KASPERSKY lab

IS THERE A REVOLUTION IN IT SECURITY ...OR IS IT JUST WISHFUL THINKING?

How to assess different security solutions, separate the facts from the hype and select the security your business needs

www.kaspersky.com

If you're re-evaluating your IT security strategy – to ensure it really is sufficient to defend your business against today's increasingly complex threats and attacks – there are a lot of security vendors vying to win your security budget.

But how do you work out which technologies are really capable of delivering the best protection... which methods could damage your productivity... which options could leave gaps in your security... and which security strategy is best suited to your business's specific needs?

As with most IT strategy decisions, it starts with separating the facts from the hype and working out which technologies really do deliver on the claims that they make.

THERE'S A LOT YOU COULD LOSE

With the continual increase in both the volume and the sophistication of modern malware, Internet attacks and cybercrime, the risks for businesses are growing. So it's more important than ever to make sure you choose the most effective security.

There's a lot more at stake than just wasting a portion of your IT budget. Choosing an inadequate security solution can have very expensive – and long-lasting – consequences for any business:

- Ransomware attacks can encrypt vital business data – causing major disruption to everyday business processes.
- Leakage of confidential information about customers can result in damaged relationships, lost sales and possible legal action.
- Loss of data about designs and other intellectual property can erode a business's hard-won competitive edge.

In a survey of 5,500 companies – across 26 countries:

- **90% admitted suffering a security incident**
- **46% had lost sensitive data, as a result of a security threat**

Source: Corporate IT Security Risks Survey, Kaspersky Lab

WHY ARE BUSINESSES STILL VULNERABLE?

Of course, IT security solutions have been available for many years. So, why are businesses still falling prey to attackers? There's no single answer.

Criminals have long-recognized how much money they can make from a successful attack against a business – so they're devoting more and more effort to developing increasingly clever techniques. The potential rewards are simply too massive for cybercrime to go away – and criminals are always going to try to outwit existing security technologies.

Then there's the role played by many victim businesses.

BUSINESS FAILINGS?

Some businesses have mistakenly assumed they'll never be a target – and have failed to implement anything beyond very basic security measures. Sadly, all businesses are targets. Even the theft of sensitive data about customers or employees can benefit cybercriminals – and cause financial losses and reputational damage for the victim business.

Other businesses may have invested in protecting key areas of their IT infrastructure, but inadvertently left other areas of their IT estate vulnerable to attacks.

Worse still, some businesses have put their trust in some revolutionary, 'silver bullet' technology that promised a lot... but delivered somewhat less.

This last category is particularly concerning – as the business may have become a victim of overzealous marketing. Then, having been lulled into a false sense of security – by unsubstantiated claims about a new technology – the business may have decided to abandon the tried & tested security that had previously kept the company safe.

Sadly, this scenario shows that some businesses are prepared to put the facts to one side and go along with claims that may have little evidence to back them up. So, why do businesses do this?

WHO'S WINNING THIS BATTLE?

The battle between cybercriminals and security vendors has been ongoing for many years. While this battle continues, it's a major distraction for any business – especially as every business just wants to focus on its core activities, develop new products or services, win new customers and grow its market share. Cybercrime and even IT security can be unwanted distractions – absorbing time that the business would rather devote to other tasks.

As a result, there's a strong desire to get back to the times when businesses didn't have to consider cyberattacks and IT security risks. However, just wishing for those times to return won't bring them back – and, as we've seen, cybercrime definitely isn't going away.

FRUSTRATION OPENS THE DOOR TO POOR SECURITY

Any new security solution that promises to deliver a 'once and for all', total answer to IT security issues – without the need for updates and ongoing vigilance – may sound like the answer to any business leader's dreams.

Unfortunately, these magical solutions simply don't exist – and just wanting 'security magic', won't make it a reality.

