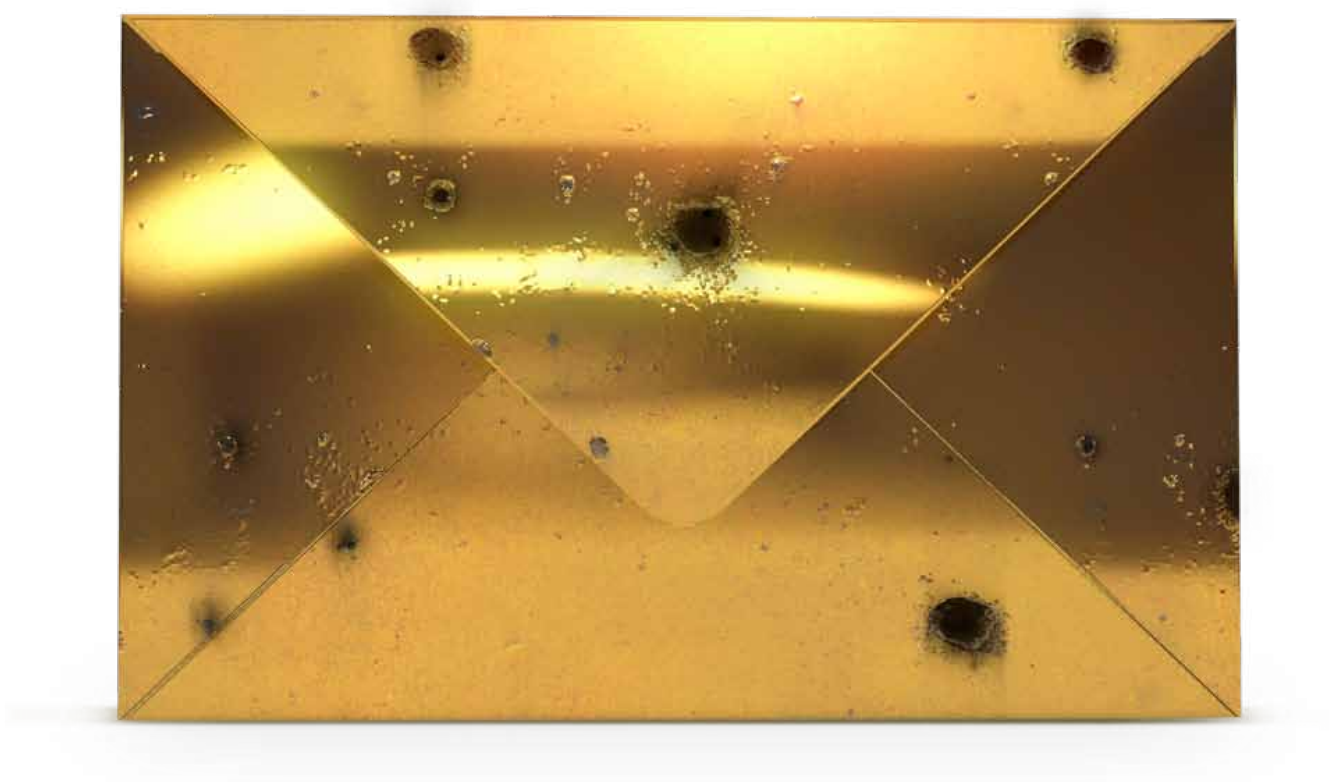
MAX Mail™

Whitepaper

Bullet-proofing Office 365 with MAX Mail



MAXfocus™
From LogicNow

Table of contents

Executive summary	3
Email's security problem	4
Understanding the CIA Triangle	5
Office 365: Moving productivity into the cloud	6
MAX Mail: Bullet-proofing your email	7
Building a broader defense strategy	10
Conclusion: An in-depth defense	11

MAXfocus™ From LogicNow

MAX Mail™

Executive summary

Email is baked into the DNA of modern business. Despite the rise of alternative channels such as social media, it continues to grow in importance for companies. For this reason it is still the most common vector for cyber attacks. Having an extra layer of defense in place has never been more important.

