KASPERSKY lab

GLOBAL IT SECURITY RISKS SURVEY

2015

usa.kaspersky.com/business-security

Global IT Security Risks Survey 2015: The current state of play

Now in its 5th year, Kaspersky Lab's Global IT Security Risks Survey collects insights from IT professionals around the world. Conducted by research specialists B2B International and analyzed by Kaspersky Lab's expert threat intelligence and research teams, the report is an essential look at the industry's prevailing attitudes and strategies towards IT security. It also serves as an industry benchmark to help businesses understand the type and level of IT security threats they face.

Why read this report?
- It spans global and cross-sector findings
- It gives you exclusive insight into the views, opinions and strategies of IT professionals from around the world
- It helps you benchmark your IT security against industry peers

The survey in summary:
- 5564 respondents
- 38 countries
- Concerning April 2014 to May 2015
- Surveyed IT professionals with a 'good working knowledge' of IT issues

Executive Summary

This year has seen another cavalcade of high profile cyber attacks making headlines. With them has come an increasing awareness among businesses that, along with the attacks that make waves in the press, there are a wide range of 'quieter' threats that are a danger to their operations.

In particular, there's a growing realization that in our hyper-connected world, it's not just their own security that businesses should be concerned with. Consequently, the vulnerability of third parties – especially those connected to financial transactions – has risen up the agenda.

For instance, of those surveyed this year, **72%** would pay close attention to a bank's security record before choosing to work with them. Furthermore, **90%** of larger organizations would happily pay a premium to make their transactions more secure.

Of course, money is far from the only resource businesses need to protect. As the IT landscape changes and more and more data moves outside the companies it belongs to, there are concerns that Software as a Service (SaaS) providers aren't doing enough to keep it secure. It's an issue **37%** of respondents cited as a worry.

In some respects this awareness of threats has been met with a proactive response. There's been a **15%** rise in the deployment of anti-malware software and **66%** of businesses are now protected with a fully implemented security solution.

However, many are still opting for a one-size-fits-all approach, rather than a joined up strategy that takes into account the need for specialized protection. For instance, use of anti-malware on mobile devices is down **8%** and only **26%** of respondents with a virtualized environment protect it with a tailored solution.

This lack of investment seems to be down to a perceived lack of value. But this is nothing new. The value of security has always been most apparent in hindsight and many organizations are failing to grasp how much a breach could hurt them. The average cost of a data breach for **SMBs** and **Enterprises** stands at **$38k** and **$551k** respectively and **60%** of businesses that suffer a breach find their ability to function severely impaired.

It's time for businesses to recalibrate the way they think about their security budgets. Seen as a separate expense to IT infrastructure, it appears hard to justify until disaster strikes. But understood as an essential part of the IT environment – including mobile devices and virtualized machines – its value is obvious, especially in the context of the damage and huge costs it can prevent.

GReAT insight

"The Carbanak attack, uncovered early in 2015, has made it clear that cybercriminals are now focusing their efforts on financial institutions as well as other types of business."

Perception versus reality

As an IT decision maker, you're responsible for keeping your organization's IT network secure. It's your job to protect private and sensitive data, and to safeguard your business assets across physical, virtual and mobile devices.

It's safe to say that security is high on the agenda for businesses of all sizes, globally. In our 2015 Global IT Risk survey, **50%** of IT professionals listed security as a top three concern. But are they satisfied with their current level of IT protection? Not really. Almost half of organizations surveyed (**47%**) felt their IT security didn't meet expectations when it came to safeguarding their financial transactions.

In the last 12 months, organizations have significantly bolstered their provision for anti-virus and anti-malware software, with many reporting that they are now 'fully' protected. And enterprise companies are already responding to the need to adopt a wider suite of security measures.

It's no wonder really, given that **32%** of businesses believe that they've been the subject of a targeted attack, either in the past or at the time of this survey being conducted. In other words, nearly one in three companies fear that they've suffered a data breach – a rise of **7%** from this time last year. This correlates with the insight that **52%** also think that their organization needs to improve its incident response plans for data breach and IT security events.

Currently, **46%** of businesses believe the number of attacks on companies like theirs is increasing – a drop of **3%** from last year. More people believe there's been no change in the number of attacks, up from **39%** to **44%** in the last year. And **10%** think there's been a drop in the number of attacks, down from **11%** in the previous two years. Also, perceived crypto attacks against our respondents are up from **37%** to **45%** in the last year.

