

# THE SECURE ENTERPRISE

Technologies and strategies to help  
keep your business running smoothly

**KASPERSKY**<sup>®</sup>

THE POWER OF PROTECTION

[kaspersky.com/enterprise](https://kaspersky.com/enterprise)  
#EnterpriseSec



Eugene Kaspersky  
Chairman and CEO, Kaspersky Lab

## PROTECTING TODAY, SECURING THE FUTURE

**Every day, billions of people access and share information online. Data moves constantly between businesses, employees, customers and suppliers – all over the world.**

All this connectivity brings enormous commercial benefits, but also presents a considerable and growing risk to security. New cyberthreats emerge daily – threats that can have a devastating impact on us as individuals, businesses and societies.

For many years I've been working closely with governments and law enforcement agencies around the globe advising on the dangers we face and the crucial importance of cybersecurity. Unfortunately, the threats are becoming increasingly sophisticated. We only have to look at some of our most recent discoveries – including Carbanak, Equation and Darkhotel – to see how the threats are evolving.

Preventing cyberwar and cyberterrorism is already high on the agenda of our world leaders. While for enterprises, now is the time to revisit their IT security strategies – to ensure they meet the demands of today's complex and ever more challenging environment.

As a security company, we know it's not enough to react to new threats as and when they arise. That's why we invest so much of our resources and effort into our world-leading threat research. We never stop anticipating and preventing IT security threats, while our multi-layered protection technologies are designed to capitalise on our extensive global security intelligence. Our approach is simple: better intelligence combined with better technology results in better security.

**“WE ARE ALWAYS READY TO COUNTER CYBERCRIME, REGARDLESS OF ITS ORIGIN, TARGET OR SOPHISTICATION. THE EFFECTIVENESS OF OUR SOLUTIONS IS MADE POSSIBLE BY THE FUSION OF OUR PROVEN TECHNOLOGICAL CAPABILITIES AND OUR WORLD-LEADING SECURITY THREAT RESEARCH. THIS COMBINATION PRODUCES RESULTS THAT ARE UNMATCHED BY ANY OTHER IT SECURITY ORGANISATION.”**

Nikita Shvetsov  
Chief Technology Officer  
Kaspersky Lab

Malware affects everyone – from individuals to large enterprises and governments. Cybercriminals are using increasingly sophisticated weapons to defraud businesses, steal data and achieve financial gain. Cyberterrorism and cyberwar are now a reality and, while a growing number of cyberattacks are politically or socially motivated, cyberterrorists and hacktivists are targeting businesses.

Global organisations are being subjected to targeted attacks – so called ‘Advanced Persistent Threats’ (APTs) – from sophisticated and determined groups of criminals. Although many of these high-profile attacks are well-reported, the trend is for attackers to use stealthy techniques – so the attack can evade detection and continue to access sensitive or commercially valuable data.

#### **OUR STRATEGY**

At Kaspersky Lab, our strategic and R&D focus is on where emerging threats lie – and where organisations are most vulnerable.

Our heritage and expertise has always prioritised the protection of endpoints. Today, the range of endpoints is more varied – including physical, mobile and virtual endpoints, and even critical national infrastructure – and all of those endpoints are more exposed than ever before.

We help large organisations to protect these vulnerable areas – by using an approach that harnesses our advanced threat intelligence to deliver a higher standard of protection.

#### **TECHNOLOGY LEADERSHIP**

Though distinct, these threats don’t exist in isolation. Together, they form part of a wider security landscape. The ability to overcome any of these threats requires a deep understanding of all of the threats. Security solutions must be built on extensive and predictive security intelligence – not single-purpose offerings designed with a narrow focus.

We believe that creating effective security solutions requires the broadest possible perspective. This principle guides our technology strategy and results in organically built, integrated solutions that deliver superior protection and better performance. Again, better intelligence combined with better technology results in better protection.

One key element in our security intelligence is the Kaspersky Security Network (KSN). It receives vast amounts of cyberthreat data on evolving malware of all types, from all corners of the globe. This data – coupled with analysis from our world-renowned Global Research and Analysis Team (GReAT) – means we’re uniquely placed to deliver solutions that not only neutralise present threats but also help to defeat future dangers. So our customers benefit from protection against the latest threats.

