WHITE PAPER

CDW PEOPLE WHO GET IT

EMAIL SECURITY: DEFENDING THE ENTERPRISE

Learn more about email protection and examine some of the tools that can make protecting this critical asset easier.

Executive Summary

Email is the most common communication vehicle used by organizations of all shapes and sizes. Among the more than 100 billion email messages sent every day are sensitive information, critical requests and other essential business data. IT staff bear the burden of ensuring the confidentiality, integrity and availability of the information contained within the communication.

This white paper explores the email security landscape, including an assessment of the threats organizations face and the building blocks of an effective email security strategy. It also provides an in-depth look at email security solutions offered by McAfee, Symantec and Trend Micro and examines the key decision factors for selecting a product. Finally, it provides an overview of the importance of email policies for employees.

SHARE THIS WHITE PAPER

Table of Contents

The Situation

It's hard to find an organization that doesn't depend on email to conduct day-to-day business activities. While many firms and individuals have tried to reduce their reliance on email, these efforts have largely fallen by the wayside.

In fact, a recent McKinsey study found that knowledge workers spend 28 percent of their time reading and answering email from colleagues, business partners and customers, exchanging sensitive information that could pose significant risk to the organization if disclosed to unauthorized recipients.

Diverse threats pose a challenge to the security of email communication. Malware – including viruses, worms, Trojans and spyware – threatens to intercept the contents of email messages and pass them along to third parties. Denial-of-service (DoS) attacks jeopardize the ability of email systems to function properly and carry critical business communication.

Spam messages can sap productivity when they require employees to sort through cluttered inboxes. Employees may also inadvertently email sensitive information to an outside party or misuse email for inappropriate communication.

Users tend to leave sensitive information in their inbox such as documents or passwords. If an account is compromised, the attacker gains access to the inbox. Doing a simple keyword search for "password" can aid attackers in advancing their foothold within an organization.

Email infrastructure patching and configuration checks left undone can result in a misconfigured mail system exposed to the Internet. This could be used to enumerate usernames of individuals in the organization. Once this information is known, the attacker could proceed with a phishing attack or attempt to guess the account password.

The threat landscape is changing as well. Gone are the days when the greatest threats to information security were posed by teenage hackers using simple tools to hack into systems in the middle of the night. Modern adversaries are sophisticated and well-funded – governments, organized crime figures and terrorist organizations now use the tools of cyberwarfare to achieve their objectives. Organizations may be the target of international crime, economic espionage or other nefarious pursuits that jeopardize the security of email messages.

IT shops are charged with protecting the security of email communication, providing confidentiality, integrity and availability to this critical messaging tool. However, complete lockdowns are not the answer.

Email must flow freely around the enterprise to allow communication in a manner that, while secure, does not inhibit the ability to conduct business. Effective email security requires a combination of effective technology, policies and processes.

Email Risks

The risks facing email communication are widespread, ranging from individual hackers seeking sensitive information to nations engaged in economic espionage. The tools available to those seeking to undermine email security range from the mundane use of spam and phishing messages to sophisticated DoS attacks designed to cripple an organization's email infrastructure, preventing legitimate use.

Spam messages: These are as old as email itself and include unsolicited messages with a variety of intentions. Many seek to sell products or services to consumers, often providing the opportunity to purchase black market items, such as prescription drugs or counterfeit goods. These messages are more than a nuisance, as organizations must size their email infrastructure to handle the increased messaging volume that spam creates.

Phishing attacks: These represent a variation of spam with more dangerous intentions. These unsolicited messages don't seek to sell products but instead attempt to fool unsuspecting users into disclosing sensitive information. Malware can be sent in phishing attacks attempting to trick the user to open a file. These files can look like legitimate documents – for example, PDF or Word documents – but there is a zero-day exploit waiting to be triggered when users open the file. Once the exploit is triggered, the malware is installed and compromises the user's computer.

Malicious Code: Email may also be used as a vector for the delivery of malicious code. Hackers seeking to infect a system with a virus, Trojan horse, spyware or other type of malware may simply attach the installer to an email message, hoping that recipients will open the attachment on a system lacking appropriate anti-virus software. Similarly, links provided in messages may direct users to a site hosting malware installers that jeopardize the security of infected systems. Once compromised, these hijacked systems may be used to send spam. They can also be used as entry points for attacks on an organization's internal network.

