Adaptive Defense

CLOSING THE GAP IN MALWARE DETECTION

ADVANCING THE STATE OF THE ART IN ENDPOINT PROTECTION

panda

pandasecurity.com

Executive Sumary

Adaptive Defense, is a new approach to takes a new approach the predominant "prevention-based dynamics" which have dominated the security industry since its inception, and the anti-malware industry in particular. Where anti-malware companies gain a temporary advantage until it gets closed with new evasion techniques by the malware creators.

Under these dynamics, anti-malware companies and malware creators keep playing an arms race to gain a temporary lead, a "window of detection" until it gets closed with new evasion techniques, requiring increasing investments and resources just to maintain an appearance of a "balance of power".

The new trust-based approach, is based on three principles:

- Continuous monitoring of all behavior of running programs at the endpoints.
- Continuous classification and risk assessment of running programs in real or near real time. Based on a big data approach together with expert review by analysts if needed.
- Maximum transparency/convenience, so that there is no need for end-user or admin input for the service to run.

Although perfect protection will never be achieved, the new approach significantly raises the bar making it harder for malware to remain uncovered and to bypass existing security defenses.

However, since new incidents will happen, Adaptive Defense also provides the necessary forensic capabilities to respond -to determine when the malware infiltrated the system, who was affected, what was targeted and how did it get there.-

Introduction

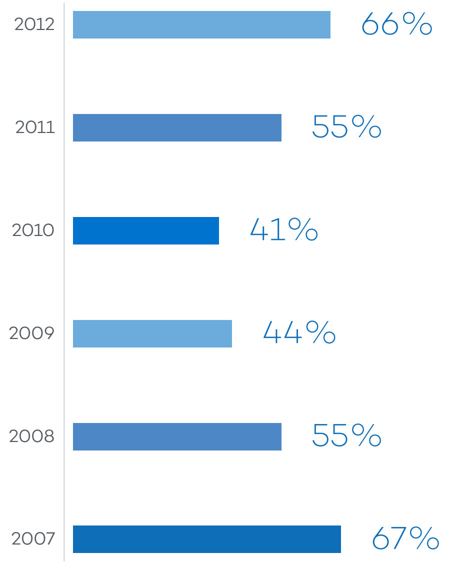
Despite continued and increased investments in security (in 2013, enterprises spent more than $13 billion on firewalls, intrusion prevention systems, according to Gartner), endpoint protection platforms and secure Web gateways), “it is clear that the battle against malware is not being won or in the battle against malware, enterprises have not gained an advantage”.

On the contrary, highly publicized breaches, together with the even more famous revelations about state-sponsored spying activities continue to support the perception of a very high general risk, and of porous and indefensible networks.

As Gartner notes, “*all organizations should now assume that they are in a state of continuous compromise*”. According to the Verizon Data Breach Investigative Report, 85% of the attacks remained undetected for weeks or more, and 92% of the attacks were not detected by the organizations themselves. It is very likely then that the overall risk has remained at similar levels in the past.

As a famous politician once said, ”there are things we do not know we don’t know”.

Percent of breaches that remain undiscovered for months or more



Source:
Verizon Data Breach Investigations Report 2013.

The detection gap

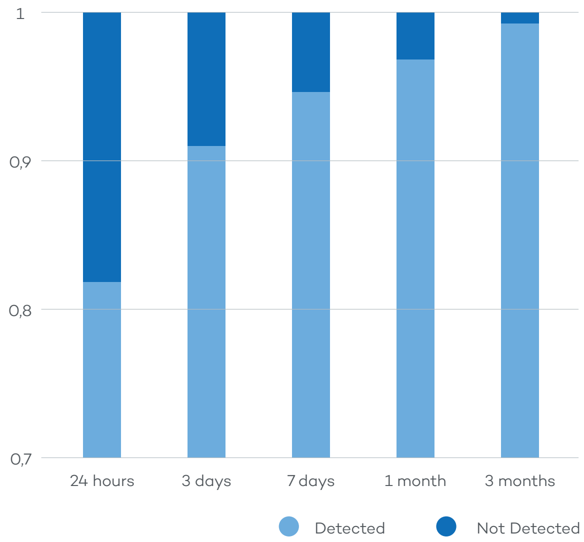
In an internal study conducted by PandaLabs in 2013, all malware samples collected on a daily basis were put to the test against a large number of antimalware products.

