

pandasecurity.com



Practical Security Guide to Prevent Cyber Extortion

European organizations are the ones that suffer the highest number of sensitive data theft.

The outlook for 2016 is that **Europe will continue to be at risk of cyberattacks.**



91% of SMEs have been targets of IT attacks

Source: Shopper Software Security in SMBs. Nielsen, April 2015

A person is sitting at a wooden table in a cafe, holding a smartphone in their right hand and a white mug with a black stripe in their left hand. In the background, a laptop screen displays a ransomware message from CTB-Locker. The message reads: "Your personal files are encrypted by CTB-Locker." followed by a progress bar and several paragraphs of text, including a warning: "Warning! Do not try to get out of this screen. If you do, you will lose your files." The overall scene is dimly lit, suggesting an indoor setting.

Ignoring malware attacks is a risk not worth taking.

Panda presents you with advice to keep your company safe and your mind at ease.

What is Cyber Extortion?

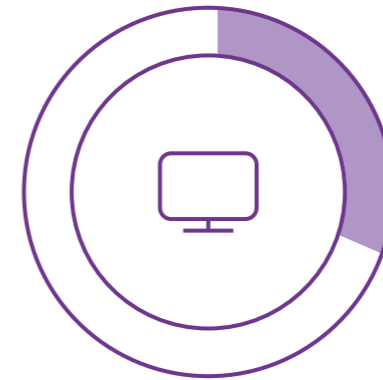
Cyber extortion is a form of blackmail in which victims of an IT attack are forced to pay to avoid its effects.

One of the most widespread methods of cyber extortion is ransomware. This attack encrypts the victim's information and then demands a ransom in order for the information to be decrypted and returned.

Once involved in the blackmail, having paid the ransom demanded by the cybercriminal, the victim of a cyber extortion usually receives an email with the code to decrypt their information. The method of payment is usually Bitcoin, a digital currency that can be exchanged for real money (1 Bitcoin = \$380). In fact, they usually use this payment method to hamper its traceability. However, the payment doesn't guarantee that the business won't be attacked again in the future.

Other similar attacks that use this kind of extortion are ones which infect your computer and access its webcam, then blackmail you so that they do not spread the videos.

The majority of attacks start with emails that include attached documents or by visiting unsecure websites.



39%

Unsafe and fraudulent websites



23%

Software download



19%

Malware received by email

Sources of Infection
Source: Shopper Software Security in SMBs. Nielsen, April 2015

How do cybercriminals
use ransomware for
attacks?

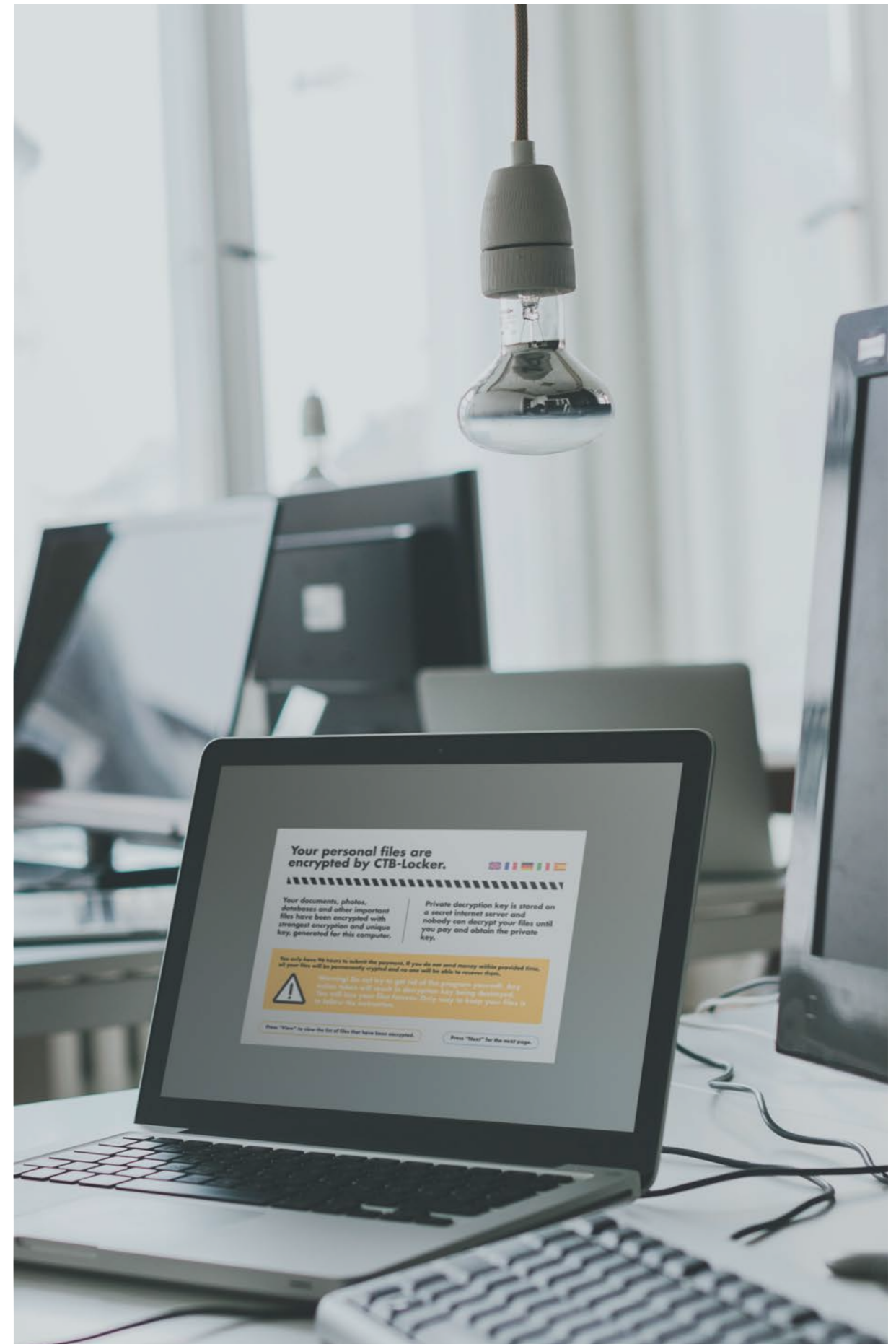
Ransomware such as Cryptolocker, Cyptowall, or Coinvault threaten the integrity of files that are found on the computer or network drives that they have access to.

