KASPERSKY lab

GLOBAL
SECURITY
INTELLIGENCE

THE SECURE ENTERPRISE

#EnterpriseSec
kaspersky.com/enterprise

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 among 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, and today the terms cyberwar and cyberterrorism are high on the agenda of our world leaders. Now it's time for enterprises to reinforce their IT security strategies to meet the demands of today's ever more challenging environment.

At Kaspersky Lab, we believe that it's not enough to react to new threats as 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, and our technologies are designed to leverage our extensive global security intelligence. Our approach at Kaspersky Lab is simple: better intelligence combined with better technology results in better protection.

We are committed to bringing the benefits of this protection to enterprises around the world, helping to defend them from cyberthreats in all forms – today and into the uncertain future.

“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 – a combination which produces results that are unmatched by any other IT security organisation.”

Nikita Shvetsov
Acting Chief Technology Officer
Kaspersky Lab

Malware affects everyone – from individuals to large enterprises and governments. Cybercriminals are using steadily more sophisticated weapons to defraud business, steal data and achieve financial gain. A growing number of some cyberattacks are politically or socially motivated with cyberterrorism and cyberwar now a reality.

Global organisations are being subjected to targeted attacks, so called ‘Advanced persistent threats’ (APTs), from determined groups of criminals. While some of these are high-profile and well-reported, the trend is for attackers to use progressively stealthier techniques to stay undetected while gaining access to sensitive and often commercially valuable data.

OUR FOCUS AND 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 been focused on protecting the endpoint, and today’s endpoints are more varied and exposed than ever before. Today endpoints can be mobile, virtual or even critical national infrastructure.

These areas are also the most underserved by the IT security marketplace. Our focus is to help large organisations protect themselves against these vulnerable areas with a new approach – one that harnesses our advanced threat intelligence to deliver a better standard of protection.

KASPERSKY LAB TECHNOLOGY LEADERSHIP

Though distinct, these threats don’t exist in isolation. Together they form part of a wider security landscape, and effectively overcoming any one of them depends on understanding them all. The world requires security solutions built on extensive and predictive security intelligence – not single-purpose offerings designed with a narrow focus. And we believe creating these 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, means better protection.

One foundation of our security intelligence is the Kaspersky Security Network (KSN). It obtains vast amounts of cyberthreat data on evolving malware of all types, from all corners of the globe. This, coupled with analysis from our world renowned Global Research and Analysis Team (GReAT), means that Kaspersky Lab is uniquely placed to deliver solutions that not only neutralise present threats but also stay one step ahead of future dangers.

THE KASPERSKY SECURITY NETWORK

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

FRAUD PREVENTION
Online and mobile banking – all risks covered

Hundreds of millions of dollars are stolen from online financial service providers every year, and the threat level is still rising. Well-organised cybercriminals are now targeting banks twice as often as any other kind of institution[1].

But the sheer number of attacks is only half the problem, because changes in customer behaviour are leaving banks more vulnerable than ever.

98% of consumers regularly use online banking services or shop online[2]

Today, the vast majority of Internet users frequently bank or shop online[2], but they're often unaware of the risk of accessing their accounts from unsecured devices. Mobiles are particularly vulnerable, and with a steady rise of consumers using mobile banking facilities, criminals are already developing specific methods to exploit these valuable targets.

The threats facing customers are real, and if they aren't protected, neither is their bank.

The Kaspersky Fraud Prevention platform allows financial institutions to offer enhanced security for their core operations and their customers. Kaspersky Fraud Prevention can even help banks make their customers' mobile applications more secure, stemming the growing tide of cyberthreats that target mobile devices. And our intelligence keeps clients at the forefront of security effectiveness, ensuring that even as the landscape shifts, effective, relevant responses are always in place.

[1] Global Economic Crime Survey 2014, PricewaterhouseCoopers
[2] Consumer Security Risk Survey 2013, B2B International in conjunction with Kaspersky Lab

[1] Cyberthreats to ICS systems: you don't have to be a target to become a victim. Industrial Security 2014, Kaspersky Lab

35% of incidents in industrial networks are caused by malware attacks[1]

Once, industrial control systems were isolated and their operators thought that would keep their infrastructure secure. In reality, isolation alone 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 to the Internet leaves these systems with a whole new set of vulnerabilities – and if a network is breached by malware, the consequences can be catastrophic.

Though the most sophisticated cyberweapons are designed with select targets in mind, once launched, they can fall into the hands of any number of groups with hostile agendas and be repurposed for new targets. This means all critical infrastructure needs the highest possible level of protection.

