YOUR DATA UNDER SIEGE: GUARD THE GAPS WITH PATCH MANAGEMENT.

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

Be Ready for What’s Next
Until recently, most businesses took a traditional, perimeter-based approach to information security. The thinking was: “If we build a wall high enough, nothing will get in.” That was fine until cyber criminals started looking for unguarded cracks in the masonry, forging counterfeit keys for the padlocks and tricking the guards into letting them in.

Today’s threat landscape is more than any traditional, anti-virus-only security strategy can handle. There’s simply too much going on. Between 1992 and 2007, Kaspersky Lab identified approximately two million unique malicious programs. By 2009, that figure increased to 33.9 million and 2010 hit a new record, as 1.5 billion malware incidents were recorded; more than a third of them browser-based.

By 2012, Kaspersky Lab experts were detecting an average of 200,000 new malicious programs every single day. No wonder only 31 percent of IT specialists had heard of the most widespread threats in 2012!¹ There’s so much out there, you can’t possibly keep track of every threat. Even the U.S. National Security Agency has shifted its stance to one that assumes a breach.² The reality for business is that the weakest link in the security chain is already sitting on their systems – or sitting in front of them.

Say hello to your applications. Their vulnerabilities, in the hands of the all-too-human end users who download and launch them, make applications one of the biggest threats to your business’s information security today. This risk is compounded by the complexity of your IT infrastructure and a constantly evolving threat landscape. If you don’t know what you’ve got, how can you secure it?

Third party applications accounted for a massive 87 percent of vulnerabilities in 2012.³ That same year, Kaspersky Lab recorded more than 132 million applications at risk. Given that the average user has about 72 programs installed on his/her machine⁴, tracking, finding, patching and blocking these vulnerabilities is no small task.

If you don’t find them, it’s safe to say that the criminals will; all five of the major vulnerabilities found in Java in 2012 were actively exploited by criminals.⁵ In 2010, weaknesses in Microsoft Office were among the most frequently exploited. Criminals never stop looking for ways into your systems.

---

³. Secunia Vulnerability Review, March 14, 2013
⁴. Secunia Vulnerability Review, March 14, 2013
⁵. Evaluating the Threat Level of Software Vulnerabilities, Kaspersky Lab, 2013
Almost every program has vulnerabilities, but you’d be wrong to assume that Microsoft applications account for most of them. As this pie chart illustrates, the most susceptible applications have two things in common: they’re widely used and they’re third party applications. Focus solely on patching Microsoft OS and programs, and you’re only covering a small fraction of potential threats.

So where do you begin? How can you find out which programs are installed on which endpoints? And which of these contain vulnerabilities? Did all the updates you sent out last week go to all the endpoints they were supposed to? Did any of your users switch off before the update process was completed? Will the patches and updates for a particular piece of software affect the functionality of others? Is there some way you can test these things? How do you know which vulnerabilities are the most critical? Can you schedule less important updates for after hours?

If you’re running systems management technology with automated vulnerability scanning and patch management, the answer to all of these questions (and a lot more) is “Yes.”

Managing and administering software updates while constantly monitoring for potential vulnerabilities is one of the most important, challenging and resource-intensive tasks faced by an IT department. With criminals repeatedly scanning systems for any sign of weakness, it’s vital that IT administrators can find and fix gaps in security before they’re exploited. The first step in achieving this goal is to establish exactly what software – and which version – is sitting on your systems. These inventory checks are often so complex and demanding that IT departments avoid them, reducing the effectiveness of any vulnerability scanning and patching initiative.

You need a systems management solution to automatically perform this for you, compiling an up-to-date picture of the software and hardware landscape you’re responsible for.

Managing and administering software updates while constantly monitoring for potential vulnerabilities is one of the most important, challenging and resource-intensive tasks faced by an IT department.
What browser versions are people using? Are employees running software you don’t want them to use? Have people added devices such as smart phones to the network without permission? It’s important to monitor all these factors if you want to keep your system safe.

Another key benefit of the inventory process is its ability to highlight the presence of legacy software on your systems. These outdated applications can represent a significant threat, sitting on your systems, unknown and unpatched, just waiting for a targeted attack that’s likely to go undetected in organizations where no one even remembers the software is there.

While an overwhelming majority of popular vulnerabilities were detected in 2011 and 2012, Kaspersky Lab research has found that almost two-thirds of discovered software flaws were found in programs released in 2010 or earlier, reinforcing the need to get an accurate inventory of your system’s software.

The first vulnerability scan you perform is likely to reveal a grim picture. If you keep tight controls over user administration rights on endpoints, expect to see near-obsolete software and versions of software that many employees are reluctant to upgrade “because they just work.”

Don’t worry. You’ve discovered some of the most vulnerable points you (and the criminals) are searching for and you are experiencing a typical problem:

- According to Kaspersky Lab research, more than 70 percent of users of the most vulnerable programs (Abode Reader, Flash and Java) are “highly reluctant” to update. In fact, seven weeks after Oracle released a new version of Java, fewer than 30 percent of users had upgraded. Major Web browser updates take about a week to reach the same uptake levels.