DoS Attacks: Attackers may be able achieve their objectives without actually gaining access to the contents of email communication or the systems that send and receive messages. This type of attack, known as a denial-of-service attack, may involve exploiting a vulnerability in the organization's email infrastructure, causing it to crash. Brute force DoS attacks may simply flood an organization's email server with fake messages that consume all available server resources, causing network congestion that prevents legitimate messages from getting through.

Insider Threat: When evaluating the risks to email communication, organizations should not overlook the insider threat. Employees with authorized access to the email system

may, intentionally or accidentally, cause damage to the organization through misuse. One common way this occurs is the accidental leakage of information outside of authorized channels.

Inappropriate Content: Employees may also misuse email in a manner that violates the law or company policies by sending or receiving inappropriate content. An email message containing a risqué cartoon may be amusing to some but offensive to others, creating a human resources issue and potentially exposing the organization to liability for sexual harassment. Other potentially problematic email content includes pornography and hate mail.

In some industries, organizations are bound by regulatory requirements that prohibit certain uses of email. For example, healthcare providers covered by the Health Insurance Portability and Accountability Act (HIPAA) must ensure that they do not send sensitive health information via unencrypted email.

The Email Security Strategy

Entities seeking to secure their email environments should establish a comprehensive strategy designed to protect both the email infrastructure and its users from the wide variety of mail-related threats. The challenge facing technologists is that they must create a flexible solution that meets the organization's security and operational needs in an effective and efficient manner while respecting financial constraints. Well-designed security strategies use a toolset that embraces five important characteristics:

1. Technology enablement: While managing user behavior is important, the enterprise must also have a robust set of technical security tools that allow the consistent enforcement of security policy. These tools should support enterprise-grade logging, analysis and reporting functionality that provides security staff with a comprehensive view of the organization's threat landscape.

2. Web management: Application administrators in IT organizations are stretched thin and often manage a wide variety of applications. Any tools adopted by the organization should use web-based management platforms that allow administrators to quickly and easily check on system status, troubleshoot problems and adjust configuration settings.

3. Integration: Email security solutions operate among many components of an enterprise security strategy. Effective tools should integrate with security information and event management (SIEM) systems to provide organizations with a unified view of their security status.

4. Automatic updates: Tools in the email security suite should offer automatic updating capabilities, allowing administrators to configure the system to remain current on patches and signature updates without manual intervention. This reduces the time that IT managers are required to spend on the system, allowing them to focus on value-added activities.

5. Ease of use: An enterprise's email security technologies should fit seamlessly into the IT architecture, allowing quick, efficient deployment and facilitating smooth ongoing management and monitoring. Organizations using virtualization technology may also need solutions that offer a virtual appliance deployment option to avoid introducing new hardware into the environment.

Enterprises implementing an email security strategy should identify products with these characteristics that also meet their specific email security requirements. Email security products handle four main requirements, and enterprises should determine which products meet their security objectives before shopping around for a technology solution. These four requirements include:

1. Anti-malware: A primary function of email security suites is to ensure that users do not send or receive viruses, worms, Trojan horses or other forms of malware using the email system. The solution should perform signature-based

Security for Mobile Email

Mobile computing is here to stay. Users demand anywhere, anytime access to their email. They also want to be able to access their email accounts on the device of their choosing — whether it's a notebook PC issued by an organization's IT staff or a personally owned smartphone or tablet. The era of bring-your-own-device (BYOD) computing has arrived, and IT departments are being called upon to provide this access in a secure manner.

Many organizations turn to mobile device management (MDM) solutions to maintain secure configurations on mobile devices. These products allow IT staff members to apply security policies to smartphones and tablets, ensuring that they remain configured in a manner consistent with company policy and standards. MDM also allows IT groups to limit the applications that may be installed on a device and remotely lock a device or wipe its contents should it fall into the wrong hands.

In a BYOD environment, users may balk at the idea of having the company install a complete MDM solution on a device that they personally own. Mobile email management (MEM) products may offer a palatable alternative. MEM applications allow users to securely access an organization's email system in a manner that segments the data from other applications installed on the device. This approach, known as containerization, allows the organization to establish a secure beachhead for corporate email on a device without affecting other purposes for which the user may have the device.

scanning of all messages and attachments, identifying potentially malicious code. Upon detecting malware, the system should either remove the offending code before delivery or quarantine the message for further analysis and action. In addition to scanning attachments, the system should verify that any URLs contained in the message do not appear on a list of known malicious websites.

