YOUR DATA UNDER SIEGE: DEFEATING THE ENEMY OF COMPLEXITY.

With Kaspersky, now you can. kaspersky.com/business

Be Ready for What’s Next
There are three important truths in today’s cyberlandscape:
First, your company is the custodian of valuable, confidential data, applications and IT infrastructure that drive nearly half of all economic activity. Second, all companies face the same security threats. And third, you are challenged by the complexity and expense of maintaining an effective security infrastructure in the ever-changing and hazardous cyberbusiness world. Regardless of the size of your business or the industry you serve, complexity is the real enemy of your company’s cybersecurity.

If you are the victim of a security breach, do you have the resources and stamina to weather the incident? Do you know how to sidestep the perils in the first place? The frequency and complexity of malware and Trojan threats are overwhelming for even the most established IT departments. Every single day, cybersecurity experts identify another culprit—TorRAT malware, the Shylock Trojan, the Chameleon Botnet, as well as a slew of other, nameless threats. By any name, these vulnerabilities allow cybercriminals to access your company’s confidential data and/or financial information while wreaking havoc on your IT infrastructure.

The volume and severity of cyberthreats and malware is so large that half of all businesses consider it their top operational risk. According to analyst firm IDC, SMBs will spend $5.6 billion on security technologies by 2015.

Most businesses like yours already employ some form of antivirus/anti-malware software on their servers and endpoints. Most have a firewall or some network-level security protection and many are adding security to email and collaboration servers.

You don’t necessarily need more security technology – what you do need is more effective security platforms that incorporate key security requirements and protections across multiple operations, disciplines and technologies.

Despite these basic security investments, most businesses are still vulnerable. Without realizing it, you may lack some or all of the security tools you need to safeguard your systems. Worse, you may be unable to effectively utilize the security software and appliances you already have in place. On an individual basis, these security investments are good at resolving specific issues. For example, antivirus is good at identifying and blocking malware and patch management is good at installing updates to resolve application vulnerabilities. However, these security systems don’t always work harmoniously, and have the potential to drain resources and make mistakes that expose your business to cyberattacks.

Disparate security technologies typically don’t talk to each other. This lack of interoperability means each new system installed to protect data and IT systems adds another unique management console, process and change management system and reporting protocol.

Your investment in security applications and IT infrastructure is inefficient and ineffective. Not only are you not getting security value from the technologies, but your resources may be overtaxed by toggling between various management consoles, reconciling dissimilar reports and data and chasing work orders. This multiplicity of security systems wastes time, money and productivity. Worst of all, it leaves gaps in security management processes, which in turn leaves vulnerabilities open and data at risk.

In IT management parlance, this is known as “the single pane of glass” through which security administrators can see, control and protect all things ranging from networks to endpoints and mobile devices. As more productivity and business applications are added, the business repertoire is stretching the already overburdened security fabric.
To understand the growing security management challenge, let’s examine what’s creating the need for security in your business. This is the fastest growing segment of the IT marketplace. We know that businesses like yours are investing in tools and systems to make your company more nimble, productive and profitable.

You go mobile because you want to encourage your employees to be more responsive to business opportunities and stand out from the competition. You purchase new software because you want to make your businesses smarter and more effective. For these reasons, your expectations of IT and its role in your business are growing exponentially.

Businesses like yours are adopting technologies that deliver the promise of ubiquitous computing. Employees are using personal tablets and Smartphones for work purposes. Your company is fielding its own fleets of mobile devices and applications. You’ve embraced collaboration tools, such as Microsoft SharePoint and Google Docs, to reduce the data storage and bandwidth burden imposed on email and promote free-flowing information between departments. You’ve enhanced email as a communication tool by adding social collaboration applications. While these systems help you save time and work smarter, they require maintenance and store copious volumes of data.

