KASPERSKY lab

RETHINKING SECURITY

Fighting Known, Unknown and Advanced Threats

kaspersky.com/business

REAL DANGERS AND THE REPORTED DEMISE OF ANTIVIRUS

Regardless of its size or industry, your business is in real danger of becoming a victim of cybercrime. This fact is indisputable. Open a newspaper, log onto the Internet, watch TV news or listen to President Obama's recent State of the Union address and you'll hear about another widespread breach. You are not paranoid when you think that your financial data, corporate intelligence and reputation are at risk. They are and it's getting worse.

Somewhat more controversial, though, are opinions about the best methods to defend against these perils. The same news sources that deliver frightening stories about costly data breaches question whether or not anti-malware or antivirus (AV) is dead, as reported in these articles from PC World, The Wall Street Journal and Fortune magazine.

Reports about the death by irrelevancy of anti-malware technology miss the point. Smart cybersecurity today must include advanced anti-malware at its core. It takes multiple layers of cutting edge technology to form the most effective line of cyberdefense.

This eBook explores the features that make AV a critical component of an effective cybersecurity strategy to fight all hazards targeting businesses today — including known, unknown and advanced cyberthreats.

"Merchants, he said, are either not running antivirus on the servers managing point-of-sale devices or they're not being updated regularly. The end result in Home Depot's case could be the largest retail data breach in U.S. history, dwarfing even Target."

~ Pat Belcher of Invincea[1]

1. Mike Mimoso, Threatpost, "Feared Home Depot Breach Sparks More Interest in Backoff PoS Malware," September, 2014, https://threatpost.com/feared-home-depot-breach-sparks-more-interest-in-backoff-pos-malware/108083

KNOWN THREATS

During 2013 and 2014, Kaspersky Lab detected approximately 315,000 malicious samples each day. From online attacks, malicious URLs and other nasty objects including scripts, Web pages, exploits and executable files, Kaspersky Lab estimates that 80 percent of these cyberthreats fall under the heading of "known" threats.

Although known malware is prevalent and perceptible, it is not innocuous. Older, well-known malware is often used to launch more sophisticated, targeted attacks. This is possible because many systems do not have proper or regularly updated security in place, third-party applications are outdated and long known vulnerabilities are not patched. Some of the most well-known data breaches began with simple malware. If not detected and removed, malware can weaken the security perimeter and expose your business to advanced threats that lead to loss of valuable financial and personal data and corporate intelligence — putting your organization's reputation at risk.

Kaspersky Lab solutions repelled

367,431,148

attacks launched from online resources located all over the world.[2]

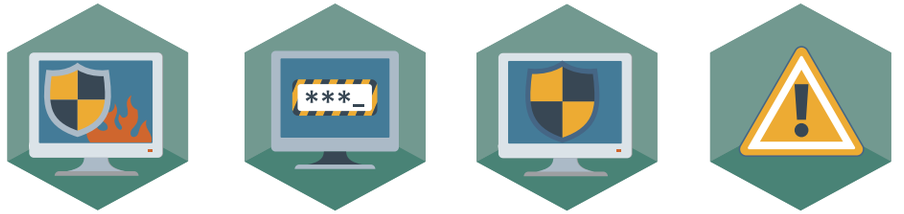
2. Kaspersky Lab, Kaspersky Security Network, 2014

AV'S ROLE IN FIGHTING KNOWN THREATS

From the moment a Web page is opened, a file is downloaded or an application launched, Kaspersky Lab's advanced anti-malware engine kicks into gear to simultaneously check, detect and protect against known, unknown and advanced Web and mail-based viruses, Trojans, rootkits, worms, spyware, scripts, adware and other known malicious objects and threats, using the following AV features:

A Network Attack Blocker scans all network traffic, using known signatures to detect and block network-based attacks, including port scanning, denial-of-service (DoS) attacks, buffer overruns and other remote malicious actions launched against programs and services running within the network. Traffic from attacking computers is blocked and infected systems on the network are prevented from distributing their payload by having their IP addresses blocked. Attack signatures are included in Kaspersky Lab's antivirus databases and are regularly updated.