A relatively high percentage of the malware released in the wild is not being caught in time. In fact, even one year after the malware was collected, close to 1% of the samples were not being yet detected (over 70.000 samples in absolute terms).

The results serve to illustrate the gap that always exists in products focused on detection.

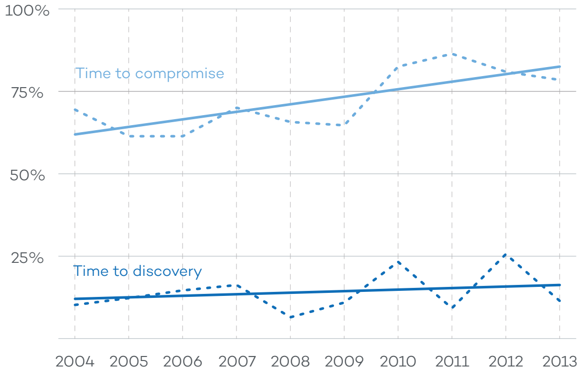
Verizon Data Breach Investigative Report 2014. Attackers are getting better at compromising systems, faster than the security industry is able to discover the compromise (the gap is widening).

Malware not Detected by AV Industry



Graphic. Detection gap of anti-malware products.

Percent of breaches where time to compromise / time to discovery was days or less



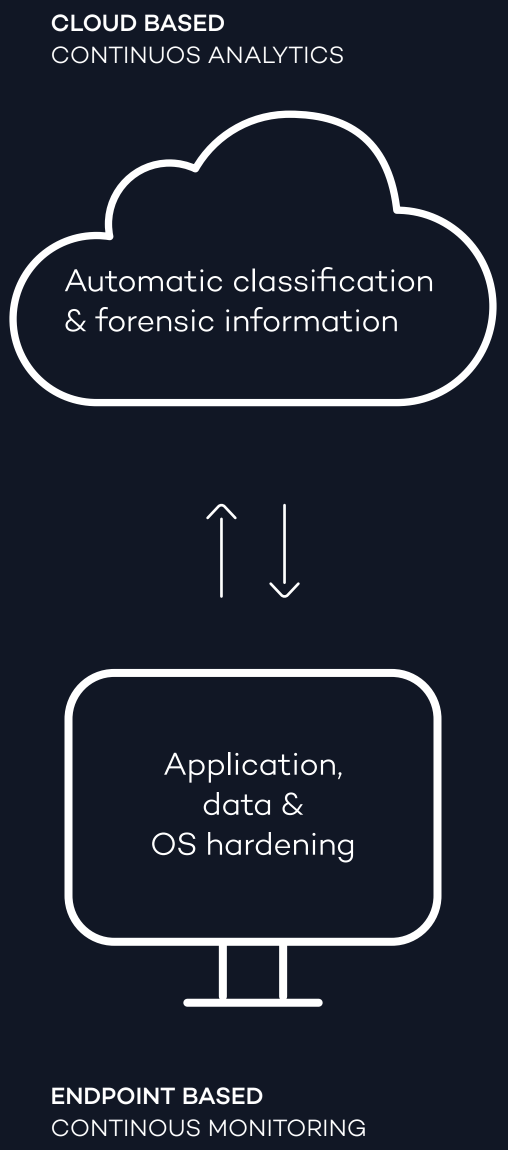
What is Adaptive Defense?

Adaptive Defense is a security solution that validates 100% of running applications in an organization. Developed for enterprise customers, it consists of an agent sitting at the endpoint, and a cloud-based infrastructure, together with continuous back-end assistance from analysts at PandaLabs.

Adaptive Defense transparently classifies all executable programs (PE files) running at the endpoint, with a guaranteed accuracy close to 100% (99.999%). It also provides application, data and OS hardening (behavior enforcement) as another protection layer, to ensure that commonly used applications are not successfully exploited because of existing vulnerabilities, and that sensitive OS areas are not accessed abnormally.