The malware encrypts the data so that it can only be decrypted using a key that the cybercriminals will hand over if the business pays the requested ransom.

If you are one of the companies affected by ransomware then you usually have between 48 and 72 hours to pay the ransom. If you don't pay during this timeframe then the cost of decrypting your data could increase.

If they offer you an extension but the payment hasn't been completed, it's possible that they will delete the decryption key, making it impossible to recover the company's files.

Even if the payment is carried out, there is no guarantee that your data will be returned. This is because it is possible that the software developed by the cybercriminals contains bugs that cause a corruption in the decryption process, or law enforcement agencies are constantly trying to interrupt the cybercriminals infrastructure.



What to do if you
are a victim of cyber
extortion?

Don't give in to the cybercriminals' blackmail.

There is no guarantee that this will solve the problem.

In fact, in many cases, the victim of the blackmailing has given over the amount demanded but without receiving the decryption key (or even a corrupted key). None of these outcomes can help get the kidnapped information back.

Repeated blackmailing is also common. Once the information is returned, the cybercriminals install processes which continue to encrypt the company's data in no time.

On other occasions, the cybercriminal negotiates a higher amount than originally demanded, depending on the perceived desperation of the victim or the company's financial situation.

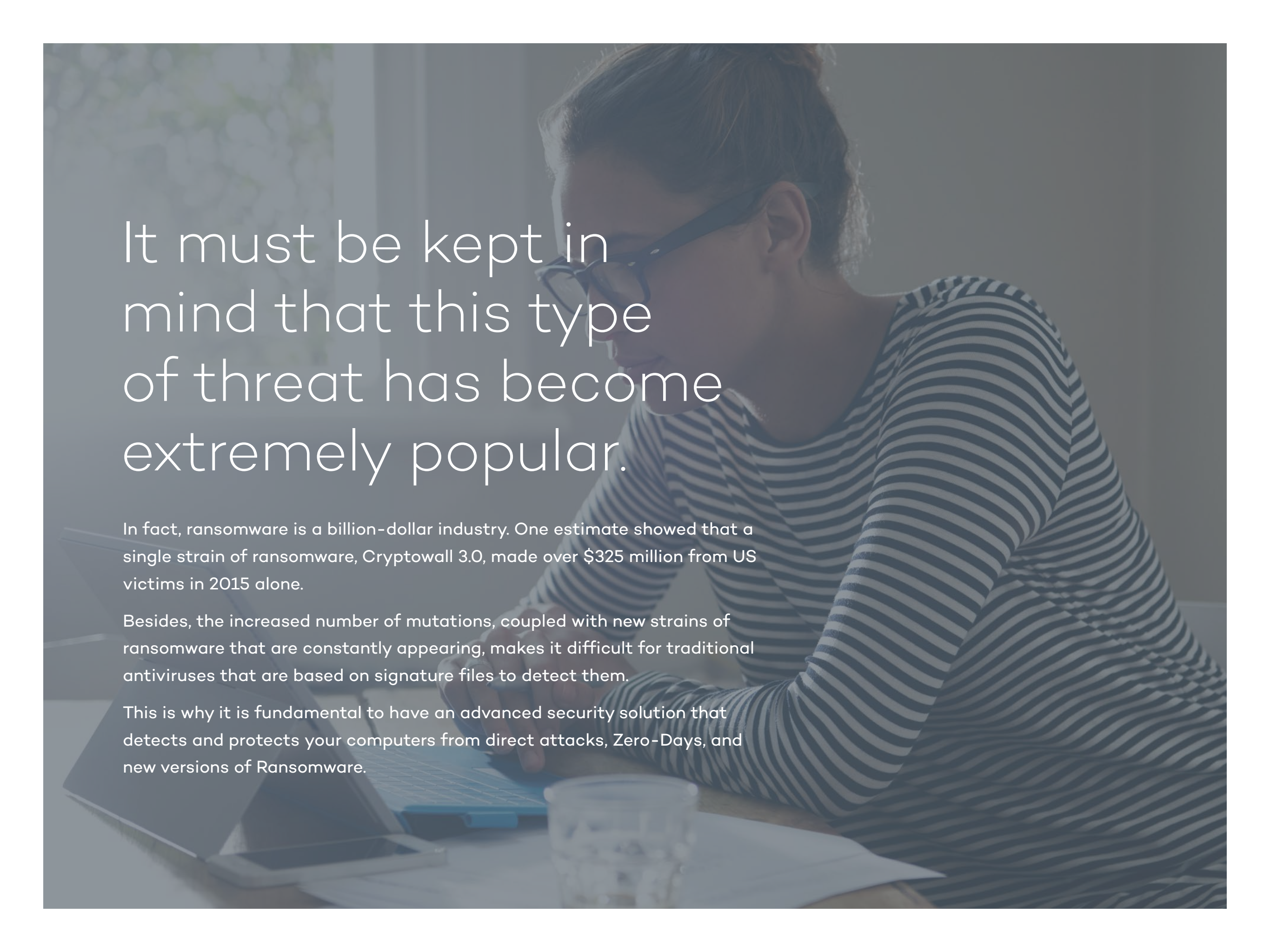
Completely wipe all traces of malware from your computers.