1 Email is the lifeblood of most companies, but it is also one of the least secure means of communication. As it has become ubiquitous over the years, it has become a carrier for malicious software and web links that can bring down entire enterprises.

MAX Mail provides an additional line of defense for Office 365's cloud-based email system. With a long heritage in providing support for on-premise systems, it is also a powerful way to protect and augment cloud-based systems, too. MAX Mail provides Office 365 users with:

- **Confidentiality**
  A range of security features protect corporate data from email-based attacks.
- **Integrity**
  MAX Mail's archiving capabilities use cryptography and checksum technologies to provide a secure, verifiable, and independent copy of an organization's entire email history, including all content and metadata.
- **Availability**
  Cloud computing doesn't guarantee complete continuity. Cloud systems go down, just as on-premise ones do. MAX Mail provides customers with the ability to ensure their end users can continue to access and respond to email, when the primary email infrastructure – whether on-premise or in the cloud – is offline.

MAXfocus™ From LogicNow

Email's Security Problem

2 When first invented in 1971, networked email didn't face the same challenges that it does today[1] Back then, the Internet was barely born, and it was a rarefied space with few participants, mostly from the same military and academic communities. Spam, phishing, and email viruses didn't exist. Passwords were optional.

Today's Internet landscape is entirely different, with a range of bad actors, including:

- **State actors**
  These are hackers hired and trained by governments to crack overseas systems. Many governments have elite units trained for these purposes, including China's Unit 61398[2] and North Korea's Bureau 121[3]
- **Criminal gangs**
  Often coming from Eastern Europe, these gangs are highly organized, with networks of specialist contractors handling different functions. They run cybercrime like a business.
- **Corporate spies**
  Corporate cybercriminals will engage in cyber-espionage, targeting company secrets and selling them to the highest bidder.
- **Hacktivists**
  Often relatively unskilled, hacktivists can organize in packs and target organizations for personal or ideological reasons. They often seek to publicly humiliate their targets.
- **Cyber-terrorists**
  These expert hackers can often carry out more sophisticated attacks, typically for ideological or political reasons.

Email as a key entry point for attacks

All of these attackers frequently use email as a path into a target organization, in the following ways:

- **Social engineering**
  Even when their computers are protected by antivirus systems, employees can still be susceptible to manipulation. An email purporting to be from an IT consultant asking for a corporate email account, or pretending to be from a CEO's personal email demanding a list of key customers for a particular department, can unlock valuable company secrets.
- **Phishing**
  A variation on social engineering is phishing. Criminals frequently send mass emails purportedly from financial institutions, attempting to get users to log into fake websites with malicious payloads.
- **Spearphishing**
  Spearphishing is a more sophisticated attack, launched after gathering detailed information about a targeted individual and their company. Often accompanied by malicious attachments, it is another attack that can lead to malware infection.
- **Malware infection**
  Typically an effect of an email attack, malware can infect a computer via a link to a malicious website, or an infected file. Malware can be the beachhead for an advanced persistent threat, in which attackers can establish a foothold in an organization's network, and then begin stealing data.

Understanding the CIA Triangle

3 Information security is often described using three concepts: Confidentiality, Integrity, and Availability. These three terms are all seen as crucial to a solid information security strategy, and are therefore commonly identified as the CIA triangle.

Confidentiality

Confidentiality is typically mapped to privacy. It refers to the rules limiting access to information, and as such is directly linked to cybersecurity. If data is deemed accessible to those outside an organization, and perhaps to some people inside it, that is a risk – and measures should be taken to enforce rules around confidentiality.

Integrity

Effective retention of important data is a core requirement for most businesses to be successful. Integrity refers to the trustworthiness of this data – information can be said to have integrity if it can be proven not to have changed. Typically, the integrity of a record is guaranteed with the help of metadata (data used to describe the record and its contents).

