# CLOSING THE GAP IN MALWARE DETECTION

## DISRUPTING THE DETECTION-BASED DYNAMIC

PANDA SECURITY

## EXECUTIVE SUMMARY

Panda Advanced Protection Service, is a new approach to disrupt the detection-based dynamics which have dominated the security industry since its inception, and the anti-malware industry in particular. 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 ever increasing investments and resources just to maintain an appearance of a "stabilized front".

This new approach, based on an agent sitting at the endpoint, and backed by a cloud-based infrastructure and assistance from PandaLabs' experts, 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, and 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 for malware to remain uncovered and to bypass existing security defenses. However, since new incidents will happen, Panda Advanced Protection Service also provides the necessary forensics capabilities to respond, to determine when the malware infiltrated the system, who was affected, what was targeted and how did it get there.

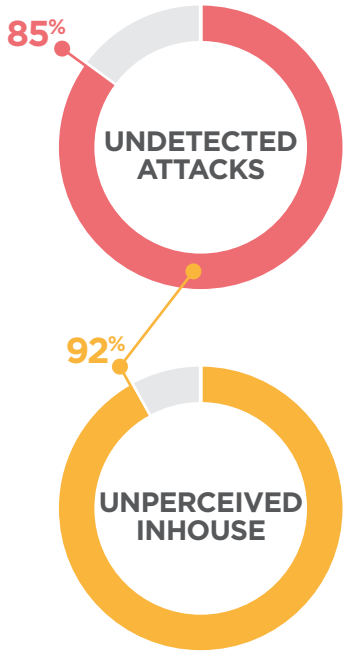
## INTRODUCTION

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 has not improved.

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

As Gartner says, «*all organizations should now assume that they are in a state of continuous compromise*». However, no one really knows how the situation now compares to that of the preceding years, given the general unwillingness of IT departments and security vendors to share infection and breach data.

No one wants to share statistics about their own failure rates. 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 Mr. Donald Rumsfeld's once said, "*there are things we do not know we don't know*".




## THE DETECTION GAP

Gartner's analyst Dan Blum perfectly summarized the problem of existing dynamics in a report he wrote back in 2007 (still working for Burton Group, later acquired by Gartner), when he said:

> An organization's platform and its risks are never in equilibrium for long; as long as equilibrium exists, risks are under control and the bad guys are denied their payday. But bad guys need to feed their families, so they're constantly developing innovative ways to disrupt the risk equilibrium. As soon as one bad guy develops a new attack, other bad guys can flock to it and may quickly create large losses. When this happens, risk costs escalate rapidly, and businesses pressure platform product vendors to reduce their escalating risk taxes. This dynamic drives the security market to be always consolidating but never consolidated.
> Dan Blum (Burton-Gartner).

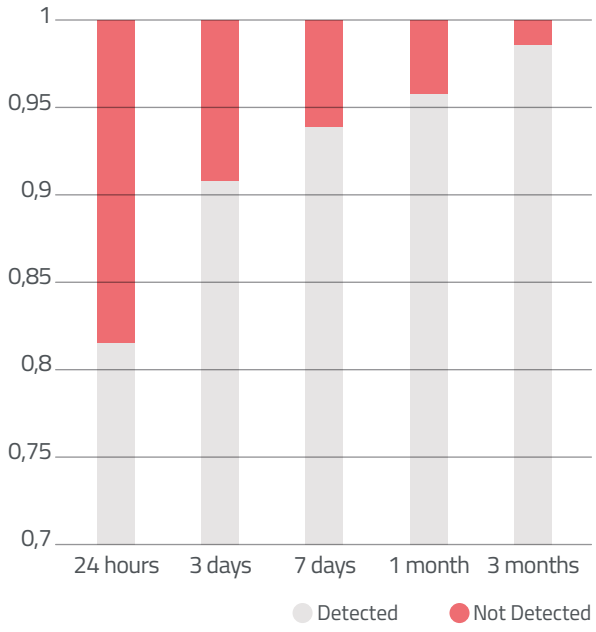
This conclusion is as valid today as it was seven years ago. In fact, the appetite of investors in the endpoint security market has increased substantially in the last year. More start-ups are appearing with newer approaches, while at the same time some of these are already being acquired by larger players. The same problems persist and malware creators continue innovating with new forms of evasion. They only need to test their creations against the security products, which are publicly available to install and scrutinize.