To do this, Panda recommends using **Cloud Cleaner** in offline mode, a solution that specializes in removing all traces of advanced viruses from affected computers.

Recover all your encrypted files.

To do this it is necessary to have previously activated the File History (in Windows 8.1 and 10) or System Protection (Windows 7 and Vista), which will allow for changes made by the malware on data files to be reversed.

It is also recommended that you make security copies of critical files every so often. Should you have a recent backup of your important documents we advise scanning these for any remnants of malware before restoring them.

A woman with glasses and a striped shirt is sitting at a desk, looking at a laptop. The image is dimmed to serve as a background for the text.

It must be kept in mind that this type of threat has become extremely popular.

In fact, ransomware is a billion-dollar industry. One estimate showed that a single strain of ransomware, Cryptowall 3.0, made over \$325 million from US victims in 2015 alone.




Besides, the increased number of mutations, coupled with new strains of ransomware that are constantly appearing, makes it difficult for traditional antiviruses that are based on signature files to detect them.

This is why it is fundamental to have an advanced security solution that detects and protects your computers from direct attacks, Zero-Days, and new versions of Ransomware.

What does a malware consist of and what are the most common types?

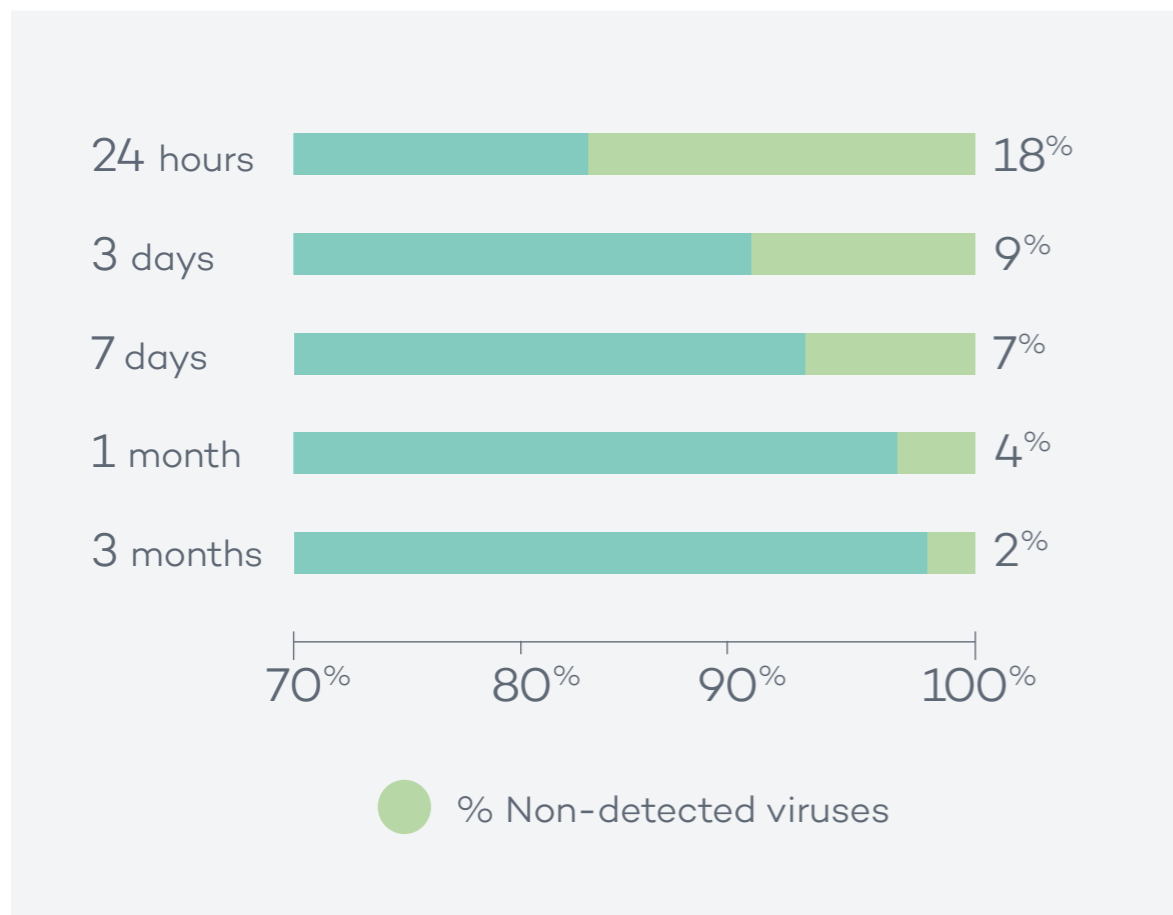