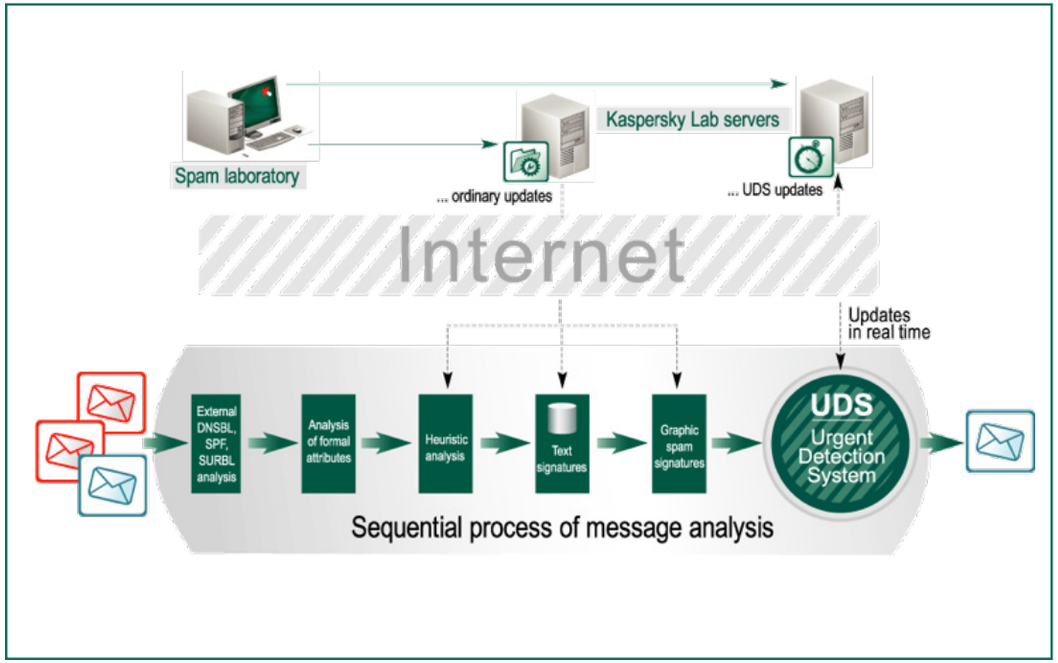
URL Filtering scans and checks URLs in inbound/outbound traffic against Kaspersky Lab's database of known malicious and phishing sites. Anything on this blacklist of malicious sites is blocked, preventing Web-based attacks, server-side polymorphic malware and botnet command and control (C&C) servers.



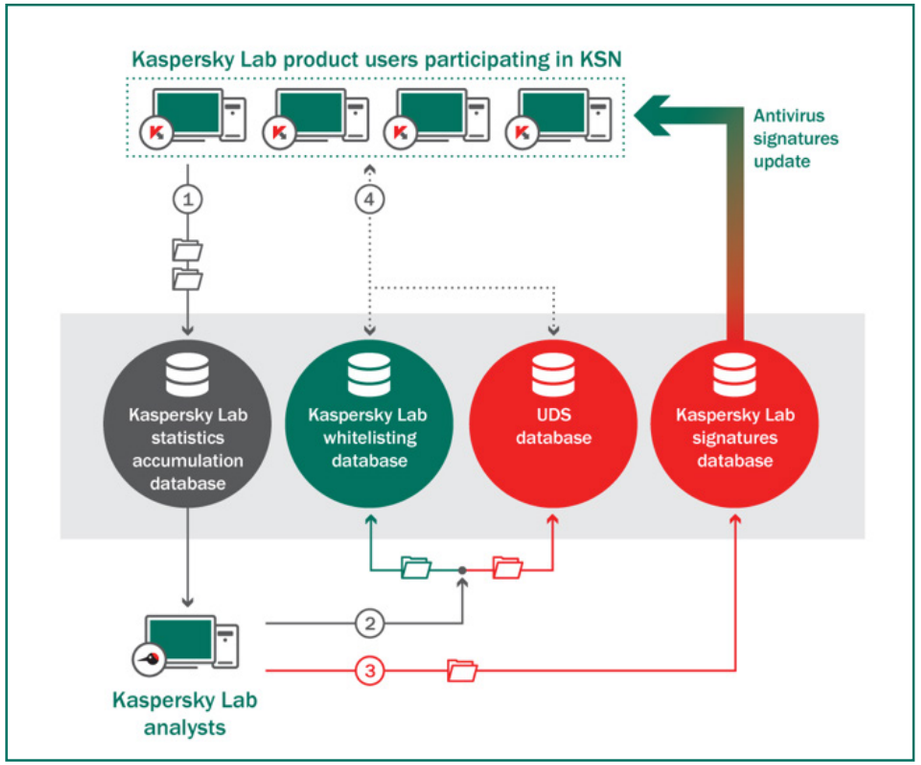
Kaspersky Lab's anti-spam engine also adopts a multi-layered approach, using several techniques to identify and manage unwanted messages. All incoming mail is scanned, filtered and sorted for unwanted messages — according to administrator-defined policies and settings. Reputational analysis, keyword/phrase and malicious or phishing links are all used to identify spam messages. Messages are further evaluated based on analysis of both the content and the mail's service information. Heuristic analysis of mail headers provides details of source server, AV scan status, application used to create the message and level of urgency applied. Embedded and attached images are analyzed and compared with spam patterns in Kaspersky Lab's signature database.

This regularly updated database is further strengthened by Kaspersky Lab's unique Urgent Detection System (UDS), which blocks even the newest and fastest-spreading spam through the creation of real-time, anonymized connections to Kaspersky Lab's anti-spam laboratory servers. This means protection is provided instantly, without the need to wait for the regular updates.

KASPERSKY LAB'S ANTI-SPAM ENGINE WORKS ON MULTIPLE LEVELS TO DETECT AND MANAGE UNWANTED, DANGEROUS MESSAGES.



