KASPERSKY lab

Kaspersky Security for Microsoft Office 365

NEXT-GENERATION PROTECTION FOR EMAIL

3.5m

emails are sent every second.

It only takes one to bring down your business.

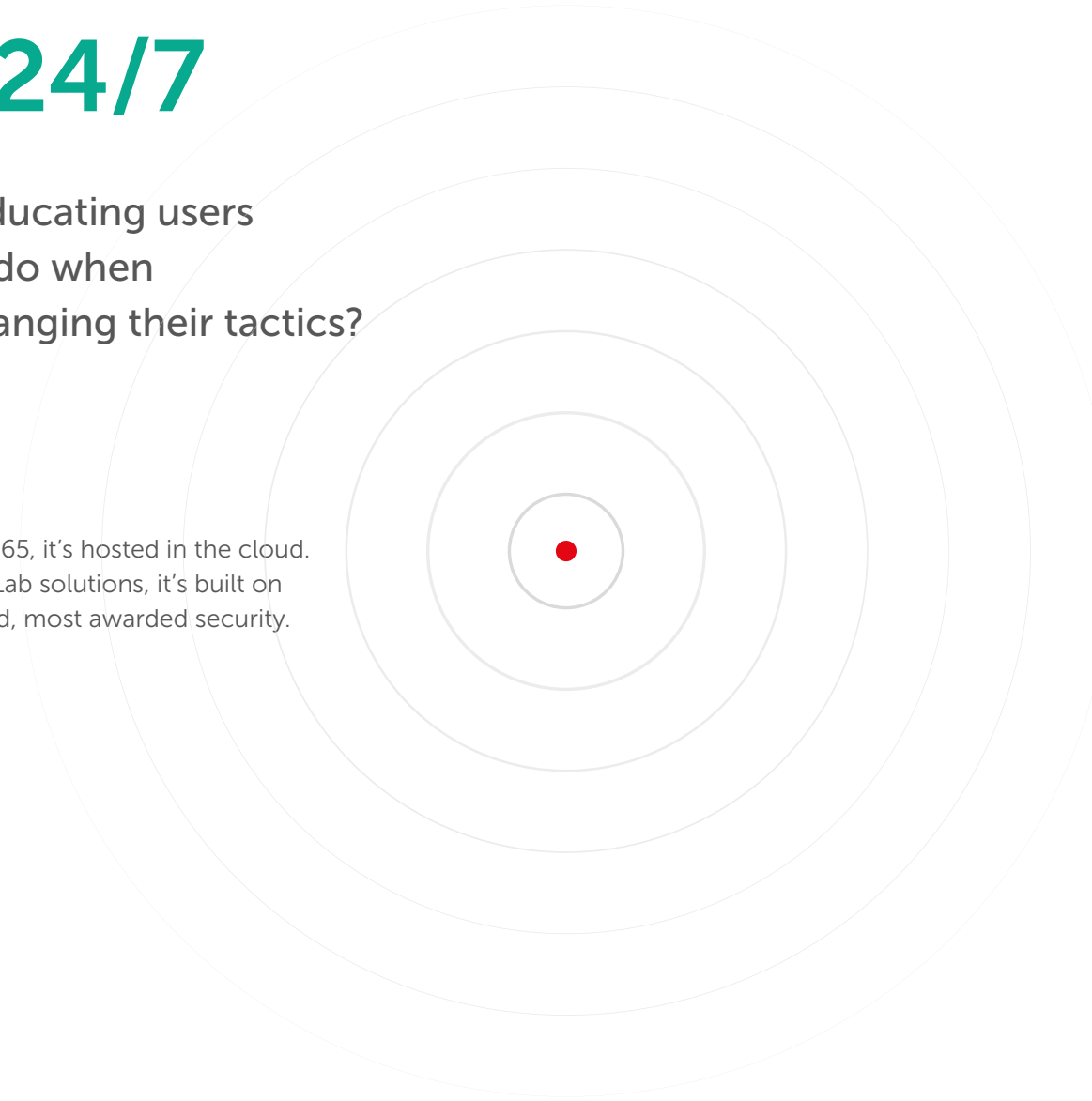
When Office 365 meets cyberthreat 24/7

Most businesses have put time and effort into educating users on the threat of dodgy email. But what can you do when cybercriminals and spammers are constantly changing their tactics?

When email is the number one malware vector for business[1], relying on default or built-in security settings to protect you is risky.

Kaspersky Security for Microsoft Office 365 helps your business to detect and block spam and malicious email before it becomes a problem – without slowing productivity or accidentally deleting legitimate traffic.

Like Microsoft Office 365, it's hosted in the cloud. And like all Kaspersky Lab solutions, it's built on the world's most tested, most awarded security.