Availability

Availability is often associated with continuity. In modern business environments, information and communication are recognized as important services needed for employees to be productive, and the constant availability of those services is important. If email becomes unavailable for whatever reason, then a company's processes and productivity could suffer, with potential lost revenues as a result.

MAXfocus™ From LogicNow

Office 365: moving productivity into the cloud

4 Historically, general office productivity software packages, including word processing, spreadsheets and email, were implemented on-premise at a customer's office. As a wide variety of software and services have moved to the cloud, so too has Microsoft embraced online offerings for its productivity software.

In 2011, the company released Office 365, which replaced its previous hosted software offering, Microsoft Business Productivity Online Service. A core component of Office 365 is email hosting, through a hosted version of Microsoft Exchange Server. Microsoft improved the product's email security in early 2014, when it replaced its original Forefront Online Protection for Exchange (FOPE) with Exchange Online Protection (EOP).

Microsoft offers several features within EOP that attempt to address the CIA triangle. While the software giant has taken significant steps to improve security within its service offering, there are still inherent vulnerabilities for businesses in relying wholly on a single vendor, particularly one that has not had a historical focus on security.

Typically, cybersecurity experts advocate a technique called 'defense in depth', which uses multiple layers of protection, ideally from different vendors, to bolster a company's security.

MAX Mail: Bullet-proofing your email

5 MAX Mail from LogicNow is an email security service hosted in the cloud. The service ensures users are protected by continuously improving, comprehensive layers of security encompassing highly accurate spam detection, robust virus defense, and built-in email continuity, to maximize their productive use of email. The service is available either as a stand-alone product, or integrated into the MAXfocus Remote Management platform.

Benefits of cloud-based email security

MAX Mail brings customers the full benefits of cloud operation. Customers can secure their email by simply updating their DNS "MX" records to redirect inbound email to LogicNow's servers, which provide a first line of defense. Customers do not have to invest in or maintain any hardware, and MAX Mail is able to block threats before they reach a company's email server – even if, as with Office 365, that email server is cloud-based.

Security as a Service offers a fast on-ramp to better defense against email-borne threats and provides customers with multiple benefits:

- **Predictable costs**
  Cloud-based email security is provided on a per-mailbox basis. This eliminates the risk of a capital investment and makes operating costs easier to predict, because there are no hardware replacement costs to allow for, and no infrastructure management overheads.

- **No on-premise equipment maintenance**
  With traditional on-premise email security solutions, the hardware running the security software must be maintained. Even appliances carry an operational overhead, needing replacement firmware upgrades occasionally. And eventually, all hardware must be replaced. With a cloud-based system, this is all taken care of behind the scenes.

- **Reduced management overhead**
  With cloud-based email security, delving into command-line interfaces to manage software processes are a thing of the past. Infrastructural nuances are shielded from administrators, who only have to worry about setting permissions and policies using an easily understandable online interface.

- **Greater reliability and scalability**
  An on-premise solution is typically limited to a single device that is ultimately a single point of failure, with limited scalability. In the event of an attack or large-scale spam run, any single device is vulnerable, no matter how efficient. With multiple systems in multiple geographically distributed data centers, MAX Mail leverages the cloud to provide substantially greater reliability and scalability, which in turn reduces risk for a critical part of the company's infrastructure.

MAXfocus™ From LogicNow

MAX Mail and the CIA Triangle

MAX Mail is specifically designed to enhance the CIA triangle for all email users, whether they are running on-premise servers, or cloud-based services such as Office 365's hosted version of Exchange. It does this by specifically targeting the three points of the CIA triangle: Confidentiality, Integrity, and Availability.

Confidentiality

Multiple layers of email protection

In modern email protection, one antivirus engine is not enough to secure a system. Cybercriminals regularly test their malware against software provided by multiple antivirus companies. The more antivirus technologies in place to defend the customer, the better.

