Time to switch — updating endpoint security. Why now is the time to act

kaspersky

Introduction

Over the past few years, companies have had to radically rethink their security strategies. The traditional digital perimeter no longer exists and, as such, endpoint security has been redefined, leading to a completely new approach.

Just look at some of the changes over the past decade. The adoption of cloud computing has had one impact on how security policies are set, but that has been compounded by the increasing use of bring-your-own-device (BYOD) within organisations, while the proliferation of remote workers has transformed the definition of perimeter and expanded the number of endpoints connecting to networks.

These new devices multiply the number of vulnerabilities, particularly when these are employees' own devices, all of which have their own security policies and vulnerabilities. To take just one example, Internet of Things (IoT) often get lost from endpoint monitoring and can be easy target for external threats. As such, any endpoint protection must take these devices into account.

If your current systems can't handle this shift, it's time for change. The good news is that such a radical move fits in well with current thinking on IT – many companies are looking to transform their landscapes.

There could be many reasons for making a change: the company could have outgrown an existing provider, they may have been compromised by a previous attack or the organisation may have restructured its underlying IT structure, for example, by becoming more cloud-based or, as mentioned earlier, by adopting a BYOD policy.

In such circumstances, a solution from an endpoint security provider bought several years previously may no longer be fit for purpose. The modern business can't rely on anything that's not designed for current procedures and real thought must be given to the way forward.

Obviously, it's important to realise that replacing a long established product is not a decision to be taken lightly but given that this is the time to act, we're going to look at some important elements involved in making the right decision.

1. Independent test results

When you're doing something as important as changing security provider, it's important that you have all the information to hand,

In the past, companies have been burned by choosing a product that promised so much but delivered too little. When making a change, it's vital that companies pick a product that can meet its demands.

With so much confusion around, one of the best ways in which to assess the worth of any particular endpoint security product is to examine what the independent test labs are saying about it. These are organisations without any axe to grind who can examine product features rigorously.

What makes this especially vital is that some security vendors make claims about endpoint security that can't be justified: only independent testing can isolate the false and exaggerated claims from the reality.

With this in mind, it's imperative to look at the ways that vendors of security products are rated. While they make claims about the effectiveness of their offerings, when subject to the type of rigorous testing that the labs can provide, some of the claims are seen to be exaggerated – or in some cases, completely false. Organisations looking to make changes, need to examine the different labs' results carefully.

For example, research from test lab AV-Test into this field revealed that, in tests, only one company, Kaspersky, scored maximum points detecting the modern fileless-based threats. Not only did it score highest in detection, but Kaspersky also scored highest in protection too.

But that's just one test; to get a clearer idea of how individual companies perform – different tests have different criteria and different conditions. To get a better idea look at the results of several tests. Any organisation that is considering adopting a new security system must look in greater detail at what each vendor offers and whether their claims stack up. Look for products that are at the top of the list – particularly if they're hitting the top slot consistently.

This is an important benchmark to consider when choosing a new product – don't just believe the vendors' claims, get everything independently verified.

2. Threat prevention

One of the reasons for making a change is the growing sophistication of threats. Older products, designed for the IT landscape of a decade ago, may not be able to cope with modern attacks.

It's important that any upgrade can handle these. For example, one of the perils of endpoint security is the rise of so-called 'fileless' attacks. These are particularly tricky to handle as they are specifically designed to avoid triggering anti-intrusion protection.

Fileless-based attacks use system files to run malicious code, for example by launching attacks against a system process such as iexplore.exe or javaw.exe. By doing this, they avoid leaving a trace. What makes such an attack so sophisticated is that blocking them would mean blocking legitimate software too. For example, if a security admin blocked PowerShell, IT maintenance would suffer.