There are, of course, contrasts within the data. In general, IT professionals in Russia and China don't perceive the threat landscape to be getting more dangerous. Yet, those in Emerging Markets feel the threat is growing.

47% of businesses want banks to improve the security of online transactions. In other words, they don't feel that banks are doing enough to secure payments and are worried that cybercriminals could hack into their infrastructure and steal funds. They're losing confidence in what should be the easiest, safest and most convenient way to send and receive money.

And more worryingly, there's a growing lack of trust between businesses and third-party SaaS providers. **37%** are concerned that these platforms aren't secure and provide an easy way for cybercriminals to infiltrate their IT network. That's an increase of **4%** on last year and – as more companies move their day-to-day operations to the cloud – it's a percentage that could rise further.

Talking of outside interferences, **42%** are concerned about increased government involvement in their IT. This figure has risen **4%** in the last year and is particularly high in China (**50%**), the Eastern Markets (**46%**) and APAC (**50%**).

Threat levels – heading in the right direction?

First of all, let's get the bad news out of the way. In the past year, over **90%** of businesses have experienced some form of external threat. The severity of these threats ranges from the minor to the extreme, but for a business operating today, it's a very unsettling statistic.

22% of businesses lost data as a result of an external threat. But the good news is that, in the past year, there have been fewer instances of theft and 'obvious' malware than the year before. Plus, the number of organizations losing data as a result of malware fell from **33%** to **25%**.

GReAT insight

"While the headlines tend to focus on attacks on large organizations, the truth is that organizations of all sizes are potential victims of cybercriminals, looking to steal intellectual property, customer data or gain a foothold in another organization that does business with the victim company."

The changing nature of attacks

During the same period, 9% of businesses experienced targeted attacks, rising to 15% in enterprise and more than half of them (53%) reported losing sensitive data as a result.

However, **4%** fewer companies reported phishing attacks, **3%** fewer reported network intrusion or hacking, and **9%** fewer reported the theft of mobile devices by an external party. In fact, apart from only a few instances where perceived attacks have remained unchanged or increased by one or two per cent, attacks have decreased around the world.

In China and Western Europe the theft of mobile devices by an external party dropped by as much as **12%**. In North America, a perceived fall of **10%** in malware and other malicious programs was the second highest in the world after China with **13%**.

The fall in mobile thefts may be due to better encryption being implemented on mobile devices in the past year. The reason for the perceived decline in malware is most likely down to businesses simply not realising that a data loss event has occurred – a result of the ever more complex and stealthy techniques being implemented by cybercriminals. Even so, **54%** still say that they are much more concerned about the security of mobile devices than they were a year ago.

> **54%** still say that they are much more concerned about the security of mobile devices than they were a year ago.

Now, let's turn our attention to internal threats. **21%** of organizations have lost sensitive data from internal threats in the past year. And **73%** have had an internal security incident in 2015. The top threats came from software vulnerabilities and accidental actions by staff, including mistakenly leaking or sharing data. **30%** of

> **73%** have had an internal security incident in 2015.

respondents admitted that they experienced threats connected with vulnerabilities in existing software. But the problems may lie deeper, with **46%** of respondents unsure whether senior (non-IT) personnel within the organization have a good understanding of the IT security risks their companies face.

> **46%** of respondents are unsure whether senior (non-IT) personnel within the organization have a good understanding of the IT security risks their companies face.

But there's better news here, too. Accidental leaks or sharing of data has decreased by **6%** in the past year; and incidents from vulnerable or flawed software are down **2%** from last year and **8%** from two years ago. And data loss from lost or stolen mobile devices has fallen by **7%**. The drop in theft incidents seems to indicate that employees are becoming more careful with their company-provided devices when they're out and about.

One emerging issue, though, is that of trust between companies and the third party suppliers they use. There's been a strong upward trend in organizations reporting security incidents in which such partners were implicated, particularly in industries with high levels of outsourcing, such as IT or Manufacturing.

GReAT insight

"Not only is the number of targeted attacks still growing, but more worryingly the methods and skills of their developers are improving each year. They are becoming harder to detect and are sometimes almost impossible to get rid of."

What we're doing – a slow wake up call

Businesses today face a growing number of threats from increasingly clever cybercriminals intent on outwitting their victims in ever more complex ways.

The problem for these companies is that using a one-size-fits-all solution is no longer sufficient to defend against today's threats – attacks on IT networks are simply too strong and persistent.