The **Kaspersky Security Network (KSN)** is one of the most important components of Kaspersky Lab's multi-layered platform. KSN is a cloud-based, complex distributed infrastructure dedicated to gathering and analyzing security threat intelligence from millions of Kaspersky Lab users' systems worldwide. Administrators don't have to train the anti-spam engine because a database of sample messages is already available.



In Step 1, the volunteer participant in KSN's systems can opt in to send anonymized threat information to Kaspersky Lab's analyst centers. Step 2: Application-related threats and spam/embedded image data are sent to whitelisting and urgent detection system (UDS) databases, from which Kaspersky Lab users of these services will receive their intelligence (in Step 4). Step 3 shows heuristic threat analysis data being sent from analysts through to Kaspersky Lab's signature database, from which users receive their regular threat and anti-malware updates.

Blacklisting enables organizations to automatically block all known malware, along with known dangerous IP addresses and DNS. Kaspersky Lab's dedicated teams of malware analysts keep databases up-to-date with the latest malware signatures and data.

Instead of simply scanning executable files or scripts for malicious capability, the **Script and File Emulator** executes them in a safe, controlled environment that imitates a genuine operating system and environment. Everything needed to make any file or script believe it's executing in a real computing environment is there: memory, hard drive, registry, network processes, subsystems, etc., so Kaspersky Lab's technologies can take a detailed look at it and see what it's really up to.

All file actions are tracked and sent for heuristic analysis. Because everything happens in an artificial environment, no malware can actually harm the computer. Any potentially dangerous activities are weeded out prior to the file or script executing. The emulator data is yet another source of information used to keep the heuristic database up to date on the latest threats. By executing them safely, it's also possible to gain deeper intelligence into the behavior and functionality of encrypted or packed objects. It's also possible to generate single signatures for clusters of malware, enabling faster analysis and detection rates.

__33%__ of web attacks neutralized by Kaspersky Lab products were carried out using malicious web resources located in the US.[3]

3. Kaspersky Lab, Kaspersky Security Network, 2014

UNKNOWN THREATS

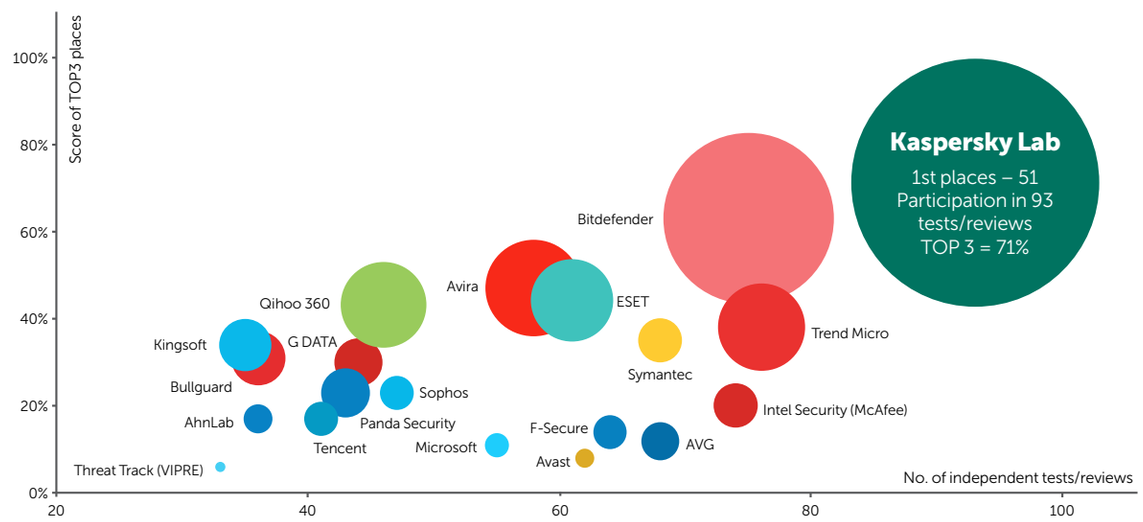
Kaspersky Lab researchers estimate that 18 percent of cyberthreats fall under the category of "unknown" threats. To detect and remove these threats that have yet to be identified, businesses need to rely on a security provider with expert research at its core.

Information security is in Kaspersky Lab's DNA. The Kaspersky Security Network (KSN) has more than 60 million Kaspersky Security Network volunteers worldwide. This security cloud processes over 600,000 requests every second. Kaspersky users around the globe provide real-time information about threats detected and removed. This data and other research are analyzed by an elite group of security experts – the Global Research and Analysis Team. Their main focus is the discovery and analysis of new cyberweapons, along with the prediction of new types of threats

Kaspersky Lab is a technology-driven company with more than one third of employees working in research and development. All solutions are developed in-house on a single code base. Kaspersky Lab's leadership and expertise is proven in multiple independent tests. In calendar year 2014, Kaspersky Lab participated in 93 tests and reviews. Sixty-six times Kaspersky Lab was named in the Top 3 and 51 times was rated first place.

