored on endpoints has increased the interest in it and the risk of suffering a data security breach due to loss, theft or unauthorized access to information.

This has resulted in regulations such as the GDPR in the European Union and the CCPA in the United States, among others, becoming more demanding in an effort to reduce the increasing likelihood of loss, theft or unauthorized access to data and the serious economic impact this may have on organizations.

Panda Full Encryption leverages **BitLocker**, a proven and stable Microsoft technology, to encrypt and decrypt disks without impacting end users and providing organizations with the added value of **centrally controlling and managing the recovery keys** stored on Panda Security's cloud-based management platform: Aether.

2.10.1 Key Features

Panda Full Encryption is an additional module for Panda Security's endpoint protection and advanced adaptive security solutions, designed to centrally manage full disk encryption and provide the following features:

Full drive encryption and decryption

Panda Full Encryption leverages BitLocker to fully encrypt the drives of your Windows laptops, desktops and servers. Panda Full Encryption dashboard provides global visibility into the network endpoints compatible with the feature, their encryption status and the authentication method used, and enables administrators to assign encryption settings and restrict encryption permissions.

Centralized management of recovery keys

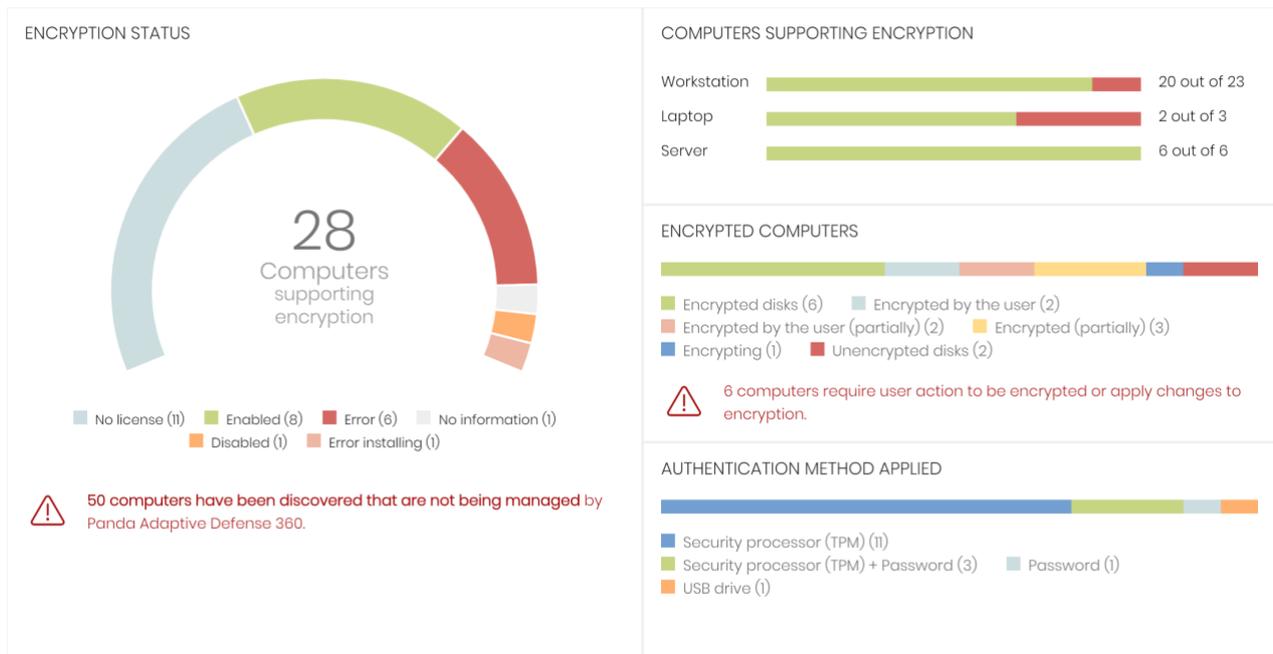
If the encryption key is forgotten, or there are changes to a computer's hardware, BitLocker will ask for a recovery key to start up the affected system.

If required, the network administrator can get the recovery key through the management console and send it to the computer user.

Lists and reports. Centralized policy application

The computer list in the console allows administrators to apply multiple filters based on encryption status. These lists can be exported for data analysis with external tools.

Define encryption policies from the console and view policy changes through audit reports you can present to regulatory bodies and institutions if required.



2.11 Data Control

Companies must ready themselves to comply with GDPR, which will come into force and bring with it dissuasive fines of up to €20 million or 4 percent of a company’s global annual turnover, whichever is greater, in the event of a breach.

The GDPR will impact all companies, industries and regions, including those outside the EU, which collect and store personal data of any EU citizens.

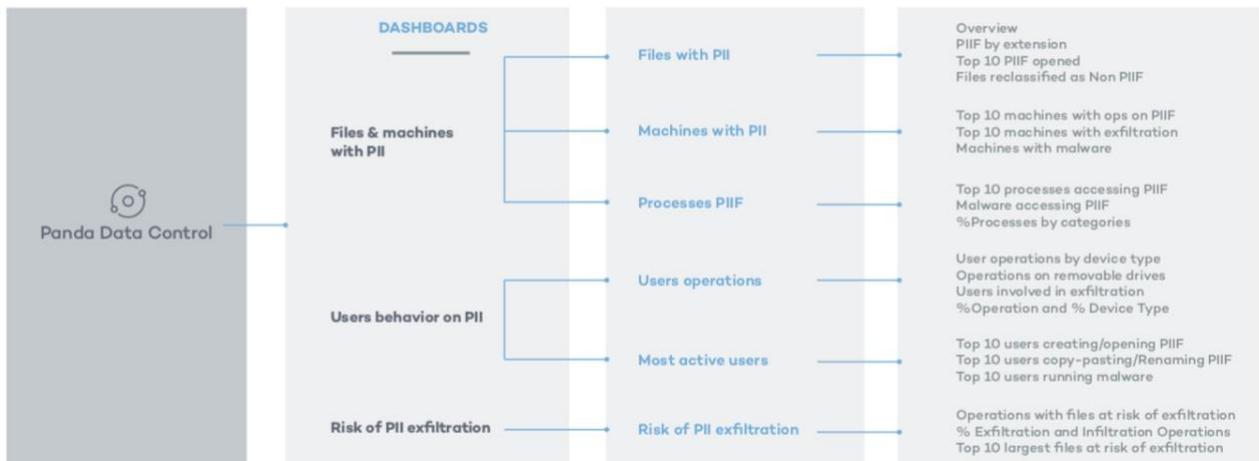
Also, companies must be ready to avoid the reputational damage caused by a data leak, and its negative effects on the confidence of employees as well as current and potential customers.

Panda Data Control is a data security module fully integrated into the Panda Adaptive Defense platform. Panda Data Control is designed to assist organizations in complying with data protection regulations, as well as discovering and protecting personal and sensitive data both in real time and throughout its lifecycle on endpoints and servers.

Panda Data Control discovers, audits, and monitors unstructured personal data on endpoints: from data at rest to data in use and data in motion.

Panda Data Control is currently restricted to EU countries.

2.11.1 Key Features



Data Discovery:

Creates an indexed inventory of all files that store unstructured personal data (data at rest), with the number of occurrences of each type of data. It classifies all information automatically.

The classification combines different techniques and algorithms of machine learning that optimize the results while reducing false positives and resource consumption on devices.

Data Monitoring:

Monitors the various types of operations performed on unstructured files (data in use), while keeping the personal data file inventory fully up to date. Any attempt to copy or move any of these files out of the network via email, Web browsers, FTP or removable storage (data in motion) is recorded by the module.

