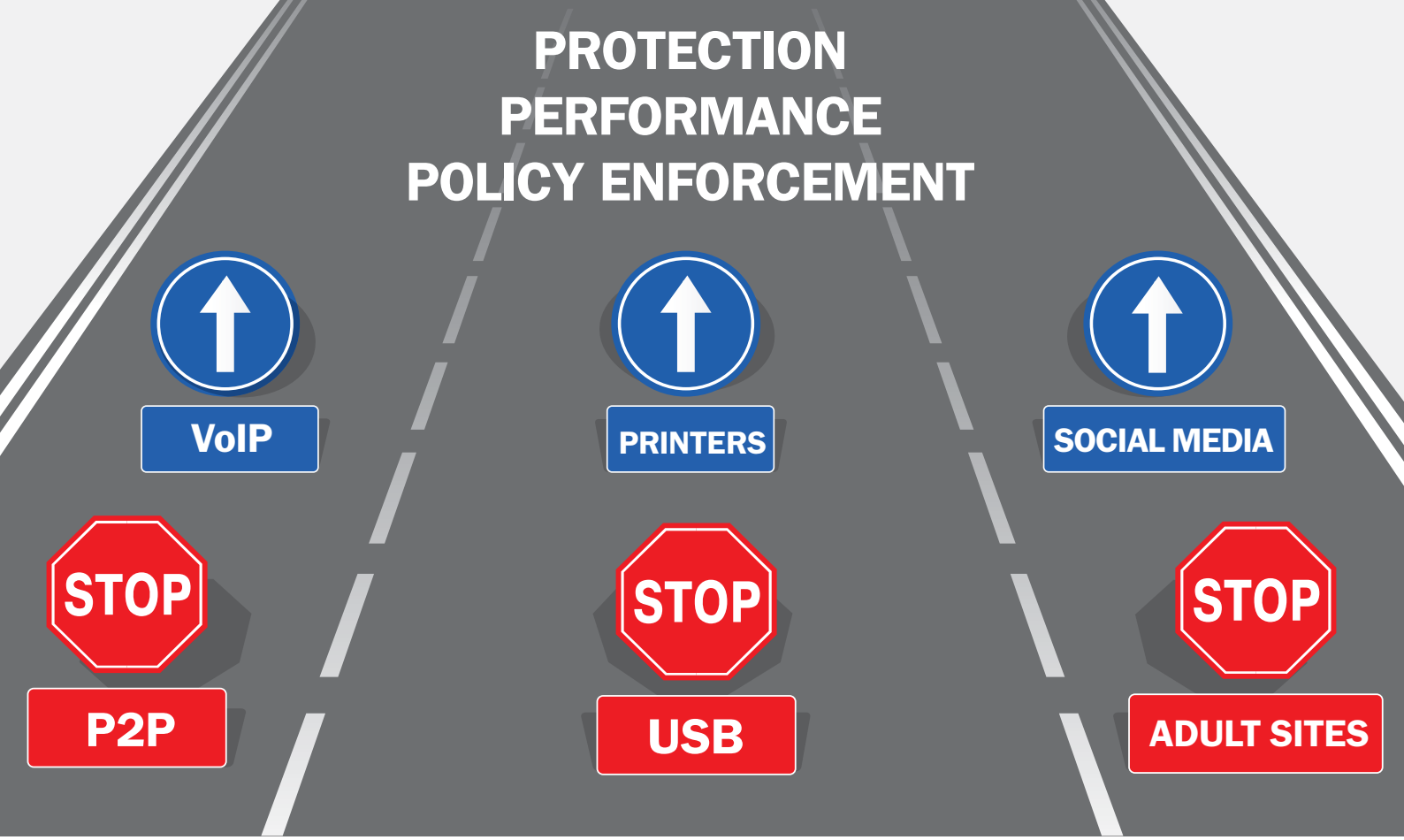

IT security. Are you in control?

Why security risks are not just a big company problem.

kaspersky.com/beready

KASPERSKY lab

Introduction

1.0

“

THERE ARE DOZENS – IF NOT HUNDREDS – OF BREACHES AT COMPANIES WITH LESS THAN 500 EMPLOYEES.