Kaspersky Lab Provides Best in the Industry Protection

IN 2014 KASPERSKY LAB PRODUCTS PARTICIPATED IN 93 INDEPENDENT TESTS AND REVIEWS. OUR PRODUCTS WERE AWARDED 51 FIRSTS AND RECEIVED 66 TOP-THREE FINISHES.



* Notes:
According to summary results of independent tests in 2014 for corporate, consumer and mobile products. Summary includes tests conducted by the following independent test labs and magazines: AV-Comparatives, AV-Test, Dennis Technology Labs, MRG Effitas, NSS Labs, PC Security Labs, VirusBulletin. The size of the bubble reflects the number of 1st places achieved.

KASPERSKY LAB'S MULTI-LAYERED, PROACTIVE TECHNOLOGIES ANALYZE AND CHECK FILES AS THEY EXECUTE, USING PROACTIVE PROCESSES TO SEARCH FOR SUSPICIOUS OR MALICIOUS ACTIVITY THAT SUGGESTS AN UNKNOWN THREAT IS AT PLAY, INCLUDING:

Kaspersky Lab's Firewall: All packets entering and leaving the network are analyzed and blocked/allowed accordingly. The firewall monitors all network connections, applying packet, application and network rules to them, depending on their specified status. Rules based on action, protocol, direction and address can be applied. Policies are applied depending on network status: public, local, trusted. Unauthorized connections are blocked, decreasing the attack surface and possibility of infection. Infected or otherwise compromised machines have their network activity limited, reducing their ability to spread malware and limiting damage caused by security policy violations.

Application Control and Whitelisting: Almost every program is vulnerable to bugs, some of which enable the execution of malicious code. These are security gaps that AV services or content filters can't always cover – and criminals increasingly seek to exploit, particularly for launching targeted attacks against carefully chosen prey. Given that the average user has about 72 programs installed on their machine[4], that's a significant attack surface. Kaspersky Lab's application control and dynamic whitelisting enable proactive defense from known and unknown threats by giving administrators complete control over the applications and programs that are allowed to run, regardless of what the end user does. This includes preventing unpatched, vulnerable applications from running until they're updated. Application control blocks or allows administrator-specified applications, including controlling how they behave – what resources they can use, what kind of user data they can access and modify, whether they write to registries etc. This means any application can be prevented from executing any action that could endanger systems or the network.

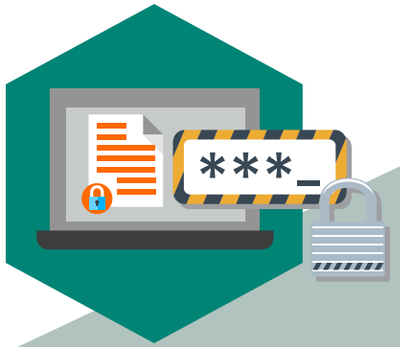
4. Secunia, "Secunia Vulnerability Review," March 2013

IT'S A THREE-PRONGED APPROACH:

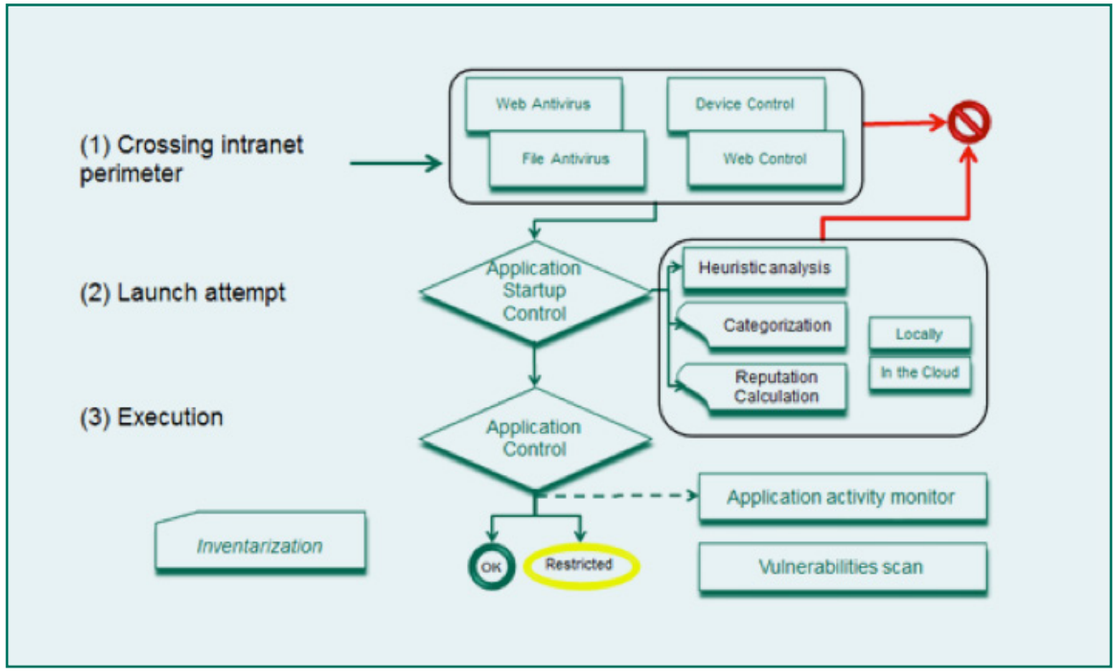
1. **Application startup control**
grants, blocks and audits application launches and drives productivity by restricting access to non-business-related applications.