However, when it comes to assessing impressive claims about new security products, the desire for a more secure business world can lead some businesses into letting their emotions take over... and that can be risky. This is especially true if a business has recently suffered a security incident and is then in a rush to define a new security strategy – sometimes without devoting sufficient time and effort to evaluating the various vendors' options.

IS NEXT GENERATION SECURITY THE SOLUTION?

Adding the words 'Next Generation' – or 'Next Gen' – to the start of any product category can help to create a powerful image. After all, who would want to buy the old generation – when a new generation of product is already available... holding the promise of bigger and better capabilities?

Unfortunately, some vendors' marketing teams appear to know all about the power of well-crafted words – and they can use them to try to catch out the unwary.

So what does Next Generation Security really mean?

There's no ANSI or ISO standard that defines what a security product has to deliver in order to be labelled 'Next Generation'. So you need to dig a little deeper to see if there's anything of substance behind the words Next Gen – or if it's just a case of a marketing team using a 'catchy' phrase that seems to imply a level of future proofing and ease of use for your security.

SECURITY IS ONGOING... AND IT NEEDS COMMITTED VENDORS

There is no substitute for protection that's based on advanced security intelligence. However, because security intelligence requires a large team of security and threat analysis experts – located across the world – very few security vendors can afford to make this level of investment.

For those vendors that can invest in global security intelligence, the best teams also devote considerable effort to anticipating new threats and determining how cybercriminals are likely to refine their techniques... so security solutions can be made ready to fend off new types of attack.

Whereas Next Gen products can be made to **sound** impressive, the reality of effective IT security is less glamourous. Vendors that deliver rigorous security for businesses recognize that it's a 'hard slog'. It takes time, effort, investment and considerable expertise – but there is no magic alternative.

THE THREATSCAPE DICTATES YOUR SECURITY STRATEGY

It's essential that all businesses protect against the full range of IT threats:

- Known threats
- Unknown threats
- Advanced threats

... and that wide threatscape calls for a multi-layered approach to business security.

Businesses can't predict exactly what their security systems are going to be subjected to – so a business that puts all its trust in a single layered Next Gen solution could be extremely vulnerable to attacks.

Because cybercriminals are constantly doing all they can to outwit business security systems, it's a mistake to rely on just one layer of security. By having several overlapping layers of security – if a threat manages to slip past one of your defenses, other layers will still be ready to offer protection.

YOUR RESOURCES DICTATE YOUR SECURITY MANAGEMENT

No business wants to spend too much time on security administration and management. So it's also important to try to source a security solution that uses a single, integrated console that lets you set up and manage security across all of your endpoints – including mobile devices and servers.

Then it's a matter of choosing between a security solution that uses on-premise management infrastructure or offers a cloud-based management console that doesn't require an on-premise server. In most cases, security solutions that have on-premise consoles will allow very granular control of security – but implementation and management tasks take up time and effort.

By contrast, some solutions with cloud-based consoles can greatly simplify security management. These solutions are particularly well suited to businesses that have very small IT administration teams – or even businesses that want to sub-contract all security management tasks to an external consultant.

Solutions that include a cloud-based console can deliver significant benefits:

- Because the console is in the cloud, there's no need to buy, set up and maintain an on-premise server for security management.
- Initial implementation can be achieved much more rapidly.
- Ongoing security management tasks require less time and effort.
- Management tasks can be performed from anywhere – using any device that has access to the Internet.

NEXT GENERATION MARKETING MYTHS

Let's consider some of the wilder claims made for Next Gen security.

Myth 1: Traditional antivirus security is no longer necessary

This is probably the biggest myth about IT security. While signature-based antivirus won't protect against unknown or advanced threats, it's a very important element in any multi-layered IT security solution. It's still a very effective way to block known malware. Furthermore, the best of today's security solutions use the power of the cloud to help deliver new signatures more rapidly – so businesses are protected against newly identified malware.

