Adaptive Defense 360

Find the answers, solve the problem

COMPLETE ENDPOINT DEFENSE INTEGRATING PROTECTION, DETECTION, RESPONSE AND REMEDIATION IN A SINGLE SOLUTION

Panda Adaptive Defense 360 is the first and only product in the market to combine in a single solution Endpoint Protection (EPP) and Endpoint Detection & Reponse (EDR) capabilities. The EDR capabilities relies on a new security model which cna guarantee complete protection for devices and server by classifying 100% of the process running on every computer through the organization and monitoring and controlling their behavior.

Adaptive Defense are 2 solutions in a single console. It starts with Panda's best-of-breed EPP solution (Endpoint Protection Plus) and adds the EDR capabilities of Adaptive Defense in order to protect against zero-day and targered attacks that take advantage of "window opportunity for malware".

Adaptive Defense 360 above and beyond AVs

New malware detection capability*	Traditional Antivirus (25)	**Panda Adaptive Defense 360**	
New malware blocked during...		**Standard Model**	**Extended Model**
the first 24 hours	82%	**98,8%**	**100%**
the first 7 hours	93%	**100%**	**100%**
the first 3 months	98%	**100%**	**100%**
% detections by Adaptive Defense detected by **no other Antivirus**		**3,30%**	
Suspicious detections		**No (no uncertainty)**	

File Classification	Universal Agent *	**Panda Adaptive Defense**
File classified automatically	60,25%	**99,56%**
Classification certainty level	99,28%	**99,9991%** **<1 error / 100.00 files**

*Universal Agent technology is included as endpoint protection in all Panda Security solutions

Phase 1: Continuous endpoint Monitoring	**Phase 2: Big Data Analysis**	**Phase 3: Endpoint hardening and enforcement**
The endpoint protection installed on each computer monitors all the actions triggered by running process. Each event is cataloges (based on more than 2,000 characteristics) and sent to the cloud*: • File download • Software Installation • Driver Creation • Communication processes • DLL Loading • Service creation • Creation and deletion of files and folders • Creation and delection of Registr branches • Local access to data (over 200 formats)	**Continuous classification of executable files.** The trustability* score of each process is recalculated based on the dynamic behavior of the process. The trustability** score is recalcuated based on the new evidence received (Retrospective Analysis) *Pattern based classification by Panda Labs. **The trustability score determines whether or not a process is trusted. If a process is not trusted, it will be prevented rom running	**The service classifies all executables with near 100% accurancy (99.9991%).** Every process is classified as malware is immediately blocked. **Protection against Vulnerabilities** **Data hardening** Only trusted application are allowed to access data and sensitive areas of the operating system. **Blocking of all unclassified process** All unclassified processes are prevented from running until they ara assinged an MCL by the system. If process is not classified automatically a security expert will classify it

THE ONLY SOLUTION TO GUARANTEE THE SECURITY OF ALL RUNNING APPLICATIONS

COMPLETE AND ROBUST PROTECTION GUARANTEED

Panda Adaptive Defense 360 offers two operational modes:

- **Standard mode allows** all applications catalogued as goodware to be run, along with the applications that are yet to be catalogued by Panda Security and the automated systems.
- **Extended mode only allows** the running of goodware. This is the ideal form of protection for companies with a 'zero risk' approach to security.

FORENSIC INFORMATION

- **View execution event graphs** to gain a clear understanding of all events caused by malware.
- Get visual information through heat maps on the geographical source of malware connections, files created and much more.
- Locate software with known vulnerabilities installed on your network.

PROTECTION FOR VULNERABLE OPERATING SYSTEMS AND APPLICATIONS

Systems such as Windows XP, which are no longer supported by the developer and are therefore unpatched and vulnerable, become easy prey for zero-day and new generation attacks.

Moreover, vulnerabilities in applications such as Java, Adobe, Microsoft Office and browsers are exploited by 90 percent of malware.