Additionally, it provides forensics traceability in case of an incident (answering the what, when, who and how of attacks).

Adaptive Defense can block questionable code before it is allowed to run (Extended mode) or allow questionable code to run until it is identified as malware (Standard mode). Adaptive Defense may also automatically clean infections in case of an incident, depending on the service package contracted by the customer.



CLOUD BASED
CONTINUOS ANALYTICS

Automatic classification & forensic information

Application, data & OS hardening

ENDPOINT BASED
CONTINOUS MONITORING

Principles:
Adaptive Defense is based on 3 principles

Continuous monitoring

All execution events are monitored and recorded for early warning, traceability and incident forensic purposes.

All event logs are available to the admin and are fully searchable, facilitating additional insights into what applications are exactly doing, how are they used, by whom, which connections are established and with which countries, when, etc.

Continuous classification of running executables

All executables running in memory are classified as malware or benign with accuracy close to 100%. Adaptive Defense uses local and cloud-based systems, correlated with locally collected data, but also with other multiple contextual data, 3rd party intelligence and our Big data analytics engine. Human-assisted classification is also performed on exceptional cases, and particularly during the initial deployment phase.

Additionally, programs must behave better in order to maintain their trust. The calculations of probabilities to determine the level of confidence is based upon proprietary clustering technology and on the empirical and historical data of all files (malware and goodware) ever seen and classified by Panda in the past. Probabilities are re-calculated continuously, as new inputs arrive, performing retrospective analysis of all previous classifications.

Transparency/ Convenience

No end-user or admin input (e.g. creation of whitelists, configuration of parameters) is needed in order for the service to work.

Adaptive Defense deploys and agent that will discover, profile and classify executable files on its own and in combination with the system in the cloud. Since Adaptive Defense is a managed service offered from Panda Security, rather than a self-contained product, it eliminates recurring tasks admins need to do when using other security solutions against advanced threats, such as prioritizing and managing alerts of suspicious activity coming from the monitoring of indicators of compromise. There are no such alerts in Adaptive Defense. All Indicators of Compromise (IOC) indicate the presence of confirmed malware, and suspiciousness is handled entirely by the service, and transparently for admins.

Adaptive Defense also eliminates the need to whitelist applications, and establish exception and approval processes, since all executable software trying to run will be classified by the system.

Main benefits

How Adaptive Defense helps companies to solve the problem of inadequate protection.

Closes the gap in detection that traditional endpoint protection products have.

Reduces the time spent investigation security incidences. All alerts coming from Adaptive Defense are confirmed.

Minimizes remediation costs in case of an incident.
Automates disinfection.

Answers the questions traditional products cannot: the what, who, when and how of security incidents.

Reduces endpoint security management costs.

Additional benefits of Adaptive Defense.

Provides real-time visibility of of all activity that happens at the endpoint, enabling admins to easily capture potentially "risky" events or policy violations.

Requires much less attention than other endpoint protection products.

Does not require any management infrastructure.

Does not require to uninstall existing security defences.

High Performance protection for virtualized desktop environments

Technology

Adaptive Dfense's intelligence inputs:

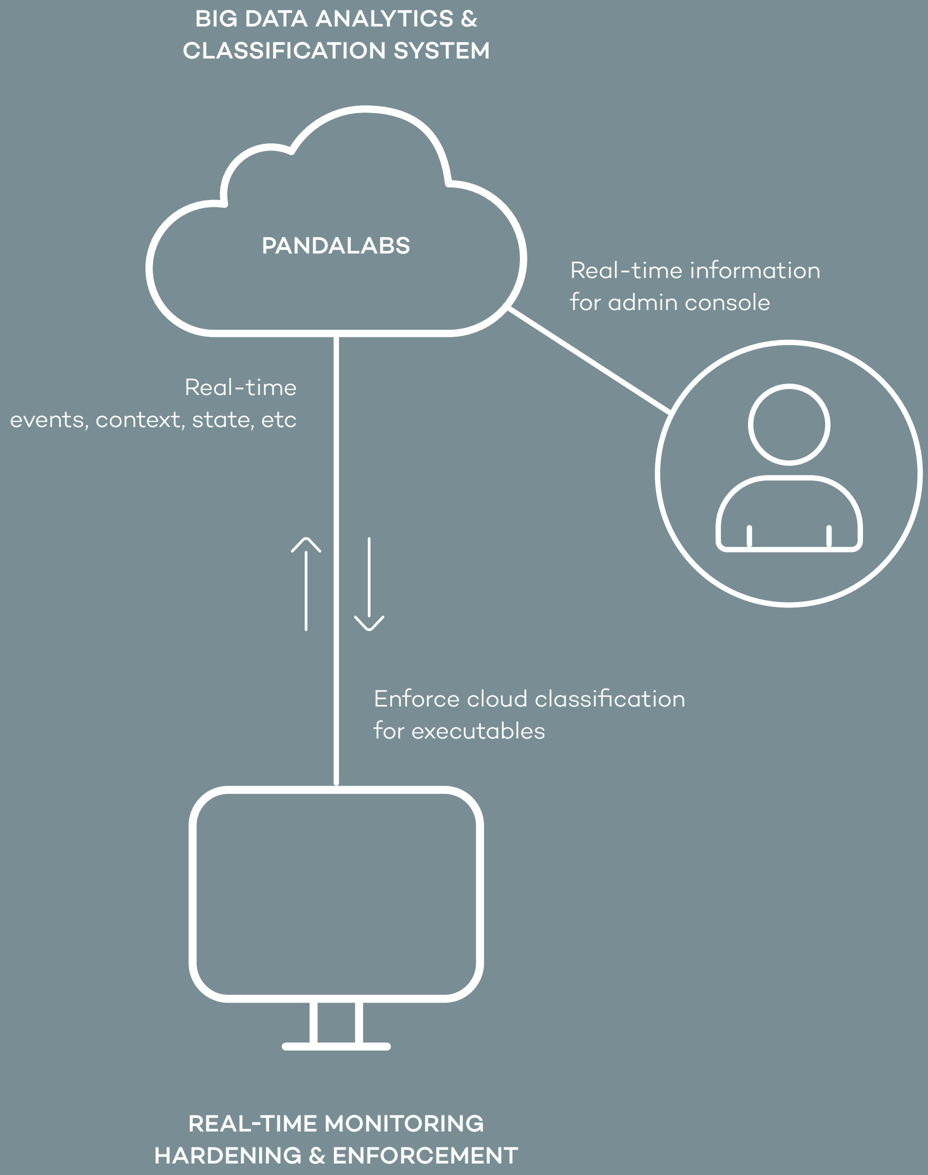
- Threats - External.
- User community.
- Threats - Internal (PandaLabs).
- Vulnerability info.
- Context.
- Software repository.

Real-time event monitoring on endpoints:

- Processes, services, PEs.
- Communications.
- Registry.
- Downloads.
- Hooks.
- etc.

Admin capabilities:

- Malware alerts.
- Forensic reports.
- Event search.


BIG DATA ANALYTICS & CLASSIFICATION SYSTEM
PANDALABS
Real-time information for admin console
Real-time events, context, state, etc
Enforce cloud classification for executables
REAL-TIME MONITORING HARDENING & ENFORCEMENT

Detection capabilities

Malware today utilizes numerous tricks to evade detection by security products. They hide under the guise of benign appearances, not performing any conspicuous actions at once, but slowly over the course of days or weeks. That is why it becomes necessary to continuously monitor all actions of all executables. A first classification of an executable, upon its first execution, may not reveal a malicious nature. Malware can wait to receive instructions or to hit upon conditions in the context in order to start showing malicious behavior or intent. Besides, legitimate programs may also contain vulnerabilities which can be exploited and make them perform malicious actions.

Adaptive Defense monitors all execution events of all executables, Any new behavior or anomaly in the execution profile of already classified executables triggers a re-classification, which takes into account not only the behavioral traces, but also the dynamic and static context of the executable (parent process, path).