Too many businesses have found that neglecting this essential layer of IT security can lead to costly and embarrassing incidents – when 'silver bullet' security solutions miss their targets or falsely block a benign entity... therefore causing disruption.

Myth 2:
Security updates 'kill' IT performance

We can all remember the very early days of IT security – when antivirus updates could be slow, unwieldy and damaging to computer performance. However, a lot has changed since then.

Thankfully, there are now security solutions that have been designed to minimize any impact on performance... while boosting security, by delivering regular updates against newly found risks – and also independently updating different security layers, in order to maintain a constantly strong level of protection.

Myth 3:
Security that minimizes connectivity can deliver adequate protection

In an effort to reduce the load on computing resources, some solutions try to make a virtue out of the fact that they generate relatively few security updates – and those updates can be rather infrequent. Unfortunately, this is not the ideal approach to freeing up bandwidth on your corporate network... or delivering efficient protection for your business.

Timely updates – for both signatures that block known malware, plus heuristics models that detect unknown threats – are vitally important in ensuring your defenses can rapidly respond to new threats. Furthermore, regular updates also help to minimize the rate of false positives – which helps to eliminate unnecessary and time consuming disruptions.

The key is to deliver those updates in a way that doesn't impact user productivity.

Myth 4:
The revolution is here... and it's called Next Gen!

When it comes to protecting your business, marketing hype and catchy buzzwords won't do the job. When there's so much at stake, it's real-world performance – and a track record of effective protection – that matter most. So always check what actually hides behind the 'Next Gen label'.

SECURITY THAT'S BASED ON PROVEN RESULTS

People often tell us that Kaspersky Lab was already Next Gen long before any other security vendor. However, because Next Gen is a fairly vague term – that can be open to misuse – it's not a phrase we like to use.

Some may think our combination of Machine Learning and world-renowned security experts is truly Next Gen. However, for us it's something we've been doing for many years... and it's part of our commitment to developing superior security – and not relying on marketing buzzwords.

We prefer to stick to the facts, avoid the hype, get on with our mission of outwitting the most tricky cybercriminals... and let our performance in independent tests 'do the talking' on our behalf.

For three years in a row, our security technologies have been the most tested and most highly awarded. In a whole series of independent tests, our products have achieved more first place awards and more Top 3 ratings than any other vendor's products.

MULTI-LAYERED SECURITY... ACROSS YOUR ENTIRE IT INFRASTRUCTURE

Our multi-layered approach to security – using signature-based protection, plus heuristics, behavioral analysis, Automatic Exploit Prevention and many other advanced technologies – is a key factor in helping us to outperform other security offerings.

Furthermore, with threat intelligence being delivered from our cloud-assisted Kaspersky Security Network (KSN), we help to provide a more rapid response to newly launched threats.

All of this means we can achieve:

- Higher detection rates
- Lower rates of false positives

We offer a choice of integrated business security solutions that can secure all of your endpoints – desktops, laptops, servers, smartphones and tablets – plus we offer a range of special security options that can protect storage systems, virtual machines and more.

In independent tests to determine the number of 'false detections of legitimate software as malware during a system scan', Kaspersky Lab technologies achieved zero false positives.

Tests run in January and February 2016 by The AV-TEST Institute.

CHOOSING YOUR SECURITY SOLUTION

Kaspersky Endpoint Security Cloud has been developed to meet the specific needs of medium-size businesses... especially businesses that have very small IT security teams – or even no in-house IT security personnel. Ideally suited to small and medium businesses, it provides:

- Protection for Windows desktops and laptops, Windows file servers and Android & iOS mobile devices*

- Ease of management – via a Cloud Console that:
  – Saves you time and money – by removing the need for a dedicated server
  – Simplifies initial deployment – by providing Ready-to-Run security functions

- Flexible licensing – via an annual license, or a monthly subscription that lets you scale your security to respond to changing needs
  *Functionality varies for different devices and platforms.