#### **THE KASPERSKY SECURITY NETWORK**

- A complex, distributed infrastructure that’s dedicated to processing depersonalised cybersecurity-related data streams from millions of voluntary participants around the world
- Approximately 60 million voluntary participants
- 600,000 data requests per second
- Average response time to a front end request: 0.02 seconds

## **IN THE FACE OF INCREASINGLY SOPHISTICATED AND EVASIVE ATTACKS, STANDARD FIREWALLS AND ANTI-MALWARE TECHNOLOGY ARE NO LONGER ENOUGH. DEEPER AND MORE PERVASIVE TOOLS ARE NEEDED.**

IT departments in large organisations face twin challenges: ever greater IT complexity and ever more sophisticated threats. The IT team's task is made all the more daunting by the vast array of applications and devices used within the typical corporate network – and by the growing number of employees conducting business over the web and through social media platforms.

Today, enterprises need more comprehensive and precisely managed IT security.

Kaspersky Lab's enterprise-level endpoint security solutions incorporate flexible control tools, data encryption and systems management functionality.

Application Control, Device Control and Web Control make it easier to enforce security policies. In addition, our Dynamic Whitelisting helps to authenticate applications and protect data and devices from malicious code and malicious websites. By combining Application Control and Dynamic Whitelisting, we help enterprises to roll out a Default Deny policy – whereby only trusted applications are allowed to launch on the business's corporate network.


Our powerful data encryption functionality helps to protect confidential and sensitive information within files, folders, disks and removable devices. If a laptop or mobile device is lost or stolen, it needn't lead to the leakage of sensitive data. With the data encrypted into an unreadable form, your business is less likely to suffer the embarrassment and costs associated with data security breaches.

In addition, the cloud-based Kaspersky Security Network continually receives global threat intelligence – to help ensure enterprises are protected against the very latest threats.

Because we believe that managing a complex IT environment doesn't have to be a complex task, we also offer a broad array of systems management functionality. By automating key security and administration tasks, delivering improved visibility and providing a single management console, we help IT personnel to free up time for other mission-critical projects.



**94% OF COMPANIES HAVE EXPERIENCED SOME FORM OF EXTERNAL SECURITY THREAT.<sup>1</sup>**



**IN 2014 ALONE,  
KASPERSKY LAB  
DEALT WITH ALMOST  
1.4 MILLION UNIQUE  
MOBILE MALWARE  
ATTACKS.<sup>2</sup>**

## **OVER THE LAST FOUR YEARS, 30% OF COMPANIES HAVE EXPERIENCED THE THEFT OR LOSS OF A MOBILE DEVICE – AND IT’S STILL THE SECOND MOST COMMON WAY FOR A COMPANY TO LOSE ITS DATA.<sup>3</sup>**

With the rise of flexible working and ‘Bring Your Own Device’ (BYOD) policies, enterprises need to ensure their security protects against cyberthreats regardless of whether users are in the office or out and about.

The amount of malware aimed specifically at mobile devices is growing exponentially. Even a one-time breach of a single phone or tablet can compromise the security of an entire corporate network. Whether it’s the result of a drive-by attack from an infected web page that the user has visited, a malicious app the user has downloaded or the physical loss of a mobile device, the damage can be considerable.

In addition, the wide range of device types – and the obvious portability of the devices – can significantly add to security management burdens.

Kaspersky Security for Mobile delivers rigorous security technologies – including advanced anti-malware, plus application control and anti-theft features – to help protect corporate networks and corporate data against a wide range of mobile threats.

A single unified management console gives enterprises centralised visibility and control over all of the Kaspersky Lab endpoint security technologies that are running on their physical, virtual and mobile endpoints.

<sup>2</sup> <http://securelist.com/analysis/kaspersky-security-bulletin/68010/kaspersky-security-bulletin-2014-overall-statistics-for-2014/>

<sup>3</sup> 2014 Global IT Risks Report, Kaspersky Lab

# KASPERSKY LAB PRODUCTS DETECTED AND NEUTRALISED A TOTAL OF 6,167,233,068 THREATS, OVER A 12-MONTH PERIOD.<sup>4</sup>

Almost every enterprise is faced with having to store increasing volumes of data, while also maintaining data access and ensuring security.

Two key technologies are vital in boosting the efficiency of data storage and data management within data centers: virtualization and storage systems. However, when it comes to security threats, these technologies are often more vulnerable than other components in a data center.

We offer solutions that focus on protecting these two essential areas of the data center. We have security products that ideally suit multi-hypervisor environments and all popular storage systems:

- Specialised security for all major virtualization platforms, including VMware, Citrix and Microsoft
- Security for both NAS and SAN storage systems – including EMC, NetApp and Hitachi

These solutions are designed to provide comprehensive security that addresses the majority of risks in data centers of any configuration – even data centers that partly operate within public clouds, such as Amazon or Microsoft Azure.