Malware is a particularly persistent problem. It's quick to evolve and changes every day, so it's very hard to combat. But more and more businesses are becoming savvy to it, which is why in the past year there's been a **15%** rise in anti-malware software deployed on workstations. **66%** of businesses today are now protected with a fully implemented security solution.

> In the past year there's been a **15%** rise in anti-malware software deployed on workstations

The rise of mobile working has meant that businesses have had to take a serious look at deploying mobile security. The proliferation of smartphones and tablets – and their subsequent targeting by cybercriminals – has meant their protection is now higher on the agenda for IT decision-makers, worldwide.

Although implementation of mobile device management is still low at **20%**, its importance is recognized by **44%** of IT professionals – an increase of **9%** from last year.

But there's been an **8%** fall in the deployment of anti-malware solutions on mobile devices. Why is this? Well, it's mainly because companies have been 'partially' implementing a solution – one that they think is sufficient to protect their employees without having to implement 'full' protection.

For some, there is also a feeling that data loss protection (DLP) isn't worth the expense. **23%** of businesses felt it was simply too expensive to justify an investment, while **33%** said they didn't have enough data to warrant its implementation.

And for those businesses that had already made the investment, only **31%** felt it had been worth it. Quite a low number, frankly, but one we imagine would skyrocket if such software had come to a business's rescue in the event of a breach. But sometimes it's hard to quantify an investment if it hasn't yet been used.

17% of businesses currently outsource their IT security decision-making to a third party or business, seeking external expertise rather than employing a de facto IT specialist in house. And among enterprise companies, **42%** now use IT security education services to help keep on top of their security, while **41%** use incident investigation services following an event. This illustrates how seriously larger businesses are taking IT security – and that they don't take any chances when it comes to ensuring they're kept up to speed with the latest from the IT security front line.

Virtualization – not yet a priority

Virtualization security helps businesses to achieve high virtualization density and maintain performance, so it's easier for them to make a better return on their investment.

Virtualization has been part of many companies' IT strategies for a while now, but its actual implementation rate remains low.

It's obviously on a lot of people's minds, with **53%** of businesses being very concerned about securing their virtualized environments. And **89%** said that having security software in place created a positive impact on the performance of their virtual machines.

> **53%** of businesses are being very concerned about securing their virtualized environments.

But there's a disparity between this level of concern and companies' willingness to actually act. Securing their business's IT virtual infrastructure was listed as a top three priority by only **19%** of IT decision-makers, while securing their cloud infrastructure was listed as a top three priority by just **22%**.

In fact, fully implemented virtual security solutions are rare; only **26%** of businesses with a virtualized infrastructure employ them. And a huge **56%** are happy to deal with the associated threats as and when they arrive.

Why is this? Well, virtualization is a highly complex issue. Even seasoned IT professionals, possessing a wealth of knowledge, can struggle to grasp the options available to them. Only a third of organizations possess strong knowledge of each solution and around one quarter have either a weak understanding of them or none at all.

One of the main reasons why IT professionals don't use specialized security is that they deem their current, non-specialized security to work well enough. **31%** didn't experience any problems with their traditional anti-virus, hence seeing no need for an upgrade. And **27%** who had experienced problems with traditional products in virtualized environments believed the issues didn't necessitate an investment in a different system. As a result, they're sacrificing performance for savings, using solutions that aren't tailored to virtual environments.

GReAT insight

"Organizations really do need to get a handle on securing virtual environments. There's a growing awareness of the risks, but there's still inertia and a lack of understanding of the specific factors involved in protecting virtualized systems."

Anti-Fraud – the need to secure every transaction

Fraud prevention is one of the most important security concerns for any business. Not only does it help to protect a company's financial transactions, it also helps to protect their image and keeps customers happy and confident in continuing to do business with them.

Almost two-thirds of businesses (**63%**) said that they make every effort to ensure their security measures are up to date.

It's never been more important to protect financial transactions. In our multi-device world, there are many ways in which cybercriminals can exploit new ways of working. While **64%** of the workforce uses a desktop with a wired connection and **50%** use a desktop with a WiFi connection, many also use smartphones to conduct business: **27%** use them to connect to WiFi networks and **18%** use them on the move with the help of mobile data.

> **72%** of businesses will look at a bank's security track record before deciding whether or not to approach them.

Due to a rise in mobile banking, financial institutions are seeing an increase in online fraud. But **48%** of these organizations state that any measures they take are designed to mitigate rather than solve the problem. And **29%** said that it was cheaper and more effective to deal with these issues as and when they arrived, rather than trying to prevent them happening in the first place. It appears then that banks are far keener on reactive spending than taking preventative measures.