The vulnerability protection module in **Adaptive Defense 360** uses contextual and behavioral rules to ensure companies can work in a secure environment even if they have systems that are not updated.

FULL EPP CAPABILITIES

Adaptive Defense 360 integrates Panda Endpoint Protection Plus, the most sophisticated EPP solution from Panda, thus providing full EPP capabilities, including:

- Remedial actions
- Centralized device control: Prevent malware entry and data loss by blocking device types
- Web monitoring and filtering
- Exchange server antivirus and anti-spam
- Endpoint Firewall, and many others...

CONTINUOUS STATUS INFORMATION ON ALL ENDPOINTS IN THE NETWORK

Get immediate alerts the moment that malware is identified on the network, with a comprehensive report detailing the location, the computers infected, and the action taken by the malware.

Receive reports via email on the daily activity of the service.

SIEM AVAILABLE

Adaptive Defense 360 integrates with SIEM solutions to provide detailed data on the activity of all applications run on your systems.

For clients without SIEM solution, **Adaptive Defense 360** can include its own system for storing and managing security events to analyze all the information collected in real time.

100% MANAGED SERVICE

Forget about having to invest in technical personnel to deal with quarantine or suspicious files or disinfect and restore infected computers. **Adaptive Defense 360** classifies all applications automatically thanks to machine learning in our Big Data environments under the continuous supervision of PandaLabs' experts.

TECHNICAL REQUIREMENTS

Web Console (only monitoring)

- Internet connection
- Internet Explorer 7.0 or later
- Firefox 3.0 or later
- Google Chrome 2.0 or later

Agent

- Operating systems (workstations): Windows XP SP2 and later, Vista, Windows 7, 8 & 8.1
- Operating systems (servers): Windows 2003 Server, Windows 2008, Windows Server 2012
- Internet connection (direct or through a proxy)

Partially supported (only EPP):

- Linux, MAC OS X and Android

CryptoLocker

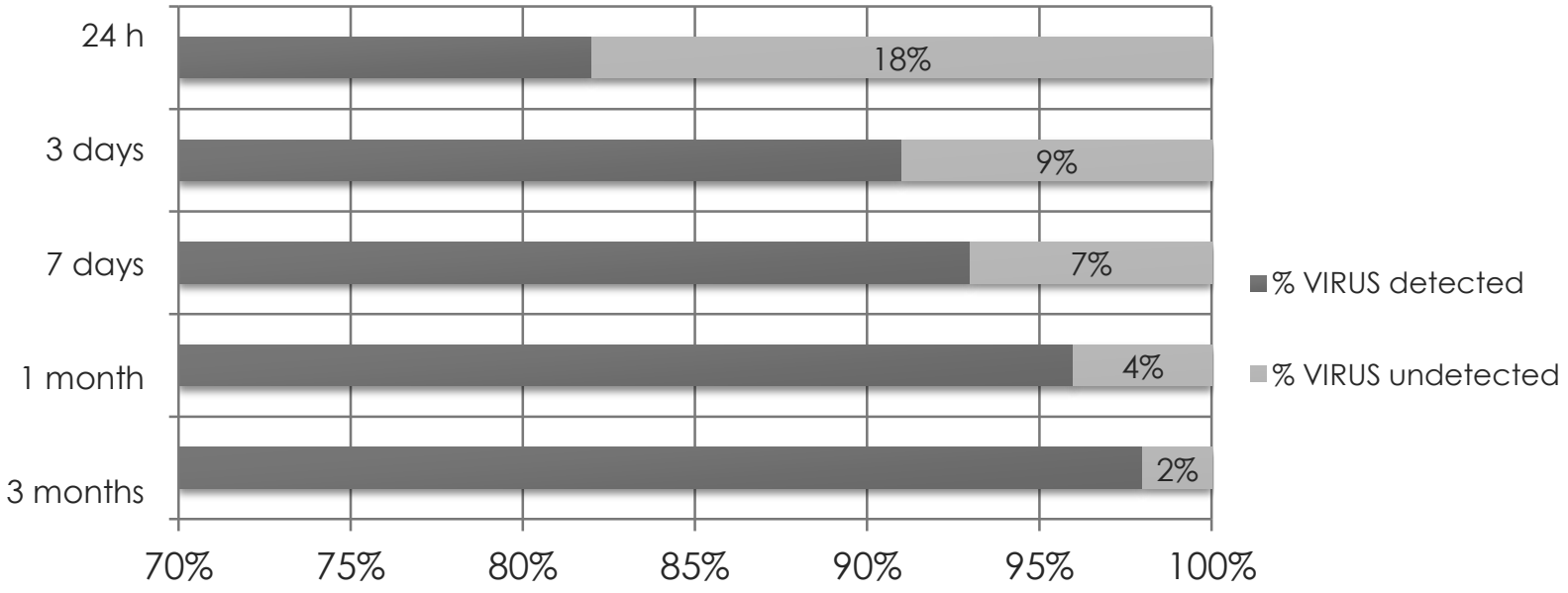
Can we stop it?