Kaspersky Endpoint Security for Business delivers granular security for larger organizations or businesses with particularly demanding security requirements. It protects a wider range of platforms:

- Desktops and laptops – Windows, Mac and Linux
- File servers – Windows, Linux and FreeBSD
- Mobile devices – Android, iOS and Windows

YOUR NEXT MOVE?

The next time a vendor offers you a Next Gen security solution, make sure you ask to see independent test results – to see how their security technologies measure up in the real world.

Meanwhile – you've seen what Kaspersky Lab security has consistently achieved in over three years of independent tests – so why not evaluate our security now... running on your own computers and mobile devices.

To get a FREE, 30-day trial of Kaspersky Endpoint Security Cloud, go to the online Cloud Console – cloud.kaspersky.com

APPENDIX 1

Example businesses and their ideal Kaspersky Lab security solution

KASPERSKY lab

Here we look at three very different types of company, assess their security needs and then consider which Kaspersky Lab security solution best fits each business's individual requirements.

BUSINESS A

- Small consultancy – with 60 employees
- Personnel work remotely or use shared desks in the office (hot desking)
- Laptops, phones and tablets are all essential for various work tasks
- Many job roles make extensive use of the Internet
- Temporary workers – including interns and contractors – may need access to confidential company data for up to 6 months
- No internal IT support team – the business uses an external IT consultant that has limited experience in IT security management
- Very limited IT infrastructure
  - Uses cloud-based computing servers, instead of running internal servers
  - Typical small office systems are used for printing, storage, etc.
- Limited IT budget
  - Most personnel use their own laptops, smartphones and tablets

WHAT THE BUSINESS NEEDS FROM ITS SECURITY SOLUTION

- Rigorous protection against Internet-based threats
- Simplified security management – without the need for specialist security skills – to help ensure an external IT support person can easily manage the business's security
- Simple licensing – with online, annual payment
- No requirements for any expenditure on additional IT hardware
- Ability to secure a wide range of different devices – including various models of laptops, tablets and phones (including iOS devices)
- Easy scalability – to roll out security to newcomers' PCs and mobile devices

IDEAL KASPERSKY LAB SECURITY SOLUTION

Kaspersky Endpoint Security Cloud – via an annual license

- Protects against known, unknown and advanced threats – including Internet-based threats
- Provides an easy-to-use, cloud-based console that simplifies security management
- Simplifies licensing – annual licenses can be set up and renewed online
- Reduces capital expenditure. Because the management console is cloud-based, there's no need to buy, set up and maintain an on-premise server that's dedicated to security management
- Supports Windows computers, iPhones, iPads and Android phones & tablets
- Scales to meet growing needs. When new personnel join, the cloud-based console makes it easy to roll out security to additional computers and mobile devices

Kaspersky Endpoint Security Cloud gives Business A the right combination of security and ease of use – without the need to buy any additional hardware or invest in training staff in specialist IT security skills. Simplified management – via the cloud-based console – makes it easy for the business to use an external consultant to set up and manage security... across all computers, phones and tablets that the business uses.

BUSINESS B

- Construction firm that is looking to expand to cover new projects – in another 10 remote cities – within the next 3 years
- Currently employs 100 people – but the headcount will grow during the next 12 months
- Every new project requires additional personnel – including site managers, procurement, etc.
- The number of temporary personnel varies during each phase of a project
- Most personnel work remotely – most of the time
- Many job roles make extensive use of the Internet
- Significant numbers of temporary workers – including project managers and specialist contractors – require access to confidential company data for 6-12 months
- No separate budget for extending security to cover the anticipated rise in headcount – instead, costs are covered within each project that the firm wins
- 1 full-time IT administrator
- Very limited IT infrastructure:
  - Cloud-based computing, instead of internal servers
  - Typical small office systems used for printing, storage, etc.
- Limited IT budget
  - Most personnel use their own laptops, smartphones and tablets