2. **Application privilege control**
regulates and controls application access to system resources and data, classifying applications as trusted, untrusted or restricted.

3. **Application vulnerability scanning and patch management**
are proactive defenses against attacks targeted at vulnerabilities in trusted applications. Kaspersky Lab's application vulnerability control is optional and disabled by default; it functions separately from the vulnerability assessment capabilities in Systems Management.

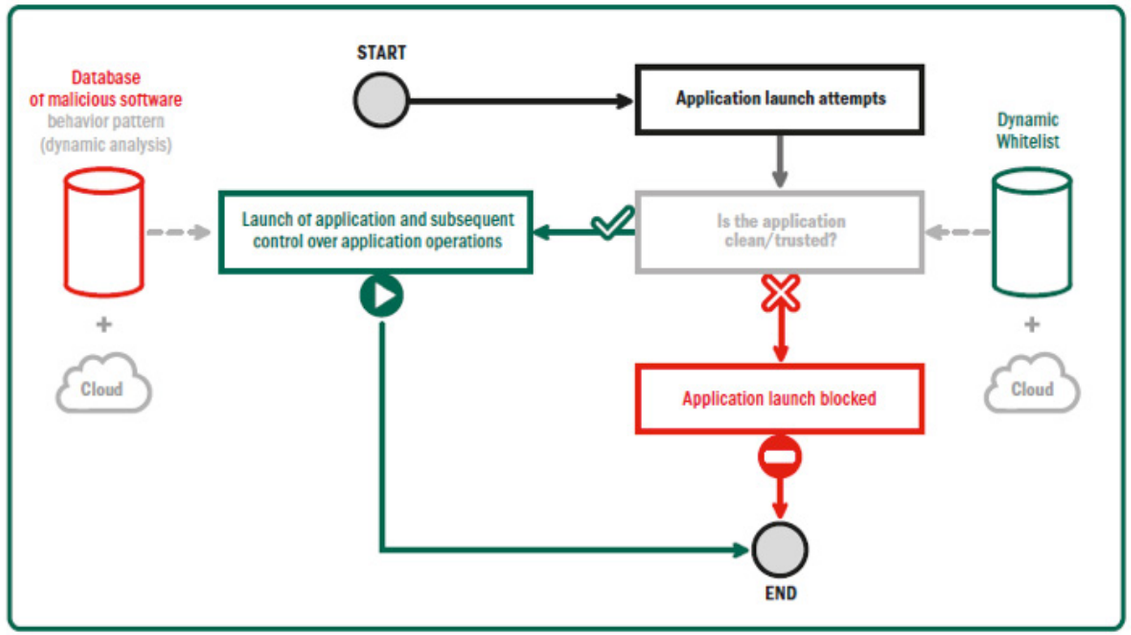


HOW KASPERSKY LAB'S APPLICATION CONTROL WORKS



KASPERSKY LAB'S APPLICATION CONTROL IS UNDERWRITTEN BY DEFAULT DENY – A HIGHLY EFFECTIVE SECURITY STRATEGY THAT SIMPLY BLOCKS ALL APPLICATIONS FROM RUNNING ON ANY ENDPOINT, UNLESS EXPLICITLY ALLOWED BY ADMINISTRATORS. BLOCKED APPLICATIONS CAN BE QUARANTINED FOR ADMINISTRATOR APPROVAL.

A Simplified Default Deny Algorithm



Application Controls and Default Deny reduce the risks posed by unknown threats. Most malware is delivered as an executable file that will not be found on any whitelist. Organizations that adopt this approach (and the supporting technologies) can thus prevent any malicious file from executing, without needing to identify or know what those files actually are.

Criminals are constantly developing new technologies and techniques to gain access to data – by ensuring only trusted, patched applications are allowed to run on your systems, you're adding an extra layer of defense.

Effectively a global threat laboratory, **Kaspersky Security Network (KSN)** detects, analyzes and manages unknown or new threats and online attack sources in seconds – and delivers that intelligence straight to customer systems. Working in concert with all the other components of Kaspersky Lab's engine, KSN enables the quickest reaction times and highest protection levels possible. Newly-detected threats and malware are reported to the Urgent Detection System, which delivers the relevant intelligence through to KSN for widespread delivery. This enables protection from unknown threats before signatures are available — traditional signature-based responses can take hours; KSN takes about 40 seconds.

Using real-time, anonymized data from 60 million volunteers globally, every file that passes through Kaspersky Lab protected systems is subject to analysis based on relevant threat intelligence – the same data ensures the most appropriate action is taken.

KSN is a good example of how the multi-layered approach to security works — with multiple components working together or supporting other functionality to deliver symbiotic, comprehensive protection, even from unknown threats. It combines signature and heuristic malware detection with other Kaspersky Lab technologies such as whitelisting and application control.