1: Verizon Data Breach Investigation Report 2017

Spam: more than just a nuisance

From bandwidth to lost productivity, spam is more than a business nuisance: the average worker spends 13 hours a year scanning and deleting it.[2]

And what about the time wasted tracking down legitimate business mail that's been mistaken for spam? Blocked mail is one thing, but it's even worse when mail is automatically deleted – a common issue with built-in security settings in cloud email.

All this before you take into account the fact that a lot of spam carries malware. 58% of all email traffic is spam. Why waste the time, resources and money you've saved by moving to the cloud on junk messages no one wants?

2: Atlassian: Time Wasting At Work

Anti-spam technologies

Kaspersky Security for Microsoft Office 365 uses next-generation spam detection and analysis, powered by machine learning and real-time, cloud-based threat intelligence from Kaspersky Security Network to detect and block constantly evolving spam techniques.

Robotized Anti-Spam with content reputation

Kaspersky Lab's anti-spam system is built around machine learning-based detection models. Robotic spam processing is supervised by Kaspersky Lab experts, enabling effective detection of even the most sophisticated, unknown spam, with minimal loss of valuable messages due to false positives.

Authenticated email support

Spoofing is one of the main tools of socially engineered fraudulent and malicious spam. Sender Policy Framework (SPF) ensures that incoming emails that appear to come from trustworthy sources are genuine – greatly reducing the risk of spoofing.

Kaspersky Security Network

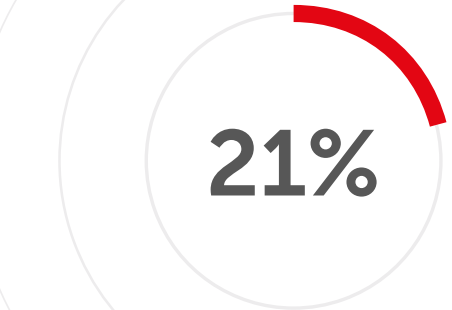
Kaspersky Security Network collects near real-time information about new spam from around the world – enabling immediate response to unknown spam, including "zero hour" and new epidemics. It does this automatically, without the need for intervention from IT staff, and helps prevent mail flooding and infections.

MassMail

Messages from a trusted source may have some spam attributes, but not actually be spam – and can even be useful for work purposes. To ensure employee productivity, these messages can be tagged as MassMail or moved to a special folder, rather than deleted outright.

Phishing: the threat's in the post

Cybercriminals use email to launch their attacks because it's the quickest, most direct route into the heart of any business.



of reported cyber incidents involve some form of phishing[3]

They also know that, despite your best efforts to educate users, a well disguised email is usually enough to persuade even a cautious user to click on a malicious attachment or link. Phishing attacks typically involve emails disguised as legitimate communications, designed to encourage users to click on a malicious link or attachment. We've all seen them – SPECIAL OFFER! LATE PAYMENT! YOUR PARCEL IS DELAYED! - they're not simply designed to entice users to click without thinking, they deliberately use persuasive language and techniques that make them convincing.

Spear phishing takes this a step further. It's much more targeted and usually singles out well-chosen people working at a company with tailor-made mails and attachments that look almost exactly like legitimate communications: a 'job application' sent to the specifically named hiring manager, with an email referring to a legitimate job advertisement; an invoice sent to the correct person in accounts, referring to a company that legitimately does business with you.

More recently, we've seen the rise of the 'Business Email Compromise (BEC)' – mail that appears to have come from someone within your own company, such as the CEO. These usually 'sanction' money transfers or solicit sensitive data. Because they're so finely tailored, these mails often make it past spam traps – they're not sent in large volumes and are usually only sent to a couple of well-chosen employees.

By hiding a file extension from casual sight or disguising an email address to look like it comes from the CEO, cybercriminals can easily exploit weak security.

3: Verizon Data Breach Investigation Report 2017

Anti-phishing technologies

Kaspersky Security for Microsoft Office 365 uses sandboxing and machine learning to filter out even unknown threats before the user can make a mistake. Even when a file extension is hidden, true file type recognition will detect and block it.

Kaspersky Security for Microsoft Office 365's next-generation anti-phishing technologies protect email from advanced and unknown threats without impacting on productivity:

Neural networks-based anti-phishing engine

Protects against unknown and zero-hour phishing using over 1000 criteria to build detection models. Supported by Kaspersky Security Network, our continuously updated threat databases protect against malicious URLs and other phishing-related threats.

Malicious and Phishing URL threat intelligence

Supported by Kaspersky Security Network (our real-world, big data-based threat intelligence network), continually updated databases are fed by automatically discovered data as well as human expertise-based threat research. This helps prevent drive-by and water-holing attacks, as well as fraud via malicious web sites.