As a leader in the fight against cybercrime, Kaspersky Lab has unparalleled insight into the threats facing the world, as well as the expertise to neutralise them. In partnership with governments and private-sector bodies, we help to create the multi-layered defences needed to protect critical infrastructure and the societies that depend on it. We recognise that critical infrastructures need a different level of protection: one that is highly configurable and fit for purpose.

Since in industrial networks process integrity takes precedence over data integrity, Kaspersky Lab is offering a specifically tuned version of its business security suite, and at the same time is leading the industry in the development of secure infrastructure technologies, better protection for PLCs and more integrated SCADA protection layers.

Gartner forecasts 12.14% growth in the worldwide enterprise market for virtualization Infrastructure software during 2014[1]

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

But as organisations worldwide face ever-greater levels of cyberthreats, they must be sure to protect their virtual environments just as fully and effectively alongside their real-world IT infrastructure. And now that many organisations are virtualizing critical systems and data, there's even more at stake.

Adding security functionality into any IT system – physical or virtual – is going to 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 infrastructures, as resource efficiency is the primary driver for implementing the technology in the first place. Unless a balance is struck between security and systems efficiency, the benefits of virtualizing could be completely undermined.

The ideal security solution has to mirror the characteristics of virtualization itself. It should be flexible, adaptable, and capable of delivering a significant ongoing return on investment by balancing protection and performance – which is precisely what Kaspersky Security for Virtualization delivers. Now, enterprises don't have to make a compromise between resource efficiency and depth of protection. With Kaspersky you get both in equal measure.

[1] Forecast: Enterprise Software Markets, Worldwide, 2010 – 2017, Q413 Update – Gartner

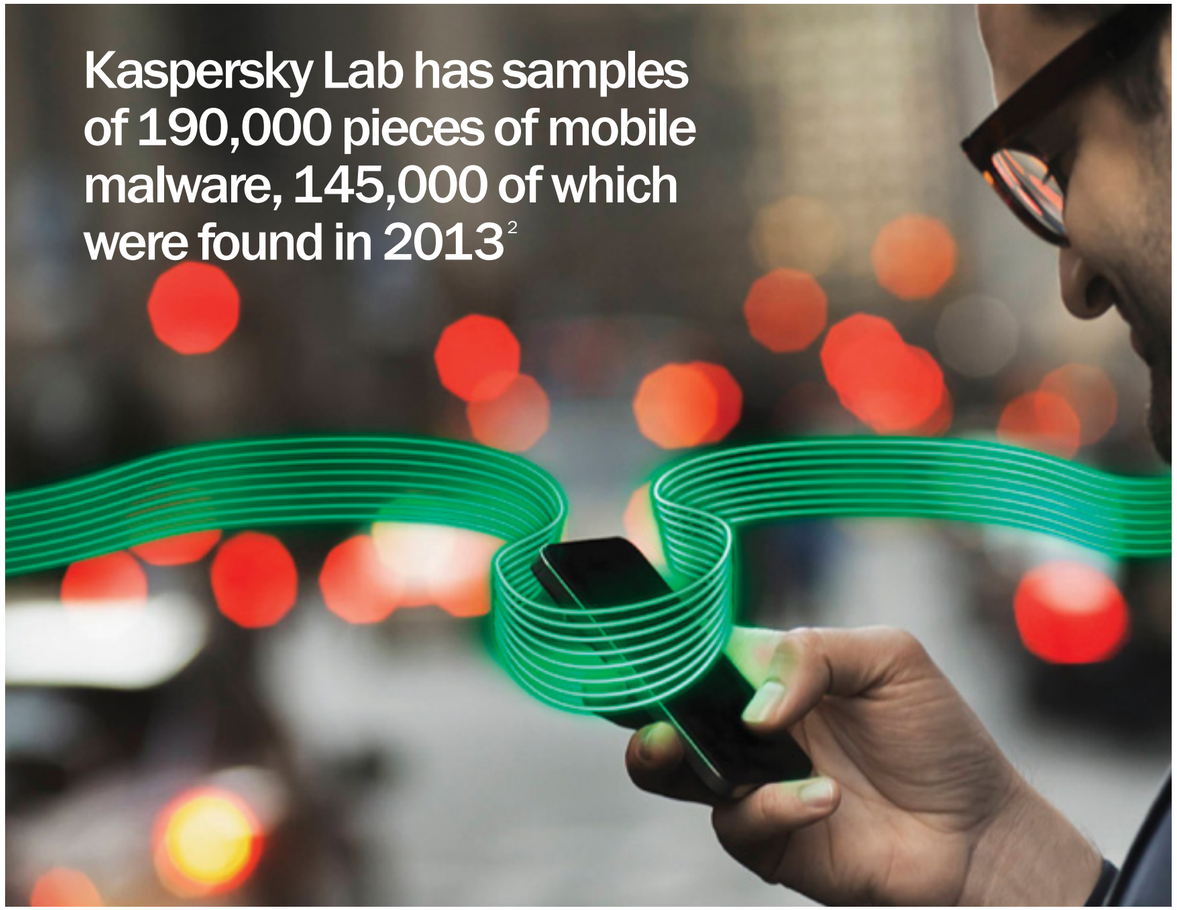
With the rise of flexible working and 'Bring Your Own Device' (BYOD) policies, every enterprise needs protection from cyberthreats wherever their employees go, and whatever hardware they're using. This means traditional security measures are simply incapable of protecting corporate data on the move.

