1. INTRODUCTION

Social media, smart devices, web-based applications, spam, phishing, malicious websites, social engineering, malware… Today’s IT professional is coping with an increasingly complex range of threats delivered across ever-blurring boundaries.

In Q1 of 2013 alone, Kaspersky Lab detected and neutralized over 1.3 billion threats. In the same period, 22,750 new modifications of mobile malware were detected – more than half the total number found in all of 2012. Kaspersky Lab neutralized over 821 million online attacks in the first quarter of 2013, while over 30 million vulnerable programs and files were detected on endpoints running Kaspersky Secure Network – with an average of eight per vulnerable computer.¹

In this environment, it’s hardly surprising that understanding and keeping up with the latest IT security threats was a concern for more than half the respondents in the 2013 Global IT Security Risks report² And with so much out there, you can’t possibly keep track of every threat.

¹ Source: Kaspersky Lab ‘IT Threat Evolution Q1 2013’ – securelist.com
² Source: Kaspersky Lab Global IT Risk Report 2013
And that’s just the outsider risks – what about end-user activity that exposes your networks to data loss? Traditional anti-malware on its own is no longer enough to protect your networks – today’s criminals are exploiting vulnerabilities associated with individual users to gain access to their wider networks. Malicious code embedded in online games, bad links in social networking applications, malware hidden in seemingly harmless office documents... Big name attacks on high-profile targets might be grabbing the headlines, but the reality is that the easiest route into business networks is human error, and our tendency to click without thinking.

You can’t lock out the Internet and you can’t see everything that happens on your network in real time. But you can manage and control it. And you can certainly control what happens when your end users do something they really shouldn’t have.

Granular application, device and web controls, combined with strong anti-malware technology can protect your business while supporting your real-world requirements for flexible usage policies. Take control of your endpoints without compromising on productivity by applying these easy-to-implement web, application and device controls.
In a hyper-connected world, vulnerabilities in web applications have become the back-door of choice for cyber criminals. Verizon’s 2013 Data Breach Investigation Report found that web applications were the vector for 22 per cent of hacking breaches. But blocking downloads will only get you so far – Google’s bots detect 9500 malicious web sites every day. And it’s not just web-based software: every day, criminals launch malware designed to exploit loopholes in legitimate business software. For example, all five of the major vulnerabilities found in Java in 2012 were actively exploited by criminals.

Application control and dynamic Whitelisting technology

Application control and dynamic Whitelisting technology can help protect systems from both known and unknown threats by giving administrators total control over the kinds of applications and programs that are allowed to run on their endpoints, regardless of end-user behaviour.

In addition to being able to block or allow certain applications, IT administrators can control how applications behave – what resources they can use, what kinds of user data they are allowed to access or modify, whether they write to registries etc. This means you can prevent any application from executing actions that could endanger both the endpoint and the network to which it is connected.

Constant, real-time monitoring of how applications are being accessed (and by whom) allows you to establish usage patterns that can, in turn, help refine policies based around end user requirements and threats.

In essence, application controls simplify and automate effective policy creation and enforcement for your business:

- Application startup control: Grant, block, audit application launches. Drive productivity by restricting access to non-business-related applications.
- Application privilege control: Regulate and control application access to system resources and data, classify applications as trusted, untrusted or restricted.
- Application vulnerability scanning: Proactive defence against attacks targeted at vulnerabilities in trusted applications.

Whitelisting – strength and control at the core

If application control is the vehicle for effective protection against complex threats, dynamic Whitelisting is the engine driving it. In fact, Whitelisting is a best practice component of any successful application control strategy. Simply put: if you don’t have Whitelisting, you don’t have genuine application control.

Whitelists are lists of trusted applications that IT professionals can use to add an extra layer of security to their existing controls. Whenever an application attempts to execute, it’s automatically checked against the Whitelist; if it’s there, it’s allowed to run according to administrator-specified rules and policies. If it’s not on your list, it’s blocked until such time as an administrator approves it. Think of it as the doorman or ‘bouncer’ to your endpoint – or you can call it by its official Information Security name: Default Deny.
3.3. Making whitelisting easier

So, you need a Whitelist. You can’t dedicate your working life to constantly compiling, revising and updating lists of acceptable, ‘safe’ applications. Think about it: you’re not just looking to control a few business applications – what about things like printer drivers, networking infrastructure software or updates?

Dynamic, constantly updated and monitored Whitelist databases are at the heart of the most effective solutions, allowing administrators to get on with other tasks, safe in the knowledge that automated, constantly updated Whitelisting databases are working in the background.

A quality Whitelisting and application control solution will allow you to adopt a best practice approach to implementation, without the complexity of having to hand-select the thousands of pieces of software that even a small business is likely to depend on for its day-to-day operations. A good program will not only make your life easier, it will include some key best practice features, among them:

• **Inventory:** You can’t measure or monitor what you don’t know you have. The best Whitelisting programs start with an inventory. Compile and maintain a record of installed software on the network in a convenient format, facilitating analysis. To make life easy for yourself, choose a solution that offers automatic inventory – this will save you the time (and the headache) of tracking down every last piece of software in use in your company. Added bonus: you can find and weed out unwanted apps as well as the good stuff.

• **Categorization:** Assign functional categories to installed software (e.g. Operating systems, business software, developer tools, peripherals, browsers, multimedia). This makes it easy for administrators to identify business-related applications – and block productivity-draining ones. Smart use of categories means you don’t have to figure out which games exactly your end users are wasting time on, you can simply block this entire category. On the off-chance they discover something completely obscure, simply add it to the list yourself.

• **Trusted updates:** Ensure regular updates of permitted software, closing down any new or previously undiscovered vulnerabilities. This should include patching, system management processes and other software deployment programs.

