ENDPOINT SECURITY FOR BUSINESS: TECHNOLOGY IN ACTION

For the threats you can see and those you can't

KASPERSKY lab

THE POWER OF PROTECTION

kaspersky.com/business

CONTENTS

94% of companies have experienced some form of external security threat

Source: Kaspersky Lab Global IT Risks Report 2014

PROTECT YOUR BUSINESS FROM THE THREATS YOU CAN SEE AND THOSE YOU CAN'T

Having the right IT security in place has never been more important.

WHAT YOU DON'T KNOW *CAN* HURT YOU

More than 30 percent of security breaches occur at companies with 100 or fewer employees.[1] 44 percent of small-and-medium-sized businesses (SMBs) have been attacked by cybercriminals.[2]

Yet many are unaware of the very real threats that cybercrime and advanced malware pose to their business. While just under a fifth of smaller businesses admit they've taken no steps to guard against cybercrime, only 60 percent actively keep their anti-malware software up-to-date.[3]

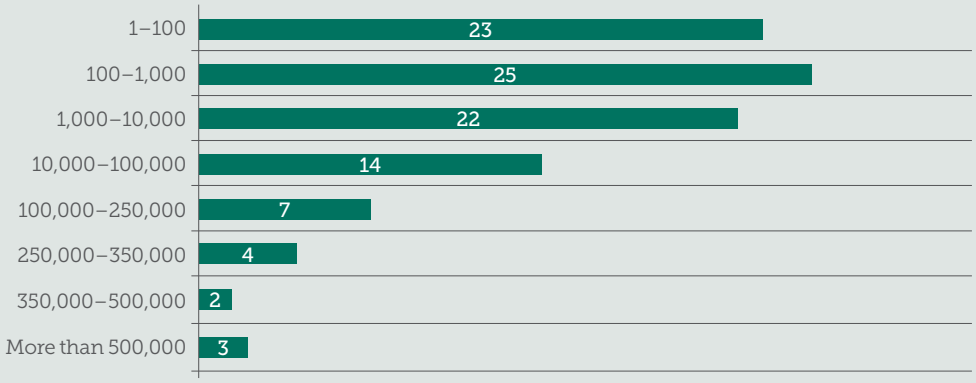
Thinking you're too small to be of interest is exactly the mindset that cybercriminals are exploiting to launch increasingly sophisticated malware against your business. They know what many SMBs don't: You are a target.

[1] Verizon's 2013 Data Breach Investigations Report
[2] 2013 survey by the National Small Business Association
[3] Kaspersky Lab, Threatpost, May 24, 2013

WHAT YOU CAN'T SEE

Let's assume you're one of the 80 percent of SMBs with some kind of IT security solution in place. Don't get too complacent: most business users grossly underestimate threat volumes.[4] Only four percent of those surveyed came anywhere close to guessing how many threats are detected each day.[4]

PERCEIVED NUMBER OF NEW MALWARE SAMPLES DISCOVERED DAILY (%)



Source: Kaspersky Lab Global IT Risks Report 2014

In this context, it's hardly surprising that some users view IT security as a "commodity," seeing little difference between the various options available to them. That's a dangerous myth; even a one percent difference in detection rates can result in hundreds of thousands of pieces of malware slipping through the nets over the course of a year. How do we know that?

- Kaspersky Lab detects 325 000 new pieces of malware every single day.
- In the second quarter of 2014, our anti-malware solutions detected 528,799,591 virus attacks on end user systems, identifying a total of 114,984,065 unique malicious objects in the process.[5]

The most dangerous threats are the ones you don't know about – the threats Kaspersky Lab experts monitor, analyze and mitigate every day. We look for trouble. And when we find it, we use more than a decade's worth of threat intelligence and expertise to provide the additional protection against the threats your organization most needs to avoid – especially when it comes to advanced malware and Advanced Persistent Threats (APTs).

There's an increasing gulf between what businesses believe the threat landscape to be and what it actually is. We've called this the "perception gap." It shows that organizations, no matter what their size, wildly underestimate both the amount and severity of the threats they face.

