

Security-as-a-Service: Threat mitigation from the cloud



You can't treat security as a set of isolated point systems. That's true of your business information in general and of your email architecture specifically. Protecting information is one side of the coin; making it available and accessible is the other and if you do both right you can improve productivity as well as avoid risk.

The cloud isn't just the most effective place to secure email, before any threats or intruders ever reach your network; it's also the most efficient. Cloud-based email services can offer full protection with the promise of availability and reliability too.

Contents

03 Securing email in the cloud

- 03 Security with universal accessibility
- 04 Email intelligence
- 04 Managing email security yourself
- 05 Risk management and security
- 05 Fragmented security systems

06 Making security a service

- 06 Security in the cloud
- 06 Security with Mimecast: at rest, in transit and in use
- 07 Anti-malware
- 07 Anti-spam
- 08 Zero-day protection
- 09 Policy enforcement
- 10 Audit trails
- 10 Securing the cloud

11 Security is holistic

- 11 Scaled-up security

Executive Summary

A cloud email platform needs to have four key features:

- Confidentiality
- Integrity
- Availability
- Control

That's what you get from Mimecast's security services, without having to patch and update a mixture of different security tools in your own network. It's a complete risk management and compliance platform, with anti-malware, anti-spam, zero-day protection, and policy enforcement. At the same time, there's a complete audit trail and secure encrypted storage on the Mimecast® storage grid.

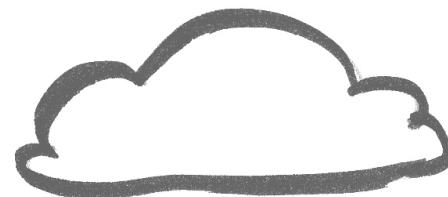
Securing email in the cloud

Security with universal accessibility

Security is more than keeping unauthorized users out of your network and viruses off your desktops. It's not just about encrypting data or blocking spam, monitoring compliance, ensuring privacy or protecting company resources, important as all of those are. If you take the wider view, security means ensuring the confidentiality, integrity and availability of business information. While line-of-business applications and back-end databases are crucial, more and more of that business information is in email on desktops and laptops, which makes it both convenient and vulnerable. It doesn't matter where in the value or supply chain you are, you're relying on email for all manner of vital communications.

Securing email – at rest, in use and in motion – is a key part of any IT security strategy and doing that in the cloud has significant advantages for confidentiality, integrity and availability. For one thing, you're protected from spam and malware before it ever reaches your premises; keeping up with thousands of new threats a day is an unnecessary battle for individual businesses to fight. For another, as with other cloud services you're gaining the expertise and economies of scale of a dedicated service, which means savings on up-front costs and ongoing administration, making a big difference to how quickly you can see value from the system you put in place.

And for email in particular, having it protected in the cloud means it's available in the cloud; as convenient as having it on your laptop but without the security risks. That makes the difference between security that gets in the way of users, forcing them to resort to insecure workarounds to get their job done, and security that gives you the flexibility and control to allow business users to stay productive. At best, security is usually seen as a necessary evil; at worst it actually hampers the business. More than 80% of IT security and business executives say they've given up opportunities for innovation in business because of concerns about



> Securing email in the cloud

Email intelligence

You can give users access to a mass of useful information about customers, products, colleagues, negotiations, existing contracts and useful contacts, just by letting them search their email efficiently. Who is the best person to work with at a company you haven't dealt with recently? How quickly does a supplier usually get back to you? How often has a potential partner been recommended by colleagues? Often, the information they need is sitting in an old message, but if mail server quotas mean they only have a few weeks of email in their inbox then they're faced with losing access to key business information or keeping PST files on their hard drive, which exposes the information to a host of security threats and impedes eDiscovery should it be required.

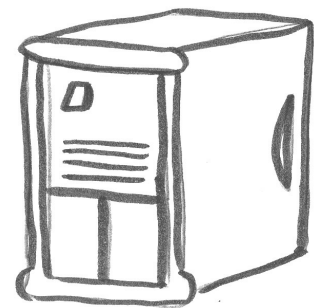
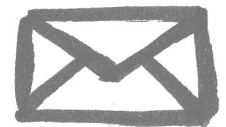
Making email available and searchable in the cloud means that it stays secure, but is still accessible. It's the best of both worlds for the user, the IT administrator and the business. Users are no longer restricted by lack of resources, and can take advantage of being able to work anywhere, and at anytime.

Managing email security yourself

Implementing on-premise infrastructure required to ensure an email system is secure and compliant takes time and requires significant post-installation maintenance. As the email attack surface is large, it's important for businesses to keep their security platform up to date – but this has significant time and budgetary impact, as well as affecting the resources available to IT departments. Time spent maintaining an email security system is time that's not being spent developing new systems or improving business processes.