• **Implement flexible rules:** Quality solutions ship with a broad spread of pre-defined rules for the most common scenarios. While this is great to get you up and running, as your Whitelisting implementation grows and matures, you’re likely to want to tweak and customize settings for your business’s unique circumstances.

Don’t limit yourself with a solution that doesn’t offer highly-flexible customization – you’ll need options around factors such as file name, source folder or vendor. You’re also likely to need flexibility around MD5 (‘fingerprinting’ for data) or ‘hashes’ – techniques that prevent criminals (or, indeed, canny employees) from attempting to sidestep your Whitelist by disguising prohibited applications and files as legitimate ones.

• **Think global, act local:** You should always work from a global Whitelist database that is comprehensive and dynamic – you simply don’t have the time or the resources to do anything like this yourself: there are over 700 million unique files in the Kaspersky Lab Whitelist, for example.
On a typical day, Kaspersky Lab uploads over one million files — that’s a big enough job to keep a dedicated, specialist Whitelisting lab busy, and it does. Global databases should be permanently available and accessible in the Cloud. As vendors of many business-leading applications are constantly updating or releasing new versions of their products, constantly updated global databases help reduce the risk of ‘false positives’.

Accepting the need for global databases doesn’t mean you shouldn’t customize your own, completely local Whitelist database, valid on your network only. Choose a solution that supports this, particularly if you develop your own custom applications.

- **Go for gold:** A Golden Image is your template of the perfect installation: All of your business-critical applications and settings, implemented according to best practice and fine-tuned to run at optimal performance.

In the real world, IT professionals seldom get the opportunity to work from a blank canvas — but whether you’re starting off on brand new machines that have never connected to the Internet, or slowly tweaking and refining your Whitelist based on pre-existing technologies, you should still develop a ‘Golden Image’. Whether you use your Golden Image as a guidance point while your application control program develops or you choose to make it the platform for your Default Deny strategy, a solution that supports you in the creation and development of one will make your life a whole lot easier. Especially if they give you a ready-made, ‘global’ template to work with.

**3.4. Black or white? Both!**
Because it only allows pre-approved applications to run, Whitelisting is the opposite of traditional anti-virus (also known as ‘Blacklisting’), which blocks software after it has been defined as malicious. By bringing the two technologies together under one roof, you’re effectively locking the back as well as the front door to your IT house.

A combination of White-and-Black-listing offers a best-practice, multi-layered protection scenario, ensuring maximum security. Indeed, Whitelisting can actually boost anti-virus performance; applications on the Whitelist don’t require the same intensive, regular levels of checking, meaning you get to save system resources and improve application performance.
4. GETTING TO GRIPS WITH DEVICE CONTROL

Now that you’ve sorted out control over the applications that can’t or can’t run on your endpoints, you’re probably wondering if you can exercise the same high level of control over devices. You can. By centrally maintaining policies around the use of removable devices and media – USB, Flash Drives, CD/DVD, Smart Cards etc. – you can significantly reduce insider risk to your organisation. Whether you’re concerned about a disgruntled employee copying sensitive data to a thumb drive or simply want to block infected portable devices from connecting to your endpoint or network, device control offers a flexible approach to doing so.

Here are some approaches you might wish to consider when adopting a device control program:

• **Define your classes:** Different devices have different capabilities and so pose different threats. Accordingly, it’s a relatively easy decision to adopt a default deny stance with, say, an image scanner. But that’s not such a practical approach when it comes to USB ports – disable a USB port and you’re also preventing the same port from being used to support secure, token-based VPN access. Which is why you need…

• **Granularity:** You need to be able to set different rules for different devices and, indeed, different users and use cases. Administrators need to be able to apply policies such as read-only, block, read and write to different devices.

This granularity should extend to being able to limit the kinds of files which can be transferred, time of day at which any given policy comes into force, type of device permitted and when. For even greater control, administrators can apply policy to the specific serial number of any given device. This granularity means you can set policies and permissions for specific device models and individual users, preventing other employees from accessing the data on certain devices.

• **Access control:** This allows complete control over access to specific device types for selected users and groups during specific time periods. This functionality can be useful if you’re trying to cut costs on, say, after hours printing.

• **Encryption:** We don’t need to tell you how easily USB or Flash drives can be lost or stolen. Best practice for device management should include an encryption component. Policies can be set to enforce this for specific device types.

• **Integrate with Active Directory:** Because you don’t want to have to chase down every single user in the business to apply policies, simply set your device control policies and push them out to your users.
A continually evolving threat landscape means it’s no longer enough for organizations to block malware and other threats after they’ve been detected. Strong blacklisting technology continues to have its place in any good security strategy, but truly comprehensive protection can only be achieved using a multi-layered approach.

You need to protect your business from traditional malware, but also from threats delivered via seemingly legitimate sources: vulnerabilities in trusted applications, malicious code embedded in popular web sites, phishing attacks delivered via email or malicious software designed to exploit automate execution features for portable media.

Kaspersky Endpoint Security for Business puts web, application and device control back into the hands of the IT professional. Our powerful tools are integrated with our industry-leading anti-malware technologies, delivering a security solution that you can customize as much – or as little – as you like. Kaspersky Lab’s dedicated global Whitelisting database is world-leading: we are the only IT security company that maintains a specialist Whitelisting laboratory supported by a team of dedicated experts. All under a single pane of glass, giving you centralized control with the minimum of fuss.

Kaspersky Endpoint Security for Business was built with the IT professional in mind: One management console, one security platform, one cost. It’s the industry’s only true security platform.
SEE IT. CONTROL IT.
PROTECT IT.

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

Be Ready for What’s Next