Costin Raiu, Global Research & Analysis Team, Kaspersky Lab

[4] Kaspersky Lab Global IT Risks Report 2014
[5] Kaspersky Lab Q2 Threat Evolution Report 2014

PROACTIVE, REACTIVE, INTELLIGENT

Kaspersky Lab has a long track record in making some of the highest profile, most relevant threat discoveries, including Carbanak (the world's biggest cyber bank heist), Dark Hotel, The Mask, Icefog and Red October. More than a third of our employees work in Research and Development. They focus solely on developing technologies to counteract and anticipate the constantly evolving threats our dedicated teams of Intelligence and Analysis Researchers investigate every day.

Kaspersky Lab's understanding of the inner workings of some of the world's most sophisticated threats has enabled us to develop a multi-layered platform of security technologies to fight against known, unknown and advanced threats. Our technologies detect and mitigate the threats you can see – as well as those you can't.

How do we do it? Here's a walk through how Kaspersky Lab's multiple anti-malware and threat detection technologies work together simultaneously, from the moment a file is loaded. It's a unique combination of intelligence-led technologies that deliver multi-layered, comprehensive threat detection and prevention across endpoints and other IT infrastructure elements.

DETECTING KNOWN THREATS

From the moment a file is about to be downloaded, web page opened or application launched, Kaspersky Lab's advanced anti-malware engines 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. Beginning with known threats, at its core, these engines comprise:

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 activity.

BLACKLISTING

Dedicated teams of malware analysts keep Kaspersky Lab's databases up to date with the latest malware signatures and data. These are used to automatically block all known malware.

URL FILTERING

Scans and checks URLs in inbound/outbound traffic against Kaspersky Lab's database of known malicious and phishing sites, blocking web-based attacks, server-side polymorphic malware and command and control (C&C) servers.

FIREWALL

Analyzes every packet entering and leaving the network, blocking or allowing them, depending on the security risk. 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.

Kaspersky Lab's signature-based technologies are built on years of accumulated knowledge and experience. According to Virus Bulletin's November 2014 test, Kaspersky Lab's anti-spam technology scored first place with a detection rate of 99.75% and zero false positives. All of the above technologies excel at blocking known malware (and thanks to Kaspersky Security Network, as described later, many threats stay unknown for only a short period of time). But what about the elusive unknown or advanced threats we mentioned earlier? We've got that covered, too.

DETECTING UNKNOWN THREATS

Once any file has passed through the signature-based checks for known threats, it's time to take a look at what happens at the moment of the launch attempt. Kaspersky Lab's multi-layered, proactive technologies analyze and check files as they execute, searching for suspicious or malicious activity that suggests an unknown threat is at play.

HEURISTICS

Heuristic analysis provides proactive protection from threats that can't be detected using conventional antivirus databases. Kaspersky Lab's heuristics enable the detection of new malware or unknown modifications to known malware. Static analysis scans code for signs of suspicious commands associated with malware, while dynamic analysis examines the machine code the file might try to execute, responding to emulated calls with likely answers to establish whether the code is safe or not.

HEURISTIC ANTI-PHISHING

In extremely new phishing attacks where only a small number of users have been affected, Kaspersky Lab's technology can look for additional evidence of suspicious activity, such as vocabulary, input forms or unreadable sequences of symbols. This is in addition to the more traditional, database-led approach described earlier.

Phishing-based threats have been the starting point for many recent, highly dangerous advanced threats.

HOST INTRUSION PREVENTION SYSTEM (HIPS)

Kaspersky Lab's HIPS adds an additional layer of protection, detecting and managing suspicious applications and activity, preventing threats from launching. HIPS helps control how applications behave, setting trust levels after the initial analysis. These levels define what resources they can use, what kind of data they can access or modify, etc. It restricts execution of potentially dangerous programs without affecting the performance of authorized, safe applications. An untrusted application will not be allowed to do anything – including launch.