But perhaps this attitude is short sighted. After all, a bank that protects its customers and helps to keep businesses safe will always be popular with prospective clients. **72%** of businesses will look at a bank's security track record before deciding whether or not to approach them.

But where does responsibility ultimately lie? **29%** of banks and payment services think it stops with their own IT department – and not with the client at all. But when asked whether they currently take any steps to protect their customers from financial transaction fraud, only **67%** said that providing a secure connection was mandatory.

And it's not just banks that need to improve their security. **48%** of businesses said that they had to improve the security of their financial transactions. In fact, most businesses believe that the ultimate responsibility for financial security lies with them, not the bank. Plus, **90%** of businesses with over 250 employees would pay for greater security if it meant more secure financial transactions. Businesses in the APAC regions, including China and Japan, would be more likely to pay compared to those in Western regions, which are less influenced by security reputations.

> **90%** of businesses with over 250 employees would pay for greater security if it meant more secure financial transactions.

GReAT insight

"It is astonishing that despite reported online fraud being on the increase, many banks still mistakenly believe that it's cheaper to deal with attacks when they happen, rather than prevent them in the first place."

Data Breaches – the costs you can see, and those you can't

It can be difficult for a business to comprehend the scale of a security breach until after it has happened. At first it may look like only data has been lost, but the long-term damage can end up being far more costly, and not just in monetary terms.

Preventing or dealing with an IT security breach is the top concern of IT professionals in every region, but the Eastern Markets and Japan **50%** named it their number one worry above all else. It's a more pressing issue than understanding the range of security technologies on the market (second) and managing change in IT systems and infrastructure (third). And it's not just the biggest concern for enterprises, it's number one for very small businesses too.

The result of a security breach can include stolen assets, data leaks and damage to a company's reputation. And the methods for remedying some of the dangers – legal and consulting fees and reactive spending, for example – are expensive and time-consuming. For **57%** of businesses attacked, significant additional costs had to be paid.

A data breach is also a huge step backwards in terms of maintaining a functioning business unit. Standard practices and processes are compromised, meaning a business can grind to a halt or be severely impeded in its performance. **60%** of businesses that suffered a data breach found their ability to function afterwards severely reduced.

The most dangerous types of attack, those that wreaked the most havoc, are phishing attacks, network intrusions and cyber-espionage. In their aftermath, costly professional services are usually required to restore normal service.

For SMBs, increased down-time resulted in, on average, $16,000 of lost business opportunities. But enterprises faced an average loss of $203,000. But when malware renders a business unable to operate, the results can be staggering. In 2015, down-time following an attack cost enterprises, on average, $1.4m. However this is down from $1.5m in 2014. But for SMBs, the cost of down-time in the last year has risen from $52,000 to $66,000. So why are larger businesses managing to reduce their losses? Well, most have taken the likelihood of an attack into consideration and have prepared themselves with better, more efficient disaster recovery tools.

In the past year, **87%** of data loss incidents required some form of additional assistance from third party professionals. These included IT security consultants and lawyers, as well as risk management consultancies.

And that's not all. **56%** of data loss events led to the business in question suffering damage to its image and reputation. Given the number of factors involved, it's hard to put an exact figure to the financial impact that such loss of face might entail.

But based on factors like the amount of money spent on reputation re-building and the amount of business lost through terminated contracts or missed opportunities we can estimate that the median cost of a data breach for SMBs is **$11,000**; and for enterprise organizations the figure is much larger, standing at **$84,000**. A serious data loss event, on average, costs an SMB around **$38,000**, while a larger enterprise faces losing a huge **$551,000**.

The estimated average spend on reactive activities for an SMB was **$8,000**, while enterprises spent **$69,000** per incident. But reactive spending isn't only confined to third parties. Both smaller businesses and larger corporations can potentially spend thousands of dollars for extra staffing, training and new IT systems.

These sums are alarming. But for SMBs, at least, the numbers are heading in the right direction. The total overall impact, which takes into account every loss and additional expenditure, fell by **12%**. Unfortunately, the situation isn't quite so rosy for enterprises. On average, the total overall impact rose by **14%**. Data breaches which involved virtual environments were over two times more costly on average than those which did not, with the figures standing at **$34K/$74K** for SMBs and **$454K/$942K** for enterprises.

What's clearly evident is that for a business still reeling from an attack, it would have been far less costly to have invested in an effective security solution in the first place.