Data Visualization:

The results of the data monitoring and discovery tasks are continuously synced on the Adaptive Defense platform and in its module Advanced Visualization Tool. This module provides tools for investigating all events affecting data at rest, in use and in motion, both in real time and retrospectively throughout its lifecycle on devices.

Panda Data Control’s dashboards and predefined reports and alerts help to cover use cases and ensure security governance of the unstructured personal data held on the organization’s protected devices.



3. Adaptive Protection

More than 200,000 new malware samples are created every single day and the great majority of these are designed to be unique files and stay hidden for long periods of time, hiding their presence even to the most evolved Endpoint Protection technology.

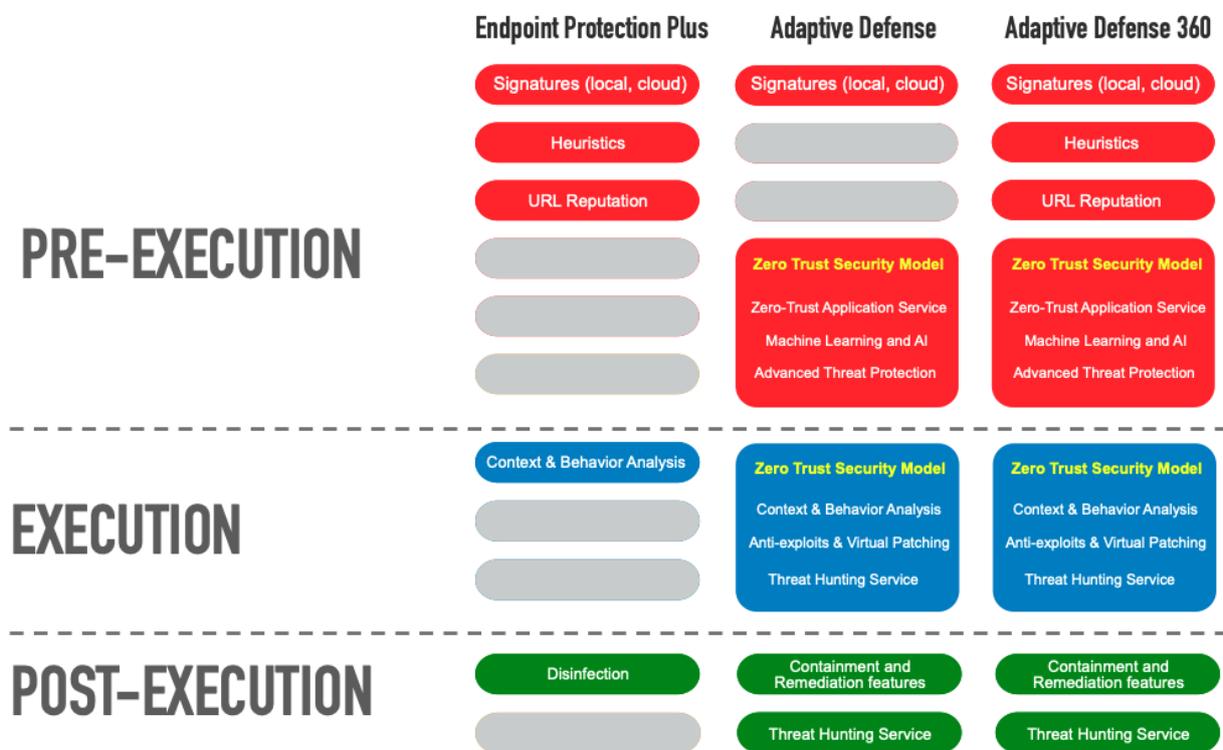


For this reason, the model provided by traditional Endpoint Protection technologies which uses signature files stored locally or in the cloud, along with behavioral engines or other similar technologies, has become inefficient. The growth of malware samples also significantly increases their window of opportunity, that period of time from the arrival of a new threat to the issuance of the signature file by a security vendor. The right security strategy has to be based on the reduction of this window of time.

Adaptive Defense 360 uses an innovative approach based on adaptive protection cycles through protection, detection, monitoring, forensic analysis and remediation.

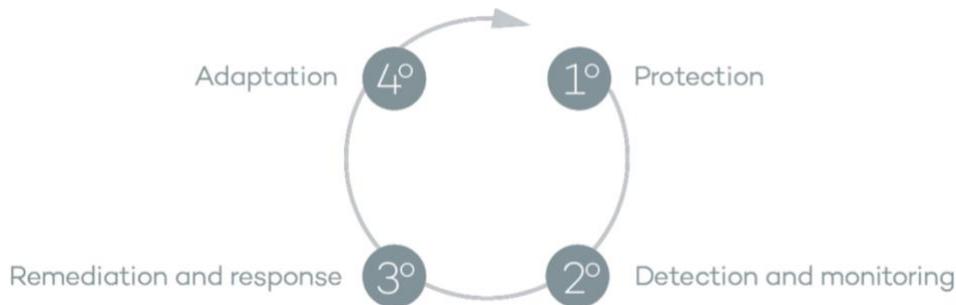
The administrators are also freed from the complex task of determining what is dangerous and what is not, dedicating their time and their resources to monitoring the overall security status of the network.

The protection model



3.1. The protection cycle

The final goal is to make it possible for companies to adapt their corporate security policies in order to prevent and react to new threats as fast as possible. The protection cycle adopted by Adaptive Defense 360 is illustrated in the below graph.



3.2. Phase 1, Protection

The first phase of the adaptive protection cycle involves tools which are necessary to protect the network against attacks and infection attempts in an efficient way. Adaptive Defense 360 is compatible with Windows, Linux and MacOS workstations and servers, as well as smartphones and tablets. Adaptive Defense 360 also provides compatibility with legacy operating systems.

Protection is a "traditional" technology module developed to protect against less complex threats like malware, viruses and trojans, based on signatures downloaded locally or accessible in the cloud and it is a basic module to the security technology stack.

Adaptive Defense 360 integrates this traditional module in order to prevent infections and unauthorized file access by malware through:

- **Anti-exploit Module**

This module aims to protect systems which are particularly vulnerable due to having reached their EOL (End of Life), like Windows XP. The fact that these systems do not receive security updates opens the possibility of compromise through exploit attacks.

The anti-exploit technology detects and neutralizes malware like Blackhole or Redkit which exploit zero-day vulnerabilities (in Java, Adobe, MS Office, etc.) to compromise systems. The protection ensured by Adaptive Defense 360 uses a three-level-detection approach, analyzing the behavior of the exploit instead of their morphology.

1. Adaptive Defense 360 provides passive exploit protection by leveraging known technologies like DEP, ASLR, SEHOP, Bottom Up Randomization and others.
2. Heuristic scanning is performed to discover if a process underwent exploitation through a vulnerability of the software. This technology is able to detect ROP, Stack pivot and other strategies used by exploits to bypass protection systems and execute the malicious code.
3. Behavior analysis is performed to detect the execution of malicious code in a process which underwent an exploit. In order to do this, Adaptive Defense 360 performs a context behavior

analysis utilizing the Panda Security Collective Intelligence platform. For further information: www.pandasecurity.com/technologies.

This layered approach allows Adaptive Defense 360 to protect the system efficiently from known vulnerabilities.

- **Permanent protection and Collective Intelligence**

Adaptive Defense 360 leverages Panda Security's Collective Intelligence, a security platform which significantly increases the capacity to detect threats.

Panda Security's Collective Intelligence classifies and automatically refines all detection data provided by its worldwide community of users, both consumer and corporate. Adaptive Defense 360 queries Collective Intelligence when necessary, ensuring optimum and unpaired detection levels, while minimizing endpoint resource consumption.