Delete, move or tag phishing messages:

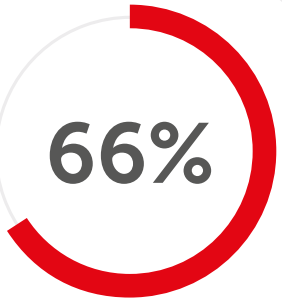
Not all unsolicited mail is junk; automatic deletion of it can cause productivity problems or impact on potentially beneficial communications. Kaspersky Lab's anti-phishing enables easy tag-based filtering and custom tags to flag potentially useful mass mail, moving it to the junk folder rather than deleting outright.

Previewed attachment analysis:

Guard against advanced phishing attacks that lead to significant data or financial losses with this unique system. It analyses attachments that can be previewed – including PDF, RTF and MSOffice files – for phishing content.

Malware: ransomware, zero-hour exploits and dodgy attachments

66% of malware is installed via malicious attachments.[4] Zero-hour and zero-day attacks often lurk inside Word, Excel, PowerPoint and other business application files, waiting for the user to click.

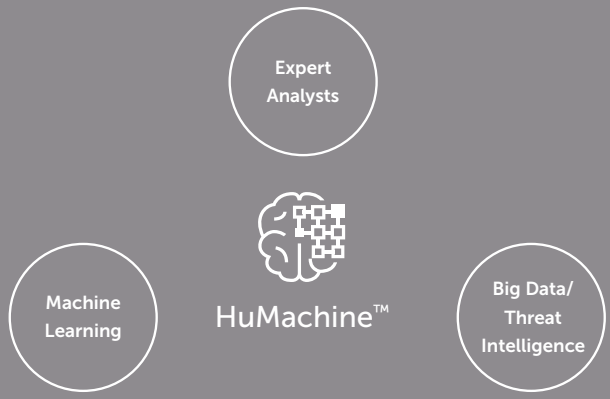


of malware is installed via malicious attachments

In many cases, malicious attachments carry malware designed to steal authentication data or log-in details using spyware – the malware is installed without the user's knowledge. Other common attachment-based attacks include ransomware – once launched, the user's data is encrypted until a ransom is paid.

What is HuMachine™

Kaspersky Lab's HuMachine©combines the very best of human expertise with big data threat intelligence and machine learning to defend against every type of threat a business faces.



4: Verizon Data Breach Investigation Report 2017.

Anti-malware technologies

Kaspersky Security for Microsoft Office 365 uses sandboxing, machine learning to determine the true nature of an attachment or file before it's allowed through. Suspicious files can be executed in a safe space to determine whether or not it's malware before allowing it through.

HuMachine-powered multi-layered threat detection

Kaspersky Lab's proven threat detection capabilities incorporate multiple, proactive layers of security that filter out malicious attachments in email. Machine learning-based detection models filter out previously unknown, zero-hour malware.

Kaspersky Security Network

Our cloud-based, global threat intelligence network uses anonymized, real-world data from over 60 million endpoint sensors globally to enable the quickest reaction times and highest protection levels possible – even as the threat landscape evolves.

Attachment filtering

Block dangerous files before they become a problem and manage undesirable messages. Real file type recognition prevents malicious files disguised as safe ones from getting through. Attachment filtering by extension enables the blocking or tagging of unwanted file types, while macro detection allows actions to be applied to potentially dangerous Office files with macros enabled. Flexible exclusions and tagging help reduce the loss of legitimate mail falling into filtering criteria.

Easy to manage, cost effective next-generation protection

You're in the cloud for convenience, resource efficiency and cost effectiveness. With Kaspersky Security for Microsoft Office 365, there's no need to sacrifice any of that for email security. A single, intuitive management console lets you take care of everything, including a single view of detected threats and statistics. There's no need for additional hardware or IT security staff training – there isn't even a distributive to install.

And it's designed to help you do this without slowing down or accidentally deleting legitimate traffic:

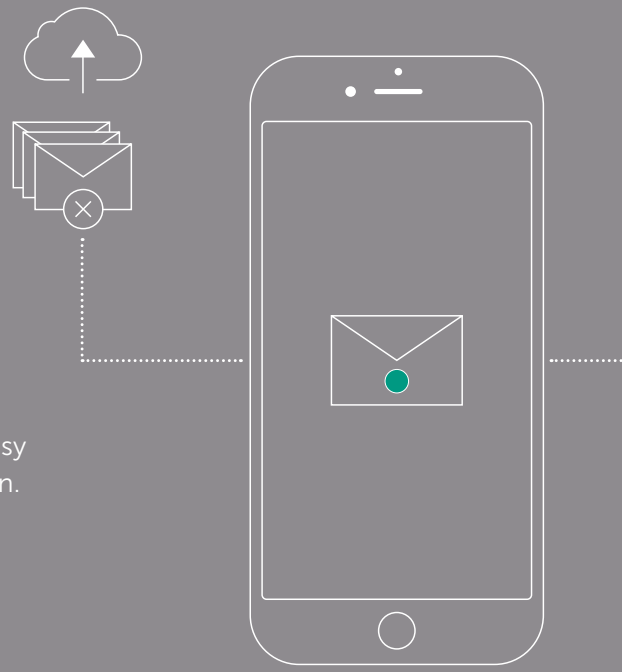
Easy management, administration and integration

