KASPERSKY lab

DEBUNKING THE TOP 5 SECURITY IMPLEMENTATION MYTHS

SWITCH SAFELY ...

Leaving your organization even momentarily exposed opens up the possibility of a cyberattack that could cripple your business. Some people mistakenly believe that such an opening is inevitable when switching security solutions. Not true! The real danger looms, not at a mythical moment during cutover, but every single day that you rely on a sub-par technology to protect your business, your employees, and your IT infrastructure.

There's a common misconception that implementing comprehensive cybersecurity to protect your business against today's sophisticated threats and attacks is a difficult and expensive task and that the benefits of replacing current solutions (even if they are highly ineffective) aren't worth the hassle. This mindset has resulted in many organizations dealing with a virtual patchwork of disparate systems that are time consuming to manage and costly to keep running. More importantly, however, is they are ineffective, leaving your business vulnerable to cyberattack.

Simply put, such misconceptions are false. This eBook aims to set the record straight by debunking the top 5 myths about implementing IT security.

MYTH 1

"I have a secure environment … don't I? All a change will do is cost me more money."

This is a pretty common assumption. However, it's not always the case for two primary reasons: 1) changes do not necessarily cost more—in some cases the total cost can be lower and 2) not all security technologies have the same ability to stop attacks—some simply have sub-par efficacy.

When we speak with prospective customers about their IT security experience, we ask if they have had a clear record with zero IT security incidents over the last year. Usually, the answer is "no." Despite the fact that businesses are dealing with an increase in malware, phishing attacks and other threats, the answer should and can be an emphatic "yes."

Not all security solutions are created equal. Saving money now by implementing a cheaper (or "free") solution may seem like the best course of action at first glance. Over time, however, this kind of bargain shopping can result in additional costs associated with increasing security in other areas, time spent managing the solution, or in the worst case scenario, mitigating the damage of a cyberattack because the inneffective solution didn't work.

According to the Ponemon Institute's 2015 Cost of Data Breach Study, 47 percent of all breaches were caused by malicious or criminal attacks. With the average total cost of a data breach at $3.79 million dollars, are you willing to bet your profit margin on inferior security?

With the average total cost of a data breach at $3.79 million dollars, are you willing to bet your profit margin on inferior security?

MYTH 2

“Switching our security solution will cause downtime and will leave my organization vulnerable to a cyberattack during the transition.”

Any organization making the investment to implement a new security suite understands the risks that today’s threats pose to businesses of all sizes and the importance of having the most effective protection available. You know that by leaving your business even momentarily exposed opens up the possibility of a cybercriminal stealing financial information, intellectual property and other data with the outcome wielding a crippling blow to your organization. The mistake some people make is that they believe such an opening is inevitable when you’re switching technologies. Instead, they should realize it’s more dangerous to continue to rely on a sub-par technology.

In actuality, a well-organized and planned out implementation that requires a “rip-and-replace” can be conducted and completed without leaving your organization open to an attack at any point. Switching from an old security system to a new solution can and should be done by replacing the incumbent product with a fully functioning product simultaneously. In addition, policies should be reconfigured before the replacement occurs. By following these guidelines, you can ensure that your new solution is up and running properly without experiencing downtime that will leave your business vulnerable to an attack.

MYTH 3

“Our end-user experience will be negatively impacted by the change.”

Proper planning is important for any security implementation, but a “rip-and-replace” requires even more careful planning to ensure a smooth transition and minimize system administrators’ manual operations. One way to avoid impacting the end-user experience is by conducting major activities associated with an implementation during off-hours. This includes the removal of current security solutions and installation of the new product on user PCs. By performing these activities using automation tools and during off-hours, employees are able to operate as they normally would without experiencing any degradation to system performance.