2. Content Filtering: Email security products should also protect the enterprise from spam and phishing messages by performing content filtering that quarantines unwanted messages prior to delivery. These solutions should provide the ability to configure the tolerance threshold so that users and administrators may balance their desire to block unwanted content with the need to allow important business communications.

3. Encryption: Email encryption provides the ability to protect the confidentiality of messages transmitted over the network by obscuring the contents from prying eyes. Email security products should offer encryption technology that facilitates the use of native encryption for users of the firm's internal email system as well as an encryption gateway that allows secure messaging with customers, partners and other external entities that use other email systems.

4. Data Loss Prevention: Authorized users sometimes attempt to send sensitive materials to unauthorized recipients, either intentionally or accidentally. Data loss prevention (DLP) technology scans email messages prior to delivery to ensure that they do not violate confidentiality rules. They may be triggered based on pattern-matching that detects, for example, the presence of unencrypted Social Security or credit card numbers, or may integrate with document management systems that use tagging to identify sensitive documents.

A wide variety of products can meet these needs, and each approaches the four main requirements in slightly different ways. Organizations should assess the capabilities of each product in relation to their technology infrastructure and security objectives.

Individual Solutions

Many vendors compete in the email security marketplace, offering a variety of technology solutions that allow IT shops to meet their security objectives. Three of the largest providers in this space are McAfee, Symantec and Trend Micro. These firms offer products that meet the anti-malware, content filtering, encryption and data loss prevention objectives of email security programs as part of a larger suite of integrated security products.

Security for Email Storage

It's very easy to get caught up in the important task of preserving the confidentiality of email messages and forget about two other significant goals: protecting the integrity of messages and ensuring the availability of the email service. IT managers should pay particular attention to the physical and logical storage technologies used in their email environments to ensure that they are designed to preserve integrity and availability.

The storage technology that supports an email system should be designed with fault tolerance and disaster recovery in mind. IT managers should choose storage solutions that can tolerate the failure of a disk and implement an appropriate backup strategy to ensure that data can be recovered in the event of a catastrophic hardware failure. Email data loss can have serious business consequences; thus, systems should be engineered to minimize that likelihood.

When assessing existing email storage, IT managers should consider whether individual employees are storing email on their devices. Many organizations are surprised to find that some users have email clients configured to use the Post Office Protocol (POP) to download email messages, store them locally and delete them from the server. This approach prevents centralized backup and increases the risk of data loss.

Finally, organizations should determine whether they have appropriate email retention policies by working with legal counsel to evaluate both regulatory requirements and business objectives. If a retention policy dictates that email be discarded after a certain period of time, the system should be configured to enforce this policy across all tiers of storage, including backups and local mail stores.

This section provides an overview of the offerings from these three vendors and how they can help mitigate the risks associated with email communication.

McAfee

McAfee, one of the oldest names in information security and anti-malware protection, offers the McAfee Email Protection product, which combines anti-malware, content filtering, encryption and data loss prevention technologies in a single product. Organizations benefit from having a single management interface for all of their email security functionality.

McAfee Email Protection leverages the same anti-malware engine that powers McAfee's full range of anti-malware products, providing assurance that users are receiving the

most current malware signatures generated by McAfee's security research team. Organizations seeking an even higher degree of assurance may choose to supplement the McAfee signatures with optional third-party virus definitions from another vendor.

One distinguishing feature of McAfee Email Protection is the product's ClickProtect feature. This content-filtering technology protects against a common phishing tactic in which hackers send out an email message that contains a benign link. As the link goes to an innocuous site, it clears the gateway email scans performed by the recipient's organization. Then, after the messages have been delivered, the attacker replaces the innocuous site with a malicious one at the same URL. Users who click the link in the email that has been delivered to their inboxes are then infected.

McAfee ClickProtect solves this problem by replacing the links in received email with URLs that redirect through McAfee's cloud-filtering service. This allows link checking incorporating the most recent threat information at the "time of click." Administrators may configure the ClickProtect functionality to apply the degree of security control appropriate for the organization's specific needs.

McAfee's email encryption features both push and pull mechanisms. In the push approach, the entire message is encrypted and forwarded to the recipient, who uses a previously generated key to decrypt it. In the pull approach, McAfee stores the entire message in the cloud, and the recipient is prompted to log in to the McAfee website to read the message over a secure, encrypted HTTPS connection.