GReAT insight

"Don't think it won't happen to you. There are numerous examples where even large businesses have gone into liquidation after a successful data breach. The cost remediation far outweighs the cost of prevention."

DDoS – a multifaceted threat

Distributed Denial of Service (DDoS) attacks are launched to disable a targeted organization's online presence or key business processes. The damage – and the associated costs – can be huge and lasting.

DDoS attacks have been around for a while, but are currently more dangerous than they've been in the last few years. The cost of launching a DDoS attack has fallen too, which has helped increase the volume of attacks rapidly. Today's attacks are also more complex, making defending against them that much harder.

Of the businesses surveyed, **50%** experienced some level of disruption due to a DDoS attack in the past year. Very often, a DDoS attack is combined with a security breach, to gain more from an attack. Last year, **45%** of DDoS attacks were combined with malware, **32%** with a network intrusion or hacking event, and **26%** with a data leak.

> Of the businesses surveyed, **50%** experienced some level of disruption due to a DDoS attack in the past year.

Which types of business were hit the most? Of those with over 10 employees, **24%** of banks experienced an attack, so did **23%** of telecommunications companies and **20%** of financial services organizations. At the lower end of the scale, **7%** of media and entertainment companies, **8%** of real estate businesses and **11%** of healthcare organizations also suffered from an attack.

The service most commonly affected by a DDoS attack was a business's public website, with almost half of surveyed businesses (**47%**) citing their website's inability to function. At 38%, the customer portal or login area was the second most affected area, while issues with communications services (**37%**) were the third most affected service.

The most common form of disruption for a business was increased page loading times. **58%** experienced significantly longer page loading times, while **34%** found page loading times were slightly increased. **43%** experienced delays of a day or longer, with some pages taking several weeks or longer to load. **24%** also experienced a complete disruption to their services.

There are many feared consequences of a DDoS attack. **27%** said their major fear was down-time that led to a loss of their reputation among customers. **27%** also said they most feared online resource down-time, which could lead to a loss of revenue or business opportunities. The second highest fear (**16%**) was the costs that would be incurred fighting the attack and restoring services to normal. In third place, at **15%**, was the possibility of losing clients as a result of an attack.

But whose responsibility is it to manage the threat of DDoS attacks? In smaller businesses, responsibility is more likely to be placed on senior management and external service providers. But in larger businesses, responsibility is seen to lie with the internal IT or security department.

Attitudes towards DDoS attacks are mixed, to say the least. Only **56%** of IT professionals believe that spending money to prevent or mitigate an attack in the future would be worth the investment. Just **52%** said they felt well informed about DDoS attacks, while **48%** said they knew the identity and motivations of those perpetrating recent DDoS attacks against them.

When asked who or what they suspect to be behind the DDoS attack they had experienced, businesses pointed their fingers at a wide variety of potential assailants – with criminals being the most accused group. **28%** of IT professionals believed it was criminals seeking to disrupt their operations. **18%** thought it was criminals seeking to disrupt or distract them while another attack took place. And **17%** said it was criminals who used the attack to hold the company to ransom.

Aside from criminals, **12%** believed attacks were launched by their competitors, with the aim of sneaking an advantage in the marketplace or to steal private information. Indeed, respondents in Russia and China were the most suspicious of their competitors. **11%** of companies also had their suspicions that political activists were behind the attack, while **5%** thought it might have been government or state powers.

GReAT insight

"Businesses need to realise that a DDoS attack is not just about taking down a website or other service: these attacks can also be used as a form of misdirection – to cover the use of sophisticated malware to steal sensitive company information."

Conclusion

Though the perception doesn't always match the reality, the truth is that cyber threats aren't going away. As ever, they're evolving to keep pace (or in some cases stay ahead) of the changing IT landscape within businesses.

Cybercriminals aren't going to stop innovating anytime soon and it's important that organizations don't allow their increasing awareness of current threats to turn into a blinding complacency regarding those yet to emerge. So as well as making a commitment to continual education, businesses need to make sure they see security as an essential part of their IT investment plans.

If you're spending on virtualization, moving resources to the cloud or trying to enable more mobile working, you need to make sure you're taking into account the fact that these opportunities bring with them accompanying risks that need to be countered.

Indeed, given its relation to these strategic concerns, cybersecurity should be entrenched as a C-suite issue, rather than something that happens as an afterthought in the wake of decisions taken at the top level. If, for example, mobile working is being discussed at boardroom level, so should the protection needed to enable and secure it. Unfortunately, as we've seen, the opposite is currently happening.