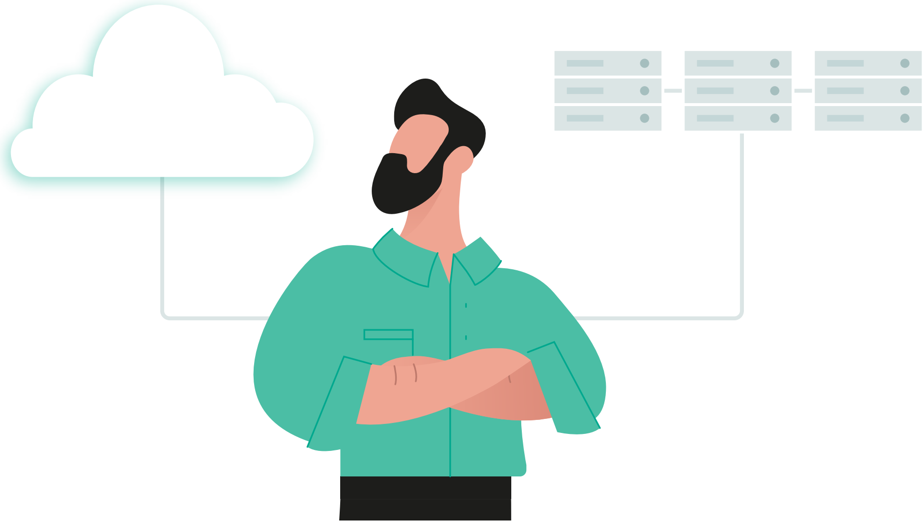
As just one example of this type of weakness, consider the way that certain manifestations of file-based malware can install a backdoor on corporate systems, enabling the establishment of a control channel to the attacker – a clear example of a weakness in an endpoint security.

There are ways to protect against attacks like this. Kaspersky, for example, offers a way in which the threat of fileless attacks can be mitigated.

The Threat Behaviour Engine incorporates several components that can be deployed.

- Behaviour analysis. This detects fileless threats early on, at the execution stage. The software can analyse execution patterns (which can include legitimate actions) to recognise malicious attacks. It will also look for the parent process of the application to see whether it's from a legitimate source.
- Remediation engine: Once such a threat has been identified, it's necessary to find a way to isolate and restore the user data to original state.
- Exploit prevention: It's important to prevent utilization of legitimate application vulnerabilities with the purpose of getting control of its process execution flow to run malicious payload.

3. Management flexibility



In the same way that legacy endpoint security may not be able to handle modern threats, it may not also be designed for a landscape where cloud dominates. According to industry body, The Cloud Industry Forum, 93 percent of companies are now embracing cloud in one form or another.

We've already seen that cloud could be one of the drivers for change within companies as they've moved from centralised data centre view of the world to one that adopts cloud principles to save money, improve flexibility or transform the business more radically.

Whatever the reason, the need to manage security effectively is going to be important, meaning that all security tools should be able to control all existing attack vectors, including the new ones introduced by the changes in the infrastructure.

This is going to be a time for great change: some workloads will fit best in the cloud and some will be better on-premise. But these may not be fixed: there may be reasons to move from one to the other and back again. The reason of change could be latency or demand to decrease the Total Cost of Ownership of the current solution. But whatever the cause, the system needs to be able to handle all changes. If an existing one doesn't, then it's time to look again.

And, because no company wants to be messing around with a variety of management tools, it should be able to handle everything from one central console, one that is equally adept with cloud and on-premise.

When a company has 'a single pane of glass' to view the entire IT landscape, that company is in a better state to deal with management issues. And when that console is strong, and able to cope with all cloud providers, organisations know that the management of the underlying security system is not going to buckle under the strain. If an existing system cannot offer this level of management, it's time to look anew.