In the real world the security landscape can be a harsh environment. Hackers are using more sophisticated attack methods to penetrate networks and steal company data; social networks are being compromised and used to distribute malware, and instigate phishing attacks; and the proliferation of mobile and cloud applications are opening new vulnerabilities ripe for exploitation.

These vulnerabilities are equally true for small and mid-sized businesses (SMBs), but too often SMBs misjudge their level of risk exposure as it is often the big corporate security breaches and embarrassing data compromises that command media attention, for example:

- In 2007, 94 million credit card records were compromised at TJX, a US discount retailer, in one of the largest information security breaches on record.
- In 2011, the personal information of more than 35 million users of SK Communications, a South Korean social networking provider, was compromised by an attack that spanned several countries.
- And, most recently, at least 100 million Sony customers were exposed to risk when their personal data was compromised.

For every one of these big security breaches, there are probably dozens – if not hundreds – of breaches at companies with less than 500 employees. Businesses often wrap themselves in a false sense of security believing that they are not as interesting or valuable to hackers and cybercriminals. That belief is wrong.

What most businesses fail to realise is that they are dealing with the same treacherous security environment as those headline-hitting enterprise players and must be mindful to the threats posed by social networks, mobile devices, advanced persistent threats (APTs) and conventional attack vectors.

Vulnerability at the Endpoint

2.0

REGARDLESS OF THE SIZE OF A BUSINESS, A BETTER SECURITY POSTURE IS A RESULT OF PEOPLE, POLICIES, PROCESSES AND TECHNOLOGY.

The common denominators in any security breach are insecure and unmanaged endpoints. The problem is only getting more complicated for businesses as they operate under the crushing weight of consumerisation and 'bring your own device' (BYOD) trends.

Mobile devices, tablets, smartphones and next-generation ultralight notebooks will open up new vulnerabilities. Businesses have to overcome bigger challenges in managing an increasingly complex mix of hardware diversity and applications with limited resources and expertise, and end-users that are unaware of the threats.

The solution for businesses is two-fold: awareness and consolidation.

- Firstly, they need to realign their thinking about security threats and educate end-users about the risks of using insecure devices, applications, clouds and websites.
- Secondly, they need to realign their security posture around better endpoint security solutions that provide multi-faceted risk mitigation.

But regardless of the size of a business, a better security posture is a result of *people, policies, processes and technology.*

This whitepaper gives key insights into the threats businesses face with the explosion of new malware, operating platforms, cloud-based applications and consumerisation; as well as outlining how to leverage comprehensive security solutions such as Kaspersky Endpoint Security 8 to better protect data, devices and end-users wherever they are.

Chaos at the Endpoint

3.0

Consider these numbers:

- Smartphone ownership in the United States climbed to 46% of the addressable market in 2012 – an 11% year-over-year increase (Pew Research Center)[1]
- The smartphone market is set to grow 38.8% year-over-year to 686 million units this year (IDC)[2]
- While tablet sales are expected to top 326 million by 2015. (Gartner, Inc.)[3]
- Apple iOS dominates the worldwide market, with a 52% marketshare (the iPhone and iPad each taking 26%) compared to 16.2% for Android (NetMarketShare)[4]
- Global sales of tablet and IP-enabled eReaders are expected to approach 500 million units by 2015, surpassing PC sales (Business Insider)[5]

'Endpoint' once meant a 'PC' and the good news is that is still true. The problem is that the 'PC' has changed – and this is presenting a plethora of new risks.

Just three years ago an endpoint was nothing more than a conventional laptop or desktop PC, probably running a version of Microsoft Windows, and a raft of client-side applications that were usually Microsoft or compatible.

That is no longer true. An endpoint can be a conventional PC – but it can also be a smartphone, a tablet or an IP-enabled digital device. These devices don't just run Microsoft Windows; they are powered by Apple iOS or the various flavours of Google's Android OS.