Once new malware is detected, analyzed, and identified, Adaptive Defense 360 automatically sends the information on the specific threat to the Collective Intelligence platform. This data is refined by the platform and made available in real-time to all other Panda Security clients in the world, hence the name "Collective Intelligence". In line with the exponential growth of new malware, Panda Security's cloud-hosted Collective Intelligence and Services are the essential add-on to traditional Endpoint Protection updates.

- **Email and Web protection**

Adaptive Defense 360 goes beyond the traditional antivirus approach, providing complete protection able to perform low-level analysis of every communication socket using protocols like HTTP, HTTPS or POP3. In this way it provides homogeneous protection for email and web applications without the complexity usually introduced by installing and configuring third-party plug-ins.

- **Firewall and Intrusion Detection System (IDS)**

Adaptive Defense 360 provides three analysis layers and network traffic protection (inbound and outbound):

- System Rules: these rules describe communication specifications (ports, IP addresses, protocols etc.) in order to allow or deny the flow of data defined in the policy
- Program Protection: these rules allow or deny the communication from programs installed on the endpoint
- Intrusion Detection: detects and blocks packets of malicious data which could negatively impact either the security or the performance of the protected endpoints.

- **Device Control**

Devices like USB flash drives, CD/DVD, SD readers, Bluetooth, 4G modems, and smartphone devices can become a vehicle for compromise. Adaptive Defense 360 allows administrators to limit the use of these devices on protected computers, blocking their access or allowing its limited use (read-only access).

- **Antispam, Antivirus and content filtering for Exchange server**

Adaptive Defense 360 provides antispam, antivirus, and anti-malware protection which includes the detection of hacking tools, suspicious applications, and potentially unwanted programs that are sent to Microsoft Exchange mailboxes.

Adaptive Defense 360 protects Exchange servers using two different technologies:

Mailbox Protection: this protection is used on Exchange servers which have the Mailbox role and scans all folders and mailboxes in the background, or as soon as new messages are received and saved in the folders by the users. Mailbox Protection acts directly on the elements present in the analyzed messages, in order to allow the cleaning (or removal) of all items considered malicious. Moreover, Mailbox Protection allows administrators to perform the scanning of the user folders on the Exchange server in the background, making the most out of server inactivity. This protection uses intelligent scanning which does not recheck already checked items, in contrast with the common practice to analyze all folders and the mailbox each time a new signature file is published by the antivirus vendor.

Transport Protection: this technology is used in Client Access, Edge Transport and Mailbox roles to scan all the traffic to and from the Exchange server. This protection does not allow the manipulation of items present in the body of the analyzed messages. The entire body of a dangerous item is treated as a single component and each action taken by Adaptive Defense 360 refers to the whole message: cancel a message, quarantine it, let it be sent/received without taking any action, etc.

- **Web and Access Control**

Adaptive Defense 360 includes features which control and limit access to the web through categories or by configuring lists of URLs/domains to allow or deny access to (whitelist/blacklist). There are 60 different web categories available to define navigation policies, which can also be time-scheduled.

3.3. Phase 2, Detection and Monitoring

In this phase Adaptive Defense 360 implements a series of new EDR (Endpoint Detection and Response) technologies, allowing the network administrator to detect and block threats.

- **Advanced Permanent Protection**

The Advanced Permanent Protection of Adaptive Defense 360 is a new and innovative technology which controls each the execution of each process on endpoints in real-time.

Adaptive Defense 360 records every action taken by processes on the endpoints and analyzes them by applying automated techniques in the Machine Learning and Big Data environments.

The service returns a classification for all processes (goodware or malware) with a precision of 99,9991% (less than 1 mistake for every 100,000 analyzed files), avoiding the false positives. Moreover, for processes which require manual (human) analysis, Panda Security runs them through its laboratories (PandaLabs), with the aim of classifying the items in the shortest time possible from the moment they have been intercepted in execution.

Adaptive Defense 360 implements three different configuration modes to define actions for known good, known bad or yet unclassified processes:

- **Audit:** in this protection mode, Adaptive Defense 360 fully reports on detected threats but does not block the reported item. This mode is useful to for a security assessment of the entire environment or portions of it.
- **Hardening:** this mode is applicable to environments where there are constant changes in the installed software or in which many potentially unknown programs are executed, as in the case of proprietary in-house software, which could require more time to classify by Adaptive Defense 360. Hardening is used to maintain an equilibrium between an adequate security posture and full productivity of the users. In this mode, blocking of unknown/unclassified programs is limited to those initially considered dangerous, based on four possible scenarios:
 1. Processes classified by Panda Security as Goodware: these are authorized to execute
 2. Processes classified by Panda Security as Malware: they are blocked, sent to quarantine or disinfected (if necessary)
 3. Not yet classified (unknown) programs deriving from external sources (internet, e-mail and other sources): these are blocked and will not be executed until Panda Security delivers a classification. Once the classification is delivered, they will be authorized to execute (Goodware) or will remain blocked (Malware)



This classification process is almost immediate in most cases. A program downloaded from the Internet and unknown to Adaptive Defense 360 can be initially blocked but will be authorized to execute in a couple of minutes if classified as Goodware.

4. Not yet classified (unknown) programs which have been installed on the endpoint prior to the installation of Adaptive Defense 360: it will be possible to execute them, but their actions will be monitored and analyzed by Panda Security. Once classified, they will be automatically authorized for execution (Goodware) or remediated (Malware).

Note: Adaptive Defense 360 will not, in any case, send sensitive information to Panda Security. Sensitive information might include but is not limited to user documents in full or in part, user data, or credentials.

- **Lock:** in environments where endpoint security is an absolute priority, and in order to provide a maximum grade security posture, Adaptive Defense 360 can be configured in Lock mode. In this protection mode, any processes awaiting classification by Panda Security will be denied execution. This means that the only processes allowed to execute will be the legitimate ones. Similar to Hardening mode, programs classified as malicious will be sent to quarantine, while unknown programs will not be allowed to execute until they are classified (as Goodware or malware).



More than 99% of all programs on any endpoint have already been classified by Adaptive Defense 360 and just a few of them will be denied execution.