CryptoLocker

Can antivirus solutions stop CryptoLocker?
Is it enough to have a backup system?

Can antivirus solutions stop this type of attack?

- **Antivirus technologies** (signatures, heuristics, content filtering, behavioral analysis) are **reactive**.
- **Traditional antivirus solutions are unable to detect 18% of new malware** within the first 24 hours, and after three months about 2% is still not detected.

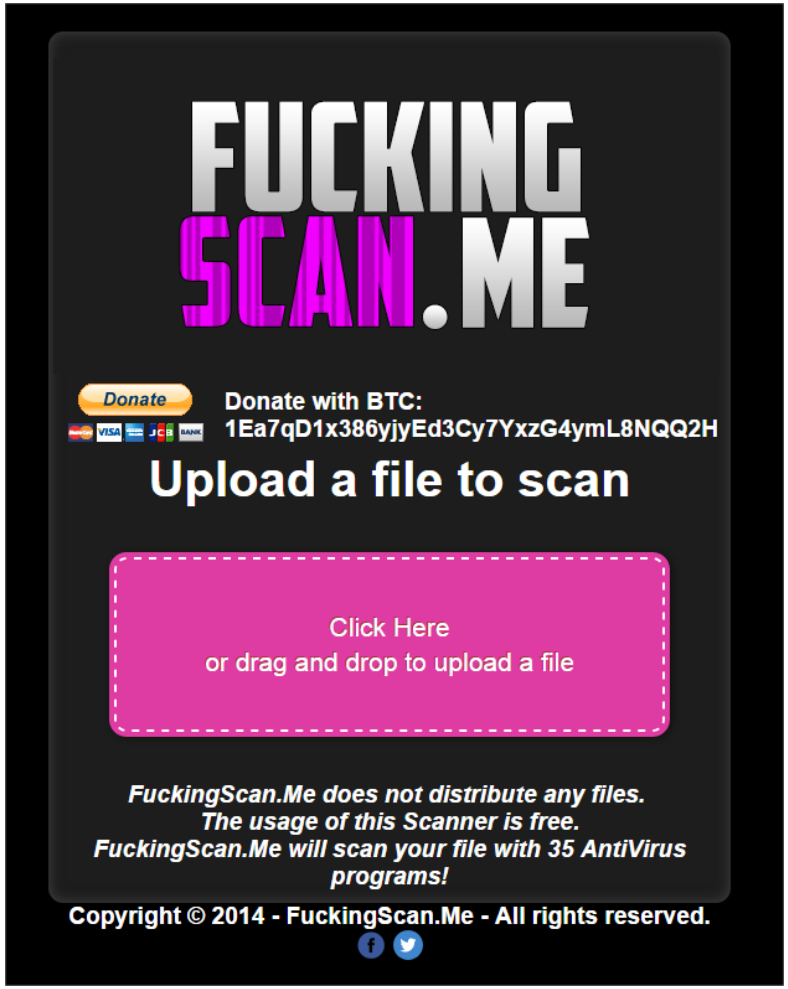


Panda Security study on the malware window of opportunity

Can antivirus solutions stop this type of attack?