The endpoint is no longer a single platform – if it ever was. The increasing use of mobile devices for e-commerce and electronic payments, such as Google Wallet, as well as mass data storage, is making smartphones and tablets an increasingly tempting target for malware writers. Security vendors including Kaspersky Lab concur that the volume of mobile malware and attacks against mobile devices are increasing exponentially. In fact, Kaspersky Lab's researchers recorded 5,255 new modifications of mobile threats and 178 new families, representing an increase by a factor of 6.4 over the course of a year. Meanwhile, researchers discovered more new malicious programmes in December 2011 alone than over the entire 2004-2010 period.

Complicating the security challenge facing businesses is the ill-placed confidence end-users have in their new devices and operating systems. Apple's Mac OS has a longstanding reputation for being more secure than comparable Windows operating systems but this perception doesn't come from the lack of vulnerabilities, but a small market share. As Apple's user base increases with the huge adoption rates of iPad tablets and Mac PCs, hackers and malware writers are going after these systems because there are a greater number of targets with richer rewards. The same holds true for Android-based smartphones and tablets, and potentially for Chrome-powered PCs.

In 2003, security researchers lead by Bruce Schneier and Dan Geer published the famed and controversial paper 'CyberInsecurity: The Cost of Monopoly'[6], which criticised Microsoft's dominance of the operating systems market and detailed how the lack of diversity was creating greater vulnerabilities and risks. Today, Microsoft is still the top OS vendor, but it no longer dominates the market. The diversity these researchers once sought is now a reality, and is creating a management and security nightmare that few businesses can afford.

While SMBs may not think of themselves as particularly enticing targets for hackers when compared to giant corporations or military contractors, cybercriminals make continuous and sustained assaults aimed at the perceived 'low hanging fruit', or the most vulnerable targets. InformationWeek reports a rise in targeted sophisticated malware[7], attacks like the ones that automatically generate phishing emails apparently sent from a trusted source – tax correspondence, for example, or a shipping notification or bank statement.

[1] Three-Quarters of Smartphone Owners use Location-Based Services – Pew Research Center, 11th May 2012
[2] IDC Worldwide Mobile Phone Tracker, 6th June 2012
[3] Gartner Press Release - Gartner says Apple will have a Free Run in Tablet Market Holiday Season as Competitors Continue to Lag – Gartner, Inc., 22nd September 2011
[4] Mobile/Tablet Top Operating System Share Trend, July 2011 to May 2012 – NetMarketShare
[5] Tablet Sales will Blow Past PC Sales to Nearly 500 Million Units a Year by 2015 - Business Insider, 14th February 2012
[6] CyberInsecurity: The Cost of Monopoly How the Dominance of Microsoft's Products Poses a Risk to Security – Bruce Schneier, 23rd September 2003
[7] Evolving Security Threats: Is your SMB Ready? - Kevin Casey, InformationWeek, 14th October 2011

IT staff are focused on keeping the network up not bolstering security systems.

Verizon Data Breach Investigations Report[9]
69% of attacks on organisations involved malware.
97% of attacks could have been avoided with 'basic or intermediate' security controls.
92% of breaches were discovered not by the targeted organiSation but by a third party.
85% of those breaches took more than two weeks to discover.

Almost all organisations record sensitive customer data or credit card numbers. In SMBs, this information is often inadequately protected, which leaves it vulnerable to a barrage of increasingly sophisticated security threats. While they don't typically store significant assets online, SMBs are easy targets due to their lack of cash flow and resources, which often translates into an outdated, unpatched, inferior or in some cases a non-existent security infrastructure.

Similarly, SMBs generally lack the resources to employ dedicated security staff, or IT personnel, trained to detect, respond to and control any security threat on their network. In an environment where employees are asked to fulfill numerous job functions, any dedicated IT staff are focused on keeping the network up and running, and responding to 'fire alarm' emergency situations – not bolstering security systems.

That lack of expertise – coupled with the fact that employees often have to spend most of their energy just running the business – can create glaring security holes and an overall lack of awareness. As such, deficiencies in security best practices can leave workers open to more attacks through apparently legitimate, if unsolicited, emails and phishing attacks aimed at infiltrating sensitive accounts. This SMB specific vulnerability was illustrated in an InformationWeek article, Who Bears Online Bank Fraud, Bank or Business?[8] highlighting how Patco, a family-owned construction firm, fell prey to the Zeus botnet in May 2009, when hackers broke into its account with Ocean Bank and stole more than $588,000 before the malicious activity was detected.