These dynamics are the result of a predominant focus on detection techniques, which aim at identifying malicious or suspicious code in the systems. The code that does not raise any flag of the detection technique is allowed to run. In some cases, some reputation queries are added, but the coverage and depth of the reputation systems are limited. It is precisely **taking advantage of these limitations how new malware enters into systems**. Additionally, anti-malware vendors are very aware of the risks of using too aggressive heuristics, in the form of false positives. **False positives are heavily penalized** by the market, and vendors tend to fine tune them taking into account a zero or near zero false positive constraint, so that the effectiveness is not maximized. In the end, and as Mr. Blum contends, the bad guys always end up developing new evasion techniques. It is a never ending story.

In an internal study conducted by PandaLabs between the months of January and June 2013, all malware samples collected on a daily basiswere put to the test against a large number of antimalware products.

A relatively high percentage of the malware that is 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 thousand samples in absolute terms). The results serve to illustrate the gap that always exists in products focused on detection.

*Malware not Detected by AV Industry*




*Graphic. Detection gap of anti-malware products.*

## TACKLING THE SECURITY TRADE-OFF

IIn order to combat general malware, advanced and targeted threats, new innovative solutions are developed, maintaining the above-mentioned dynamics.

Some solutions may operate at different layers of the infrastructure (endpoint, network analysis, network-based appliances), using different techniques, and are positioned to serve different needs of the security incident cycle (prevention, identification, investigation and response).

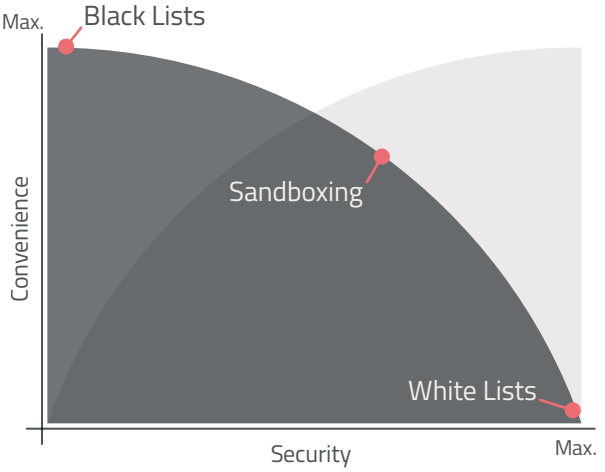
Security buyers, based on the risks they want to manage, need then to assess the capabilities of the solutions, their security effectiveness, limitations and their overall "convenience", described generally for our purposes as an assessment of their total cost and their usability.

For decades, traditional anti-virus has dominated the endpoint security industry, despite the consensus that it was not sufficient as a prevention mechanism and its great limitations as an investigation and remediation tool. However, its penetration rate is the highest among security products, due to its convenience. Anyone can use it.

In recent years, and due to the need to fill the gaps of anti-virus products, application control and whitelisting in particular were recommended by industry analysts. However, adoption has remained limited, because of the higher "inconvenience" presented by these category of products (higher operational and maintenance costs).

Over the past 12-18 months, a new market has emerged, formed by a heterogeneous mixture of approaches and products, ranging from endpoint based containment using sandboxing and micro-virtualization, to payload analysis in the gateway through the use of sandboxes. However, all of these solutions cannot yet replace existing anti-malware solutions, require additional investments and are subject to the same detection-based dynamics (attackers adapting new evasion techniques to bypass them).