The DLP features of McAfee Email Protection leverage the hundreds of data dictionaries available for use with McAfee's full DLP suite. Predefined keyword collections allow organizations to filter outbound messages that may include information regulated by HIPAA, the Payment Card Industry Data Security Standard (PCI DSS) or other confidentiality rules.

All of these features of McAfee Email Protection may be managed through the consolidated ePolicy Orchestrator (ePO) management console. ePO not only controls email security products, but also allows administrators to configure and monitor other McAfee security products in one management system.

McAfee's licensing scheme allows users to leverage physical appliances and virtual appliances for VMware as well as McAfee's software as a service (SaaS) cloud offering. The hybrid license model lets organizations freely switch users between the technologies as business needs change.

Symantec

Symantec provides a selection of products dedicated to securing the email communication of its customers. These include the Symantec Messaging Gateway, Symantec Mail Security for Microsoft Exchange and for Lotus Domino, and Email Security.cloud. These products are all managed through administrator-friendly web interfaces.

All products from Symantec are backed by the firm's team of more than 550 security researchers stationed around the globe. These researchers leverage the Symantec Global Intelligence Network, a collection of data from hundreds of millions of users and sensors that share information with Symantec on an opt-in basis, providing real-time threat intelligence that allows researchers to update Symantec products rapidly.

The Symantec Messaging Gateway combines anti-malware, content filtering, encryption and DLP technology in a single product. From a content filtering perspective, the product features "link following" technology that assesses the true destination of a shortened link and filters out links that lead to malware before the email reaches the recipient. Symantec also includes "disarm" technology that scrubs the content of all Microsoft Office and Adobe Acrobat attachments. The user receives a copy of the attachment that contains all of the document content, but removes potentially dangerous components, such as JavaScript, macros and embedded Flash content. The Messaging Gateway is available as either a hardware appliance or a virtual appliance for VMware and Microsoft Hyper-V.

Symantec offers Messaging Gateway customers two encryption options that allow rule-based encryption and message-routing features. The product integrates with a number of on-premises email encryption gateways, such as Symantec Gateway Email Encryption and third-party solutions. Users seeking a cloud-based encryption option may choose to integrate the gateway with Symantec's Policy-Based Encryption SaaS tool.

Users seeking a software solution may opt for Symantec Mail Security for Microsoft Exchange and for Lotus Domino. These products include anti-malware, content filtering and DLP as a software product installed on an existing email infrastructure.

Symantec also offers the Email Security.cloud SaaS product line that provides hosted anti-malware, content filtering, encryption and DLP for users who do not want to host their own in-house solution. In addition, customers who also use Web Security.cloud or Instant Messaging Security.cloud will also have access to a unified management portal.

All of Symantec's email security products include a basic level of DLP technology that is capable of performing keyword and pattern matching on outbound messages. Users seeking more advanced DLP technologies may take advantage of the Symantec Messaging Gateway's native integration with Symantec DLP, which includes advanced detection technology as well as a full incident management workflow.

Trend Micro

Trend Micro offers a portfolio of email security products that integrate with the broader security offerings it provides. In an environment where organizations are rapidly shifting from in-house to cloud solutions, Trend Micro's selection of email security products is able to adapt.

InterScan Messaging Security provides a gateway solution for organizations seeking to scan inbound email for threats. It combines anti-malware, content filtering and DLP capabilities in a single product that may be deployed as either a virtual appliance (on VMware or Microsoft Hyper-V) or as a software appliance on a bare metal server. InterScan licenses include the use of a software as a service prefiltering function to reduce the demand for in-house computing at no additional charge.

Trend Micro's ScanMail Suite, which is available for Microsoft Exchange or IBM Domino, provides similar capabilities as a software solution installed within an email server infrastructure. One major difference between ScanMail and a gateway solution is ScanMail's capability to view and act upon internal messaging traffic that does not cross the border and, therefore, would go unseen by a gateway product.

The anti-malware capabilities of both ScanMail and InterScan leverage the threat intelligence gathered by Trend Micro's worldwide Smart Protection Network, which is analyzed by a global team of security researchers. The network gathers 15 terabytes of threat information each day, identifying 180,000 unique threats and responding to more than 16 billion customer threat queries.

The most dangerous threats facing organizations are previously unknown, or zero-day, threats for which no malware signatures are available. Trend Micro's optional Deep Discovery Advisor package specifically targets these threats, allowing administrators to automatically quarantine suspicious documents, execute them within a sandbox environment and detect signs of malicious activity before releasing them to the user.