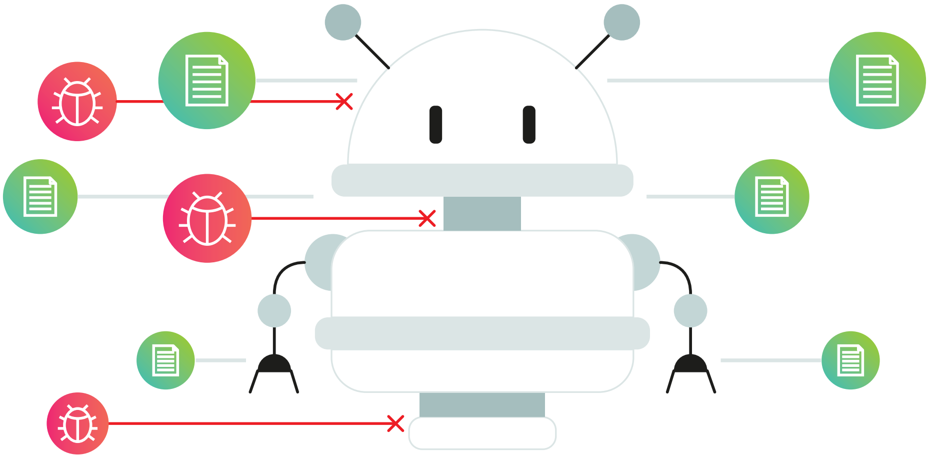
4. Remote workers support

The worldwide lockdown following the Covid19 pandemic showed that there was a real need to support people working remotely. Employees quickly found that when it came to logging in remotely from their home environment, things weren't quite as straightforward as they'd hoped they would be.

There's a fundamental issue at stake here: corporate networks need to be as secure as possible and resistant to attacks from outside but, by definition, remote workers are accessing corporate infrastructures from somewhere external, and existing software may not be robust enough.

What's therefore important is to have an endpoint protection platform in place that is able to secure endpoints remotely. This can be quite a challenge: some may not have updated their security policies for several months; some may have PCs that are using an outdated operating system – it's all quite a challenge for corporate security managers. If an existing product can't handle this – it's time for a change.

5. No management overhead with Automation



A key element in effective endpoint security is the degree of automation deployed. Any organisation that can reduce the human interaction is going to have a head-start when it comes to controlling unwanted activity. This has been particularly true in cloud deployment where the complexity of allocating workloads has become more complex and automation has reduced the need for human interaction.

Modern systems are geared up for this. We've seen in the last few years an almost unprecedented rise in the use of artificial intelligence within security products.

To take one example of how this works, let's look at Adaptive Anomaly Control (AAC), an adaptive hardening tool developed by Kaspersky that aims to bring some element of AI to security.

One of the issues that all security officers have to deal with is how to determine what are legitimate actions from external and internal sources and what's not. For example, it's not possible to block certain macros across the board because while, in certain cases they could be malicious, they could also be legitimate requests. It's hard to tell what's permissible and what's malicious and, doing so, takes a lot of man-hours.

What AAC does is to make that sort of assessment automatic. It deploys behaviour analysis algorithms to identify suspicious behaviour but also identifies when unusual activity is legitimate and allows it. By using machine learning techniques, the system is constantly being refined.

For example, an email attachment with the presence of JavaScript in the archive could indicate a threat when coming from employees in the finance department, but could be legitimate when coming from developers – AAC will modify the system so it reflects this.

This will have a major impact on staffing costs – an increased level of automation will significantly reduce overheads as there would be no requirement for specialist help. By changing your security provider, companies will benefit from all the latest advances.

6. Specialist functionality, such as Anti-ransomware

Most vendors' security products will offer a general level of protection but any organisation looking to make a fundamental change to its underlying operations will be looking for something special – particular features that bring a higher degree of sophisticated functionality to the user.

Features such as a desktop firewall, additional ransomware protection, anti-exploit technology, and, as we've already seen, fileless protection, are all areas in which endpoint security is seriously tested.

Take ransomware protection as an example. Ransomware is a growing threat facing all organisations and most vendors have techniques to tackle this. To be truly effective, it's important that not only impacted files are protected but also the disk, so that the master boot record is not tampered with.

