KASPERSKY lab

PUT TIME ON YOUR SIDE:
THE HEAVY COSTS OF PUTTING OFF YOUR CYBERSECURITY DECISIONS

A lot can happen in a business day. Deals close. Products launch. News items hit the airwaves.

A lot can happen with IT security in one day, too. In fact, at Kaspersky Lab, we detect 310,000 new pieces of malware every day, which means that every day you put off the decision to upgrade your IT security system is a day that thousands of pieces of new malware can slip through.

What does this mean in real terms?

For small- to medium-sized businesses, the **average cost of a data breach is $38,000**. Additionally, 60% of businesses that suffer a breach find their ability to function severely impaired.[1] The results of a security breach can include stolen assets, data leaks and damage to a company's reputation. Unfortunately, the methods for remedying some of these consequences are expensive and time-consuming. For **57%** of businesses attacked, significant additional costs had to be paid in the form of legal fees, consulting costs and public relations campaigns.[2]

Because high-level threats are constantly evolving, it is important to tailor your systems, keep on top of any emerging intelligence and stay ahead of the threat landscape. All of this requires a lot of time for you and your staff. How do you know where to dedicate your resources?

Kaspersky Lab has the research to help you get ahead of these decisions, tailor your approach and allocate resources appropriately so that you can save yourself time for other pressing matters.

1, 2. Global IT Security Risks Survey 2015

MAKE EACH DAY COUNT.

What would you do if you found a major data breach in your system? What would you do if you discovered that the breach had happened months ago and had gone undetected?

With the median time to detect a breach at **205 days**,[3] this is a common scenario. Most organizations who have suffered a security breach to their system don't know that cybercriminals may have been lurking there for quite a while—identifying vulnerabilities, accessing critical information and stealing records.

Cleaning up these messes is a costly and time-consuming activity that often involves backtracking to try to piece together the missing data. In fact, SMBs spend an average of **$8,000 on reactive activities in the event of a data breach**, though businesses can spend thousands of dollars more on extra staffing, training and new IT systems.[4]

The solution is a robust security solution that safeguards your organization from intrusion in the first place. With this protection as your first line of defense, you can rest assured that you will not have to spend precious resources on legal problems and reputational damage that can lead to a significant loss of business.

3. Global Incident Response from HP and Mandiant

4. Global IT Security Risks Survey 2015

THE CLOCK IS TICKING.

With all of the concerns IT managers face, downtime nears the top of the list of scenarios to avoid. Lost productivity, business continuity challenges and time spent managing employee expectations are all immediate ways that businesses lose out when their systems go down.

While not all security breaches lead to downtime, it does occur in about a third of the cases. And the costs rack up quickly. When a small- to medium-sized business is hit, the consequences of downtime are serious—**$16,000 in lost business opportunities and $66,000 in overall costs.**[5]

Unfortunately, downtime is becoming increasingly common. It is a disadvantageous scenario with more and more time needed to mitigate the effects. In just four years, the average time required to detect and respond to a cyberattack has increased by nearly 130 percent.[6]

Unless your organization wants to implement a policy of "drop everything and react," these drains on time and budgets can be avoided. With a clearcut strategy, a robust security solution, and a well-implemented system, your organization can keep things running smoothly.

5. Kaspersky Lab's Global IT Security Risks Survey 2015
6. Cybersecurity Boardroom Implications: The National Association of Corporate Directors

LOOKING TO SAVE TIME? SO ARE CYBERCRIMINALS.

2015 marked a shift. After years of increasing numbers, the number of new malware files detected every day by Kaspersky Lab fell from 325,000 in 2014 to 310,000 in 2015. So, what's going on? Is cybercrime going away?

Not at all.

Kaspersky Lab experts believe that this decrease is due to the fact that coding new malware is expensive. Cybercriminals have realized that they can get equally good results by using intrusive advertising programs or legitimate digital signatures in their cyberattacks. They are acting more like businesses now, selling quasi-legitimate commercial software and stealing legal certificates to deceive security software.

It's an approach that appears to be working. Results show that despite the cost-cutting in malware creation, **in 2015 the number of users attacked by cybercriminals increased by 5%.**[8]

Cost cutting. Efficiency. Return on investment. Like everyone else, cybercriminals are constantly looking for new and better ways to execute attacks. And they're finding them. Given their increasingly stealthy tactics, staying ahead of them is a necessity for any large enterprise.

8. "Kaspersky Lab's New Malware Count Falls by 15,000 a Day in 2015, as Cybercriminals Look to Save Money"

THE COMPLETE THREAT PROTECTION SOLUTION.

When each day brings new IT security challenges to your organization, how do you make sure that you have the most comprehensive protection available?

Start by building a plausible threat model for your organization that identifies the number of things that can go wrong, including potential failure of any of the protection layers.

Once you have this information in hand, you can use it to support employee education efforts. Oftentimes, employees don't understand the role they play in avoiding certain scenarios. With a little knowledge about what to look out for, employees can act as the first line of defense against cyberthreats for your company and report problems to IT.

Supporting all of your efforts should be a complete technological solution that provides multiple layers of defense. At Kaspersky Lab, our solutions protect against known, unknown and advanced threats through a multi-layered approach that uses advanced behavioral technology.

For the 1% of threats that are advanced, our System Watcher tool, Automatic Exploit Prevention (AEP) and Rollback functionality ensure that your organization is protected against the most pernicious threats that can inflict serious damage to your business. By applying more advanced heuristic, dynamic whitelisting and application control tools, we can fight unknown threats that make up 29% of the cyberthreat landscape. Our core, award-winning technology blocks against known dangers that make up 70% of the threat landscape.

By employing these multiple layers of threat protection, our systems check files as they execute, relying on behavioral analysis to search for suspicious activity.

Putting next generation behavioral analysis to work

Our **System Watcher** technology monitors an application's behavior when it launches on your network. If any suspicious behavior is detected, System Watcher will automatically quarantine the application. Because System Watcher keeps a dynamic log of the operating system, registry and more, it enables the rollback of malicious actions implemented before the malware was identified.

As part of System Watcher, **Automatic Exploit Prevention (AEP)** technology specifically targets malware that exploits software vulnerabilities. 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.

Also part of System Watcher, our **Rollback** functionality executes continuous, detailed monitoring of systems, enabling exceptionally accurate system Rollback functionality and limiting the impact of any infection and returning systems to previous, secure parameters.

Additionally, data from the **Kaspersky Lab Security Network (KSN)** helps us to predict what new threats might look like, how they might act and how we can reduce their impact. Without this real-time intelligence feed, you cannot predict future threats in a timely and accurate manner—making KSN a key technology to help businesses stay ahead of the security threats on the road ahead.

Comprising more than 60 million volunteers worldwide, KSN uses this real-time data about threats to ensure that your security software is always up to date and that you are protected against new threats within the shortest time.

For our customers, this means that our cloud database refreshes signature and heuristic information in nearly real time. While traditional signature-based responses can take hours, KSN's approach shrinks this time to about 40 seconds.

TRY KASPERSKY LAB

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

GET YOUR FREE TRIAL TODAY >

JOIN THE CONVERSATION

Watch us on YouTube

Like us on Facebook

Review our blog

Follow us on Twitter

Join us on LinkedIn

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

ABOUT KASPERSKY LAB

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

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

KASPERSKY lab
THE POWER OF PROTECTION