What the business needs from its security solution

- Simplified security management – without the need for specialist security skills – to help ensure an external IT support person can easily manage the business's security
- No requirements for any expenditure on additional IT hardware
- No requirement for a pre-allocated annual IT security budget – instead, the security should be scalable as and when new projects are won
- Instant scalability, without having to manage complex licenses or contracts – instead, the solution should allow instant payment for the addition of new users
- Ability to secure a wide range of different devices – including various models of laptops, tablets and phones (including iOS devices)
- Ability to manage several different usage patterns – allowing different security policies to be applied for different job roles

Ideal Kaspersky Lab security solution

Kaspersky Endpoint Security Cloud – via a monthly subscription

- Protects against known, unknown and advanced threats – including Internet-based threats
- Provides an easy-to-use, cloud-based console that simplifies security management
- Reduces capital expenditure. Because the management console is cloud-based, there's no need to buy, set up and maintain an on-premise server that's dedicated to security management
- There's no need to set an annual budget – or buy an annual license. A simple monthly subscription lets the business vary the number of users that are covered... so the business can increase or decrease the number of users on a monthly basis
- Supports Windows computers, iPhones, iPads and Android phones & tablets
- Individual policies can be set up via the cloud-based console
- Scales to meet growing needs. When new personnel join, the cloud-based console makes it easy to roll out security to additional computers and mobile devices

Because rapid, cost-effective scalability is vitally important for Business B, the monthly subscription model for Kaspersky Endpoint Security Cloud is a perfect choice. There's no need for any up-front payment for an annual license. Instead, the business can just add new users – or reduce the number of users – when it needs to. So the business gets the flexible security it needs, while also closely controlling its costs.

BUSINESS C

- B2B software development company – with 500 employees
- Expects to grow by 30% within 12 months
- Effectively plans its recruitment programs – for additional developers, testers, technology experts, pre-sales & sales personnel and more
- Most personnel are office-based – working within the corporate LAN
- Senior managers work with confidential customer data that must be stored securely
- Extensive internal IT infrastructure – including servers, storage subsystems, LAN, etc.
- Uses a variety of computing platforms – including Windows Server for production, Linux for network management and Mac computers for designers
- Standardized laptops are issued to workers, by the business – and are supported by the internal IT team
- A dedicated IT budget is allocated every year
- Constantly needs to adopt modern technologies – to increase market potential
- A highly-skilled , internal IT support team manages the business's IT infrastructure
- Because there's a wide range of job roles – including developers, team leaders, customer-facing personnel, administrative staff, back-office personnel and more – the business needs to be able to set up and manage many different security policies

What the business needs from its security solution

- Advanced security functionality – that can be managed by the business's internal IT security specialists
- Can be deployed completely within the corporate LAN
- Ability to support a very wide range of platforms – including Windows, Linux and Mac
- Support for management of mobile devices
- Ability to support a very large number of different security policies – including Web Controls, application start up restrictions and many more functions
- Advanced encryption – to help protect sensitive data

Ideal Kaspersky Lab security solution

Kaspersky Endpoint Security for Business ADVANCED

- Protects against known, unknown and advanced threats – including Internet-based threats
- Delivers more extensive security functionality – including flexible control tools
- All endpoint security functionality and security management functions run locally
- Provides a unified, single management console – for all supported devices – that runs on an on-premise server
- Protects Windows, Linux and Mac
- Includes mobile device management (MDM)
- Provides granular policy controls that enable complex sets of security policies
- Includes flexible data encryption functionality

Business C has a more complex IT estate, with a wider range of platforms to secure – including Windows, Mac and Linux computers. In addition, the business needs extra security functionality – such as data encryption and flexible control tools – so Kaspersky Endpoint Security for Business ADVANCED delivers the right solution. This option also gives the business much more granular control of IT security – so the business's skilled, internal IT team can set up individual security policies for the wide range of different job roles within the business.