Furthermore, because improved manageability helps to reduce costs and release precious IT resources for strategic business initiatives, we also provide a central management console that gives administrators control over a wide range of tasks – including remote installation and configuration, plus reporting – for both of these security solutions.

# BY YEAR-END 2016, UP TO 85% OF ON-PREMISES X86 SERVER OS WORKLOADS WILL BE VIRTUALIZED.<sup>5</sup>

Virtualization has transformed large, complex IT environments, bringing considerable benefits to enterprises.

However, with the growth in cyberthreats, enterprises must protect their virtual environments just as fully and effectively as they protect their physical IT assets. With many organisations now extending their virtualization initiatives – and virtualizing business-critical systems – there's even more at stake.

Adding security functionality into any IT system – physical or virtual – will involve some level of resource consumption. So our aim is always to maximise protection, while minimising the impact on resources. This issue is particularly critical for virtual infrastructure, as resource efficiency is the primary driver for implementing virtualization. Unless the right balance is struck between security and efficiency, many of the benefits of virtualization can be undermined.

Kaspersky Security for Virtualization has been developed specifically for virtual machine security. By delivering security that places less load on computing resources, it helps businesses to maintain high virtualization density and high performance – for improved return on investment.

Instead of having to install a full-sized security agent on every virtual machine, Kaspersky Security for Virtualization offers a more efficient way to protect virtualized environments – to help minimise the load on processors, memory, storage and I/O, while taking into account the specific requirements of virtual environments.

<sup>5</sup> Gartner Forecast Overview: Enterprise Infrastructure Software, Worldwide.  
Published: 15 August 2014

# DDoS ATTACKS IN Q2 2014 WERE UP A TOTAL OF 22% FROM THE SAME PERIOD THE PREVIOUS YEAR.<sup>6</sup>

Cybercriminals use Distributed Denial of Service (DDoS) attacks to disable an organisation's online presence or its key business processes. While the direct financial costs of a DDoS attack can be massive, victim organisations can also suffer severe damage to their brand and reputation – especially if downtime for business-critical infrastructure and processes adversely affects customer service over an extended period.

In recent years, the cost of launching a DDoS attack has reduced – and that has resulted in significant growth in the volume of attacks. At the same time, many of the attacks have become much more sophisticated.

Unlike malware attacks that tend to propagate automatically, today's sophisticated DDoS attacks rely on human expertise – and that can make DDoS attacks particularly difficult to defeat. This means it's essential to deploy defences that are built on an intelligence-led approach.

Kaspersky DDoS Protection delivers a total, integrated DDoS attack protection and mitigation solution that takes care of every stage that's necessary to defend a business against all types of DDoS attacks. Our solution includes 24x7 analysis of all of our customer's online traffic, through to alerting about the possible presence of an attack, receiving the customer's redirected traffic, cleaning that traffic and returning 'clean' traffic to the business. In addition, we generate post-attack reports and analysis.

We're the first anti-malware vendor to offer a DDoS protection solution. Because we provide a unique combination of statistical analysis, behaviour analysis and DDoS attack intelligence, we deliver a more thorough defence against DDoS attacks.

<sup>6</sup> Prolexic Quarterly Global DDoS Attack Report Q2 2014





# BY 2018, 40% OF LARGE ENTERPRISES WILL HAVE FORMAL PLANS TO ADDRESS AGGRESSIVE CYBERSECURITY BUSINESS DISRUPTION ATTACKS, UP FROM 0% IN 2015.<sup>7</sup>

Modern enterprises have to process ever-increasing volumes of information. Much of that data may be sensitive or can have significant commercial value – and cybercriminals fully realise this. By launching Advanced Persistent Threats (APTs) against a specific target, cybercriminals can steal confidential information and even spy on an organisation's employees.

Because APTs are much more complex than single items of malware, they're much harder to detect and block. Each APT attack is tailored to achieve specific objectives – against a specific target organisation – and will usually include several processes that perform different stages of the attack. Typically, the attacker will also aim to ensure the security breach remains undetected – so the data theft can continue over an extended period.

Only a few years ago, the high cost of developing an APT meant that relatively few attacks were being implemented. However, the cost of launching an APT attack has fallen to a level where cybercriminals now regard APTs as a cost-effective way to attack enterprises.