*Security Trade-Off*




*Graphic. How the industry combat the malware.*

## WHAT IS PANDA ADVANCED PROTECTION SERVICE?

It is a managed security service that closes the gap in malware detection by validating 100% of running applications, automatically and transparently.

Aimed at enterprise customers, it consists of an agent and cloud-based solution, together with continuous back-end assistance from analysts at PandaLabs. Panda Advanced Protection Service transparently classifies all executable programs (PE files) running at the endpoint, with a maximum level of accuracy. It also provides application, data and OS hardening (behavior enforcement) as another baseline 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). Panda Advanced Protection Service can block executable code before it is allowed to run or right after it (Extended Mode-Base Blocking mode). It also includes complete infection cleaning services in case of an incident, depending on the service package contracted by the customer.


## THE THREE PRINCIPLES

Panda Advanced Protection Service is based on 3 principles:

### Continuous monitoring.

All execution events of all running applications are recorded and utilized for classification, early warning and prioritization in the classification system, and for traceability and incident forensic purposes.

### Continuous classification of running executables.

All executables running in memory are classified until a Maximum Confidence Level (MCL) is reached (close to 100%), using local and cloud-based systems, correlated with locally collected data, but also with other multiple contextual, 3rd party intelligence and community-based data in a Big Data analytics engine. Human-assisted classification is also performed on exceptional cases, and particularly during the initial deployment phase.

Additionally, programs must behave accordingly 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 admin or end-user input (e.g. creation of whitelists, configuration of parameters, etc) is needed in order for the service to work. Once deployed, the agent will discover, profile and classify executable files on its own and in combination with the system in the cloud.

Since Panda Advanced Protection Service 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 Panda Advanced Protection Service. All alerts indicate the presence of confirmed malware, and suspiciousness is handled entirely by the service, and transparently for admins.

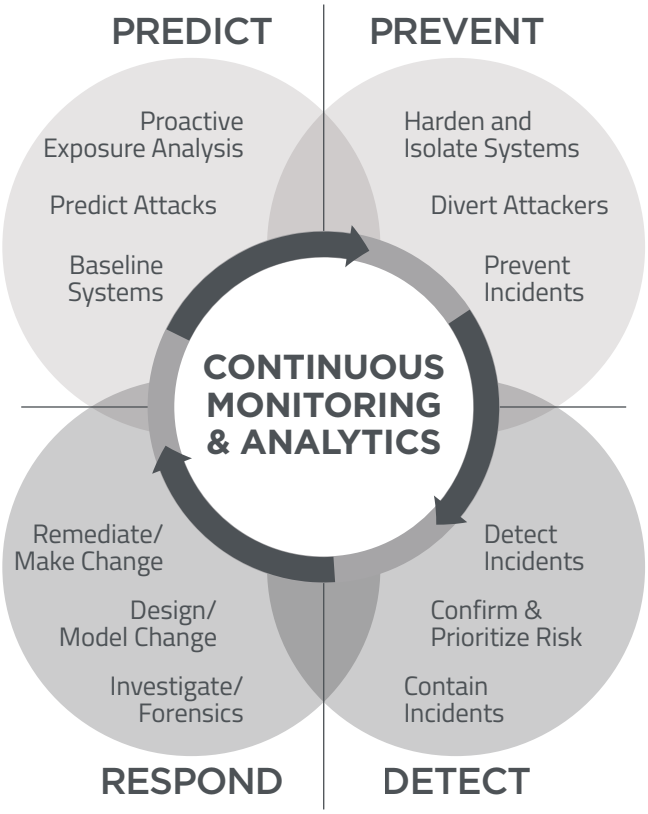
Panda Advanced Protection Service also eliminates the need to whitelist applications, establish exception and approval processes, since all executable software trying to run will be classified by the system.

## PANDA ADVANCED PROTECTION SERVICE & GARTNER'S ADAPTIVE SECURITY ARCHITECTURE

Panda Advanced Protection Service provides capabilities to prevent, uncover, trace back and respond to activities performed by malware.