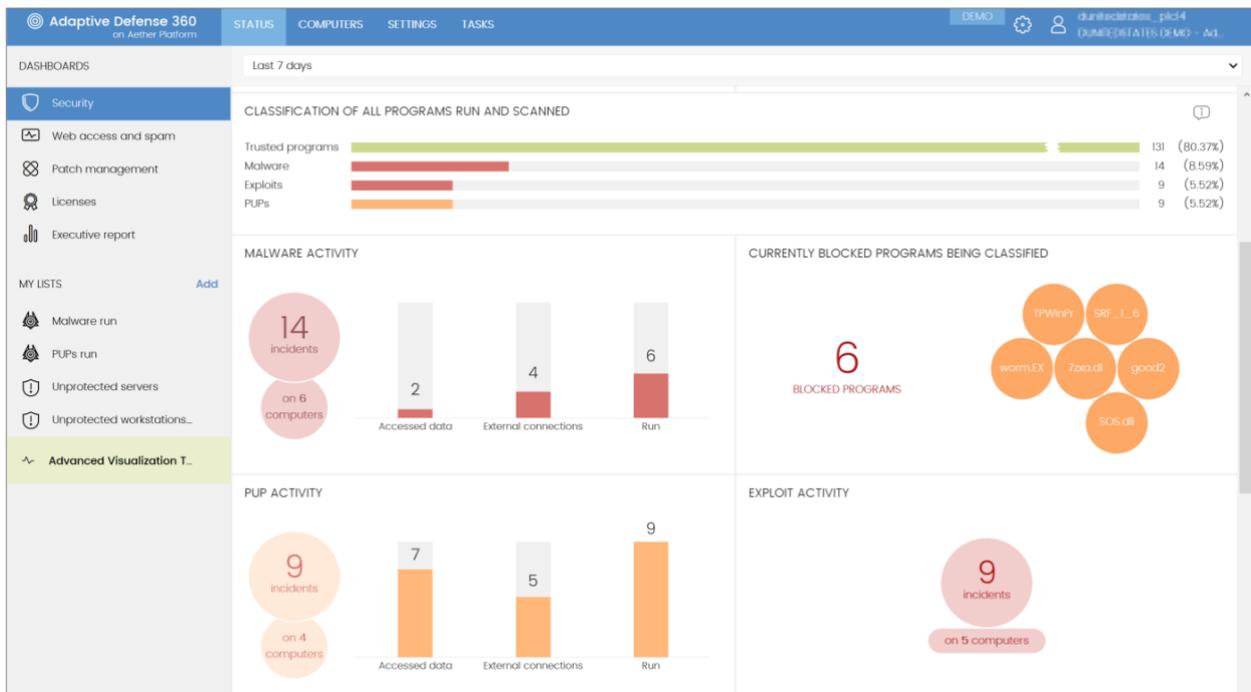
- **Visibility on the network status**

Adaptive Defense 360 provides a set of tools which allow administrators to evaluate the security status of the corporate network at a glance using the control panel, dashboard, and the status of pre-configured actions in the solution.

Most reporting tools are really nothing new. Nevertheless, Panda Security's top priority is to determine whether the network has been attacked or compromised by obtaining the necessary information in real-time, limiting the extent of an infection and its repercussions in the network.

The Adaptive Defense 360 dashboard provides fundamental information such as:

- Processes detected as unknown and subject to the ongoing Panda Security classification activity, together with a preliminary risk level evaluation
- Detailed information on actions executed by unknown processes which turned out to be malware
- Detections by infection vector and correlation with other compromised hosts
- Temporal analysis with behavioral correlation of each suspicious process detected



The Status dashboard provides administrators with global visibility with respect to both execution attempts of known malware and zero-day threat execution attempts, which are designed to remain undetected by traditional antivirus detection technologies.

3.4. Phase 3, Response & Remediation

In case of infection the administrators need to be able to step in through two lines of action: rapidly restore affected computers to their original state and evaluate the infection impact. This includes determining if there has been data loss and the severity of the attack, such as which endpoints have been compromised, etc. The Response and Remediation phases provide the tools for these two scenarios:

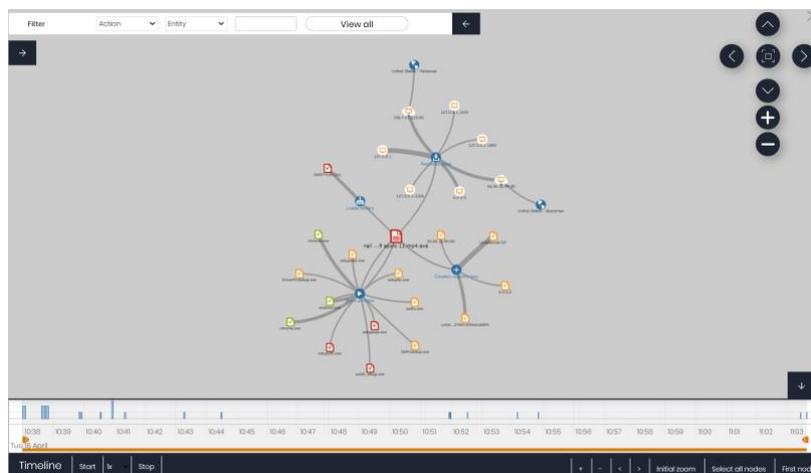
- **Response**

Administrators can use a tool for forensic analysis which lays out each action that a malware takes and includes the infection vector (the way in which the malware entered the network).

Malware life cycle on the computer View activity graph

Date ↑	Times	Action	Path/URL/Registry Key/IP:Port	File Hash/Registry Value/Protocol-Direction/Description	Trusted
4/16/2019	10:38:03 AM	Creates registry key to run	\REGISTRY\USER\S-1-5-21-3286655578-1091891218-2006878755-1004_CLASSES\CLSID\{F28C2F70-47DE-4EA5-8F6D-7D1476CDIEF5}\LocalServer32?	C:\Documents and Settings\Adminri\Mis documentos\Downloads\Neil Armstrong transmision original del alunizaje 1969 Apolo 11tmp4.exe	Unknown
4/16/2019	10:38:03 AM	Creates registry key to run	\REGISTRY\USER\S-1-5-21-3286655578-1091891218-2006878755-1004_CLASSES\CLSID\{F28C2F70-47DE-4EA5-8F6D-7D1476CDIEF5}\LocalServer32?ServerExecutable	C:\Documents and Settings\Adminri\Mis documentos\Downloads\Neil Armstrong transmision original del alunizaje 1969 A	Unknown
4/16/2019	10:38:04 AM	Creates registry key to run	\REGISTRY\USER\S-1-5-21-3286655578-1091891218-2006878755-1004_CLASSES\TypeLib\{157B1AA6-3E5C-404A-9118-C1D91F537040}\1.0\0\win32?	C:\Documents and Settings\Adminri\Mis documentos\Downloads\Neil Armstrong transmision original del alunizaje 1969 Apolo 11tmp4.exe	Unknown
4/16/2019	10:38:40 AM	Uses socket	127.0.0.1	CUDP-Unknown	Unknown
4/16/2019	10:38:40 AM	Uses socket	127.0.0.1:1630	UDP-Bidirectional	Unknown
4/16/2019	10:38:48 AM	Uses socket	0.0.0.0	TCP-Unknown	Unknown
4/16/2019	10:38:48 AM	Uses socket	54.69.3299:80	TCP-Bidirectional	Unknown
4/16/2019	10:38:49 AM	Uses socket	198.7.61.119:80	TCP-Bidirectional	Unknown
4/16/2019	10:39:52 AM	Loads	PROGRAM_FILES\MOVIES TOOLBAR\SAFETY\NUT\SAFETYCRT.DLL	9994BF035913FE8EB6BC98ECCBD580E1	No
4/16/2019	10:39:55 AM	Runs	TEMP\087B213b8b8\temp\setupesplexe	F69E31FAA4B9159ABD590D0CD2CC94A5	No
4/16/2019	10:40:33 AM	Runs	TEMP\087B213b8b8\temp\extIE_setup.exe	66D0E599FC9EDDCA4A591D4C54BA6187	No

[example of the analysis of the life cycle of a malicious item]