__12%__ of businesses surveyed by Kaspersky Lab reported run-ins with targeted attacks.[5]

5. Kaspersky Lab, "Global IT Security Risks Report 2014," November, 2014

ADVANCED THREATS

"Advanced" threats are complex attacks, consisting of many different components, including penetration tools (spearphishing messages, exploits etc.), network propagation mechanisms, spyware, tools for concealment (root/boot kits) and other, often sophisticated techniques, all designed with one objective in mind: to provide cybercriminals with undetected access to sensitive information.

Advanced attacks target any sensitive data; you don't have to be a government agency, major financial institution or energy company to become a victim. Even small retail organizations have sensitive client information on record; small banks operate remote service platforms for customers and businesses of all sizes process and hold payment information that is dangerous in the wrong hands. As far as attackers are concerned, size doesn't matter: It's all about the information. Even small companies are vulnerable to advanced threats – and need a strategy to mitigate them.

Targeted and multi-component attacks are a steadily increasing trend — particularly when it comes to businesses, where criminals are launching sophisticated, tailored attacks based on well-researched organizational vulnerabilities. Twelve percent of businesses surveyed by Kaspersky Lab reported run-ins with targeted attacks, with the combined costs of damages, remediation and other reactive spending averaging $2.54 million for enterprise organizations and $84,000 per mid-sized businesses.[6]

6. Kaspersky Lab, "Global IT Security Risks Report 2014," November, 2014

***107,215,793** unique URLs were recognized as malicious by web antivirus components.[7]*

7. Kaspersky Lab, Kaspersky Security Network, 2014

HOW KASPERSKY LAB AV DETECTS ADVANCED THREATS

Your file has been downloaded and started, 10 Kaspersky Lab technologies have scanned, analyzed, applied intelligence and variously blocked or allowed based on known as well as unknown threats. But what about advanced threats? How do Kaspersky Lab's technologies handle advanced threats and other highly sophisticated malware – the kind that often hits at file execution stage?

Complex, highly sophisticated exploits are invariably multi-layered, using a variety of techniques to bypass more traditional security technologies. Many exploits target zero-day vulnerabilities using techniques that can overcome even proactive protection technologies. These are relatively low in number, but the damage caused by even one threat slipping through the layers can be massive.

Kaspersky Lab's reputation for discovering and mitigating against the most relevant, sophisticated threats, such as Epic Turla, Careto and Red October, are the result of this dedication and commitment to research and development. Kaspersky Lab's expertise is recognized and respected among top security organizations globally. Kaspersky Lab detects and remediates any attack, regardless of its origin or purpose, cooperating and consulting with law enforcement and government officials around the globe.

Kaspersky Lab's advanced threat detection technologies are designed to detect and block these, using a range of proactive, sophisticated heuristic scanning algorithms and behavior analyzers that monitor various file behaviors, discern suspicious patterns, block malicious activities and roll back harmful changes, including cryptors.

Automatic Exploit Prevention (AEP) specifically targets malware that exploits software vulnerabilities. Even if a user downloads or opens a malicious file, Kaspersky Lab's AEP technology will prevent the malware from executing. Developed through in-depth analysis of the features and behaviors of the most widespread exploits, the resulting technology is capable of identifying exploit-characteristic behavior patterns – and blocking them from completion.

AEP's capabilities include:

Control of potentially vulnerable applications: By focusing specifically on the most targeted applications, such as Adobe Reader®, Oracle Java® and Internet Explorer®, any attempt to launch unusual executable files or code via these programs, launches additional security checks. Legitimate executables, such as checking for updates, are accounted for. But where certain characteristics of the executable file, along with any associated actions, are indicative of malicious activity, additional inspection will take place, followed by appropriate mitigating action.

Monitor pre-launch activities: How an application launches or code executes and what happens before it does so, can reveal a lot about it. Certain kinds of behavior strongly indicate malicious activity; AEP technology tracks this activity and detects the source of the attempt to launch the code. Data on the most typical exploit behaviors can help detect this kind of activity, even when a zero-day vulnerability is used – this means AEP doesn't need to know the precise nature of the exploit to understand that malicious activity is taking place.

Tracking code origins: Some exploits – particularly those used in drive-by downloads (i.e. , launched though a malicious Web page) – need to retrieve their payload from another website before executing it. AEP traces the origin of such files, identifies the exact browser that initiated them and retrieves the remote Web address for the files. It's possible for AEP to distinguish between files created with user consent and unauthorized ones – this information can help identify exploits and block them.

Prevent exploits from accessing their chosen vulnerability: Using a technique called Forced Address Space Layout Randomization with some programs and software modules, exploits can be prevented from finding the specific vulnerability or code they need to execute, for example, in memory. Repeated efforts to locate the required code are more likely to result in the application crashing than they are in the malicious code executing.