Putting security in place isn't a one-time deal. It needs ongoing management, to ensure security infrastructure is kept up to date and regularly maintained. Mail administrators need to regularly patch and upgrade software to deal with new techniques employed by malware and spam authors. Significant investment will be required for hardware and software – which is an ongoing expense – as well as subscriptions to support services. Appliance lifetimes are typically short, like PCs and servers, and they will need to be replaced every three or four years. Replacing appliances is another risk, as cover needs to be kept in place while new hardware is installed, and services are migrated between what are likely to be very different security platforms.

The cost of an administrator's time needs to be taken into account too, as effective management of an email security platform will often require the equivalent of at least one, or maybe more, full-time positions. And beyond the individual costs, this is a permanently defensive approach to security, and one that means that mail security will always be a cost to a business, where it will be hard to identify any return on security investment. Getting and collating reports to help understand the returns is an issue in its own right, as fragmented servers and services make it hard to get the right level of visibility into the operations of your mail platform. Mail security teams will find it hard to report in terms of business benefits when the only effective metric is the number of days between security failures.



> Securing email in the cloud

Risk management and security

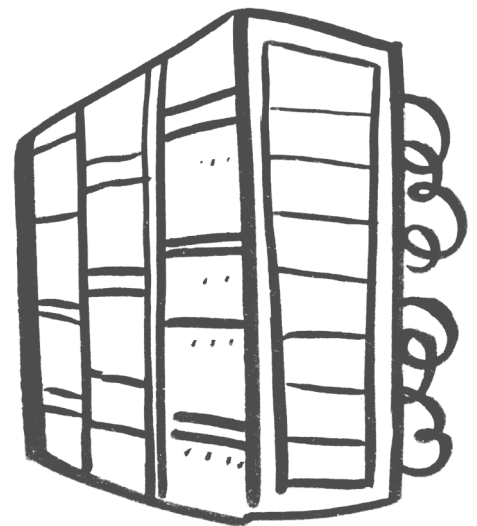
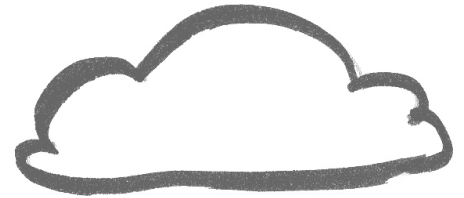
And you can't simply ignore the problem because of the costs; effective email security is a business necessity. Email introduces risks into the organization, and risks need to be managed. Insecure mail opens you up to all manner of attacks and issues. Spam gets in the way of normal mail traffic, and distracts staff. Productivity drops every time a user has to delete a spam message, and with 80 – 85% of a user's email being spam, it's wasted time that quickly adds up.

It's not just advertising spam, either. Spam is now one of the main routes malware takes into a company. A plausible message with an attachment is a ticking time bomb that could end up compromising machines, adding them to botnets and opening up their file systems to the prying eyes of criminals. It's not just obvious spam that delivers malware; it can also come from trusted sources.

Fragmented security systems

Once in place, email security infrastructure is a key component of your business protection, mitigating risks and reducing exposure to third-party threats. However it needs to be a coherent, easy-to-manage system. That's seldom the case if you have a patchwork of systems each that were put into place to answer specific threats. Separate anti-virus tools sit next to anti-spam appliances, getting updates on different schedules, while data loss prevention tools add to the complexity. Managing them all is another complex task, as they'll each have their own management tools, and system administrators will find themselves working with a mix of web user interfaces, remote desktops, and console applications. Making sure everything is up to date becomes a full time task, not to mention testing rules and updated applications to ensure they don't affect your business processes – an updated spam filter that stops customer emails from arriving is something no one wants.

There's another problem that's exacerbated by the complexity of managing your own email security infrastructure: the window of vulnerability. Email security is an arms race with spammers, phishers and malware authors – and they will often have the upper hand. Filters and signatures can only be updated after attacks have been identified and categorized, so you'll be left waiting for updates to be tested and installed hours or days after the bad guys have started using the loophole you're waiting to close. Fifty percent of systems are still unpatched 60 days after patches are released – that's a long time to risk getting infected with malware.



Making security a service

Treating security as just a series of defenses doesn't give you much opportunity to differentiate your business. The place to add value and improve productivity is through what you enable with security.