- Certain websites allow you to check if a specific file will be detected by antivirus software.
  - They check the file against more than 40 antivirus programs
  - They are free

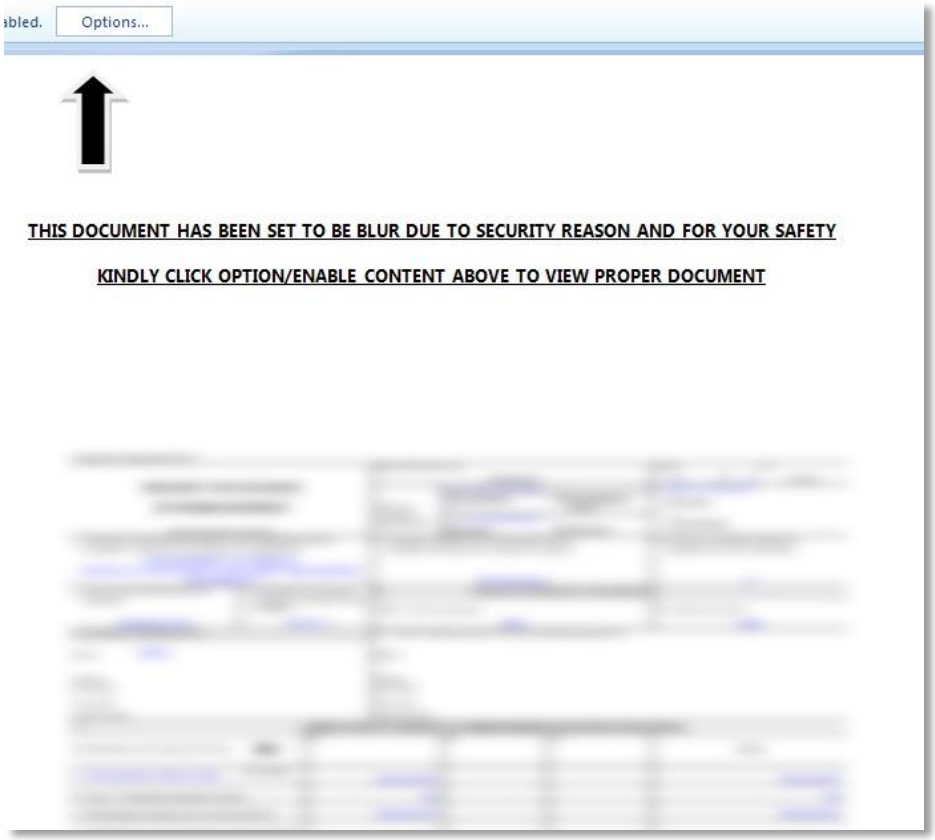
-> Hackers launch their malicious code once they know that it **WON'T be detected by any antivirus solution**.



Can content, spam and URL filters stop this type of attack?

- Sometimes, but not always

- **Macro viruses are being used again** to bypass content filters
  - Macro → Downloader → CryptoLocker
  - Macro → Downloader → CMD → CryptoLocker
  - Macro → VBS code (embedded) → Downloader → CryptoLocker
  - Macro → VBS code (downloaded)→ Downloader → Cryptolocker



Antivirus response to CryptoLocker

- Antivirus technologies
  - Specific signatures
  - Generic and heuristic detection
  - Blocking of ransomware URLs
  - "Contextual" detection: Stops the file encryption process

CONCLUSION: NOT ENOUGH

- New variants continue to infect systems
- **Anything the antivirus cannot detect IS ALLOWED TO RUN**

Cryptolocker: 10 steps to avoid the ransomware virus

Global cybercrime agencies say users already infected with the Cryptolocker ransomware have a two-week window to remove it