As an integral part of the service, customers receive only alerts on confirmed malware incidents. Any suspicious activity or executable will always be fully resolved by Panda until it is either ruled out or confirmed.

This generates important cost savings to security departments, which normally need to sift through many alerts of “potential” incidents.

“Respond” capabilities.

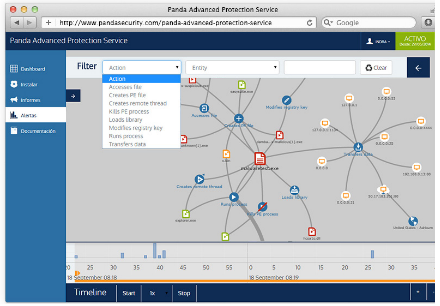
Once a malware incident is confirmed, an alert is sent to the administrator together with all available forensics information, including dwell time (how long was the executable present in the systems prior to its classification as malware), which machines/users were affected, what the executable did and when, how did it infiltrate the system, which vulnerabilities were present in the applications running at the endpoint, and which data was accessed in the attack and when. Complete remediation services of incidents are also available to customers as a professional service.

Reporting and alerts.

Alerts are sent to the administrator and they are also available in a web-based console, together with their associated forensics report. For every incident, a visual representation of the attack is offered, showing the entities, communications and actions performed, and the timeline of events.

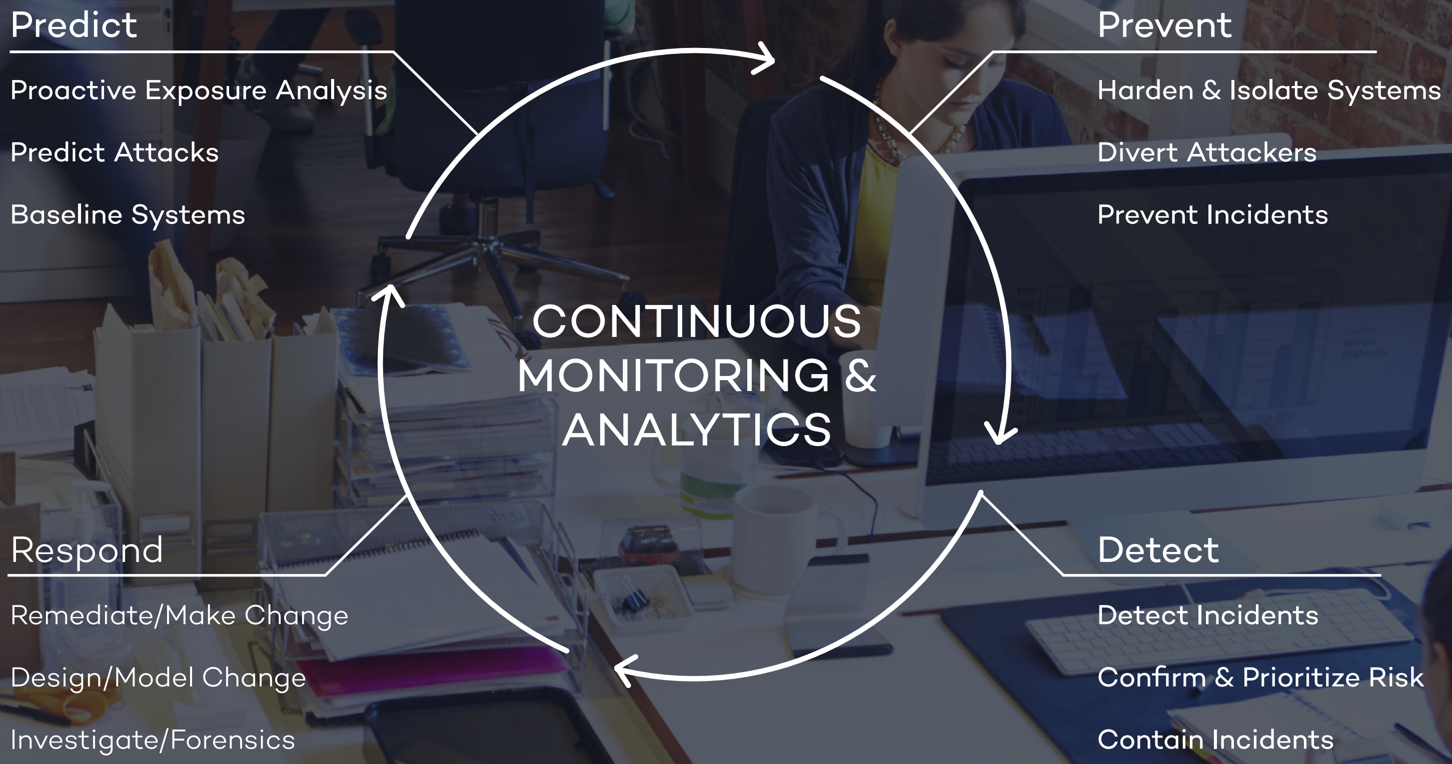
Advanced search.