Techniques like specific anti-exploit technology will also limit the effectiveness of malicious attacks. Software can be used to identify the very specialist threats thrown up by ransomware attacks. For example, NotPetya and WannaCry made use of exploits like EternalBlue and DoublePulsar to carry out their mayhem. Anti-exploit technology will spot and neutralise this small subset of techniques, enabling better protection for users.

It's important that businesses look at their specific needs and which security vendor can offer that level of protection. The chances are that existing systems can't offer what more modern ones can and it's time to think seriously about whether the legacy solutions, with a limited feature set are geared up to meet all threats. Any company harbouring doubts should be looking to make an immediate change.

7. Enhanced Visibility with Endpoint detection and response (EDR)

In the modern world, businesses need to be able to act swiftly to threats. All security products will offer some sort of protection but to be really effective, it's important to marry threat blocking with root cause analysis, so that threats can be more quickly identified.

What EDR does is to provide a way to, not only block threats, but ensure that any attacks do not hit other parts of the corporate infrastructure. It offers visibility across all endpoints, offering not only protection but analysis of any threats – drastically improving response rates to any security incident. Security managers have access to a real-time view of any threat, no matter how complex an attack. All analysis is also maintained within the corporate network, minimising any threats.

When a complex corporate network comes under attack, it's important to have as much detail as possible in a short space of time. This can ensure that other parts of the system are in less danger. Any organisation, particularly those with an extensive corporate network, will need to assess its readiness to meet threats in real time. Any delay in reacting can have catastrophic effects on the corporate network - now is the time to replace existing solutions to meet all threats speedily.

8. Sandbox for Advanced threat protection

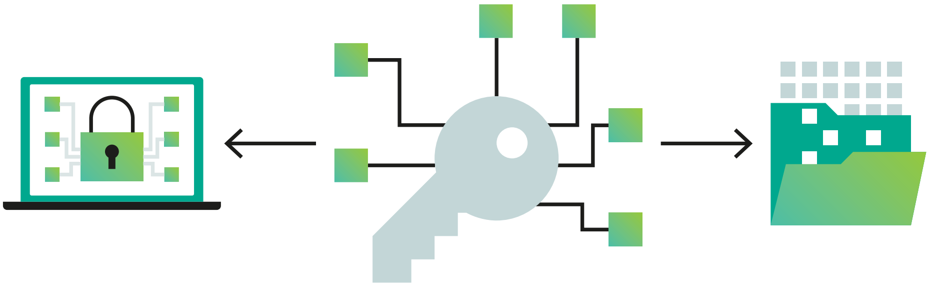
One of the common strategies that businesses deploy for protecting data is the use of sandboxes, a product that provides an additional security layer to automate detection and response to threats designed to bypass endpoint protection. The Sandbox works by detonating malicious applications in isolation, to analyse and detect even advanced exploits used in targeted attacks.

One of the issues with this approach is that it usually requires the engagement of cyber security specialists – a very expensive commodity.

The Sandbox would be especially effective if it were easy to install and operate, obviating the need for specialist staff, but also able to scale, so that a growing company would not have to rethink its strategy or deploy new protection.

Some existing endpoint products fail to offer a way to quickly identify and neutralise threats. For example, do they create rules which will detect and block similar malware attacks from entering a network? All security managers need to consider whether their current endpoint security products have that level of control – there are products that do offer it and you should be looking to switch to these right away.