Cryptolocker virus network thwarted by global operation

The Windows Club

A THREE TIME GARTNER MAGIC QUADRANT LEADER

Home News Windows Downloads Security IE Office Phone General Deals Forum About

CryptoLocker Tripwire: Free Cryptolocker Prevention Tool

RECOMMENDED: Click here to fix Windows errors and optimize system performance

The **Cryptolocker Ransomware** has been morphing into more dangerous forms and even started targeting other operating systems like Android. While those affected are always looking out for ways to get rid of or remove Cryptolocker ransomware, the old proverb still stands – *Prevention is better than cure*!

*We have earlier seen how you can block or prevent Cryptolocker ransomware attacks using CryptoPrevent, Cryptolocker Prevention Kit and HitmanPro.Alert – and by following some steps to take to stay protected & secure, by **preventing Ransomware** from getting onto your Windows computer.*

Via this post, we would like to inform you about another Cryptolocker Prevention Tool called **CryptoLocker Tripwire**.

Is it enough to have a backup system?

- Backups can be disruptive to productivity, but are effective in many cases

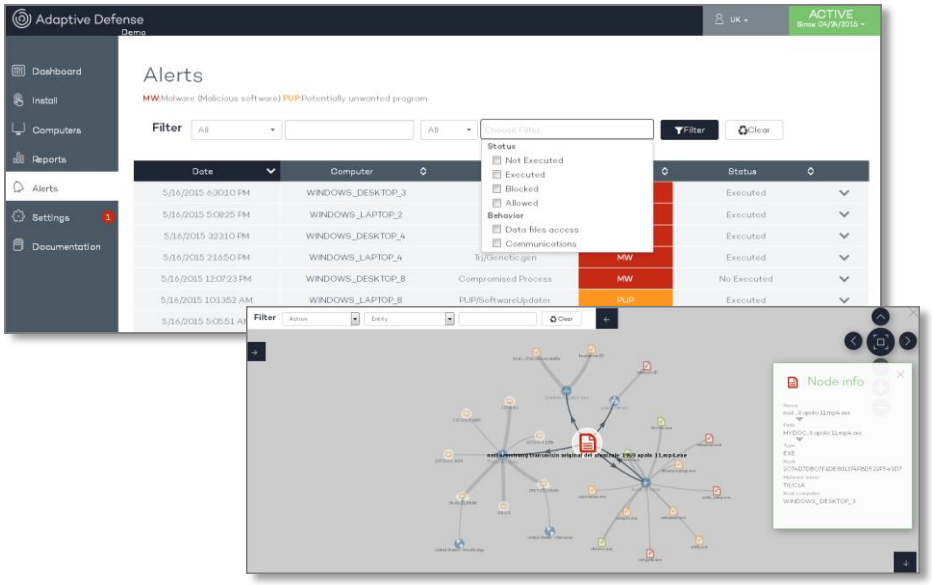
- To reduce the effectiveness of backup systems, **hackers threaten to disclose the stolen information on the Internet** if the ransom is not paid.