Although Office 365 does work with multiple antivirus partners, it reserves the right to change them without telling the customer, meaning that you never know quite what protection you're getting. MAX Mail leverages multiple antivirus engines, each with different technological frameworks, giving administrators peace of mind that should any vulnerabilities exist within the primary email infrastructure, MAX Mail will provide a robust additional layer of defense.

Going beyond signatures

Another shortcoming of some antivirus systems is that they rely on virus signatures, which look for and match the patterns of a particular virus. After the signatures have been updated to detect new viruses, customers are safe – but the signature-based approach to virus detection can leave a vulnerability window of several hours during which a company is at risk.

So-called zero-day attacks, which exploit vulnerabilities that have not yet been patched by application and operating system vendors, are increasingly prevalent and present a significant risk to companies reliant on signature-based virus detection.

Although Exchange in Office 365 includes heuristic scanning capabilities for incoming emails, EOP only updates signatures every hour. MAX Mail updates its antivirus signatures in near-real time. More importantly, MAX Mail supplements its traditional signature-based virus detection with zero-hour malware detection technology that recognizes emerging threats based on automated pattern detection rather than specific signatures, and which can therefore detect threats even in the very early stages of a new virus outbreak.

Better anti-spam

Microsoft has matured and improved its anti-spam offering, but as with antivirus, every single layer of protection helps. Traditionally, very few companies have relied solely on the anti-spam engine included within Exchange. For a nominal per-mailbox cost, IT administrators can bolster their protection against phishing scams and other junk mail.

MAX Mail's anti-spam system is designed so that administrators can "set it and forget it." For those administrators who want granular control over spam detection, the service allows administrators to configure a number of different features:

- **Filter aggressiveness**
  Administrators can fine-tune the aggressiveness of the spam filter, on an organization-wide, domain-wide, or per-user basis.
- **Daily digests**
  Customers generally choose to have detected spam messages quarantined in the cloud, while users can receive (up to three times per day) a digest of those messages. This allows for rapid review and a one-click release mechanism in the event that any legitimate message was flagged as spam.
- **Whitelisting and blacklisting**
  Administrators or end-users can maintain whitelists and blacklists to allow or block particular messages, based on sender, subject, source IP address, or other criteria.

Data jurisdiction

Data jurisdiction is a critical question for any cloud provider. No matter what security and encryption standards they adhere to, cloud-based email providers usually have the right to move your data between countries. Among other issues, this may affect government access to data under local laws, which may present a problem for some organizations.

MAX Mail uses wholly independent datacentres in both Europe and North America and guarantees customers that their data will be processed and stored solely within a designated region, thus helping to protect the confidentiality of that organization's data.

Availability

Despite vendor claims, cloud services aren't invincible, and Microsoft is a good example. The company's Office 365 has suffered numerous outages in the past few years. In November 2012, the service suffered two email outages in five day[4] In February 2013, it went down again after the company launched new services[5]. The service suffered yet another outage in June 2014 that left customers pleading for help. Then again that November, Microsoft's Azure cloud went down making apps and data unavailable[6,7].

MAX Mail provides valuable continuity

Companies depend on email for their communications and can't afford to be without it. With a geographically distributed datacentre architecture independent of other cloud providers' systems, MAX Mail provides valuable insurance for customers, by automatically queueing email in the event of a problem with the customer's primary email infrastructure, and providing end-users the ability to easily access and respond to those messages in the event of a failure with Office 365.

Integrity

The importance of archiving

Companies must have a record of their historical emails. Not only is email a tremendous repository of intellectual property – email also includes information that may one day be needed by lawyers or auditors. Whether the need is to harness the intellectual property contained within email, or to have a verifiable record of communications in the event of a dispute, an email backup is not sufficient. Only an email archive provides a reliable, tamperproof record, with appropriate access rights and controls.

Moving beyond native Office 365 archiving

The native archiving within Office 365 is limited. The company's Exchange Online archiving function is more advanced, but must be purchased on a per-mailbox basis. Even then, customers face a problem: the archive is by the same company hosting the operational mailboxes. What if something catastrophic were to happen?