Well, it is any type of malicious program or IT code whose objective is to infiltrate networks and computers to cause damage, spy, and steal information. The most dangerous types of malware are:

-  **RANSOMWARE**
It blocks the PC, removing all user control, encrypts files and demands a financial ransom to return them.
-  **EXPLOIT**
It takes advantage of a security fault or vulnerability in the communication protocols to enter your computer.
-  **SPYWARE**
It collects names, access details, passwords, and any type of information about your company.
-  **PHISHING**
It creates a false URL to obtain your data and steal your identity, with the aim of stealing from your bank accounts.

-  **TROJAN**
It installs various applications so that hackers can control the computer. They control your files and steal your confidential information.
-  **APT (ADVANCED PERSISTENT THREAT)**
It's a computer process that penetrates your security to control and monitor it, being able to continually extract information for business or political means.
-  **SCAM**
It tricks you with false promotions such as holidays or lotteries, then asks you for money to access the "prize".
-  **BACKDOOR**
It opens a "back door" to take control of your system.
-  **KEYLOGGER**
It collects and sends all keystrokes completed by the user.
-  **BOT**
It is a program that remotely controls your PC.
-  **WORM**
It infects all of your computers, slowing down the network and even blocking access to communications.

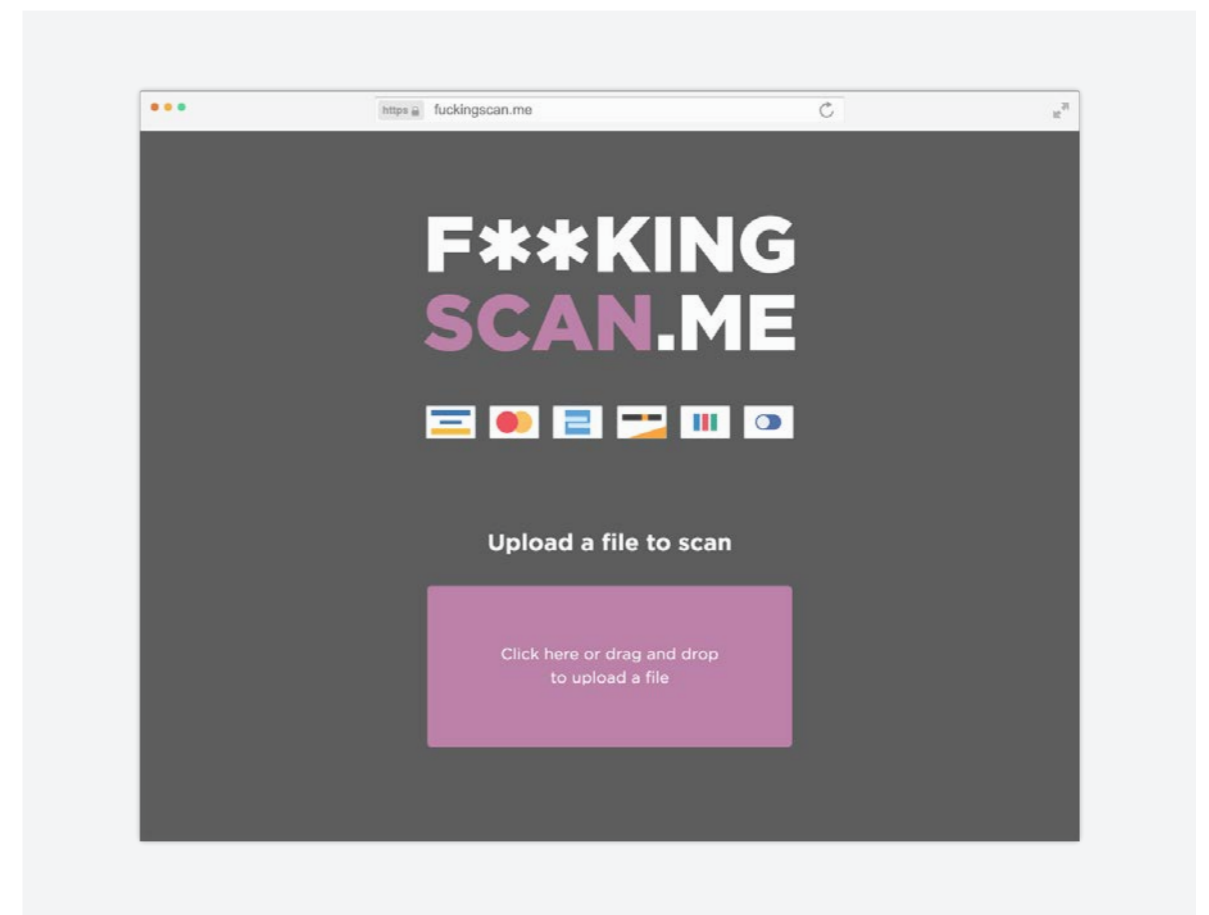
Evolution of malware, complexity and sophistication.

