single point of contact

WHITE PAPER

Bullet Proofing Office 365 with SolarWinds Mail Assure

solarwinds msp

EXECUTIVE SUMMARY

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.

SolarWinds® Mail Assure™ provides an additional line of defense for all email services, including cloud-based email system from Office 365®. SolarWinds Mail Assure provides Office 365 users with:

- CONFIDENTIALITY
  A range of security features protect corporate data from all email-based attacks (spam, virus, ranswomare, phishing, malware etc.).
- INTEGRITY
  SolarWinds Mail Assure archive stores an encrypted copy of inbound and outbound emails for backup and later access using 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-premises ones do. SolarWinds Mail Assure provides customers with the ability to ensure their end users can continue to access, view and respond to email, when the primary email infrastructure—whether on-premises or in the cloud—is offline.

Cloud computing doesn't guarantee complete continuity.

EMAIL'S SECURITY PROBLEM

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.

When first invented in 1971, networked email didn't face the same challenges that it does today.

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 1.21[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.

» CYBERTERRORISTS
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.
- SPEAR PHISHING
  Spear phishing 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.

Even when their computers are protected by antivirus systems, employees can still be susceptible to manipulation.

UNDERSTANDING THE CIA TRIANGLE

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, integrity, and availability are all seen as crucial to a solid information security strategy.

» 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.

OFFICE 365: MOVING PRODUCTIVITY INTO THE CLOUD

Historically, general office productivity software packages, including word processing, spreadsheets, and email, were implemented on-site 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.

Typically, cybersecurity experts advocate a technique called "defense in depth," which uses multiple layers of protection.

SOLARWINDS MAIL ASSURE: BULLET PROOFING YOUR EMAIL

SolarWinds Mail Assure includes 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.

SolarWinds Mail Assure brings customers the full benefits of cloud operation.

BENEFITS OF CLOUD-BASED EMAIL SECURITY

SolarWinds Mail Assure 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 SolarWinds MSP's servers, which provide a first line of defense. Customers do not have to invest in or maintain any hardware, and SolarWinds Mail Assure 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-PREMISES 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-premises 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 across

U.S. and E.U, SolarWinds Mail Assure uses the cloud to provide substantially greater reliability and scalability, which in turn reduces risk for a critical part of the company's infrastructure.

In modern email protection, one antivirus engine is not enough to secure a system.

MAIL ASSURE AND THE CIA TRIANGLE

MSP Mail Assure is specifically designed to enhance the CIA triangle for all email users, whether they are running on-premises 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. SolarWinds Mail Assure 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. SolarWinds Mail Assure filtering system updates in real-time with input from over two million domains. This provides up- to-the-minute spam and malware detection and protection with nearly 100% filtering accuracy and close to zero false positives.

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.

Traditionally, very few companies have relied solely on the anti-spam engine included within Exchange.

SolarWinds Mail Assure'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 ACCURACY
Administrators can fine-tune the accuracy of the spam filter on an organization-wide, domain-wide, or per-user basis.

» EMAIL SCOUT REPORTS
Customers generally choose to have detected spam messages quarantined in the cloud, while users can receive 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.

SolarWinds Mail Assure has multiple data centers in the U.S. and Europe. The software on these servers is fully controlled by Mail Assure, and (as long as the sending server/recipient server supports it), all traffic to and from the Mail Assure servers is properly encrypted to help ensure nobody external can read the emails in transit. Mail Assure does not retain a copy of your legitimate emails on any server (unless the destination server is unreachable or archiving is enabled).

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 days[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].

Companies depend on email for their communications and can't afford to be without it.

ALWAYS-ON EMAIL CONTINUITY

Companies depend on email for their communications and can't afford to be without it. With a geographically distributed data-center architecture independent of other cloud providers' systems, SolarWinds Mail Assure 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, view 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, tamper-proof 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?

Not only is email a tremendous repository of intellectual property—email also includes information that may one day be needed by lawyers or auditors.

SolarWinds Mail Assure provides a secure, cloud-based archive that is completely separate from the Microsoft infrastructure. SolarWinds Mail Assure uses the same strict data jurisdiction policies, strong encryption, tamper-proof storage, and checksum technology to validate message integrity. Messages are fully indexed and searchable. Customers can import existing historical messages into the the product's Archive.

BUILDING A BROADER DEFENSE STRATEGY

SolarWinds Mail Assure is part of a broader defense strategy, thanks to their inclusion in the SolarWinds MSP platform, which includes other security components, such as web protection from http- or https-based threats delivered by malware-infected websites.

SolarWinds® RMM 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. RMM scans servers, workstations, and other devices within a customer's network for malware, so threats can be promptly remediated.

Scanning client side devices 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.

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 data-center 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.

By employing a third party system to complement your email provider's security, you make things more difficult even for determined attackers.

About Single Point of Contact; Single Point of Contact is a managed security service provider dedicated to helping businesses implement the right IT security solution. Our goal is to help customers reduce risk, respond to threats faster, achieve compliance and ensure data is secure with our security monitoring tools. For more information on our services and how we can help avoid costly mistakes, contact us today.

single point of contact