A recent Gartner report, *"Designing an Adaptive Security Architecture for Protection from Advanced Attacks"*, sheds light on the limitations of traditional protection approaches, and recommends vendors to integrate 12 different capabilities for more effective protection against advanced threats.

Panda Advanced Protection Service already embraces the core principles of this new architecture, by continuously monitoring the activity of all executables at the endpoint, and by applying cloud-based analytics to the intelligence received in real-time, both from the endpoints and from additional external sources.




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

## PHASES

| DEPLOYMENT | BASE BLOCKING | EXTENDED BLOCKING |
|---|---|---|
| Monitoring | Monitoring | Monitoring |
| Discovery | Discovery | Discovery |
| Learning | Learning | Learning |
| Profiling | Profiling | Profiling |
| | Anti-exploit | Anti-exploit |
| | Known Malware | Known Malware |
| | 100% Classification | 100% Classification |
| | Immediate alerts | Immediate alerts |
| | | Immediate Blocking |
| | | Immediate Resolution |

### Deployment Phase

I. 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 Panda Advanced Protection Service 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.

II. Monitoring events.

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

1st File downloads
2nd Software installation
3rd URL to file download
4th Hosts file modification
5th File age
6th Driver creation
7th Window hook/unhook
8th Process communications (IPs, ports, protocols)
9th PE creation, modification
10th DLL load
11th Service creation
12th PE mapping
13th File delete/rename
14th Folder creation
15th Archive Creation/Open
16th Registry Key Creation/Modification
17th Thread creation on remote process
18th Kill process
19th SAM access
20th Data access (over 200 file formats)

# MODES OF OPERATION

## Base blocking

After the deployment phase, which may last a few days or up to two weeks, depending on the size and complexity of the network, Panda Advanced Protection Service starts protecting it first by creating a baseline of hardening and enforcement, so that:

I. 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.

II. 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.

III. All executables are classified with an accuracy of almost 100% (99.9999%). In this mode of operation, executables which are not classified yet with a MCL are initially allowed to run, but if the system classifies a program as malware, then it will be immediately blocked.

Under the Base Blocking mode, endpoints are hardened against exploit-based attacks targeting commonly used applications and against anomalous access to data by untrusted executables. Detection, prioritization and containment are all performed by the system automatically. New malware is uncovered as a result of the required classification of all executables. If several executables are pending a full classification, the monitoring of all their activity helps to prioritize them, so that risk is managed at all stages. The new malware is then contained and its actions logged and presented to the administrator for further investigation if needed.

## Extended blocking

A customer may choose to implement the Extended Mode for some or all computers in its network. The Extended Mode contains the same baseline of hardening and enforcement as in the Base Blocking Mode, and additionally, every time an executable tries to run and it cannot automatically be classified with a MCL, it will be blocked until it does. It usually takes seconds or minutes, and exceptionally it may take a few hours, depending on the characteristics of the program.

Once a program is blocked, the end user will receive an on-screen notification, informing about the blocking. Two types of users can be set during the deployment stage: basic and VIP.

Basic users will not have the option to override the blocking, although they can "protest" by clicking on a button. This personal end-user reputation will be fed into the system as another input to consider.

On the other hand, VIP users will be able to override the blocking, but malware will be blocked once classified, regardless of the user.

## Reporting and alerts

In both modes of operation, admins receive two different reports: a daily activity report, showing stats about the Panda Advanced Protection Service installation, machines, critically vulnerable applications found, etc; and immediate alerts every time malware is classified.

The alert will contain a forensic report of all the actions performed by the malware since it landed into the system, including the URL from which it was downloaded (if that was the infection vector), which other machines in the network are infected with the same malware, which vulnerable application was used to infiltrate the network, etc. Admins can also access the same information by logging to the console.