The technology used by traditional antiviruses (signature files, heuristic) are reactive. **18% of new malware isn't detected by traditional antiviruses in the first 24 hours, and 2% is still undetected 3 months later.**



Can these antiviruses stop advanced threats?

No antivirus can do this. In fact, There are websites online that allow you to see if a certain malware will be detected by an antivirus. **Hackers then launch their malicious code once they have verified that it won't be detected by any antivirus.**



Panda Security's 5 Recommendations to prevent Cyberattacks

1

Make your users aware

Make sure that your users know the risks of phishing and that they don't download unknown applications - or ones not provided by the company - and to avoid untrusted websites.



2

Be aware on the Internet

Set out policies for surfing the Internet that controls the reputation of websites that can be accessed.



3

A solution that fit your needs

Ensure that you have the security solution that your company needs and keep it updated.

A solution with different security layers that should be able to detect and block advanced threats.



4

Develop internal protocols

Establish protocols and security measures to control the installation and execution of any software. You should also check the inventory of your applications frequently.



5

Keep your systems & applications updated

Determine a policy for updating your applications and for blocking or eliminating them if they aren't needed by the company.

It is very important to get protected from applications that, even they are trustworthy (such as Java, Office, Chrome, Mozilla or Adobe), they can have some vulnerabilities or security holes that can be exploited by cybercriminals.





Image: The toolbars present a big security risk.

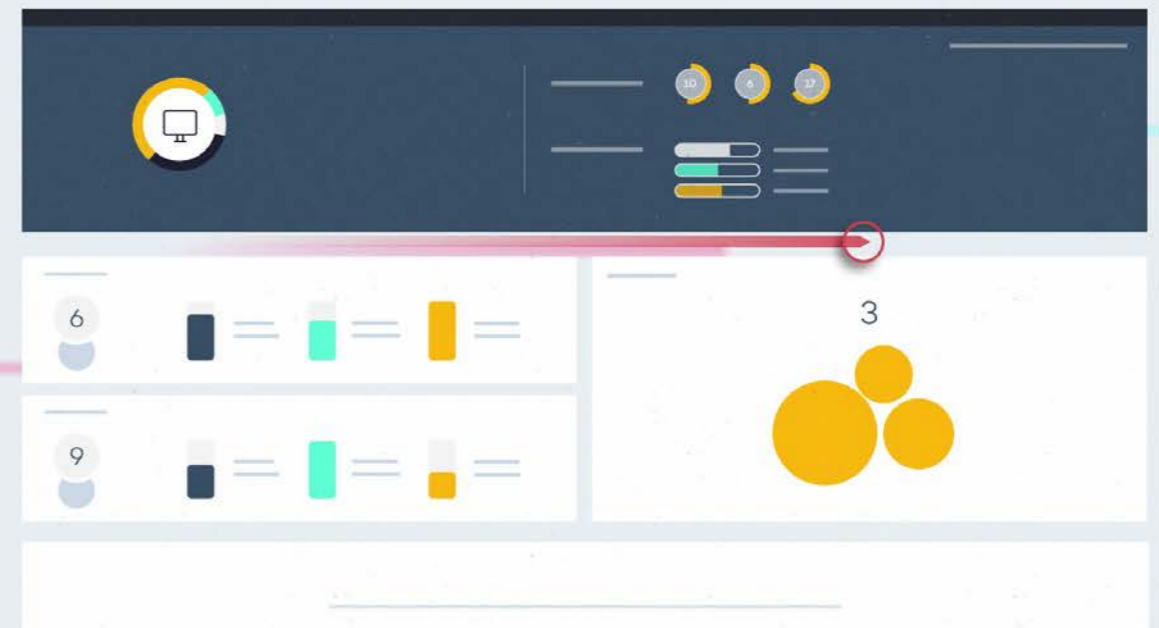
How can you really
protect your company?