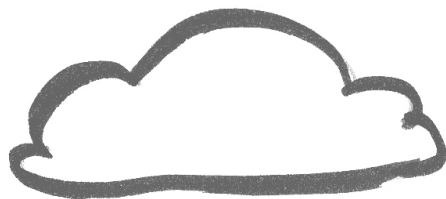
Security in the cloud

You could outsource the management of your on-premise email infrastructure, but the problems (and costs) of the DIY security architecture remain. The alternative is to shift the burden of management off the IT department by moving it out of your network completely. This approach is often partially in place, with anti-spam facilities already outsourced to services that partly or wholly run in the cloud. Important as they are, anti-spam and anti-virus services are only part of the security story, especially in light of the current regulatory environment. Putting all your email security in the cloud will relieve your IT department of a considerable burden. There's no need to test patches, no need to wait for updates to install – and above all, little or no down time.

Security with Mimecast: at rest, in transit and in use

Mimecast's unified email management service provides a lot more than email management and business continuity. It's a complete email risk management and compliance platform, able to protect your mail while it's stored, when users are working with it, and while it's being sent and received. The layers of protection include anti-malware tools, anti-spam, anti-phishing, Denial of Service protection, policy enforcement and encrypted storage.

Email is one of the main gateways into your business, and its security is a key requirement at all times. Regulatory requirements mean that a larger proportion of email now needs to be stored for many years, and you need to be sure that its integrity is preserved, and that full audit trails exist to show just who looked at a message, and where and when. That's all part of the role of Mimecast's security platform, which aims to ensure that your mail is always secure, whenever and wherever it's being read.



A well-designed security system needs to provide businesses with four key features:

- It needs to be available at all times, to the appropriate users
- It needs to provide a business with the means to ensure the integrity of its systems
- It needs to be confidential (making sure that only your company and partners can access mail and mail based processes)
- It needs to give you the means to control user actions

Delivering all four is a complex task, and requires a mix of tools and technologies making it well suited to a cloud service.

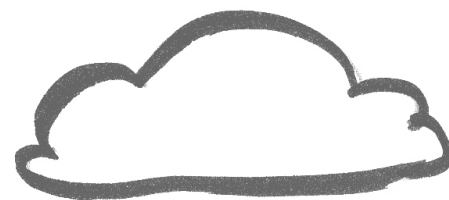


Making security a service

Anti-malware

No two anti-malware tools are identical. They all work differently, and they all update on different schedules. Some push out updates to their signature files every few minutes, with weekly or even daily updates to their engines. Others are slower, but offer a wider range of anti-virus features. It's important to use a mix of different anti-virus engines if you want to keep a network as secure as possible with as wide as possible coverage. If one engine is being updated, the others will still be working, and messages will continue to flow, but if you're doing this in house you'll need to find a way of staggering updates.

Building a suite of anti-malware tools takes time, as you need to continually monitor evolving threats and available technologies in the market. Another good reason to work with a cloud service is it can use its dedicated resources to ensure you always have the best in class anti-virus tools protecting your mail. That's why Mimecast uses multiple anti-malware technologies from Cloudmark, Commtouch, Clam, AVG, Eset and its own anti-malware stack. Intrusion Prevention tools look for not just traditional malware, but also specially crafted attacks that take advantage of application and operating system vulnerabilities.



Anti-spam

The same is true of anti-spam tools and services. An effective anti-spam solution is a mix of different tools and approaches. Producing the most effective blend requires significant investment – and continual monitoring. False positives need to be kept to a minimum, as do false negatives. With spam techniques and sources changing from hour to hour and day to day, an email security network needs to be able to respond quickly, something that's difficult for a small network without full-time support. By using a cloud service, both large and small business get access to enterprise-grade tools and software, as well as the enterprise-grade staffing and support needed to keep the service running.



Effective anti-spam protection also comes from accurate reputation services. Mail accepted by a customer of a cloud email service will count towards the reputation score of the sender, and mail that's rejected will compromise that reputation. Low reputation scores can mean a message is automatically flagged as spam, stopping you being able to email some companies at all.

Maintaining your email reputation with cloud services like Mimecast will avoid this problem. While on-premise mail services can subscribe to reputation services, they can be hard to manage, and it's often unclear what the source of, or how accurate, the reputation data is. A cloud service with many clients will automatically have a large and diverse user base from which to build its own reputation service, so you get effective protection.

Making security a service

Phishing messages that try to trick users into revealing bank account or confidential corporate information are still a serious problem. Finely targeted so-called 'spear-phishing' attacks are on the increase too. A cloud mail service can protect its clients by using a dynamic URL list of known phishing sites; Mimecast constantly refreshes and updates this list and proactively checks new domain registrations to see if they need to be added to the list – particularly looking for new registrations that are a deliberate mis-spelling or lookalike of a financial or commercial domain. Phishing messages often contain similar contents; with a large enough number of messages you can create fingerprints to help detect current and future versions of the attack and Mimecast updates its fingerprint database every 45 seconds.