No doubt, you are genuinely conscientious and exercise reasonable security best practices as part of your IT operations. You may be forced to focus on staying in compliance with government regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and/or the Health Information Technology for Economic and Clinical Health Act (HITECH); customer or partner security requirements and/or standards, such as ISO 27001; other industry standards, such as the Payment Card Industry Data Security Standard (PCI DSS); and, if you’re in the education sector, the Children’s Internet Protection Act (CIPA) and the Children’s Online Privacy Protection Act (COPPA). Regulations like these are sometimes implemented in response to past concerns and don’t always reflect current technology or threats. It’s possible to be compliant but not secure.
So you are doing your best. But is it good enough? Security investment is about due diligence and providing a reasonable level of security. Many companies are also investing in technologies that go beyond conventional antivirus software and firewalls. Perhaps you’re already buying mobile device management (MDM) technology to control and contain the influx of smartphones and tablets. Maybe you’re even adding encryption to your email and file-sharing systems to ensure that confidential customer information is kept safe from the prying eyes of hackers. Some of you are implementing patch management systems to track and push software fixes across operating environments to prevent applications from becoming security breaches.

Despite this grand technology investment, you may have limited resources to manage these various security platforms. Even if there is an IT administrator and a fully-staffed IT department, disparate security systems simply don’t talk to each other. Every time a systems administrator runs a report, implements a change, responds to an alert or updates software, he or she must go to a different management console for each specific application. The real issue is this manual coordination of supposedly synergistic technologies. When operating in concert, these technologies will enhance the effectiveness…but not if they’re too complex.

If you have five different security applications, and it takes five minutes to perform a single function on each platform to engage in a coordinated security action, it will take 25 minutes overall to implement the change. Then, you need to add the effort required to verify that the change was implemented properly, as the reporting mechanisms for each application are different. Sometimes there are also different steps for computers that are connected to the system and mobile devices that are connected via VPN. The net result is a security administrator who will spend hours sifting through reports and screens to perform a function that should be relatively automatic. The number of steps required to reconcile security actions and reporting inevitably leads to mistakes.

The higher the complexity of security technologies and the more time it takes to effect change, the greater the security cost, the increased likelihood of human error and the lower the return on your security investment. In theory, this process is manageable. In practice, it’s a nightmare. No matter how good the security administrator is, the number of steps required to reconcile security actions and reporting will inevitably lead to mistakes – and these mistakes are opportunities for hackers and malware to infiltrate defenses. And, of course, time is the friend of the hacker. The more time hackers have to enumerate a network or device, the more likely they are to exploit vulnerabilities and steal precious information.

Even if there is an IT administrator and a fully-staffed IT department, disparate security systems simply don’t talk to each other.
Cybersecurity risks and hacker attacks have never really been one dimensional, but they haven’t always been as sophisticated as they are on today’s threat landscape. Businesses of all shapes and sizes are running a daily gauntlet of malware, advanced persistent threat (APT) attacks, unsecure software and an exponentially greater probability for human error that could lead to data leaks, compromises and corruption.

Security challenges go far beyond malware, but viruses, worms and Trojans are a big part of the problem. Over the last four years, malware proliferation has exploded, with all major security companies reporting annual rates of three million new samples. Most malware is a variant of an original sample, but this doesn’t make them any less potent. The sheer volume makes it difficult to keep up.

More disconcerting is the shift in what malware is attacking – namely the application layer. Malware used to target the OS, with Windows being the mark of choice. Today, malware has escalated up the proverbial stack to applications, so much so that Windows often doesn’t even make the list of the Top 10 vulnerable software packages. Malware that targets applications is dangerous on two levels. First, applications are where data is generated and resides. Second, the volume, sourcing and diversity of applications make it difficult to stay current with patching and code updates.

According to SecureList, “70 percent of all vulnerabilities target three common applications: Microsoft’s Internet Explorer (browser), Adobe’s Portable Document Format (PDF), and the universe of Oracle Java-based applications, many of which run in browsers and on mobile devices.” Users are accustomed to downloading applications to their PCs and Smartphones, creating dozens of managed and unmanaged applications, each carrying a number of potential vulnerabilities.