Panda Security has developed the first solution that guarantees continuous monitoring of 100% of the active processes.

Panda Security has developed the only cybersecurity solution that is capable of protecting your company against direct attacks, Zero-Days, or any type of advanced threat, including Cryptolocker.

It is the first product on the market that guarantees to completely protect computers and servers, thanks to continuously monitoring 100% of the processes on the endpoint.

Adaptive Defense 360

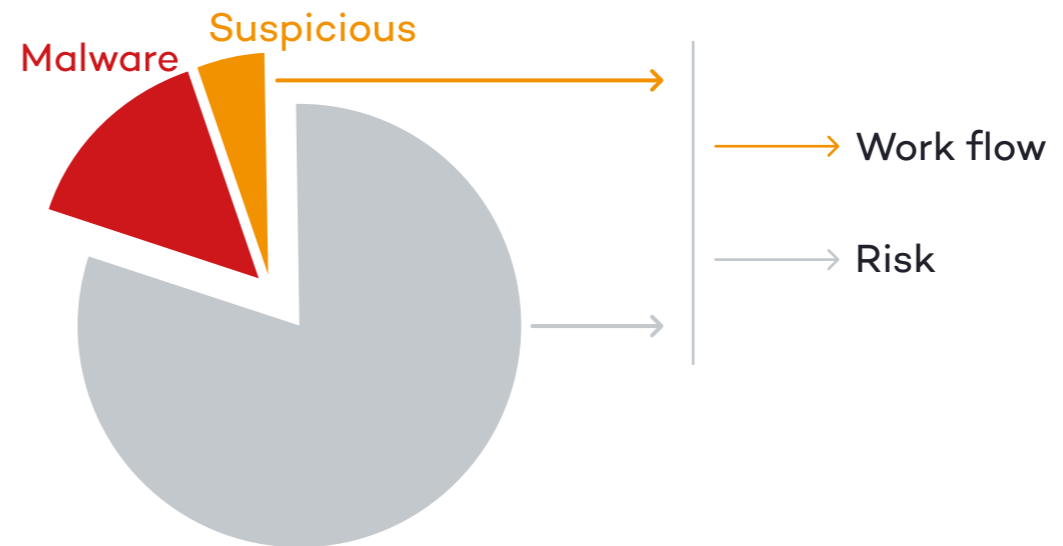


Adaptive Defense 360 offers the greatest security levels available, far ahead of any other antivirus on the market.

Adaptive Defense 360 monitors, registers, and classifies 100% of the running applications which, combined with EDR features, allows us to detect and block the malware that other protection systems don't even see.

Traditional Antiviruses

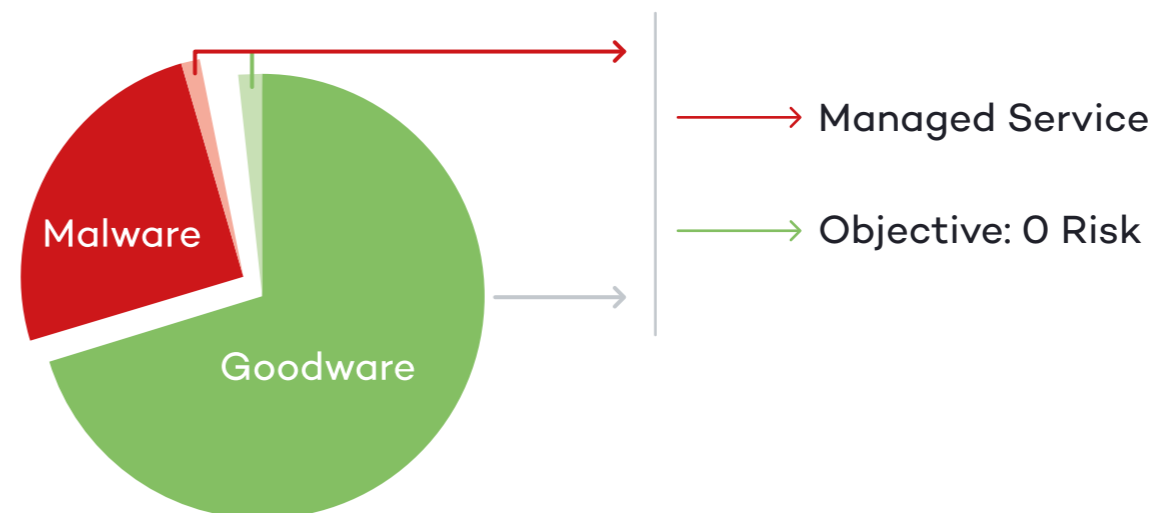
They only recognize malware but nothing else.