Zero-day protection

It's hard for a single-site mail system to offer effective zero-day protection against new threats. The key to effective zero-day protection is working with an enormous number of incoming emails, looking for the signs of a malware outbreak or a new type of spam. Any zero-day protection scheme needs to be able to identify possible malware, and quarantine it before it can be delivered to your users. Mimecast's Zero Hour Adaptive Risk Assessor (ZHARA™) examines suspicious messages as part of the process of splitting them into isolated pieces for processing and storage in the Mimecast grid.

Possible malware is automatically routed to the Dark Traffic, Analysis Group to be reverse engineered. The system also monitors the pattern of incoming connections and the profile of traffic from mail servers to look for unusual behavior and help protect against distributed Denial of Service attacks. None of this is possible unless you're dealing with a large enough amount of email to receive new threats quickly and you have the expertise to detect and remediate problems. In addition to the tens-of-millions of emails Mimecast deals with on behalf of its customers every day, Mimecast uses a network of honeypots to gather spam and malware in the wild, proactively protecting customers from attack.

Cloud services like Mimecast can provide security without compromising email delivery speed; email is an important business tool and it needs to be delivered in a timely fashion. With this combination of pro-active techniques, Mimecast is able to stop an average of 99.5% of malware and spam at the protocol level, without needing to analyze the content. And even though it uses a variety of detection engines to ensure all threats are detected, the Mimecast Mail Transfer Agent, ARMed SMTP™ undertakes much of the analysis in parallel to avoid slowing down email to an unacceptable level.



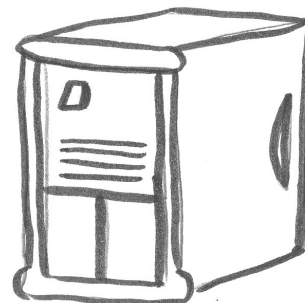
Making security a service

Policy enforcement

Email security isn't just about protecting your staff from threats in incoming messages. It's also about managing the content of the messages they sent. Controlling exactly what information leaves your network is becoming increasingly important, to protect customer data and to make sure your business complies with the appropriate regulations. It's also important to make sure that you apply appropriate controls based on user roles: your CEO is likely to want to be able to send anything, while your customer service staff probably don't need to be able to send attachments or messages that contain customers' personal information.

This is where policy enforcement tools come into play. A cloud service will be able to give you one dashboard where you can control everything from user access to mail, to what they can send – and to whom. Data loss prevention tools let you scan for key words and phrases to make sure sensitive information isn't leaving your company, and the same tools help you ensure your business complies with all the appropriate regulations. Policy enforcement tools can also be used to make sure that all mail you and your staff send is encrypted, and signed with appropriate digital signatures – giving you a level of integrity and non-repudiation that is hard to match with conventional on-premise mail tools.

Mimecast offers TLS (Transport Layer Security) encryption, sending messages through a secure tunnel to the target mail server, which can be triggered by the domain, the specific email address or keywords in the subject or body of the message. If the target mail server doesn't support TLS, Mimecast can utilize 'closed circuit' messaging to deliver it through secure Webmail; that gives tamper proof secure mail with non-repudiation without having to exchange digital certificates in advance. And when staff need to share files with customers, partners or vendors but you don't want the risk of an attachment leaving the business or can't guarantee the receiving server can handle the attachment type or size, Mimecast can automatically strip the attachment and replace it with a URL for accessing the file on a secure Mimecast Web server.