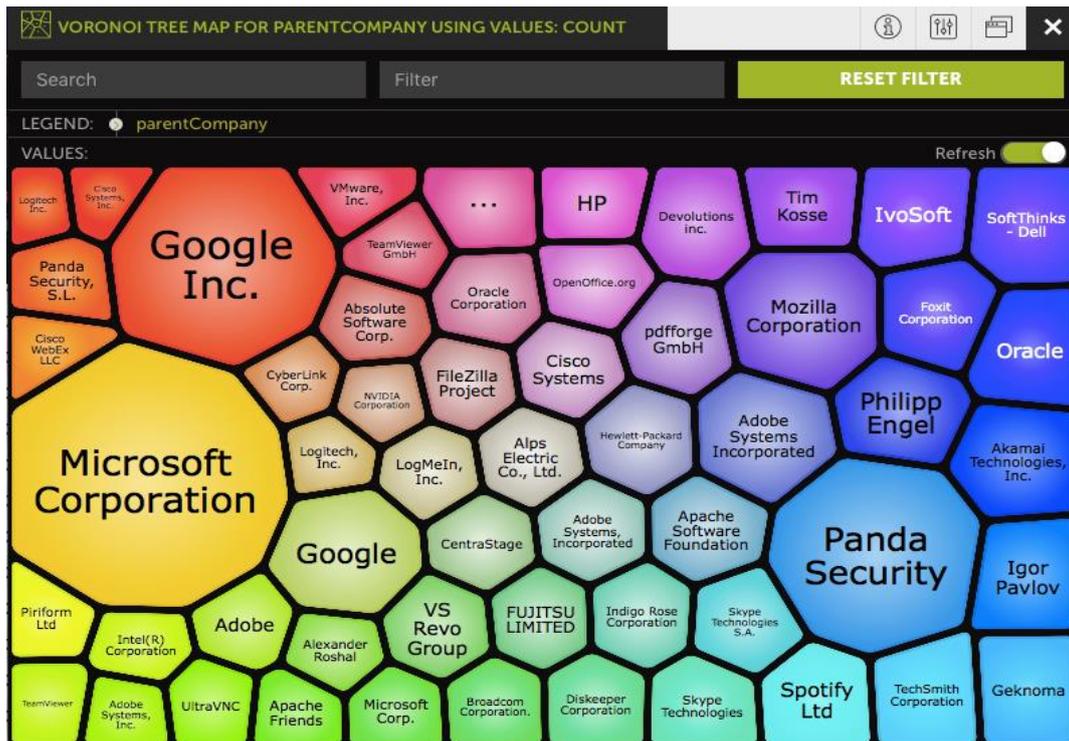


[example of the analysis of the life cycle of a malicious item in graphical view]

Moreover, in order to contain a possible threat, the **isolation** feature is able to separate any host from the rest of the network. IT personnel can also define the specific applications or processes

authorized to open sockets in isolation mode, in order to guarantee productivity even in case they are compromised. Along with the explicitly authorized processes, the communication from the Panda Security agent to the Adaptive Defense platform will always be ensured in order to remotely manage the host.

The optional module Advanced Visualization Tool (AVT), previously described, gathers every single action taken by the processes executed by users and makes the data available for deeper analysis. It is possible in this way to extend the forensic analysis feature and perform queries or advanced investigations with this module.



- **Remediation**

Adaptive Defense 360 delivers numerous remediation tools - some of them automatic, others manual. The automatic tools include a traditional disinfection module, typical of antivirus solutions, together with a simple but efficient quarantine management used to contain suspicious items or to delete them.

3.5. Phase 4, Adaptation

After an infection is singled out, analyzed and remediated, the administrator can validate and adapt security policies in order to avoid future instances of the same situation.

Thanks to the forensic information gathered by the Advanced Search, more generic security policies can be reviewed in this phase: from a hardening of the policies applied on perimeter firewalls (particularly for outbound traffic), better control of removable devices, a new download policy for the internet-borne executables, to employee training on the use of computer tools and security.

Panda Data Analytics can be adopted as the company SIEM or integrated with an existing SIEM for this purpose.

Adaptive Defense 360 can be used to strengthen the security of the endpoint through the different protection modules:

- **Lock Mode:** if most users tend to use the same software repeatedly, occasionally installing programs of undetermined sources, a plausible solution which could dramatically reduce the risk represented by possible zero-day attacks is to set Adaptive Defense 360 in Lock Mode. It will prevent the execution of any illegitimate or dangerous programs.
- **Anti-malware policy:** the planning of additional file scans and the enabling of vector-specific protection settings, for example e-mail or web, will help to better protect endpoints.
- **Content Filter:** applying policies to control internet surfing, through web & content protection components, will reduce the access to questionable websites from which users could download malicious contents (without even knowing).
- **Device Control:** another commonly used infection vector are removable USB devices, SD cards, or smartphones used as mass storage devices. By limiting or completely denying access to these devices through the endpoints you will reduce the risk of malware infections.
- **Firewall and IDS:** prevents unauthorized communication to and from programs which are not dangerous themselves, but could open sockets to download trojans and other malware. Firewall and IDS can be used to prevent malware from spreading to other computers in case of an infection. Adaptive Defense 360 examines all actions taken by malware and through forensic analysis tools provides complete visibility in order to improve the security posture of our clients.

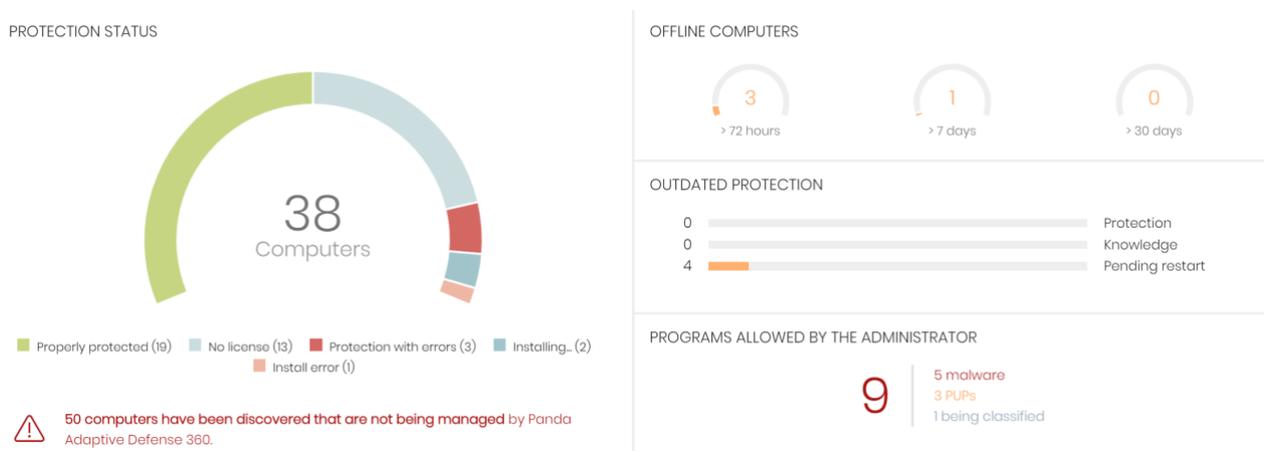
3.6. Main components

Adaptive Defense 360 can be managed through an adaptive web console and can be used from any device, including smartphones and tablets. It is comprised of the following main areas:

- **Status:** administrators need to have the overall security status accessible through a simple and efficient control panel. The Status panel provides information on detected activities, malicious programs, unclassified elements, and many other pieces of information.
- **Computers:** this section facilitates the management of all computers which have the Adaptive Defense 360 agent. Through dedicated views it will be possible to manage endpoints that are protected, not protected, without a license, excluded, etc. It is also possible to manage groups of computers or to protect new computers.
- **Installation:** the tools to install or uninstall the Adaptive Defense 360 agent (or a third-party security solution during the deployment phase), can be obtained here. It will then be possible to define the operating system to install the agent on (i.e. Windows, Linux, Android, etc.), generate a link for the installation download or to use automated network deployment methods.
- **Settings:** through this panel Adaptive Defense 360 can be completely configured in its every component. Settings policy definition is made possible thanks to the customization of profiles which can be applied to groups of computers.

