BEST PRACTICES

Security Controls

www.kaspersky.com

YOUR GUIDE TO BEST PRACTICES WITH SECURITY CONTROLS.

Cyber espionage and state sponsored threats have been making the headlines lately, but the fact is that the same technology can and will be used against businesses like yours.

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 click on or install something they really shouldn’t have. Here’s how…

1. DON’T JUST BLOCK, CONTROL

Social media, smart devices, web-based applications, spam, phishing, malicious web sites, social engineering, malware. Keeping up with increasingly complex threats delivered over ever-blurring boundaries is becoming a significant challenge for IT managers.

And that’s just the risks coming from outside your company. What about the end-user activity that exposes your business to security and data breaches? Malicious code embedded in online games, bad links in social networking applications, malware hidden in seemingly harmless office documents… Today’s criminals are exploiting vulnerabilities associated with individual users to gain access to business networks and the sensitive data on them.

Application, device and web controls, combined with strong anti-malware technology, can protect your business without impacting on productivity and flexibility. Take control of your business technology by applying these easy-to-implement web, application and device controls.

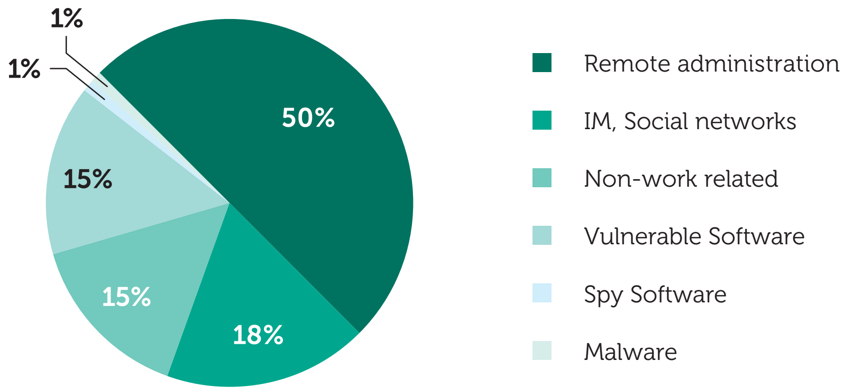
Mind the app

In a hyper-connected world, vulnerabilities in web applications have become a back-door of choice for cyber criminals. In 2014 alone, Kaspersky Lab detected and neutralized over **6.2** billion attacks launched from online resources globally[1], compared with **1.7** billion in 2013[2].These attacks were launched by **9.7** million different host computers[3]. Kaspersky Lab detects some **325,000** new malicious files every day[4].

With one in every **14** downloads containing malware[5], simply blocking downloads will only get you so far… every day, criminals launch malware designed to exploit vulnerabilities in legitimate business software: third party applications account for an average of **75** per cent of vulnerabilities[6].

[1] Kaspersky Security Bulletin, December 2014
[2] Kaspersky Security Bulletin, December 2013
[3] Kaspersky Security Bulletin, December 2014
[4] Kaspersky Security Bulletin, December 2014
[5] Kaspersky Security Bulletin, December 2014
[6] Secunia Vulnerability Review 2014

The reality for IT security professionals is that the weakest link in the security chain is often already sitting on their systems – or sitting in front of them.



2. APPLICATION CONTROL AND WHITELISTING: KEEP THREATS OFF LIMITS, PREVENT SECURITY BREACHES

Application control and dynamic Whitelisting technology can help you to 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 behavior.

In essence, application controls empower you to create and enforce security and usage policies for your business more effectively:

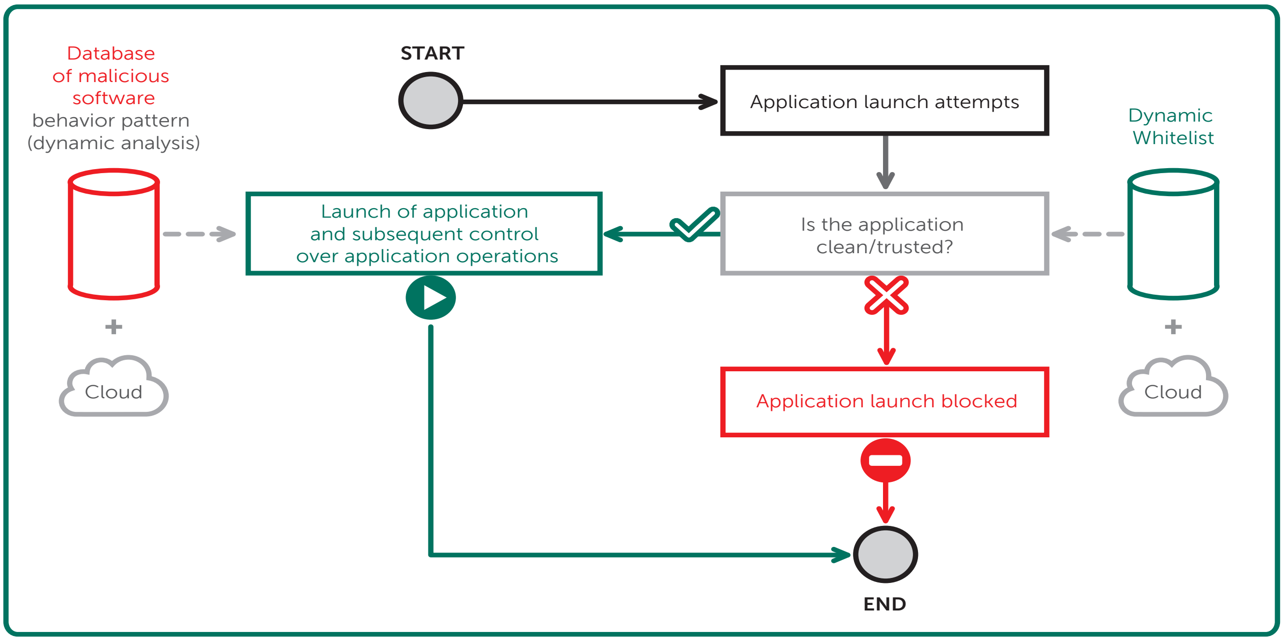
- **Application startup control**: Grant, block, audit application launches. Drive productivity by restricting access to non-business-related applications.
- **Application privilege control**: Regulate and control application access to system resources and data, classify applications as trusted, untrusted or restricted.
- **Application vulnerability scanning**: Proactive defense against attacks targeted at vulnerabilities in trusted applications.
- **Applications Monitoring**. As well as being able to block or allow certain applications, IT you need to be able to monitor how applications behave – what resources they use, what types of user data they are accessing or modifying, whether they write to registries etc. Using this information, 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.

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.



Consider a Default Deny Approach to Whitelisting

A Default Deny configuration setting is most effective security posture to adopt in the face of ever-evolving threat vectors. It simply blocks all applications from running on any workstation – unless they've been explicitly allowed by the administrator.

While it does sound like the kind of block-all strategy that isn't going to win you any friends around the office, Default Deny strategies built on effective Whitelisting mean you can still allow your end users a little flexibility.

It's not so much a question of blocking absolutely everything as deciding precisely what it is you're going to allow.

The best way of finding out exactly how running a Default Deny scenario would actually affect your business is to give it a try. A sandbox environment will allow you to observe the actual effects of implementing Default Deny on your IT system, and trial any necessary adjustments, with no disruption to your systems or users. You may be surprised, when you test it out, at how little this strategy would actually impact your users in practice.

Use whitelisting databases

So you decide to work with Whitelisting. But 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 backgroun

Other Tools You May Need

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 myriad 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 a software 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 exactly which games 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. And your exploratory trials of Default Deny may lead you to creating new categories based on your findings.

- **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, determined 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 almost 500 million unique files in the Kaspersky Lab Whitelist database, 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.

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.

3. GET TO GRIPS WITH DEVICE CONTROL

You’ve sorted out control over the applications that can’t or can’t run on your endpoints; now exercise the same high level of control over devices.

Significantly reduce insider risk to your organization by centrally maintaining policies around the use of removable devices and media – USB, Flash Drives, CD/DVD, Smart Cards etc. 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 to consider when adopting a device control program:

- **Define your classes**: Different devices have different capabilities and so pose different threats. It’s a relatively easy decision to adopt a default deny stance with, say, an image scanner. But 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**: 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. Your life is going to be made a lot easier here if you can apply these rules simultaneously to multiple devices.

  For even greater control, you need the ability to apply a policy to the specific serial number of any given device. Then you can set policies and permissions for specific device models and individual users, preventing other employees from accessing the data on these devices.
- **Access control**: Gives you 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**: Best practice for device management should include an encryption component. We don't need to tell you how easily USB or Flash drives can be lost or stolen. Policies can be set to enforce encryption 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 defined user base.

4. ARE YOU ALONE?

One last question – who is going to be doing all these good things? Is it you? And is this the full scope of your IT responsibilities? Working with controls, or managing security in general, may well be just one part of your working life; though we hope your business recognizes the importance of this one part, just as much as we do.

If you are alone, or part of a small team, you need to be able to control your security as part of a wider picture, from one screen, rather than darting between consoles.

You may, on the other hand, be part of a large security team, so that perhaps your area of responsibility specifically involves one area - for example device management. In this case, you need a security system which incorporates role-based access controls (RBAC), so that you alone control security for this discipline.

But you shouldn't have to choose. There is no reason why the same security controls should not be easily managed by one hard-pressed individual or by different members of a busy team. It's all about integration. A security system where everything, including controls, works together as a single platform, is nearly always going to be a good thing.

FINALLY...

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 the power 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 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.

Twitter.com/
Kaspersky

Facebook.com/
Kaspersky

Youtube.com/
Kaspersky

Kaspersky Lab, Moscow, Russia
www.kaspersky.com

All about Internet security:
www.securelist.com

Find a partner near you:
www.kaspersky.com/buyoffline