As they can't classify anything suspicious, these attacks represent a huge security problem for the traditional antivirus (especially targeted and zero-day attacks).

Adaptive Defense 360

It monitors absolutely all the active processes.



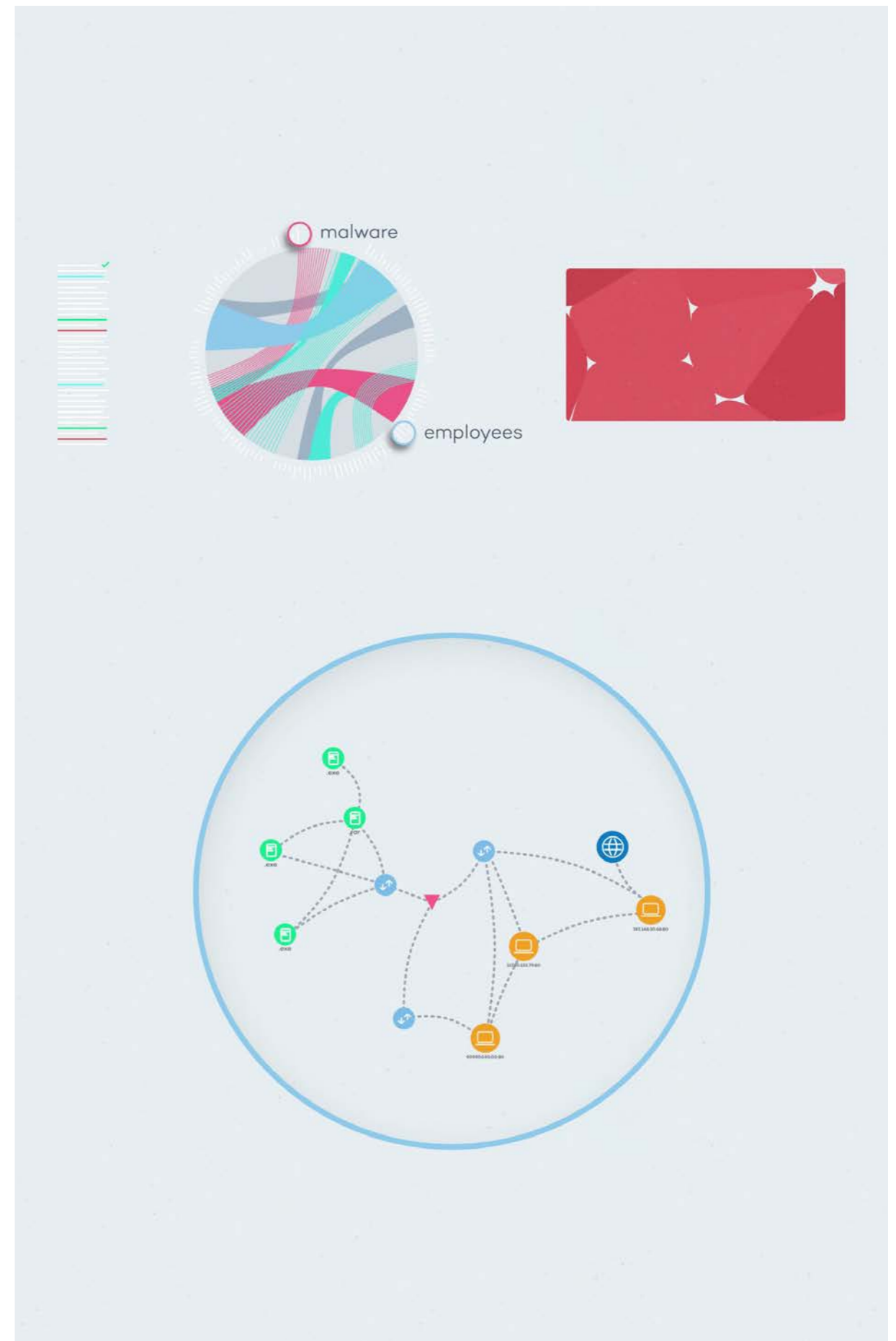
Adaptive Defense 360 knows with certainty if a process is good or bad, it classifies absolutely everything so that there is no suspicion.

Being able to control absolutely everything that happens on your computers allows you to:

Detect information leaks, both from malware and employees and from any archive that contains data (pdf, word, excel, txt,...).