Panda Adaptive Defense

The solution to CryptoLocker and other advanced and zero-day threats

The Adaptive Defense model

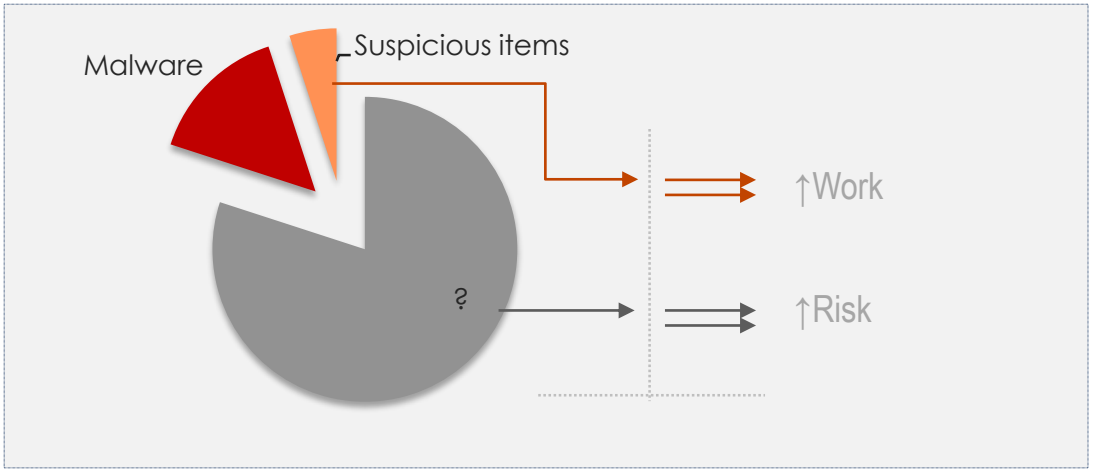
A model based on trustability, file classification and application execution control.



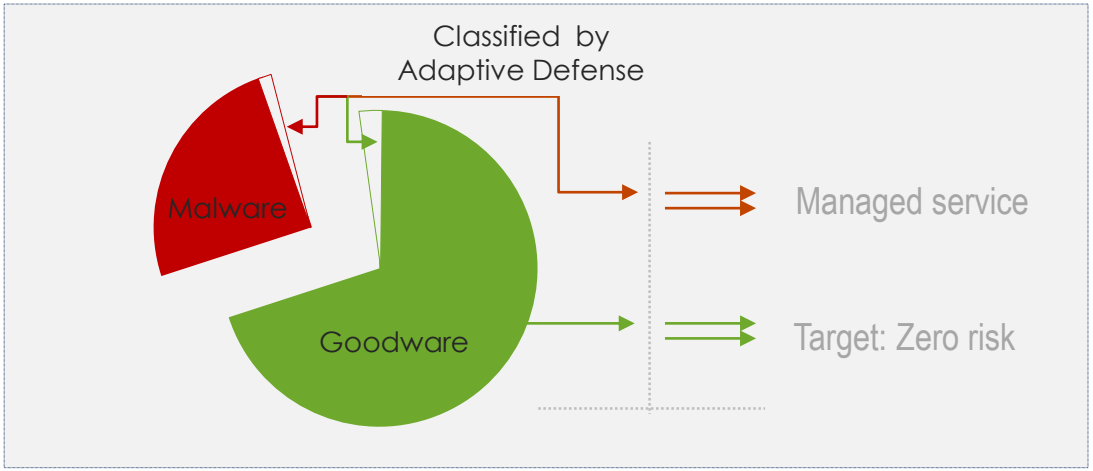
- **Audit**
  - Only monitors, does not block
  - Reports on malware found
- **Hardening** (default mode)
  - Blocks malware and unknown files coming from the Internet. Stops **CryptoLocker**-type ransomware and any other zero-day attack
- **Lock**
  - Full blocking. Only trusted applications are allowed to run.

CONCLUSION: WE DON'T ALLOW ANYTHING TO RUN UNTIL WE KNOW EXACTLY WHAT IT IS

Traditional antivirus solutions Vs Adaptive Defense



Traditional antivirus solutions (can identify malware but nothing else)



Adaptive Defense (monitors and classifies all running processes)

CryptoLocker

What are we seeing in customers' organizations?

What are we seeing in customers' organizations?

Customers with traditional AVs are getting infected with **CryptoLocker**

What are we seeing in customers with Adaptive Defense installed?

Adaptive Defense service	Current antivirus	No. of installations	**CryptoLocker attacks neutralized**	Period
Contracted	Symantec Endpoint Protection	338	**62**	Last 45 days
In trial	Panda Endpoint Protection	278	**3**	Last 30 days
Contracted	McAfee	2726	**49**	Last 60 days

Thank you!