3.7. Status

The status panel provides complete visibility on used licenses, their expiration date, and the client endpoints not connected in the last 72 hours, 7 days and 30 days. Moreover, it makes it possible to monitor the client protection status in an easy and efficient way, e.g.: status of the definition updates (for the traditional modules), clients in need of a restart, clients with protection errors, and clients which are not protected by Panda Security.



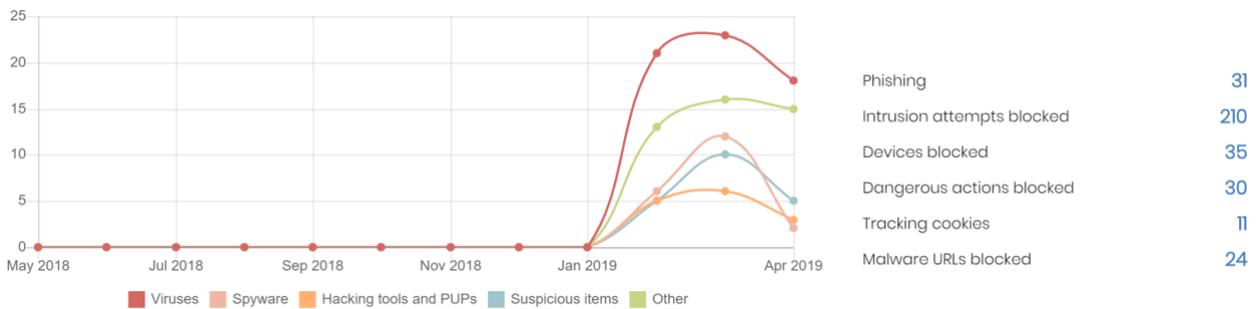
From the Status window it is also possible to access all information regarding detected threats, potentially dangerous programs, and applications classified as trusted (Goodware). Through the time filter it is possible to visualize a different period from the 7-day suggested by default.

CLASSIFICATION OF ALL PROGRAMS RUN AND SCANNED

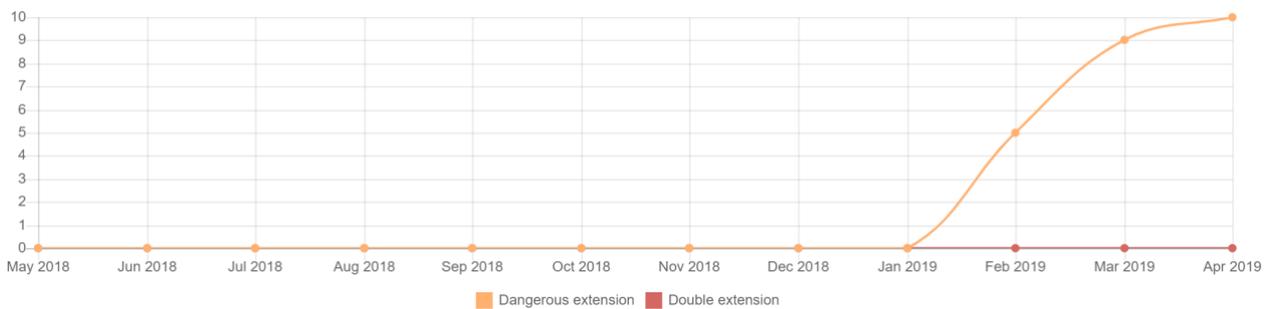


In the example below you can visualize all the threats detected by traditional technologies: phishing, intrusion attempts, blocked devices, dangerous actions, tracking cookies, malware URLs and content filtering.

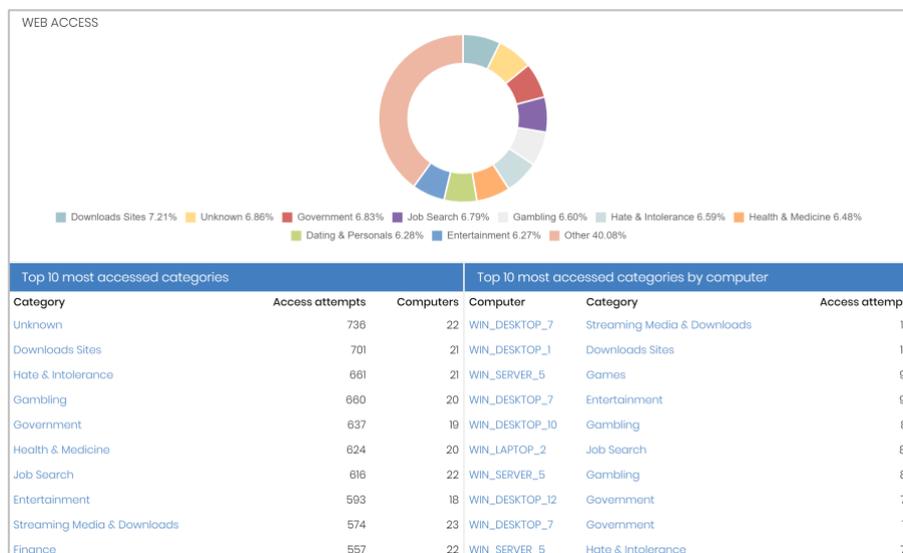
THREATS DETECTED BY THE ANTIVIRUS



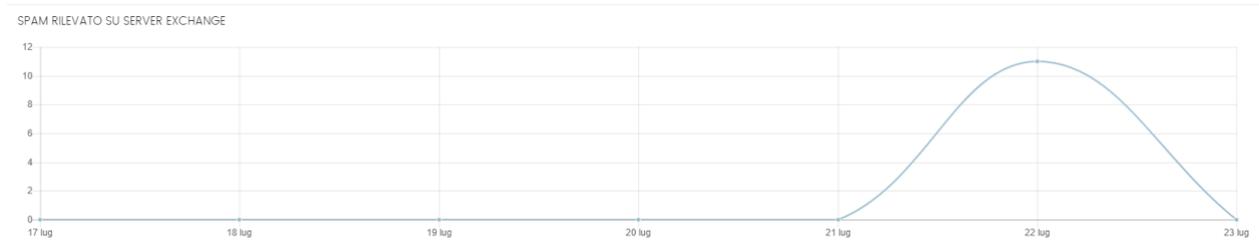
CONTENT FILTERING FOR EXCHANGE SERVERS



It is also possible to visualize web access and website categorization (allowed and blocked URLs):



Antispam for Microsoft Exchange:



Status summary of assigned licenses:

PANDA ADAPTIVE DEFENSE 360

25 trial licenses



Your licenses will expire on 4/11/2020 (360 days left)

Within the "Executive Report" five different types of reports can be generated (License status, Security status, Detections, Web access and spam, Available patches) both on demand or scheduled, defining a convenient automated schedule for systems administrators.

[View](#) [Schedule](#)

Dates
Last month

Computers
All computers

Content

- License status
- Security status
- Detections
- Web access and spam
- Available patches

[View](#) [Schedule report](#)

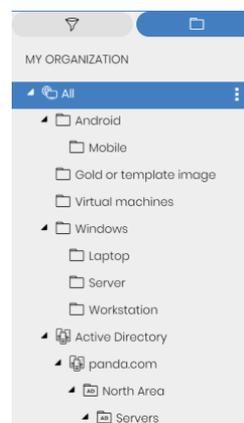
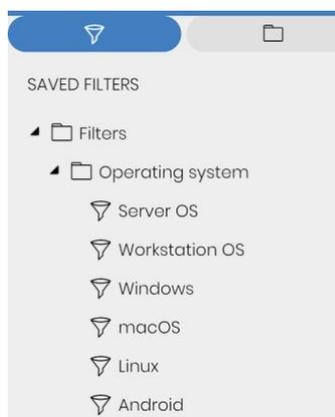
3.8. Computers

In the Computers section it is possible to see all the information regarding endpoints with Adaptive Defense 360 installed, to manage their settings, to perform operations like isolation or restarts, to plan AV scans and much more. Additional endpoints can be added by choosing the most suitable deployment method.