---

2. SecureList, March 2012
The increasing diversity of device and operating platforms on which businesses transact data only amplifies the security challenge. It was once argued that the monolithic dominance of Windows on the computing landscape hurt security because it gave hackers a broad attack target. Platform diversification, some experts suggested, would make it harder for hackers to exploit systems.

Today, mobility and open-source trends have made Apple’s iOS and OS X and Google’s various flavors of Android operating systems as prolific as Windows. The volume of security vulnerabilities have shifted to these platforms, but this increasing number of operating systems and the tens of thousands of applications written for them are making it nearly impossible to chronicle and remediate vulnerabilities. This trend is seen in the diversity of vulnerable applications and operating systems.

Application and operating system proliferation is only half the story; the other half is mobility, in which millions of small, portable and data-laden devices are circulating in the business workspace. Last year, millions of Smartphones entered circulation, and that number is expected to grow to nearly 1 billion by 2015. A research analyst firm Gartner forecasts that the total number of tablets sold will climb to 326 million by 2015. All of these mobile devices are finding their way into work environments. End-users are looking to mobility as a means of blending their professional and personal digital lives. Wireless connectivity, cloud services and file-synchronization applications are making these devices highly desirable targets for physical theft.

In the U.S. alone, hundreds of Smartphones are lost every hour. The numbers are even higher on global studies. Some reports peg the number of lost or stolen laptops and tablets at U.S. airports at 12,000 per week. And studies have shown that the average person who finds a Smartphone will try to access files, text messages and other sensitive data on the device. Thieves and hackers with stolen mobile devices will compromise them to lift valuable data or use them to penetrate the networks to which they are connected. The direct monetary damage of device loss and theft is estimated at $30 billion annually; the indirect costs of any associated hackings are unknown. With limited resources, businesses like yours are struggling to keep up with the waves of technology innovation that can help improve business performance but also expose data to mounting security threats.

Beyond Coordinated:
Integrated Security Platforms

But what if antivirus, encryption, patch management, MDM, intrusion prevention and other security technologies were placed under the “single pane of glass?” What would that look like from a functionality and value proposition perspective?

Unified threat management technology (UTM) provides some clues. Introduced a decade ago, UTM appliances combine the functional applications of different security technologies on a single prepackaged machine. UTMs are primarily designed for network-level security and include antivirus, firewall, intrusion prevention, content and Web-filtering and virtual private networks (VPN).

A consolidated security platform is the best win for your business. You want a “single pane of glass” security platform because it enables insight into risk exposure, applications and devices in one place. A single console allows you to set controls and policies to protect data, devices and assets. And by extending more security functions with greater ease and speed, you’ll have increased protection over your entire infrastructure and data domain.

The advent of security platforms like Kaspersky Endpoint Security for Business provides consolidated management and reporting across all endpoints and data types will provide your business with the security capabilities you need and the reduced complexity you seek.

Call Kaspersky today at 866-563-3099 or visit us at www.kaspersky.com/business, to learn more about Kaspersky Endpoint Security for Business.

Now you can SEE IT, CONTROL IT, PROTECT IT, with Kaspersky Lab.

About Kaspersky Lab

Organizations need intelligent security technologies to protect their data – and they also need intuitive and uncomplicated IT efficiency tools. Kaspersky Lab’s 2,500 employees are driven to meet those needs for the 300 million plus systems they protect – and the 50,000 new systems a day that are added to their number.

Kaspersky Systems Management is a component of Kaspersky Endpoint Security for Business. Combining award-winning anti-malware, IT policy enforcement tools, centralized management and cloud-assisted protection, Kaspersky’s business security products are the right choice for your organization.

Talk to your security reseller about how Kaspersky can bring secure configuration to your networks, the devices that run on them – and more!