MYTH 4

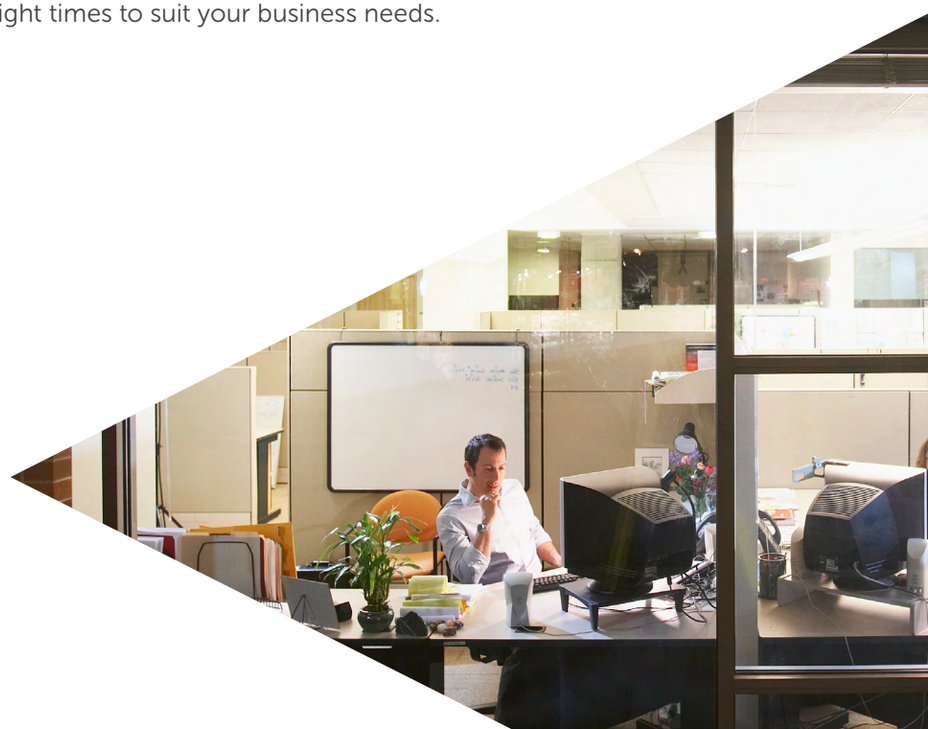
“My overworked IT team doesn’t have time to implement a new security solution.“

This is a very understandable concern. Many business leaders are worried that an implementation of a new security suite requiring a “rip-and-replace” will cause a strain on their already extremely busy IT department, shifting focus away from other, mission-critical IT projects. However, this doesn’t have to be the case. Today, it’s possible to manage the implementation through a single console, making this process easy on an IT team. Organizations can easily remove the incumbent solution from all workstations and simultaneously implement the new solution, all the while managing the process from a “single pane of glass” view. This strategy also eliminates the hassle associated with patchwork security that is harder to manage and, in most cases, costs an organization more money to operate.

MYTH 5

“When the job is finished, we’ll be on our own and we’ll have to deal with any switch problems without assistance.”

While this myth may be true for some software vendors, there are exceptions. First and foremost, any cybersecurity company providing a security solution should provide free basic support during business hours. And for those organizations that want higher levels of support, you should have the option of purchasing at a level that offers you the right amount of support at the right times to suit your business needs.



SUMMARY

You only have to pick up a newspaper to know that sophisticated attacks are on the rise. A security implementation—particularly one that requires a "rip-and-replace," can seem like a daunting task. It's more important than ever to ensure that you have the best solution in place to safeguard your business. With proper planning and understanding of the facts, you can provide protection from known, unknown and advanced threats.

It's more important than ever to ensure that you have the best solution in place to safeguard your business.

PROTECT YOUR BUSINESS NOW.

Join the conversation.

Watch us on YouTube


Like us on Facebook


Review our blog


Follow us on Twitter


Join us on LinkedIn

GET YOUR FREE TRIAL NOW >

Learn more at
kaspersky.com/business

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.

To learn more about Kaspersky Endpoint Security for Business, call Kaspersky Lab today at 866-563-3099 or email us at corporatesales@kaspersky.com.

www.kaspersky.com/business

* 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.

KASPERSKY lab
THE POWER OF PROTECTION