<input type="checkbox"/> Computer ↑	IP address	Group	Operating system	Last connection
<input type="checkbox"/> ANDROID_1		Mobile	Android (7.1.1)	4/18/2019 3:26:48 AM
<input type="checkbox"/> ANDROID_2		Mobile	Android (7.1.1)	4/18/2019 3:26:49 AM
<input type="checkbox"/> ANDROID_3		Mobile	Android (7.1.1)	4/18/2019 3:26:49 AM
<input type="checkbox"/> ANDROID_4		Mobile	Android (7.1.1)	4/18/2019 3:26:54 AM
<input type="checkbox"/> ANDROID_5		Mobile	Android (7.1.1)	4/18/2019 3:26:54 AM
<input type="checkbox"/> ANDROID_6		Mobile	Android (7.1.1)	4/18/2019 3:26:55 AM
<input type="checkbox"/> LINUX_DESKTOP_1	192.168.0.12	All	Fedora (25)	4/18/2019 3:26:54 AM
<input type="checkbox"/> LINUX_LAPTOP_1	192.168.0.11	All	Fedora (25)	4/16/2019 3:26:48 AM
<input type="checkbox"/> MAC_DESKTOP_1	192.168.0.57	All	macOS Mojave (10.14)	4/18/2019 3:26:48 AM
<input type="checkbox"/> MAC_DESKTOP_2	192.168.0.188	All	OS X El Capitan (10.11)	4/18/2019 3:26:54 AM
<input type="checkbox"/> WIN_DESKTOP_1	192.168.0.60	Workstation	Windows 7 Ultimate 64 SP4	4/18/2019 3:26:45 AM
<input type="checkbox"/> WIN_DESKTOP_10	192.168.0.210	Workstation	Windows 10 Pro (1607)	4/18/2019 3:26:53 AM
<input type="checkbox"/> WIN_DESKTOP_11	192.168.0.223	Workstation	Windows 8.1 Enterprise 64 SP2	4/18/2019 3:26:53 AM
<input type="checkbox"/> WIN_DESKTOP_12	192.168.0.141	Workstation	Windows 10 Pro (1607)	4/18/2019 3:26:55 AM
<input type="checkbox"/> WIN_DESKTOP_2	192.168.0.165	Workstation	Windows 8.1 Enterprise 64 SP3	4/18/2019 3:26:46 AM
<input type="checkbox"/> WIN_DESKTOP_3	192.168.0.222	Workstation	Windows 10 Pro (1607)	4/18/2019 3:26:46 AM
<input type="checkbox"/> WIN_DESKTOP_4	192.168.0.176	Workstation	Windows 8.1 Enterprise 64	4/18/2019 3:26:47 AM
<input type="checkbox"/> WIN_DESKTOP_5	192.168.0.213	Workstation	Windows 7 Ultimate 64 SP1	4/18/2019 3:26:47 AM
<input type="checkbox"/> WIN_DESKTOP_6	192.168.0.71	Workstation	Windows 8.1 Enterprise 64 SP1	4/18/2019 3:26:49 AM
<input type="checkbox"/> WIN_DESKTOP_7	192.168.0.240	Workstation	Windows 10 Pro (1607)	4/18/2019 3:26:51 AM

Default search filters are available in the console. You can also to create personalized filters which focus on hardware, software, settings, licensing, module specifics (Data Control, Advanced Visualization Tool and Patch Management).

In the same section it is possible to set organizational groups to segment the endpoints or to leverage an existing Active Directory (AD) Organizational Unit (OU) structure. Adaptive Defense 360 also makes it possible to manage mixed groups of hosts both from AD and local groups.



By selecting a device you can visualize its detailed information and verify which modules of the product are active on it, including error messages and a summary of the applied policies and detections.

Adaptive Defense 360 makes hardware and system performance information from every managed host available: CPU, memory and local HDD, software inventory, and applied security settings. It is possible to visualize the same kind of information even for mobile devices.

< Back
WIN_DESKTOP_12
↻ 📁 📁 🗑️ 🔍 ⋮



WIN_DESKTOP_12

IP address: 192.168.0.141

Active Directory path: WORKGROUP\local\Computers\Workstations\Division\WIN_DESKTOP_12

Group: All\Windows\Workstation

Operating system: Windows 10 Pro (1607)

Details
Hardware
Software
Settings

Computer

Name:	WIN_DESKTOP_12
Description:	Change
IP addresses:	192.168.0.141, 10.202.136.17, fe80:5d66:dc58:9b8c:7e84, fd:ad:21:31:, 192.168.56.1, 192.168.56.50
Physical addresses (MAC):	04:0A:E5:C2:DE:14, 00:0E:A6:F8:FE:FF, 00:0E:A6:F9:1B:6D, 00:15:AF:0A:C3:12
Domain:	WORKGROUP
Active Directory path:	WORKGROUP\local\Computers\Workstations\Division\WIN_DESKTOP_12
Group:	All\Windows\Workstation Change
Operating system:	Windows 10 Pro (Version: 1607) (Build: 14393.693)
Exchange Server:	Not installed
Virtual machine:	No
Is a non-persistent computer:	No
Licenses:	ADAPTIVE DEFENSE 360 (TRIAL) ⊗
Agent version:	113.01.0000
Last bootup date:	4/18/2019 3:26:55 AM
Installation date:	4/13/2019 3:26:55 AM
Last connection:	4/18/2019 3:26:55 AM

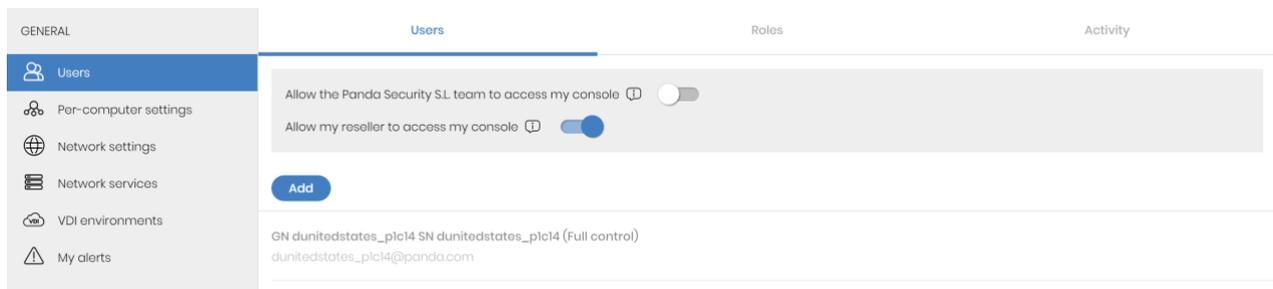
3.9. Settings

Configuration policies are managed in this section. (Users, Computer Settings, Network Settings, Alerts, Security settings: Workstation/Mobile).

3.10. Users

Through this section it will be possible to:

- create new users, and give full console access to Panda Security Support and/or to the Partner/Reseller Support staff
- create different permission profiles ("Roles")
- see the activity log showing user actions taken in console ("Actions") and the tracking of console access ("Sessions")



3.11. Computer Settings

Through this section it is possible to:

- Manage upgrade schedules for Panda Security components;
- set a password which will be requested during the uninstall process of the Adaptive Defense 360 agent, to temporarily disable some software modules, and the related anti-tampering services.