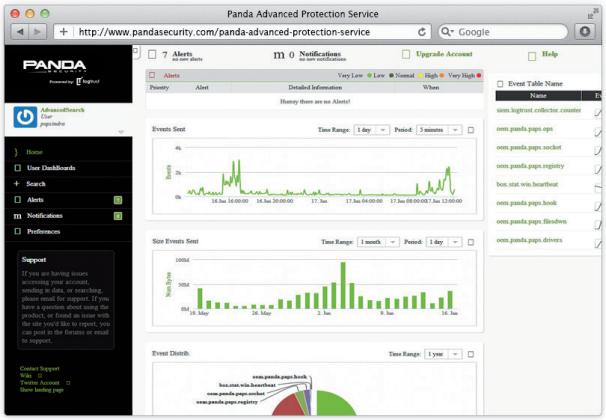



*Photo. Panda Advanced Protection Service Dashboard.*

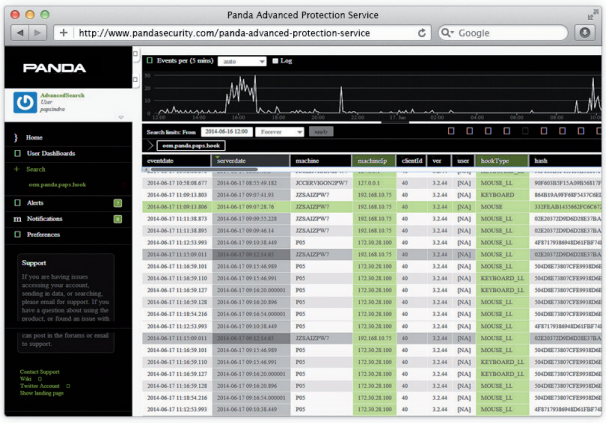



*Photo. Panda Advanced Protection Service Events.*

## TECHNOLOGY

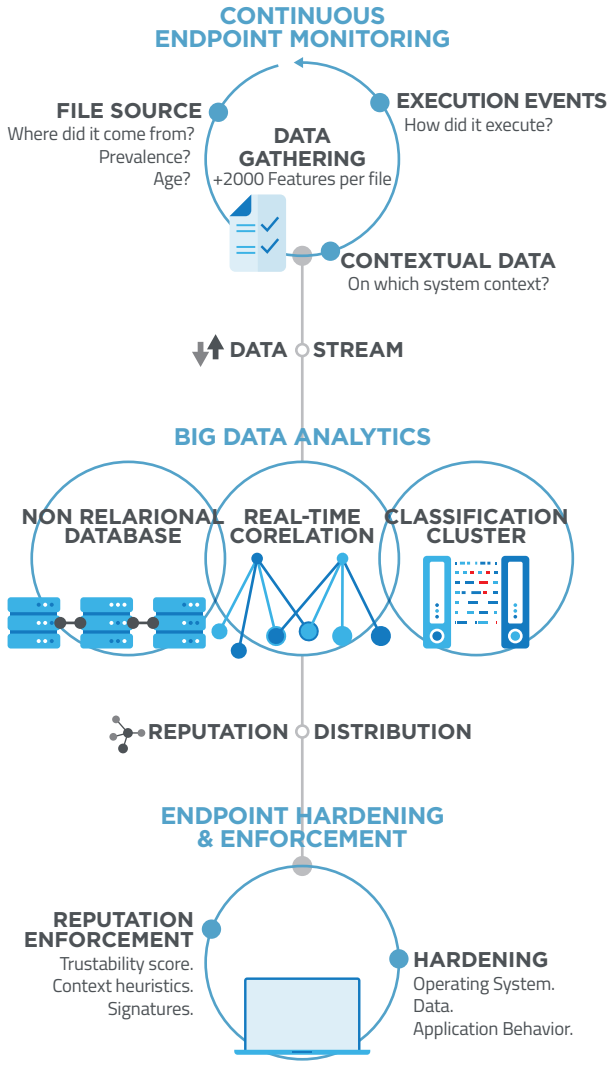



*Figure. Big Data Analytics and Endpoint Enforcement*

Panda Advanced Protection Service is based on a technology integrating multiple inputs, internal to the endpoints, and external such as threat and reputational information, feeds from third parties, as well as from Panda's own community of users.