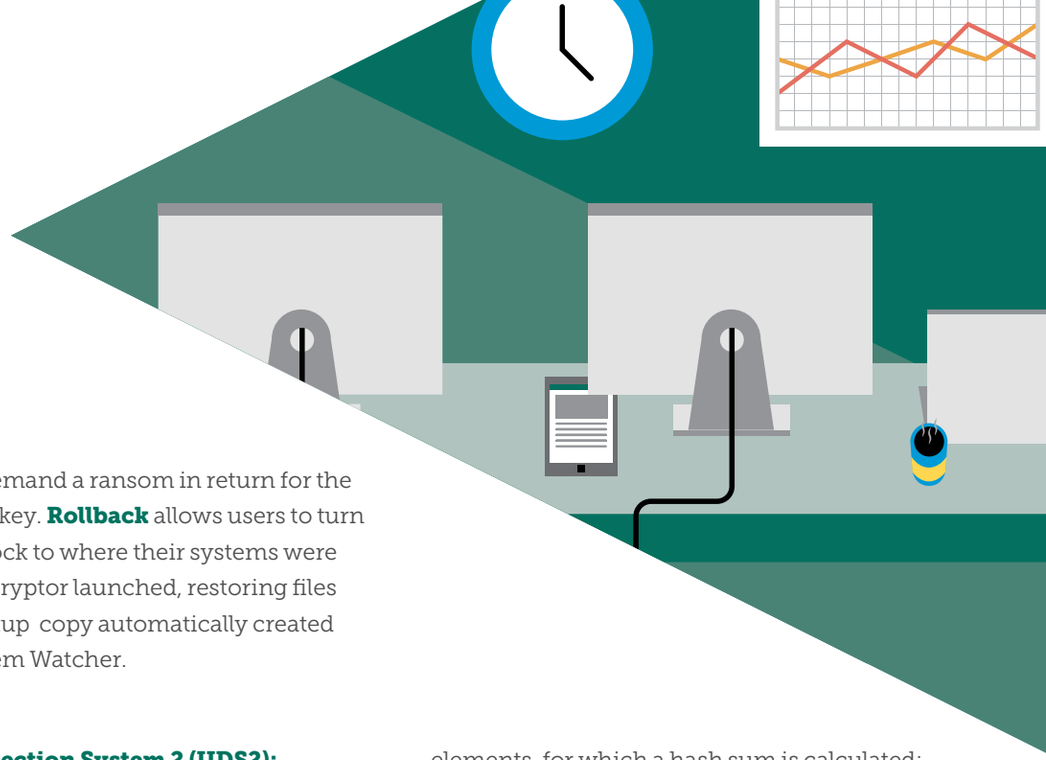
AEP acts like a safety net, an extra layer of security that complements Kaspersky Lab's other technologies, such as antivirus and anti-spam filters.

Kaspersky System Watcher monitors and collects data on application and other important system activities. This information is provided to the other Kaspersky Lab protection components detailed here, providing a proactive security approach. Any activity that corresponds to threat patterns is dealt with according to administrator-set policies (the default setting is to terminate the malicious process and quarantine for later analysis if desired).

The driver that intercepts file operations for Kaspersky Lab's AV component also gathers information on changes made to the registry, while the firewall gathers data on the network activity of applications. All of this information is fed into System Watcher which, in turn, has its own module capable of reacting to complex system events, such as installation of drivers.

Critical security issues related to vulnerabilities in the Java platform are managed by the Java2SW module. Malicious actions, regardless of signature availability, are blocked, with a low false positive rate – destructive behavior patterns are the most reliable indicator of malware.

This continuous, detailed monitoring of systems enables exceptionally accurate system Rollback functionality, limiting the impact of any infection and returning systems to previous, secure parameters. Rollback is particularly effective against the fast-growing class of malware known as cryptors or ransomware – where criminals infect a system, encrypt important documents without the user's knowledge



and then demand a ransom in return for the decryption key. **Rollback** allows users to turn back the clock to where their systems were before the cryptor launched, restoring files from a backup copy automatically created using System Watcher.

Urgent Detection System 2 (UDS2): UDS2 builds on UDS's known threat detection capabilities, using a more advanced signature called shingles to block new versions of spam containing subtle modifications that may help it slip through the net. Kaspersky Lab's technologies extend well beyond a basic endpoint security approach – layered security protects each element in a layered infrastructure, constantly filtering out threats and reducing the channels by which they can be introduced. UDS2 ensures that messages are analyzed and divided into separate elements, for which a hash sum is calculated; a shingle is a combination of these sums. UDS2's cloud-based technology can cope with more advanced spam-related threats because it doesn't require a perfect match between shingles to detect spam. Even modified spam messages can be blocked; combinations of existing shingles can be used to detect spam without requiring repeated re-assessments or new signature creation. This reduces response times and, crucially, drives more efficient spam filtering –further reducing the threat surface.