- Some of the vulnerabilities Kaspersky Lab has uncovered on endpoints were first identified as long ago as 2003. There was a patch available, it just hadn’t been installed.

With system management technology, detailed information on vulnerabilities is gathered, analyzed, assessed, and then automatic fixes are scheduled based on whether the risk is “Critical,” “High” or “Warning.”

Choose a solution that can evaluate the vulnerability status of your network and generate reports that either show individual endpoints by severity of weakness or allow you to click on the vulnerability name in an aggregated table to view a list of all affected endpoints. Automating updates and patching is important, but you also need to manage how those updates work with your other security tools, such as antivirus and application controls, as well as other applications.

One vendor’s patch can sometimes wreak havoc with another piece of software. Sometimes patches are released too soon, before dependencies and other issues have been resolved, creating conflicts and limiting the functionality of other software. Web-based applications, in particular, can be susceptible to this – scripting tools that operate only with specific browser versions or applications that have complicated Java dependencies, for example.

The right solution will make it easy for administrators to test deployments prior to implementation. You should be able to do this on selected individual endpoints, specified groups, or even a set percentage of randomly chosen computers within a specified group likely to be affected. Issues discovered should be manually excluded from the overall patch process.
Effective strategy

Vulnerability scanning, implemented in tandem with an effective patch management strategy, can help you to keep one step ahead of criminal hackers. An effective strategy should take care of that for you.

• **Keep up to date**: Outdated software creates weak spots across your business, whether it’s on your servers or at the endpoint. Use automated, regularly-scheduled vulnerability scans to keep you abreast of weak points, allowing you to automate the implementation of patches and fixes.

• **Automate**: Effective patch management improves reliability and IT efficiency. By automating the deployment of software updates and the administrative tasks that go with it, the right technology helps minimize downtime associated with patch deployment, auditing and roll-back.

• **Roll back the clock**: Updates/installations don’t always run smoothly. Sometimes, patches can cause instability or are incompatible with other software or drivers on your machines. Your security technology should address this issue simply. The Kaspersky solution includes integrated image/provisioning functionality, making it easy to roll back to a fully-functioning, optimized system.

• **Gain complete visibility**: By automating scanning, you’ll have complete visibility into the current state of patching and updates on all machines.

• **Prioritize**: Comparing the results of your scans against multiple vulnerability databases will help you to gain an understanding of the risks associated with any vulnerability. In addition to Microsoft Windows Server Update Services (WSUS) and Secunia Vulnerability Database, Kaspersky Lab’s dedicated Security Network (KSN) works in tandem with vendors and millions of users globally to ensure the most detailed, up-to-date information on software and vulnerabilities is available. Over one million files are added each day. Based on this intelligence, you can prioritize patching, rolling out less urgent fixes after hours and spreading the load on your network.
• **Implement Dynamic Whitelisting**: Integrated, dynamic whitelisting functionality boosts vulnerability scanning and patch management through the addition of an extra layer of security: application control. Because today’s “safe” application is tomorrow’s threat that needs to be patched, isolated or blocked.

• **Conduct deep analysis of each new threat**: Instead of the usual “just block it” approach, every detected threat is analyzed to understand the initial intention of attack. From heuristic and signature-based analysis to source detection and reputational analysis, everything is compared against Kaspersky’s real-time Security Network (KSN), which detects and analyzes millions of threats globally each day. This gives you a more risk-aware, agile security posture.

• **Report**: Accurate, up-to-date and detailed information is a vital part of any security and risk management strategy. By running reports on your scans, you add another layer of insight – allowing you to examine and report on potential weak spots, spotting and tracking changes and also giving detailed insight into the patch status of every device and system on your network.

Targeted attacks, advanced persistent threats, automated attacks and zero-day vulnerabilities all shrink the time between vulnerability discovery and the creation of an exploit. By automating and scheduling regular scans and patch implementation, IT administrators can streamline their patching and vulnerability scanning processes without compromising on their effectiveness.
Vulnerability scanning and patch management form two components of a wider systems management approach to IT security. By integrating key functionality such as dynamic whitelisting, application control, vulnerability scanning and patch management with complementary technologies such as inventory management, imaging/provisioning and network admission control (NAC), Kaspersky Lab is able to deliver a level of security far greater than the sum of its parts.

Add in the vital, full-featured spectrum of antivirus, anti-spam, web controls, and anti-spyware technologies, and you can not only see where the vulnerabilities in your systems lie, but control and protect them too.

As IT professionals struggle to do more with dwindling resources and budgets, there’s a danger that complete visibility and control over business networks will be lost as administrators are forced to focus on urgent issues, often to the detriment of essential, yet mundane, tasks.

By centralizing and automating many essential configuration and management tasks, IT administrators can not only save themselves time, but money too. Effective systems management, driven by centralized configuration, vulnerability scanning and patch management tools, supports many of the best practices that optimize IT resources while enforcing your company-specific policies.

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

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!

Learn more at www.kaspersky.com/business.