3.12. Network settings

In this section you can manage all communication aspects between agents and the console, in particular:

- Language: it is possible to choose the local client interface language
- Proxy: set the company's proxy address or force the communication through a machine with the Panda agent installed (allowing the protection of endpoints which might not have internet access - "air-gapped").
- Advanced Options: enabling/disabling of real-time agent communication

Cache and Discovery hosts can be designated to distribute upgrades in the LAN via peer-to-peer and to perform the discovery of hosts in the network which are not protected by Adaptive Defense 360 (and then launch the automatic deployment of the agent if desired).



3.13. My alerts

You can select which alerts you want to receive via e-mail, indicating the recipient's address through this panel:

Alert Category	Enabled
Malware detections	Yes
Exploit detections	Yes
PUP detections	No
A program that is being classified gets blocked	Yes
A file allowed by the administrator is finally classified	Yes
A malware URL is blocked	Yes
Phishing detections	Yes
An intrusion attempt gets blocked	No
Blocked devices	Yes
Computers with protection errors	Yes
Computers without a license	Yes
Install errors	Yes
Discovery of an unmanaged computer	Yes

3.14. Workstations and Servers

Through this area all security features for the Windows/Linux/OSX platforms can be granularly managed, for example:

- General (local alerts, signature updates, uninstall process of third-party antivirus products, exclusions)
- Advanced protection (Endpoint Detection and Response functionalities)
- Antivirus
- Firewall
- Device Control (control/prevent interaction with external connected devices)
- Web Filtering (category-based web filter)
- Antivirus for Exchange Server
- Antispam for Exchange Server
- Content Filtering for Exchange Server

Name: WorkstationAndServer Settings

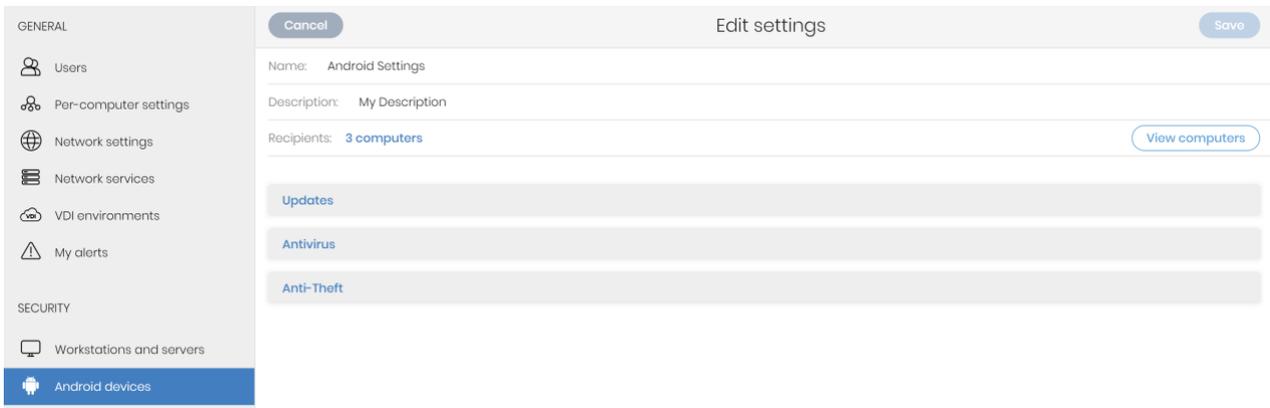
Description: My Description

Recipients: No recipients selected yet

- General
- Advanced protection (Windows computers)
- Antivirus
- Firewall (Windows computers)
- Device Control (Windows computers)
- Web access control
- Antivirus for Exchange servers
- Anti-spam for Exchange servers
- Content Filtering for Exchange servers

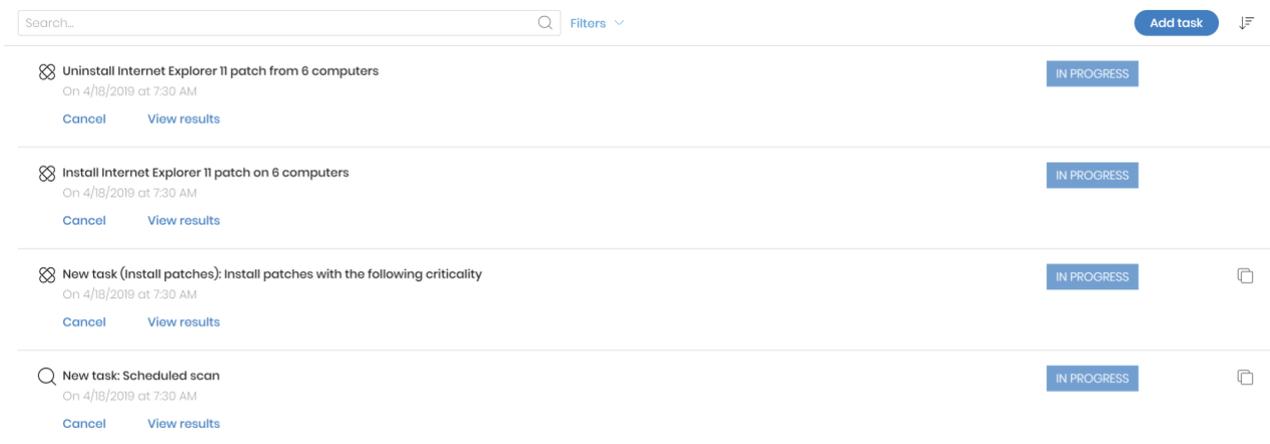
Android Devices

This section manages Android device settings. It will be possible to manage the update mode (e.g. through the Wi-Fi network) and define the protection behavior.



3.15. Tasks

The Tasks section allows defining scheduled tasks (e.g. anti-malware on-demand or scheduled full scans) and to check progress, view and edit existing tasks.



4. Advantages

The set of services provided by Panda with the Adaptive Defense 360 platform have differentiated and unique characteristics compared to a traditional endpoint security vendor.

- Services are distributed and managed completely without the need for an on-premise infrastructure, physical or virtual.
- No licensing distinction exists between server, client, or mobile devices and the solution is available for various platforms.
- The solution protects endpoints and servers, blocking all potentially dangerous process which might execute, DLLs, system calls or processes which are deemed unknown because of their behavior or due to their characteristics not being considered reliable by Panda Security.

- The solution enables monitoring and traceability of all actions happening as a consequence of the execution of any application (process) on endpoints or servers.
- The solution provides, for every single security incident, forensic analysis tools which allow granular investigation of a possible malicious attack. It detects and records all necessary information for the identification of modifications performed on the attacked system(s).
- Adaptive Defense 360 automatically classifies all applications as either trusted (Goodware), malicious (Malware), or potentially unwanted programs (PUP), without the intervention of the local IT administrator.
- It also traces down the behavior of classified applications as dangerous or potentially unwanted. The tracing includes information on files downloaded by the application, installed software, created drivers, communication established with the LAN or public networks, loaded DLLs, creation of services, generation or deletion of registry keys and access to files and folders, among others.
- The solution includes, at no extra charge, a Threat Hunting & Investigation Service. This service is designed to protect clients from hacker attacks, even if those attacks are not necessarily connected with malicious applications.
- The solution bears an optional Data Analytics platform, which can integrate or replace an existing corporate SIEM.

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 18,000 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.

WatchGuard® Technologies, Inc.

North America Sales: 1.800.734.9905

International Sales: 1.206.613.0895

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features, or functionality will be provided on an if and when available basis. ©2021 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, and AuthPoint are either trademarks or registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part No.WGCE67476_051321