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

Beyond this, the security challenge presented by mobility is the proliferation of device types and the portability of the hardware, which makes visibility and management of corporate information assets a daunting task.

As a product that's been protecting against mobile malware for more than 10 years, Kaspersky Security for Mobile offers a highly adaptable way to protect corporate networks from the threats inherent in a mobile infrastructure.

Most importantly, Kaspersky's management console allows enterprises to see, control and protect their data across all their endpoints - all from one place. So the enterprise is secured, regardless of how mobile the data is.



In 2013 18% of companies experienced data leakage from mobile devices, and 30% faced security threats as a result of devices being lost or stolen[1]

[1] Global Corporate IT Security Risks – Kaspersky Lab
[2] Mobile Malware Evolution: 2013 – Kaspersky Lab May 2013

In the face of increasingly sophisticated and evasive attacks, standard firewalls and antivirus technology are no longer enough. Deeper and more pervasive tools are needed.

IT departments in large organisations face twin challenges: ever greater complexity, and ever more sophisticated threats. Their task is made all the more daunting by the vast array of applications and devices their staff use every day, and by the growing number of employees conducting business over the web and through social media platforms.

For enterprises today, more comprehensive and precisely managed IT security is required. Kaspersky Lab endpoint control technology delivers this and is a foundational part of our technology strategy. Our security solutions for enterprise incorporate powerful control tools, including 'dynamic whitelisting' to authenticate applications and protect data and devices from malicious code, applications and websites. And we constantly obtain global threat intelligence to stay ahead of new and emerging threats, providing automatic updates through the cloud-based Kaspersky Security Network.

Uniquely, this technology is available in a single, integrated security platform – making IT security management easier, faster and more effective. Kaspersky Lab endpoint controls provide an essential link between setting IT security policies and making them actionable.