All the inputs are fed to a Big Data analytics engine, further composed in turn in a set of components to aggregate, correlate and process the inputs. The end result is a classification cluster whose goal is, in simple terms, to bring every file passing through it into a "good" or "bad" score, with a "Maximum Level of Confidence", or MLC.

The MLC reflects the probability that a file classification (either malware or goodware) is accurate, and it takes into account all the empirical data PandaLabs has for all malware and goodware samples ever recorded. The accuracy of this knowledge source is recalculated continuously as new events arrive into the system.

Using the static, contextual, behavioral and external inputs, and if needed, even running the executables in an infrastructure of physical machines (not VMs), probabilities are assigned using a proprietary hierarchical clustering algorithm. All executables are classified until the MCL is reached. Executables which do not reach the MCL in a first round are subject to additional rounds of classification using additional layers of filtering and correlations, until they do, even performing manual analysis on exceptional cases. The key aspect of this approach is that no executable will be left without an MCL classification.

## SUMMARY OF BENEFITS

**Close the gap in malware detection**

Protection against malware (virus, Trojans, spyware, etc) known and unknown, and against advanced threats.

Protection against exploit-based attacks against vulnerabilities in commonly used applications, such as Java, Microsoft Office, Adobe and browsers. Such protection mitigates the risk especially in those systems which are hard or impossible to patch, due to internal or external circumstances, and especially for Windows XP, given its EOL.

Protection for Virtualized Desktop Environments.

Identification of applications with critical vulnerabilities.

Protection against anomalous access to sensitive data, applications and sensitive areas of the Operating System. Panda Advanced Protection Service protects against anomalous access of distrusted executables trying to access data, or trying to encrypt them (such as the Cryptolocker family), or which try to access sensitive areas of the OS, such as the Security Accounts Manager (SAM).

### Minimize remediation costs in case of an incident

Panda Advanced Protection Service offers complete visibility and forensic information in an incident, which in turn help speed up remedial actions and protection against future attacks. Panda Advanced Protection Service identifies infected machines, all actions taken by malware, the exact time in which the malware entered the system for the first time, the infection vector, the affected files, etc.

Cleaning assistance in case of infection. Panda offers an added service in which Panda's professionals fully assist customers in cleaning and remediating the effects of an infection.

### Transparency and zero management infrastructure

Panda Advanced Protection Service is based on an agent which works transparently for admins and end-users. It does not require the installation or maintenance of servers, databases or consoles.

## CONCLUSION

The detection-based dynamics which have dominated the security industry since its inception are not enough against the current situation, where malware creators keep playing an arms race to gain a temporary lead, a "window of detection" until it gets closed with new evasion techniques.

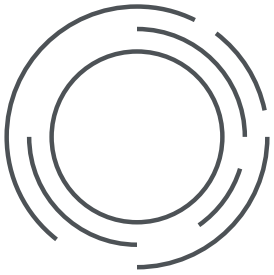
A new approach, based on an agent sitting at the endpoint, and backed by a cloud-based infrastructure and assistance from security expert is needed.

Panda Advanced Protection Service is based on three principles:

1. Continuous monitoring of all behavior of running programs at the endpoints
2. 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
3. Transparency/convenience, so that there is no need for end-user or admin input for the service to run.

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

However, since new incidents will happen, Panda Advanced Protection Service also provides the necessary forensics capabilities to respond, to determine when the malware infiltrated the system, who was affected, what was targeted and how did it get there.



# CLOSING THE GAP OF MALWARE DETECTION

## DISRUPTING THE DETECTION-BASED DYNAMIC

PANDA SECURITY