APPLICATION CONTROL AND WHITELISTING

Application control blocks or allows administrator-specified applications. Kaspersky Lab's approach is built on Dynamic Whitelisting – continuously updated lists of trusted applications and software categories that are only allowed to run according to specified rules and policies. Kaspersky Lab has a dedicated whitelisting lab and database of more than one billion files, growing at a rate of one million per day.

Application Controls and Whitelisting reduce the risks posed by threats we don't yet know about; 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.

KASPERSKY SECURITY NETWORK

Acting as a global, cloud-based threat laboratory, Kaspersky Security Network detects, analyzes and manages known, unknown and new threats and online attack sources in seconds – and delivers that intelligence straight to customer systems.

Using real-time, anonymized data from 60 million endpoint sensors 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; working together with all the other components of Kaspersky Lab's engine, Kaspersky Security Network enables protection from unknown threats before signatures are available – traditional signature-based responses can take several hours, Kaspersky Security Network takes about 40 seconds.

DETECTING ADVANCED THREATS

Your file has been downloaded and started; Kaspersky Lab technologies have scanned, analyzed, applied intelligence and either blocked or allowed based on both known and unknown threats.

But what about Advanced Threats?

Kaspersky Lab's advanced threat detection technologies are designed to detect and block advanced threats, using a range of proactive, sophisticated behavioral mechanisms that monitor process behaviors, discern suspicious patterns, block malicious activities and roll back harmful changes, including Cryptors.

Let's take a look...

SYSTEM WATCHER

This monitors and collects data on application and other important system activities using tracking activities and discerning behavioral patterns. This information is provided to the other Kaspersky Lab protection components we've described. Any activity that corresponds to threat patterns is dealt with according to administrator-set policies – or use the default setting, which is to terminate the malicious process and quarantine for later analysis.

The driver that intercepts file operations for Kaspersky's anti-malware 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.

Malicious actions and destructive behavior patterns suggestive of malware are blocked.

AUTOMATIC EXPLOIT PREVENTION (AEP)

This technology specifically targets malware that exploits software vulnerabilities. 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 acts like a safety net, an extra layer of security that complements Kaspersky Lab's other technologies. It works in conjunction with Kaspersky Lab's System Watcher.

ROLLBACK

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 mechanisms are updateable and work with created and modified executable files, MBR modifications, important Windows® files and registry keys.

DEFAULT DENY

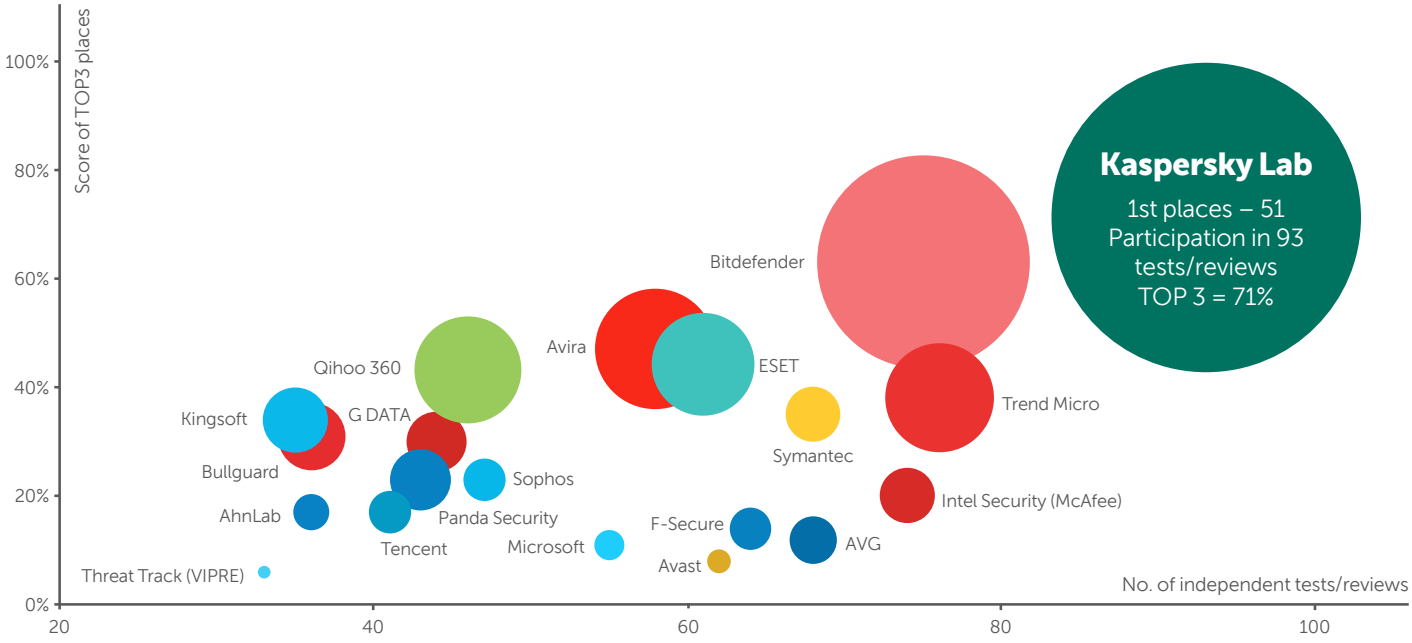
Increasingly viewed as the most effective security posture to adopt in the face of ever-evolving, advanced threats. It simply blocks all applications from running on any workstation – unless they've been explicitly allowed by the administrator.