At-a-glance dashboard:

One screen for daily, weekly or monthly monitoring and status on threats, statistics, detections etc.

Easy configuration:

All settings are grouped on a single screen for ultimate ease of configuration and review.



Test before rollout:

Choose which mailboxes to protect, enabling easy configuration testing or flexible policy application.

Multi-tenancy:

Enable several administrators to manage the solution using different accounts.

Backup:

Many users have issues with legitimate mail being mistaken for spam. With lower false positives and administrator control over what happens to suspicious mail, Kaspersky Security for Microsoft Office 365 significantly reduces the chances of this happening. Deleted mails are placed in backups and can be searched for and restored – no more 'disappearing mails.'

Notification:

Enable rapid incident response with administrator notifications for spam, phishing, virus attacks or attachment policy violations.

Single sign on:

One console and sign-on to manage security for different endpoints, devices and Exchange Online.

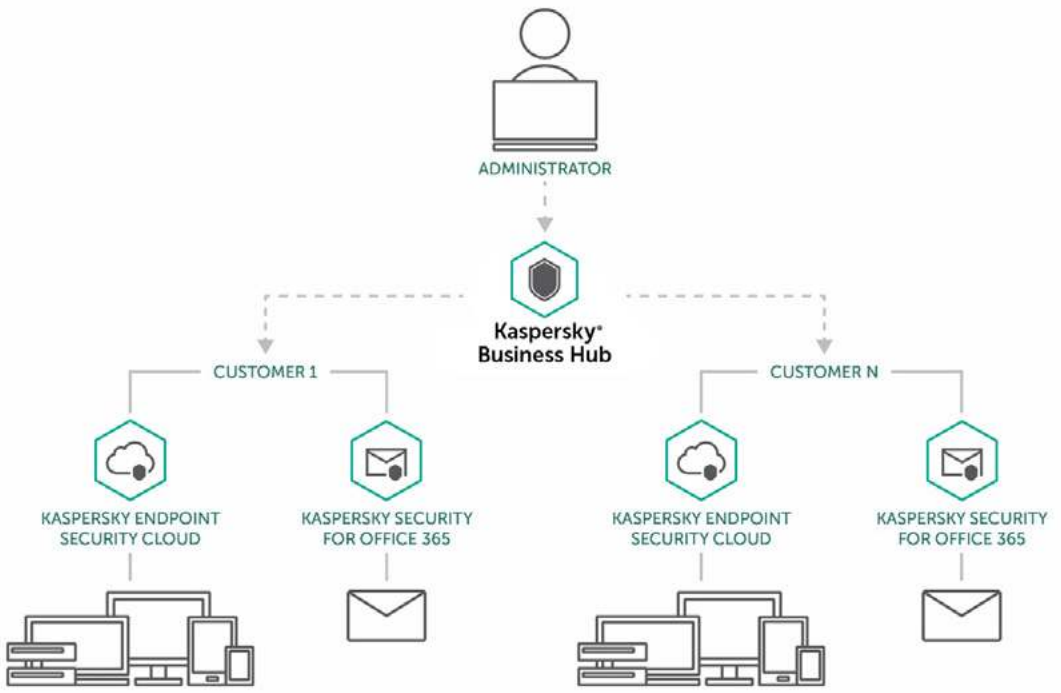
Kaspersky® Business Hub

Kaspersky Business Hub – a single console to manage your company's protection.

Experience our intuitive interface, simple management and superior protection for different devices and productivity tools. Simply connect from any device you choose - any time, any place, you're in control.

The following products are managed from Kaspersky Business Hub:

- Kaspersky Endpoint Security Cloud
- Kaspersky Security for Microsoft Office 365



Kaspersky® Security for Microsoft Office 365

When it comes to protecting your Microsoft Office 365 mail, the best strategy is making sure threats are detected and blocked before they can become a problem.

Kaspersky Security for Microsoft Office 365 is designed to help you do this without slowing down or accidentally deleting legitimate traffic.

Discover how our next-generation security technologies can make your Microsoft Office 365 mail even easier to secure and manage.

Try it for free at cloud.kaspersky.com