Because there's a major element of human ingenuity involved in tailoring and implementing an APT attack, high-quality security intelligence is a vitally important factor in successfully defeating these threats.

Kaspersky Lab has been credited as the first to detect many of the world's most dangerous APTs – and we regard threat intelligence as the essential foundation for building efficient protection technologies for endpoints and networks. We believe that combining intelligence and security products and services enables a powerful, multi-layered counter-APT strategy that helps to block security gaps, rapidly identify when a 'live' attack is underway, block threats and deliver post-attack forensic analysis.

<sup>7</sup> Gartner, Attack on Sony Pictures Is a Digital Business Game Changer. Published: 9 February 2015

## KASPERSKY INDUSTRIAL SECURITY SOLUTION

Protecting the public and protecting society

In the past, industrial control systems were isolated and the industry thought that was sufficient to keep their infrastructure secure. In reality, isolation has never been enough to guarantee security. As recent high-profile cases have shown, attacks can come from anywhere – and even control of a nuclear facility can be lost to malware introduced through a USB port.

Today, the need to connect systems to the Internet introduces a whole new set of vulnerabilities – and, if a network is attacked by malware, the consequences can be catastrophic.

Although many cyber-weapons are designed with specific targets in mind, they can go on to affect other organisations. After a new cyber-weapon has been launched, that same cyber-weapon can fall

into the hands of any number of groups with hostile agendas – and the weapon can be repurposed to attack new targets.

All critical infrastructure needs the highest possible level of protection against a growing range of threats.

As a leader in the fight against cybercrime, Kaspersky Lab has unparalleled insight into the threats facing the world – plus the expertise to neutralise those threats. In partnership with governments and private-sector bodies, we help to create the multi-layered defences that are necessary to protect critical infrastructure. We recognise that critical infrastructure needs a different level of protection.

For industrial networks, process continuity always takes precedence over data confidentiality and data integrity. We're leading the industry in the development of secure infrastructure solutions, specialised protection for PLCs and more integrated SCADA protection layers.

# 40% OF INDUSTRIAL SECTOR IT PROFESSIONALS REPORTED IDENTIFIED OR SUSPECTED BREACHES – UP FROM 28% IN 2013.<sup>8</sup>

<sup>8</sup> SANS Institute: 2014 Control System Security Survey

<sup>9</sup> Cyberthreats to ICS systems: you don't have to be a target to become a victim. Industrial Security 2014, Kaspersky Lab



**40% OF MALWARE ATTACKS ON INDUSTRIAL FACILITIES RESULT IN AT LEAST FOUR HOURS' DOWNTIME.<sup>9</sup>**

**73% OF BUSINESSES CONSIDER A BANK'S REPUTATION FOR SECURITY WHEN CHOOSING WHO TO TRUST WITH THEIR ACCOUNTS.<sup>10</sup>**

**82% SAID THEY WOULD CONSIDER LEAVING A BANK THAT SUFFERED A DATA BREACH.<sup>11</sup>**

Even though banks already have some level of fraud protection, is it really enough to keep a bank safe and preserve valuable client relationships?

Every bank's online financial services are under threat. Hundreds of millions of dollars are at stake. Any security incident can cost a bank money and time – and jeopardise long-term relationships with loyal clients. Today, security systems that were relied upon in the past can only do so much. People remain the weakest link in the security chain and it takes proactive protection to stop a simple mistake turning into a costly crisis.

Kaspersky Fraud Prevention adds a vital defensive layer to a bank's existing fraud protection. It takes care of bank customers that use a PC or a Mac – via Kaspersky Fraud Prevention for Windows and Kaspersky Fraud Prevention for Mac – and Kaspersky

Fraud Prevention mobile SDK helps to protect users who prefer to access their bank accounts from mobile devices.

Kaspersky Fraud Prevention does more than remediate after a fraud incident – it enables banks to take proactive steps to stop fraudsters before they can do any harm. It actively stops cybercriminals from stealing users' data – helping to eliminate the causes of fraud.

In addition, our intelligence helps ensure our banking clients remain protected – despite the constantly changing threat landscape.