Making security a service

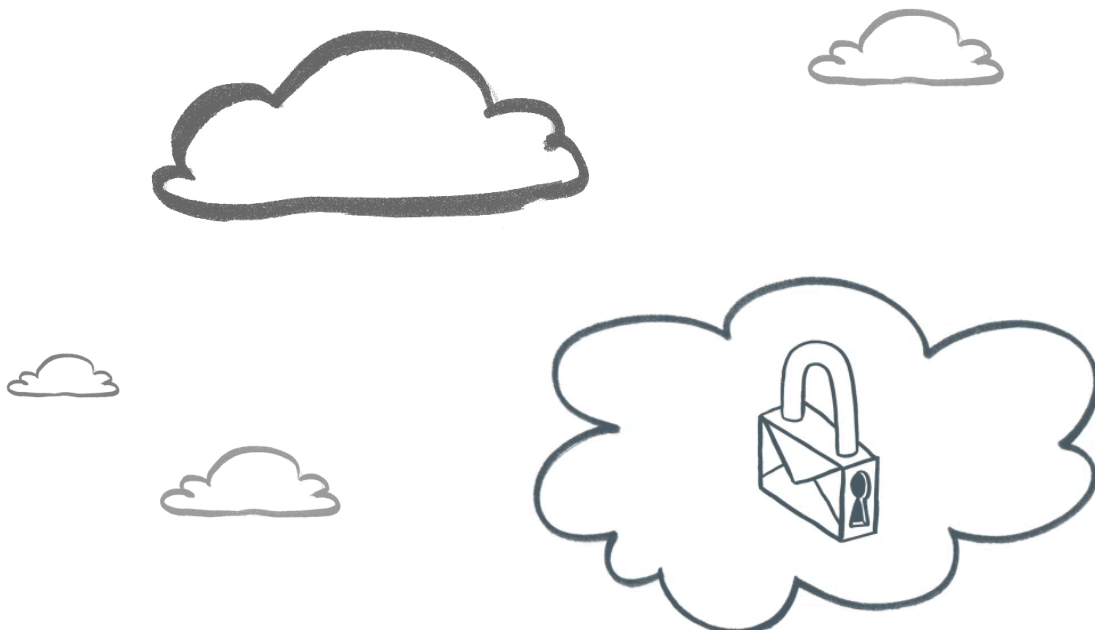
Audit trails

In the cloud doesn't mean out of sight; with Mimecast you can still view a complete audit trail for your mail, indicating who sent it, who read it (and how many times), and even where they read it. Audit trails give you the tools you need to ensure that your users aren't attempting to circumvent regulatory restrictions, as well as giving you the assurance that you will be able to provide proof of user actions if regulators or legal actions require it.



Securing the cloud

Your mail may be secure as it travels across the Internet, but what about the cloud service that's hosting your mail? It needs to be able to protect itself (and your mail) from Denial of Service attacks, it also needs to make sure that your mail is strongly encrypted and partitioned well away from any other customers – using different encryption keys to ensure that only you and your staff can access your mail. Mimecast's storage grid is separate from its processing grid, and spreads stored email across multiple geographically dispersed data centres in each territory ensuring data is stored in its jurisdiction. Content is stored using AES 256 encryption, and the keys are fragmented across the grid, reducing the risk of anyone accessing your mail either inadvertently or deliberately.



Security is holistic

Scaled-up security

Outsourcing your email security to a cloud service gives you a full-time security service. Cloud services support large numbers of users, and economies of scale mean that they have staff dedicated to manage their security tools. Heuristic spam and malware detection tools running in the cloud can detect problematic messages quickly, because scanning all the messages targeted at all their clients' mailboxes gives them so much material to work with. Malware patterns will show up quickly, and detection rules will be applied as soon as they have been reliably developed.

These techniques mean that cloud services have a very short, or non-existent, window of vulnerability to new spam and malware messages. A cloud service can also offer increased protection by using several protection mechanisms – typically using several anti-malware and anti-spam tools, or more than one heuristic analysis tool. With more tools, your email presents a much smaller attack surface, reducing your business risk. You could run multiple protection tools in house, but that increases the burden of management and can reduce the performance of your mail servers.

One area where cloud services excel is helping to calculate ROI. A single place to manage all your email security means there's one place to get reports on system performance. A per-user billing cycle also means that it's easy to tie costs to departments and specific business processes, making it easier to calculate the service ROI. A fixed fee also makes it easier to include the service costs in departmental budgets, rather than lumping costs into a single annual IT budget. There's another benefit too, in the shape of no capital costs. All the equipment needed to run an email security service is hosted and managed by the cloud service provider – so there's no need to budget for new servers and security appliances.

Cloud services are designed to do one thing and to do it well, so by entrusting your email security to a cloud provider you're working with experts. Of course no two services are the same, so you should evaluate the capabilities of your chosen service carefully, to ensure suitability with your needs.

Security may be part of your wider business issues, but it's also a fundamental IT issue. Unless security is part of your business' core expertise you'll be able to reduce risk, cost and complexity by using cloud services to achieve unified security. Keeping your email in the cloud ensures you can keep it secure and make it universally accessible, therefore extracting the business value from it without any of the usual disadvantages. With cloud security like Mimecast's you could derisk email and turn it into a true business resource.



Mimecast is a leading provider of essential cloud services for Microsoft Exchange. Mimecast delivers enterprise email management services that include security, continuity and archiving. This suite of services provides total end-to-end control of business email, while minimizing risk and reducing both cost and complexity. Founded in 2003, Mimecast serves thousands of customers worldwide and has offices in Europe, North America and Africa.