STRATEGIES FOR COPING WITH TARGETED ATTACKS

Many respected technology-focused organizations have already developed strategies for coping with targeted attacks. Gartner, for example, has issued guidelines for dealing with social engineering techniques, including keeping pace with an evolving threat landscape through ongoing information security education and educating users on the threats posed by social engineering techniques.[8]

Among the technical security issues addressed by Gartner, two key recommendations emerge: "Upgrade your perimeter and network-based security" and "Focus your protection strategies on malicious content." In this context, Gartner mentions Kaspersky Lab among the leading vendors for Application Control and Whitelisting, capable of providing all the functionality needed to mitigate advanced threats.[9]

8. Gartner, "Best Practices for Mitigating Advanced Persistent Threats," September 12, 2013, https://www.gartner.com/doc/2589029/best-practices-mitigating-advanced-persistent
9. Gartner, "How to Successfully Deploy Application Control," January 25, 2013, https://www.gartner.com/doc/2316916/successfully-deploy-application-control

According to KSN data, Kaspersky Lab products detected and neutralized a total of

1,325,106,041

threats in the third quarter of 2014.[11]

Application Whitelisting is the most valuable strategy any organization can adopt to fight advanced threats. It forms a powerful layer of protection against the executable components of advanced threats, including as-yet-unknown threats. Interest in application control for desktops and servers has been increasing steadily over the last five years.

Kaspersky Lab's solution implements Dynamic Whitelisting. Gartner has described proper implementation of Application Control as continuously updated from a cloud database – making it dynamic. Application Control with Dynamic Whitelisting can help protect systems from both known and unknown threats by giving administrators total control over the applications that are allowed to run on endpoints, regardless of end-user behavior.[10]

10. Gartner, "Competitive Landscape: Critical Infrastructure Protection," December 16. 2013, https://www.gartner.com/doc/2637923/competitive-landscape-critical-infrastructure-protection
11. Kaspersky Lab, Kaspersky Security Network, 2014

WHY AV STILL MATTERS FOR KNOWN, UNKNOWN AND ADVANCED THREATS

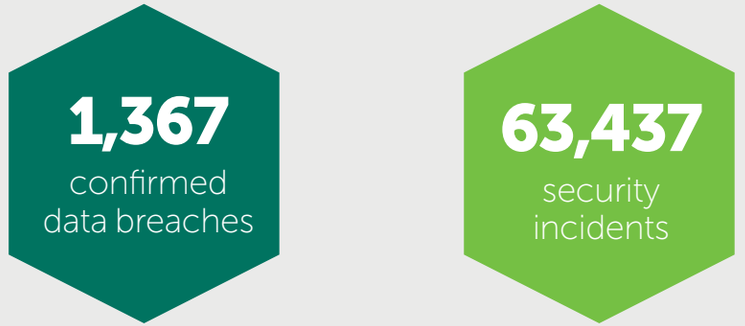
While no one is suggesting that signature-based anti-malware technologies, on their own, are enough to protect against an increasingly sophisticated and varied threat landscape, condemning them as useless puts your business at risk. In fact, sole signature-based software will not be viable for another 10 years, at least, which is why security solutions like Kaspersky Lab's have evolved into multi-layered security.

In the second quarter of 2014, Kaspersky Lab's anti-malware solutions detected 528,799,591 virus attacks on end user systems, identifying a total of 114, 984, 065 unique malicious objects—or 114,984, 065 opportunities for a major data breach.[12] According to the "2014 Verizon Data Breach Report," there were 1,367 confirmed data breaches and 63,437 security incidents in 2013.[13] The severity and cause of these incidents vary depending on the goals of the cybercriminals and, sometimes, the size of the potential victim.

With these odds, are you willing to take the risk of ignoring the benefits of AV?

12. Kaspersky Lab, "Q3Threat Evolution Report 2014," November, 2014, https://securelist.com/analysis/67637/it-threat-evolution-q3-2014/
13. Verizon, "2014 Verizon Data Breach Investigations Report," http://www.verizonenterprise.com/DBIR/2014/

According to the "2014 Verizon Data Breach Report," there were 1,367 confirmed data breaches and 63,437 security incidents in 2013.[14]



14. Verizon, "2014 Verizon Data Breach Investigations Report," http://www.verizonenterprise.com/DBIR/2014/

TRY KASPERSKY LAB

Discover how Kaspersky Lab's premium security can protect your business from malware and cybercrime with a no-obligation trial. Register today to download full product versions and evaluate how successfully they protect your IT infrastructure, endpoints and confidential business data.

Get Your Free Trial Today >

JOIN THE CONVERSATION

Watch us on YouTube

Like us on Facebook

Review our blog

Follow us on Twitter

Join us on LinkedIn

Learn more at http://usa.kaspersky.com/business-security

ABOUT KASPERSKY LAB

Kaspersky Lab is one of the world's fastest-growing cybersecurity companies and the largest that is privately-owned. The company is ranked among the world's top four vendors of security solutions for endpoint users (IDC, 2014). Since 1997, Kaspersky Lab has been an innovator in cybersecurity and provides effective digital security solutions and threat intelligence for large enterprises, SMBs and consumers. Kaspersky Lab is an international company, operating in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide. Learn more at www.kaspersky.com.

Contact Kaspersky Lab today to learn more about Kaspersky Endpoint Security for Business and our other IT security solutions and services:
http://usa.kaspersky.com/business-security
(866) 563-3099
corporatesales@kaspersky.com

KASPERSKY lab
THE POWER OF PROTECTION