**JUST 51% BELIEVE THAT FINANCIAL ORGANISATIONS DO ENOUGH TO PROTECT SENSITIVE INFORMATION.<sup>12</sup>**

## KASPERSKY SECURITY INTELLIGENCE SERVICES

For emerging threats – forewarned is forearmed

# KASPERSKY LAB AUTOMATICALLY PROCESSES OVER 325,000 NEW MALWARE SAMPLES EVERY DAY.

With cyberattacks becoming ever more widespread and sophisticated – and the criminals behind them constantly innovating – it's not enough to take a reactive stance. Unless a business's IT security team fully understands the nature of the threats it faces, defending against those threats may be impossible.

By sharing our up-to-the-minute intelligence with our customers, we help businesses to guard against threats. Our broad range of intelligence services helps ensure a business's security operations centre (SOC) or IT security team is equipped to protect the business from the latest online threats.

Even if your business does not use any Kaspersky Lab products, you can still benefit from our Security Intelligence Services.

Kaspersky Lab's Security Intelligence Services constantly monitor the threat landscape – identifying emerging dangers and taking steps to defend and eradicate. So, whatever the scale of the threat – from phishing emails impersonating a brand to the latest global trend in cybercrime – our clients benefit from access to the latest security intelligence.

In addition to 'raw intelligence' and tailored reports, our experts are also available to investigate attacks launched against a specific client. In such cases, our experts will identify the perpetrators, analyse their methods and determine how the threat can be nullified.

We also offer education services that provide SOCs with the knowledge they need to detect and counter attacks before damage is caused.

The range of Security Intelligence Services we offer includes:

- Threat Intelligence
  - Threat Data Feeds
  - Botnet Threat Tracking
  - Intelligent Reporting
- Education Services
  - Cybersecurity Fundamentals
  - Digital Forensics
  - Malware Analysis and Reverse Engineering
- Investigation Services
  - Malware Analysis
  - Digital Forensics
  - Incident Response

**THE TARGETED CYBERATTACK LOGBOOK**  
<[HTTPS://APT.SECURELIST.COM/](https://APT.SECURELIST.COM/)>  
**CHRONICLES GROUND-BREAKING MALICIOUS CYBER CAMPAIGNS INVESTIGATED BY KASPERSKY LAB'S GLOBAL RESEARCH & ANALYSIS TEAM (GREAT).**



**WHY KASPERSKY LAB?**  
A global perspective



**THE POWER OF PROTECTION**

# WORLD-LEADING PROTECTION AGAINST KNOWN, UNKNOWN AND ADVANCED THREATS.

Kaspersky Lab operates in more than 200 countries and territories worldwide, and our technologies protect over 400 million people and 270,000 organisations. We employ over 3,000 highly qualified specialists, led by our chairman and CEO – Eugene Kaspersky – who has earned many international accolades, including being named a Top Global Thinker by Foreign Policy Magazine in 2012.

Our Global Research and Analysis Team (GReAT) is made up of the industry's elite analysts. It's an integral part of our R&D department and the team provides leadership in anti-threat intelligence, research and innovation – both internally and externally. Our customers also benefit from the Kaspersky Security Network, which processes cybersecurity-related data in real time – to give us early visibility of new threats and allow us to develop countermeasures.

In addition to helping enterprises and individuals to protect themselves from cybersecurity threats, we also cooperate with respected international and local organisations. Our work with INTERPOL and Europol – as well as national and regional law enforcement agencies – focuses on implementing countermeasures that disrupt malware operations and cybercriminal activity.

During our investigations, our technical experts analyse all elements of an attack – from its infection vectors and malware components, to its command and control infrastructure and exploitation methods. The insights we gain feed into all of our solutions – helping us to detect and remediate malware attacks, regardless of their origin or purpose.