Lightning Strikes the SMB

The Greek god Zeus cast fear into the hearts of men in ancient times but in May 2009, the mythical god's lightning bolt came down hard and fast on an unlikely target: Patco Construction Corporation, a family-owned construction company in Sanford, Maine, United States.

Via a malicious email opened by an unassuming employee, the Zeus Trojan stole passwords and siphoned around $100,000 per day from Patco's online account with Ocean Bank, a small branch business of People's United Bank. Nearly $600,000 was stolen before Patco noticed the breach, contacted the bank, and prevented hackers from stealing another $240,000.

In the end, Patco sued Ocean Bank to recoup its losses, alleging that the bank was negligent for not properly verifying the stolen Patco credentials. In June 2011, the court ruled that, although it did not authenticate the stolen logins and passwords, the bank was not liable for what, in essence, was Patco's breach. The judge noted that Patco should have secured its applications and endpoints better.

Patco's story is not an uncommon one; it is a lesson for all businesses. Lock down the information at the endpoint where it resides to defend against data loss and compromise. At Patco, a combination of end-user education on the variety and sophistication of threats, and a proven endpoint security suite could have prevented enormous financial damages and a lot of legal trouble.

[8] Who Bears Online Bank Fraud, Bank or Business? - InformationWeek, Kevin Casey, 27th June 2011
[9] 2012 Data Breach Investigations Report - Verizon Business, 2012

A New Kind of Social Disease

4.0

NEARLY ONE IN EVERY FIVE MINUTES SPENT ONLINE IS SPENT ON SOCIAL NETWORKING SITES AROUND THE WORLD.

Poorly protected and unpatched endpoints are only part of the problem. There are whole new considerations presenting themselves: the cloud and social networks.

To fully appreciate the power of social networks and the rise of the social information age, look no further than Facebook, which stands as the world's largest social network with more than 900 million active accounts and this is growing daily. Facebook adds more than 700,000 new pages a day, up from 465,000 between September and April 2012. But with a global population of 7.5 billion people, Facebook still has some way to go before it reaches total market saturation. But raw membership numbers don't tell the full story behind Facebook. Facebook's real threat is its impact on time – with each user spending an average of over 15 hours per month on Facebook.[10]

Now, consider how many other social networks there are: Pinterest, Twitter, Google+, Tumblr, YouTube, Apple Ping, AOL, LinkedIn and so on. While the average amount of time spent on each of these sites is substantially less than Facebook, the combination of daily visits across the social spectrum is eating up a significant portion of an end-user's day. According to comScore social networking sites now reach 82% of the world's online population.[11] In addition, nearly one in every five minutes spent online, or 20% of the time, is now spent on social networking sites around the world – a stark contrast to March 2007, when the category accounted for only 6% of time spent online.

Here's an eye-opener: The majority of Facebook users are 25 years old or older, so when do they spend all this time on Facebook and other social networks? Chances are some of that time is spent perusing social networks at work!

Despite user protests that Facebook is a useful business communication and collaboration tool, some companies have curtailed or blocked social networking sites to prevent productivity drains. Still, most businesses simply allow open access to social networks, for reasons ranging from keeping employees happy to enabling marketing and dissemination of information about the organisation.

Lost productivity should be a real concern to businesses, but so too should the potential for data loss and malware infections spreading through social media tools.

[10] Facebook, YouTube, our collective time sinks (stats) - Pingdom.com, February 2011
[11] It's a Social World, Top 10 Need To Knows About Social Networking and Where It's Headed - comScore, December 2011

ONLY 37% OF USERS SAY THEY HAVE USED FACEBOOK'S PRIVACY TOOLS TO CUSTOMISE WHAT INFORMATION APPLICATIONS ARE ALLOWED TO SEE.