9. Data Protection with Encryption Management



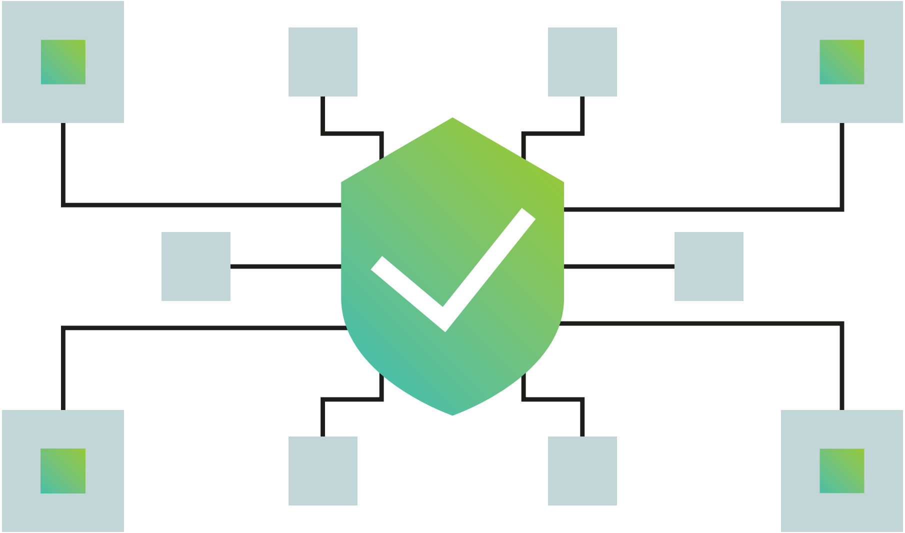
Ideally, products will have integrated tools for data encryption. These can take two forms: Full disk encryption (FDE) which prevents data leakage via loss of a laptop and File-level encryption (FLE) which protects files on the move when they are transferred in untrusted channels. It's possible to set policies so only certain users can see the unencrypted files.

Whatever the form, the introduction of encryption does inhibit the way a user works – it's carried out transparently.

With FDE whole disks are encrypted, whatever the form - HDD, SSD or flash-drives. It also offers protection when a computer is booted; guaranteeing only safe software is loaded.

The lack of an effective encryption option within an endpoint protection product should be ringing alarm bells. There have been plenty of examples of laptops and other devices being lost or stolen, leaving unencrypted files open. If any company has an extensive number of mobile devices within its domain and there are concerns that unencrypted files could be released into the wild, it's time to change security.

10. Vulnerability management and Systems Hardening



It shouldn't just be about being reactive to threats; the ideal product would also look to assess how prepared and robust your system is to counteract them. For example, is there a way to ensure that all software has been patched so that it's up to date?

It seems like something basic but not every endpoint solution can do this. There's a need for effective patch management to ensure that security vulnerabilities can be detected at an early stage. It sounds obvious but many attacks are perpetrated against software which already has an available patch.

It's essential that pre-emptive measures are taken; scanning for and patching vulnerabilities will ensure that systems are best prepared to meet all levels of threats.

Conclusion

The world is changing rapidly. And companies are adjusting their IT infrastructure to meet those changes. As we've seen, many organisations are finding that their security products are no longer fit for purpose when it comes to dealing with this new business paradigm. Now is the time to look anew at what's protecting the business and whether it's able to meet all expected needs.

An endpoint security product should be able to meet all the strains placed upon it; such a product will have a variety of elements in common: it will be able to handle cloud and on-premise with ease, managing them both from a common platform. It will be fully automated with little need for human intervention. It will be able to offer a range of features and the company should be able to back up all their claims by subjecting the product to a battery of tests from reputable labs.

In such a climate of rapid change, businesses need to be aware that the security products that they use will be able to handle all the stresses put on them. As the world grows ever complex, it's important that products are able to handle the changes.

The chances are that any systems purchased some time ago will be struggling to cope with many modern threats but by switching to a more modern, automated, fully comprehensive system, any company will be better able to cope with a full range of sophisticated attacks.

Kaspersky Endpoint Security Cloud Plus, premium cloud security capability and cloud data protection **from the world's most tested**, most awarded security vendor, protects Windows desktops and file servers, Mac OS workstations, iOS and Android smartphones and tablets; manages endpoints from anywhere via the cloud-based console; saves time and resources with no need for hardware/software procurement, provisioning and maintenance. **Learn more** from a peace of mind provider.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for Enterprise: kaspersky.com/enterprise
Threat Intelligence Portal: opentip.kaspersky.com

www.kaspersky.com