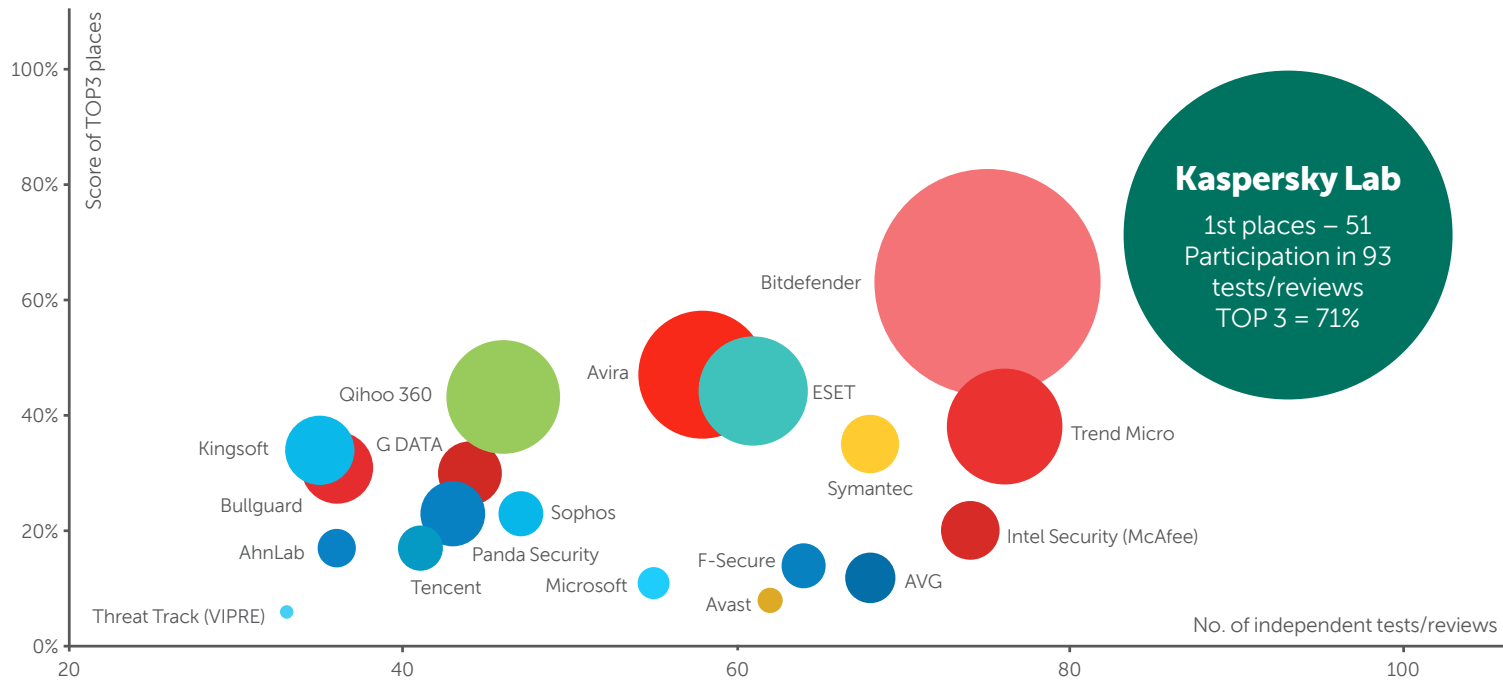
Right now, we're developing a secure operating system and we're also working on solutions to protect against the potentially devastating impact of attacks on critical infrastructure.

It's no exaggeration to say that it's our mission to save the world from cybercrime:

- 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. On 51 occasions, our products took first place – and 71% of tests rated Kaspersky Lab in the top three.
- Over a third of our staff work in R&D – delivering a 38% growth in technology patents from 2012 to 2013.
- We were the first to discover many of the world's most sophisticated threats, including Carbanak, Equation, DarkHotel, Regin, Duqu, Flame, Gauss, Red October, Icefog and The Mask.
- Approximately 120 industry-leading companies trust us to help protect their customers – including using Kaspersky Lab for technology integration, private labelling or co-branded products, pre-installation and bundling of our products.

**IN 2014 KASPERSKY LAB PRODUCTS PARTICIPATED IN 93 INDEPENDENT TESTS AND REVIEWS. OUR PRODUCTS WERE AWARDED 51 FIRSTS AND RECEIVED 66 TOP-THREE FINISHES.<sup>13</sup>**

# **KASPERSKY LAB PROVIDES BEST IN THE INDUSTRY PROTECTION\***



\* 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: Test labs: 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.

<sup>13</sup> [http://media.kaspersky.com/en/business-security/TOP3\\_2014.pdf](http://media.kaspersky.com/en/business-security/TOP3_2014.pdf)

# PROTECTING TODAY, SECURING THE FUTURE

An increasingly sophisticated and complex threat landscape calls for a multi-layered security platform that defends against known, unknown and advanced threats.

Visit [kaspersky.com/enterprise](https://kaspersky.com/enterprise) to find out more about Kaspersky Lab's unique expertise and Security Solutions for Enterprise.

[FIND OUT MORE](#)

## 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](http://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.

## JOIN THE CONVERSATION

*#EnterpriseSec*



Watch us on  
YouTube



Like us on  
Facebook



Follow us on  
Twitter



Join us on  
LinkedIn



Review  
our blog



Join us on  
Threatpost



View us on  
Securelist