In light of the Internet's inherent anonymity, users might feel more comfortable sharing information online from the comfort of their homes or offices than they would face to face with a total stranger. Meanwhile, only 37% of users say they have used the site's privacy tools to customise what information applications are allowed to see, according to InfoSecurity Magazine.[12]

So accidental data leakage can occur through an employee using Twitter to share news about a product release – or posting a frustrated status update about the company losing a deal to a competitor. But data loss can also mean the malicious disclosure of sensitive information designed to harm the company. Information that could linger, cached in cyberspace infamy, long after being removed from the site.

The exponential rise and rapid spread of malware delivered virally via social media is a significant problem. For years, numerous variants of the Koobface worm, ran rampant on users' machines. Meanwhile, Trojans and Internet worms continue to plague social networking users, typically enticing them with some kind of game or video before installing itself on their systems. Other attacks steal login credentials by requiring users to re-enter names and passwords into a fake login page.

However, what puts endpoint security in disarray is the countless third-party applications in the form of adware, online games and surveys embedded in social network sites, not the sites themselves. Once they have bypassed security mechanisms, the loosely filtered applications entice unsuspecting users with any number of distractions – quizzes about their personal life or the possibility of seeing who was checking out their profile page. Before users know it, they have downloaded malware onto their systems and spread the infection to everyone on their contact list.

Security suites such as Kaspersky Endpoint Security 8 not only safeguard PCs and mobile devices against malware infections spread across social websites; they also include application controls to limit usage by disabling risky add-on applications and features.

[12] Nearly 13 Million Facebook Users Are Clueless About Privacy Controls - InfoSecurity Magazine, 3rd May 2012

Application and Cloud Contaminants

5.0

“

UP TO 85% OF ALL VIRUS INFECTIONS STEMMED FROM AUTOMATED DRIVE-BY ATTACKS CREATED WITH COMMERCIAL EXPLOIT KITS.

The industry has dubbed devices such as the Apple iPhone a ’smartphone’. In reality, smartphones and their tablet cousins aren’t all that smart or interesting without their applications and cloud-based services. These applications and cloud services are also the source of new attack vectors and malware distribution.

Vulnerable third-party applications, which are increasingly exploited by hackers, routinely vex users. Unfortunately for the SMB, some of the most common third-party business tools are also the biggest targets, including Java Runtime Environment (JRE), Adobe Flash, Adobe Acrobat and Reader, Internet Explorer and Apple QuickTime, according to TechTarget.[13]

These common, vulnerable and unpatched third-party tools can essentially make the web-browsing experience on conventional PCs and mobile devices even more perilous, further exposing users to an array of attacks that include drive-by downloads, cross-site scripting and other zero-day threats. A study conducted by Copenhagen-based research firm CSIS Security Group A/S found up to 85% of all virus infections stemmed from automated drive-by attacks created with commercial exploit kits, nearly all of which targeted the third-party tools mentioned above.[14]

In addition, popular peer-to-peer (P2P) applications such as Skype, and file-sharing tools such as Dropbox, further erode fragile endpoint security systems. Illicit download sites, as well as legitimate cloud file-sharing applications like SugarSync and Huddle, are often vehicles for malware distribution. Attacks are executed when unfiltered or unscanned malicious files are freely delivered to recipients and downloaded onto vulnerable systems.

Even barring malware attacks, P2P and file-sharing sites clearly expose the endpoint so users can inadvertently save a private file to a shared drive or folder, enabling unauthorised users to access sensitive information. These applications pave the way for a user to accidentally open share drives or folders that contain sensitive information, increasing the risk of identity theft.

These cloud-based risks are only increasing as consumerisation and BYOD trends continue. End-users want to access information and applications whenever and wherever they are. For that kind of ubiquity, they turn to the cloud. At the very least, businesses need security applications that constantly sample an endpoints’ web connection, the files transmitted over shared drives and any cloud services, to prevent malware from spreading over P2P networks.