[1] Kaspersky Security Bulletin 2013

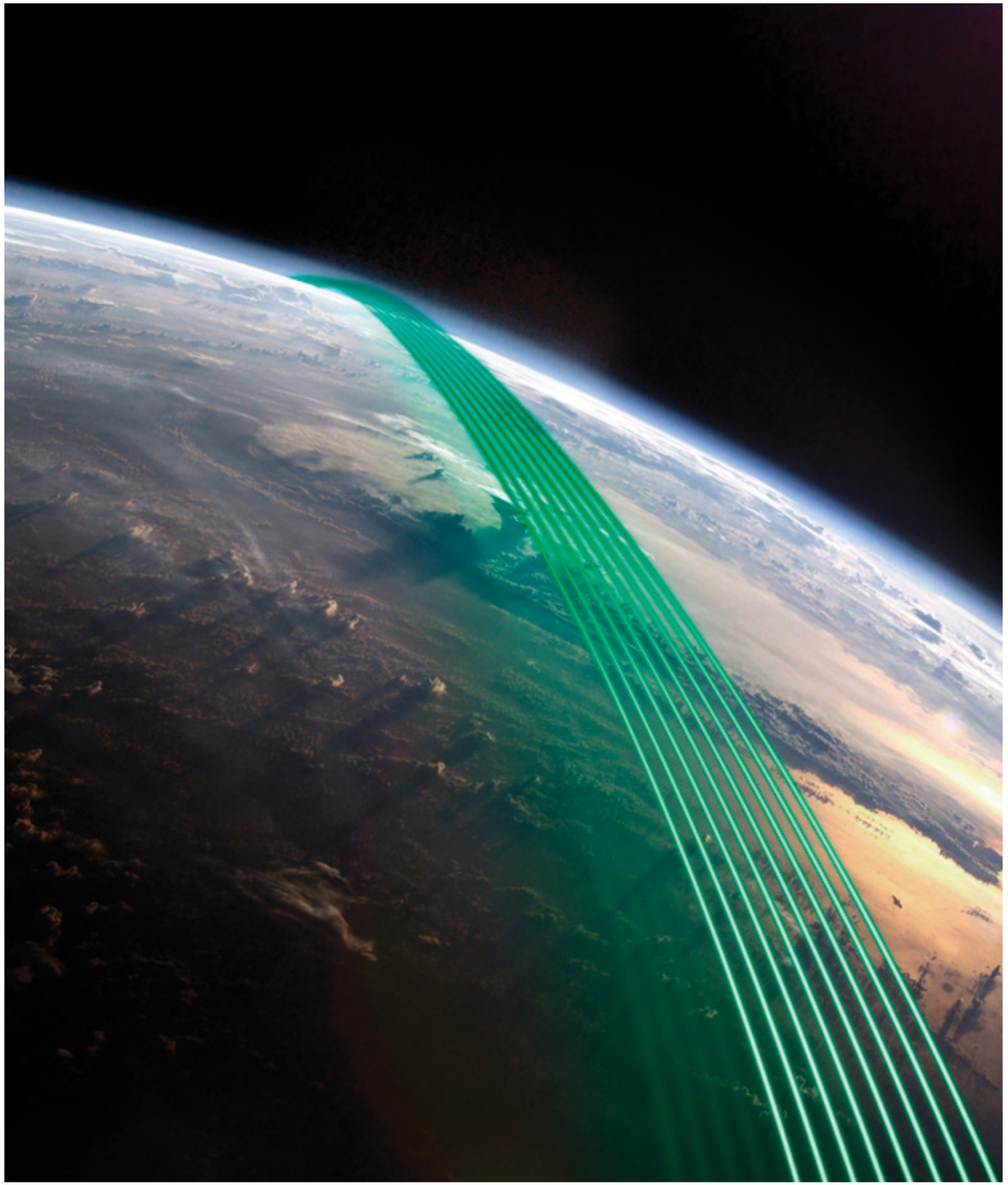
Kaspersky Lab detects over 315,000 new malware samples every day

Unless IT departments understand the nature of the threats they face, defending against them is impossible. And with cyberattacks becoming ever more widespread and sophisticated – and the criminals behind them constantly innovating to undermine the security of their targets – it's not enough to take a reactive stance.

Enterprises need to know what's looming so they can have responsive defences in place.

Kaspersky Lab's Security Intelligence Services constantly monitor the threat landscape, identifying emerging dangers and taking steps to defend and eradicate. By combining our world-leading knowledge of malware and cybercrime with a detailed understanding of our clients' operations, we're able to create bespoke reports that provide actionable intelligence for an enterprise's specific needs. So whatever the scale of the threat – from phishing emails impersonating a brand to the latest global trend in cybercrime – our clients stay several steps ahead.

Alongside raw intelligence and tailored reports, we're able to investigate attacks launched against our clients, identify the perpetrators, analyse their methods and determine how they can be nullified. Meanwhile, our education services provide IT departments with the knowledge they need to detect and counter attacks before they cause damage. And Security Account Management provides constant access to a Kaspersky Lab expert – so we can address potential vulnerabilities swiftly before they are exploited.



In independent tests, Kaspersky Lab products finish in the top-three positions more often than any other vendor

Kaspersky Lab operates in more than 200 countries and territories worldwide, and our technologies protect over 300 million people. We employ over 2,800 highly qualified specialists, led by 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 the wider R&D department of Kaspersky Lab and provides leadership in anti-threat intelligence, research and innovation, 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 private citizens and enterprises all over the world protect themselves from cybersecurity threats, Kaspersky Lab cooperates with international organisations such as INTERPOL and Europol, as well as national and regional law enforcement agencies worldwide to implement countermeasures that disrupt malware operations and cybercriminal activity.

During our investigations, we use our technical expertise to analyse all elements of an attack, from its infection vectors and malicious programs, to its supported command & control infrastructure and exploitation methods. The insights we gain feed into all of our solutions, helping us detect and remediate malware attacks, regardless of their origin or purpose – so all our experience is leveraged for the benefit of our clients.

And right now, we're developing a set of solutions including a secure operating system for industrial control systems (SCADA systems) 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.

- Kaspersky Lab achieves the industry's best results in independent product tests: in 2013 Kaspersky Lab endpoint products participated in 75 tests and reviews. On 42 occasions they took first place, and 86% 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 sophisticated threats such as Duqu, Flame, Gauss, Red October, Icefog and The Mask.
- Kaspersky Lab has more than 80 global partner and technology OEM agreements, including with IBM, Cisco, Juniper Networks, HP, Microsoft and Qualcomm.