Default Deny means all new, file-based malware varieties are automatically blocked, even for targeted attacks.

A SMALL CHANGE CAN MAKE A BIG DIFFERENCE

As we've seen, even a single additional percentage point in detection rate can translate into hundreds of thousands of pieces of malware slipping through the nets. We've also seen how Kaspersky Lab's additional nets of mitigation, detection, and analysis can catch unknown and even advanced threats before they can do their work.

KASPERSKY LAB: BEST IN THE INDUSTRY PROTECTION*



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.

Independent test results consistently demonstrate that Kaspersky Lab provides the best protection in the industry. In 2014 alone, we participated in 93 independent tests and reviews, ranking first 51 times and finishing in the top three a record 71 percent of the time. That's just one of the reasons why OEMs – including Microsoft, Cisco Meraki, Juniper Networks and Alcatel Lucent – trust Kaspersky Lab to provide the security they ship within their own products.

All of Kaspersky Lab's security technologies are developed and maintained in-house, from the same code base, meaning they all integrate seamlessly with each other, building a multi-layered platform that's greater than the sum of its parts.
This level of integration also translates into enhanced performance, faster updates and a unified look and feel across all solutions – giving you time to focus on what you do best, while Kaspersky Lab takes care of security.

* 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.

GET STARTED NOW: FREE 30-DAY TRIAL

Discover how our premium security can protect your business from malware and cybercrime with a no-obligation trial.

Visit **kaspersky.com/trials** today to download full product versions and evaluate how successfully they protect your IT infrastructure, endpoints and confidential business data.

GET YOUR FREE TRIAL NOW

JOIN THE CONVERSATION

Watch us on YouTube

Like us on Facebook

Follow us on Twitter

Join us on LinkedIn

View us on SlideShare

Review our blog

Join us on Threatpost

View us on Securelist

ABOUT KASPERSKY LAB

Kaspersky Lab is the world's largest privately held vendor of endpoint protection solutions. The company is ranked among the world's top four vendors of security solutions for endpoint users*. Throughout its more than 17-year history Kaspersky Lab has remained an innovator in IT security and provides effective digital security solutions for large enterprises, SMBs and consumers. Kaspersky Lab, with its holding company registered in the United Kingdom, currently operates in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide. Learn more at www.kaspersky.com.

* The company was rated fourth in the IDC rating Worldwide Endpoint Security Revenue by Vendor, 2013. The rating was published in the IDC report "Worldwide Endpoint Security 2014–2018 Forecast and 2013 Vendor Shares" (IDC #250210, August 2014). The report ranked software vendors according to earnings from sales of endpoint security solutions in 2013.