MAX Mail provides a secure, searchable archive

Within MAX Mail, the integrated MAX MailArchive system provides a secure, geographically distributed, cloud-based archive that is completely separate from the Microsoft infrastructure. MAX MailArchive uses the same strict data jurisdiction policies, strong encryption, tamperproof storage, and checksum technology to validate message integrity. Companies can define simple or highly granular message retention policies, based on criteria including sender, recipient, and subject. Messages are fully indexed and searchable, and can be manually or automatically tagged for rapid retrieval. Administrators can also define role-based access to archived messages.

Customers can also import existing historical messages into the MAX MailArchive system, either on their own or via a professional service offered to help with that process.

Building a broader defense strategy

6 MAX Mail is also part of a broader defense strategy, thanks to its inclusion in the MAXfocus platform, which includes other security components such as web protection that protects users from http- or https-based threats delivered by malware-infected websites.

MAXfocus also includes a facility for scanning client-side devices. This provides yet another layer of protection in the unlikely event that a rogue infection does escape detection from the cloud-based email and web protection systems to compromise a machine. MAXfocus scans servers, workstations, and other devices within a customer's network for malware, so that threats can be promptly remediated.

MAXfocus™ From LogicNow

Conclusion: an in-depth defense

Security is a constantly evolving challenge. The Internet is a melting-pot of threats, which mutate as quickly as security companies do their best to stop them. There is always the danger that reliance on a traditional and narrow approach to security will leave you vulnerable to a sophisticated attack.

By employing a third-party system to complement your email provider's security, you make things more difficult, even for determined attackers. Now they have to circumvent multiple layers of defense, multiple defensive technologies, and multiple datacenter infrastructures.

Email continues to be the leading vector by which malware is distributed. Security operates on a spectrum. Customers will certainly benefit from Office 365's built-in security, but for a nominal monthly expense per mailbox, with no other investment in hardware or software and no managerial overhead, companies can supplement their security posture with specialized protection against email-borne threats. At the same time they have the assurance of email continuity and the option for a fully integrated and independent email archive – comprehensive email security and true peace of mind.

References

1 "The First Network Email", Ray Tomlinson http://openmap.bbn.com/~tomlinso/ray/firstemailframe.html

2 "Hello, Unit 61398", The Economist, Feb 2013 http://www.economist.com/blogs/analects/2013/02/chinese-cyber-attacks?spc=scode&spv=xm&ah=9d7f7ab945510a56fa6d37c30b6f1709

3 "In North Korea, hackers are a handpicked, pampered elite" Reuters, Dec 2014 http://www.reuters.com/article/2014/12/05/us-sony-cybersecurity-northkorea-idUSKCN0JJ08B20141205

4 "Microsoft hit by second Office 365 email outage in five days", ZDNet, November 2012 http://www.zdnet.com/article/microsoft-hit-by-second-office-365-email-outage-in-five-days/

5 "Microsoft Office 365 hits pothole", GigaOm, February 2013 https://gigaom.com/2013/02/01/microsoft-office-365-hits-pothole/

6 "Microsoft Suffers Another Cloud Outage As Exchange Online Users Left In The Lurch", CRN, June 2014 http://www.crn.com/news/cloud/300073234/microsoft-suffers-another-cloud-outage-as-exchange-online-users-left-in-the-lurch.htm

7 "Azure outage hits Microsoft Office 365 users & websites", CloudPro, Nov 2014 http://www.cloudpro.co.uk/cloud-essentials/4645/azure-outage-hits-microsoft-office-365-users-websites

MAXfocus™ From LogicNow

Connect with us!

Please get in touch if you have any questions about any of our services.


+44 (0) 1382 309040


UK uksales@maxfocus.com
US ussales@maxfocus.com
AUS apsales@maxfocus.com


plus.google.com/+Maxfocus/posts


linkedin.com/groups/MAXfocus-1986499


@maxfocus

MAXfocus™ From LogicNow