All the activity inputs collected and processed by Adaptive Defense, for all executables, can be searched, filtered, or plotted in charts and graphs. The visibility and granularity of events allow for additional use cases, such as the discovery or identification of running applications in real time, usage data (which programs are being used, by whom, and when), geolocation of communications, and potential misuse of data.



Screenshot. Visual timeline of actions performed by malware.

How Adaptive Defense works



Predict

Proactive Exposure Analysis

Predict Attacks

Baseline Systems

Prevent

Harden & Isolate Systems

Divert Attackers

Prevent Incidents

CONTINUOUS MONITORING & ANALYTICS

Respond

Remediate/Make Change

Design/Model Change

Investigate/Forensics

Detect

Detect Incidents

Confirm & Prioritize Risk

Contain Incidents

Source: Gartner, Designing an Adaptive Security Architecture for Protection From Advanced Attacks, Neil MacDonald, February 2014

How Adaptive Defense works

Deploying the agent:

After choosing the proxy configuration, the agent (an MSI or exe) should be ideally deployed on all machines in the network using active directory policies if available, although it can be deployed by any other means with the appropriate administrative permissions.

Once the Adaptive Defense agent is installed, it starts gathering general information about the machine and it registers on the service, enabling a unique association of the machine with the customer and the events collected.

Monitoring events and application profiling:

Once registered, the agent starts monitoring the activity of all running executables. Some of the events collected are:

File downloads, Software installation, URL to file download, Hosts file modification, File age, Driver creation, Window hook/unhook, Process communications (IPs, ports, protocols), PE creation, modification, DLL load, Service creation, PE mapping, File delete/rename, Folder creation, Archive Creation/Open, Registry Key Creation/Modification, Thread creation on remote process, Kill process, SAM access, Data access (over 200 file formats), etc.

All running executables are profiled and classified. Classification is based on a continuously updated knowledgebase of goodware and malware, and on the analytics of static, dynamic (observed behavior locally and at the community) and contextual inputs of every executable file.

Preventive capabilities:

- Known malware is immediately blocked, using a combination of agent and cloud- based intelligence.
- Commonly-used applications such as Java, Adobe, Microsoft Office and browsers are generically protected against exploit-based attacks, using contextual and behavioral rules which prevent their exploitation.
- Data and certain sensitive areas of the Operating System are hardened against unauthorized access by third party applications, allowing access to those legitimate applications which have been profiled and classified during the deployment period.

All executables are classified with an accuracy of almost 100% (99.999 Executables classified as malware will be automatically blocked. Applications can be blocked pre or post execution, based on the policy chosen by the administrator. That is, under a pre-execution block policy ("extended blocking"), un-classified executables at the time of execution will be blocked until its classification is resolved. On the other hand, under a post-execution block policy ("standard blocking"), unclassified executables at the time of execution will be allowed to run until its classification is resolved, and they will only be blocked if they are confirmed as malware. Classification usually takes seconds or minutes, and exceptionally a few hours.

- Legitimate programs can also be blocked based on a black list specified by the administrator, out of productivity reasons or other concerns.

panda