[13] Time To Ban Dangerous Third Party Apps? Exploring Third Party App Security, Eric Parizo, TechTarget, January 2012
[14] This Is How Windows Get Infected With Malware - Peter Kruse, CSIS Security Group A/S, 27th September 2011

Protecting the Endpoint

6.0

WHAT'S NEEDED IS A MULTI-FACETED SECURITY SOLUTION THAT PROVIDES MANAGEABILITY, OPTIONS FOR MULTIPLE OPERATING SYSTEMS, ANTI-VIRUS AND SPAM CONTROLS, POLICY ADMINISTRATION FOR DEVICES AND APPLICATIONS, AND A VULNERABILITY SCANNER.

Here are the facts: businesses are losing control over their endpoints. In fact, soon many won't even own their employees' endpoints.

Security threats are on the rise from multiple vectors, so it's absolutely imperative that they find a way to fill the gaps. In other words, it's time for businesses of all sizes to take control of their security posture.

The expense and effort required to secure and manage an increasingly diverse endpoint population is taxing for all companies. What's needed is a multi-faceted security solution that provides manageability, options for multiple operating systems, anti-virus and spam controls, policy administration and enforcement for devices and applications, and a vulnerability scanner to point out areas where exploits can occur. Hackers know the weak links in the chain are insecure and vulnerable applications, so one of the first stops on any companies security journey should be deploying application control and whitelisting technologies.

Kaspersky Lab is different in its development of market-leading security technology and its inclusion of features and security controls in a single suite. **Kaspersky Endpoint Security 8 for Windows** (EP8) offers more than just high-performing anti-virus and malware protection technology; it includes powerful tools to protect data and safeguard both endpoints and their users from malicious code, applications and websites. EP8 includes a software firewall and intrusion prevention application that detects and blocks hacker attempts to take over an endpoint. It also scans all Simple Mail Transfer Protocol (SMTP) and Post Office Protocol 3 (POP3) emails to ensure no compromised messages deliver malware. Its **Urgent Detection System** engine identifies phishing attacks and malicious websites, ensuring users don't accidentally expose themselves to hackers' traps.

Beyond malware and web threats, EP8 is a powerful security suite constantly on guard to minimise endpoint risk exposure. Its **Vulnerability Scanner** identifies unpatched software that could leave applications and computers open to compromise. The **Device Control** feature allows administrators to limit or block mass-media devices from connecting and transferring files, minimising exposure to malware and data loss. Its **Application Controls** give administrators and end-users the ability to regulate applications, or even stop them from activating, increasing performance and minimising the potential attack surface. The **Application Privilege Control** feature can restrict applications from accessing computing resources, denying them the ability to execute.

As for cloud-based applications, social networks and applications embedded in social networks - EP8 includes controls for those too. The **Web Controls** and **Content Filtering** features scan HTTP traffic and URLs to determine the trustworthiness of Internet destinations. Businesses can use EP8 settings to grant users an appropriate level of access to social and cloud applications, and provide protection from many security threats.

Security administration and management is a persistent challenge for businesses. This is where Kaspersky Lab's EP8 gives businesses the necessary options to bring order to the wide diversity of endpoint devices. Whether it's a conventional PC, smartphone or tablet, Kaspersky makes versions of EP8 for Windows, Linux, Android and Blackberry devices. The **Kaspersky Security Center 9.0** admin console provides easy-to-use management layers that simplify policy creation and administration, device management, software updates and security performance reporting.

Conclusion

7.0

Small and mid-sized businesses are exposed to just as many types and volumes of security threats as their enterprise counterparts. The lack of expertise and lack of resources required to provide security to the growing diversity of endpoints is ever more challenging. The application of a security suite with the range and capabilities of Kaspersky Endpoint Security 8 is no longer a choice – it's an imperative. The alternative is constantly chasing lost productivity, compromised data and increasing amounts of downtime – none of which any company can afford.

About Kaspersky Lab

With the increase in sophisticated malware, use of potentially malicious applications and employees bringing their own devices to work, it's even harder to manage all the potential IT security threats within your business.

With Kaspersky Endpoint Security 8, you set the rules, you control applications, web and device usage.

If it's happening in your business, Kaspersky can help you see, manage and protect it.

You're in control. You're in the driver's seat.

Be Ready for What's Next
kaspersky.com/beready