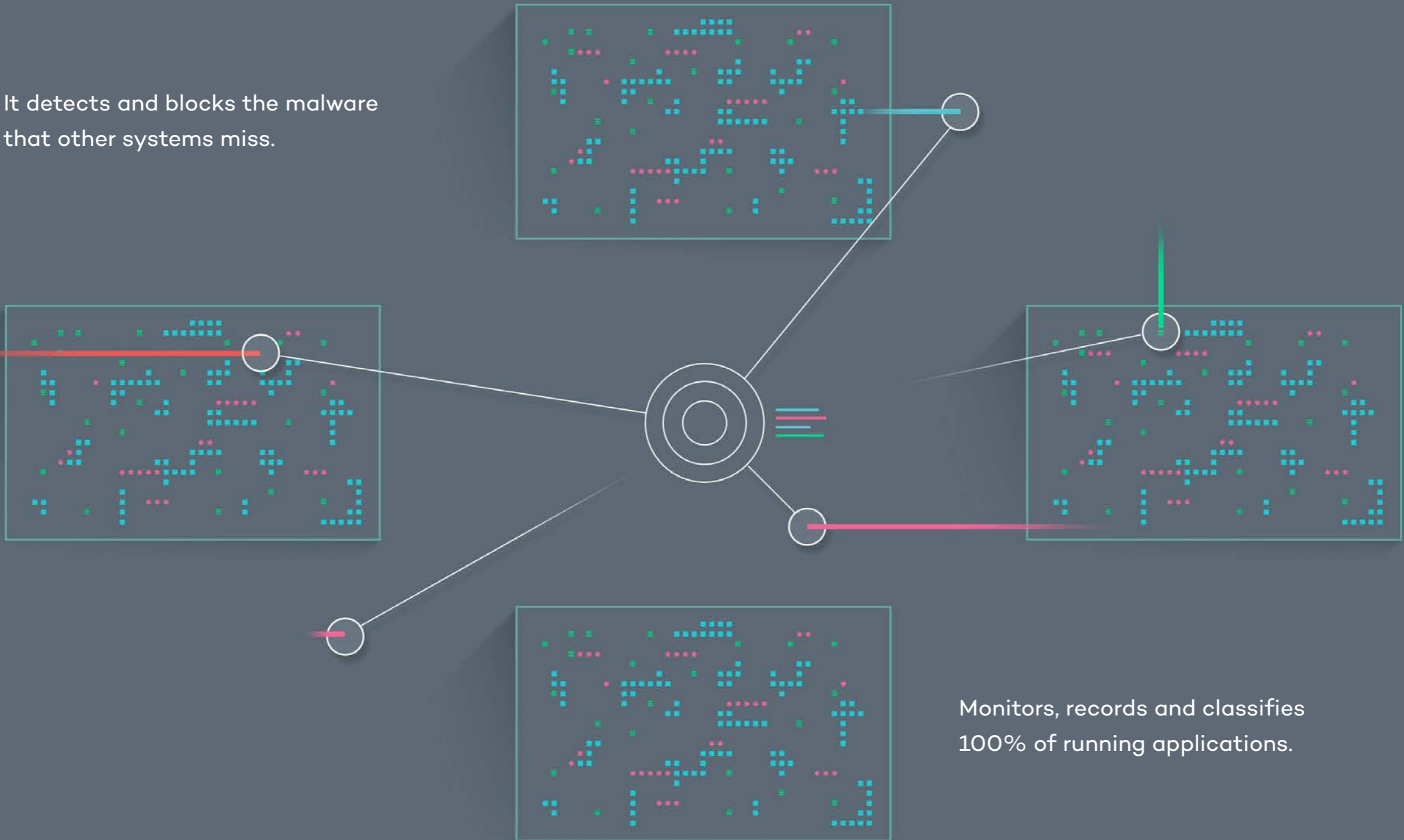
Discover and solve vulnerabilities on your systems and applications, and prevent the use of unwanted programs.

Detect direct attacks aimed at your systems.



Limitless Visibility, Absolute Control

It detects and blocks the malware that other systems miss.



Monitors, records and classifies 100% of running applications.

Adaptive Defense 360 in numbers

500K

It protects more than 500,000 endpoints and servers worldwide.

1.5M

It has categorized more than 1.5 million applications.

1.1M

It has mitigated more than 1,100,000 security breaches in the last year alone.

550K

It has saved more than 550,000 hours in IT resources, which amounts to an estimated saving of €34.8 million.

100%

It has detected malware in 100% of the environments it has been installed in, independently of the existing protection mechanisms.

Data from 2015.

What's more, it comes with **Panda Security's 25 years of experience**, which makes us a pioneer in malware detection and in implementing innovative security solutions.

Not to mention that **more than 30 million endpoints are currently protected by Panda worldwide.**

Contact us for more information

1-407-215-3020

sales@us.pandasecurity.com