This needs to change. By adjusting the way we think about and budget for security, we can ensure that it remains adequate to protect a changing IT landscape.

The GReAT Team

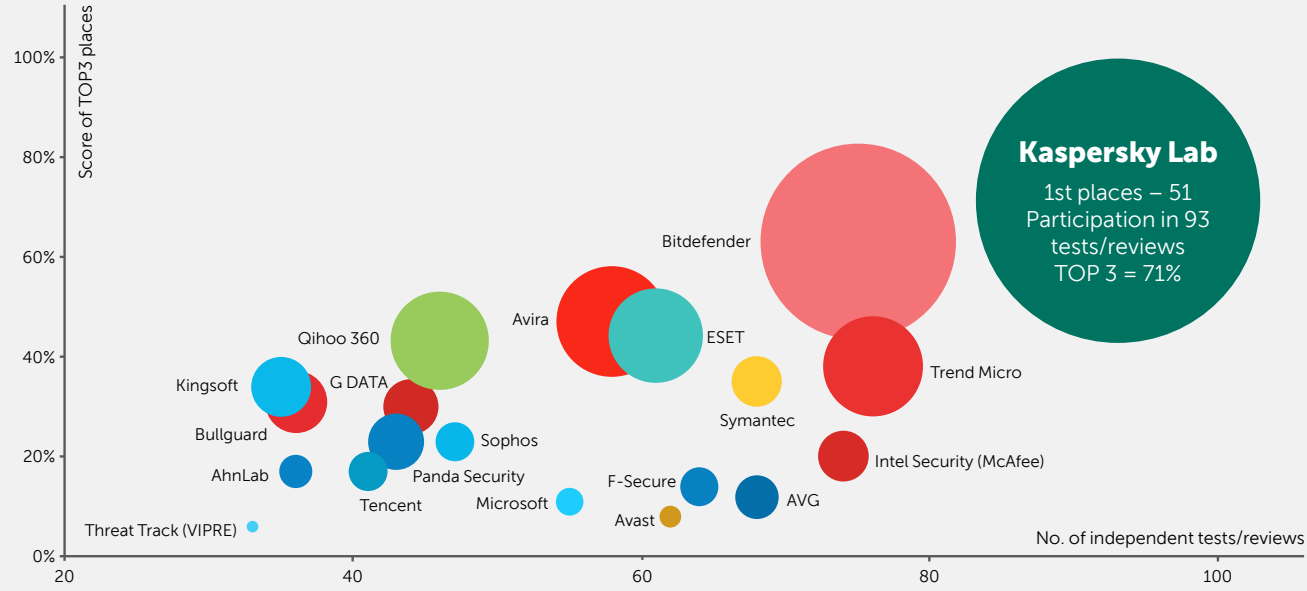
The expert insight in this report is provided by Kaspersky Lab's Global Research and Analysis Team (GReAT). Since 2008 GReAT has been leading the way in antithreat intelligence, research and innovation – within Kaspersky Lab and externally. GReAT has been at the forefront of analyzing some of the world's most sophisticated threats, including Stuxnet, Duqu, Flame, Red October, NetTraveler, Careto, Equation, Carbanak and Duqu 2.0.

Why Kaspersky?

Kaspersky Lab is one of the fastest-growing IT security vendors worldwide and is firmly positioned as a top-four global security company. Operating in almost 200 countries and territories worldwide, we provide protection for over 400 million users and over 270,000 corporate clients – from small and medium-sized businesses to large governmental and commercial organizations.

Our advanced, integrated security solutions give businesses an unparalleled ability to control application, web and device usage: you set the rules and our solutions help manage them. Kaspersky Endpoint Security for Business is specifically designed to combat and block today's most advanced persistent threats. Deployed in conjunction with Kaspersky Security Center, it gives security teams the administrative visibility and control they need – whatever threats they face.

In 2014 Kaspersky Lab products participated in 93 independent tests and reviews. Our products were awarded 51 firsts and received 66 top-three finishes.[5]



** 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.

SECURITY POWERED BY INTELLIGENCE

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

Visit **usa.kaspersky.com/business-security** to find out more about Kaspersky Lab's unique expertise and Security Solutions.

FIND OUT MORE

JOIN THE CONVERSATION

Watch us on YouTube

Like us on Facebook

Review our blog

Follow us on Twitter

Join us on LinkedIn

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 IT security solutions (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.

usa.kaspersky.com/business-security

KASPERSKY lab THE POWER OF PROTECTION