Both InterScan and ScanMail feature integrated DLP capabilities that support scanning via pattern matching, compliance dictionaries and the use of thresholding to prevent false positives. Trend Micro does not offer a stand-alone DLP product, and the capabilities it offers are part of the main product license.

Trend Micro's optional Email Encryption Gateway is available as a separate product that automatically applies encryption to outbound email messages based on administrator-defined policy settings. This virtual appliance performs all necessary key management activities and integrates with the messaging security gateway.

Trend Micro also offers Hosted Email Security, a SaaS messaging security product that provides anti-spam and anti-malware capabilities for enterprises using Microsoft Exchange, Microsoft Office 365 or other hosted email solutions. Hosted Email Security does not offer DLP, encryption or sandboxing capabilities.

All of Trend Micro's on-premises products can be managed through the centralized Trend Micro Control Manager. This management package allows user management, policy definition and configuration of all Trend Micro security products from a central location.

Main Features of Key Email Security Products

Vendor	Key Features
McAfee	• Hybrid licensing model for physical or virtual appliances and cloud • ClickProtect technology, which works at time-of-click • Push and pull encryption methods
Symantec	• Backed by Global Intelligence Network with millions of data sources • "Disarm" feature to create clean copies of Office and Adobe attachments • Link Following, which identifies the true destination of shortened URLs
Trend Micro	• Sandboxing technology, which allows detection of zero-day threats • Integrated DLP technology • Range of flexible deployment options

Hosted Email Security Solutions

As organizations seek to simplify their IT infrastructures and reduce the burden placed on their internal staff, many are starting to turn to SaaS approaches that transfer this burden to others. SaaS providers manage all of the hardware and platform issues associated with a particular service and make it available as a cloud-based application offering. Email security products are no exception, with almost every vendor now offering some type of hosted email security solution.

Hosted email security solutions offer several major benefits to organizations adopting them. First, they reduce the complexity of an organization's IT environment. The entire burden of keeping the application up and running rests on the service provider.

Security administrators within a customer organization simply configure an already-functioning service to meet the specific security objectives of their operation. The configuration set by administrators allows each organization to implement its own acceptable-use policies, reduce data loss and maintain compliance with industry and regional regulations.

Hosted products allow for rapid implementation, requiring minimal configuration to get up and running. Vendors often provide integration support services that assist with migration. Once the initial installation is complete, most upgrades are transparent to both users and the customer organization's IT staff.

The SaaS vendor rolls out incremental updates as needed and can rapidly deliver new functionality to meet customer needs. This reduces the risk of security breaches while increasing the productivity of the organization's internal staff.

From a financial perspective, hosted solutions often reduce the total cost of ownership (TCO) and, depending on the licensing model, may allow budgeting for the service to shift from a capital investment to an operational expense. Organizations that adopt cloud-based solutions find that their budgeting process benefits from the predictable recurring costs of the SaaS model.

Purchasing a hosted email security solution also often provides organizations with access to a dedicated team of outsourced email and security specialists. By contracting with a vendor partner specializing in email security, the IT shop gains access to a team of experts that would be too expensive to assemble in-house. The vendor often provides access to the latest email security research developed by its team at no additional charge, and technical specialists are available for issue escalation in the event of a security incident.

Finally, hosted products are built on very large-scale computing infrastructures and are able to easily absorb surges in demand. This type of scalability is quite difficult to create in an in-house solution and is bolstered by the reliability that many vendors achieve by simultaneously hosting security services in multiple, geographically diverse data centers.

The Importance of Employee Email Policies

Documenting an employee email policy provides the enterprise with an effective mechanism for informing employees of expectations for their use of email, the controls that IT managers are putting in place to protect sensitive communications and the types of monitoring that the organization uses.

Every email security policy should include a section that answers key questions that employees may have regarding the acceptable use of their email accounts. It should address questions regarding the types of information that may be sent via email, personal use of company email accounts and the applicability of sexual harassment and other personnel policies in the email environment. Staff members should be reminded that inappropriate use of email is a violation of organization policy that may result in disciplinary action.

If the organization engages in any type of email monitoring, the policy should make it clear that this takes place and state that employees should not have an expectation of privacy while using the company email system. Remind them that company email is a business tool and that information sent and stored in the email system remains the property of the company and is subject to monitoring and inspection.

Security Questions for SaaS Providers

When considering any software as a service (SaaS) offering, organizations should conduct a rigorous security review to ensure that the service provider's controls are sufficient to protect the organization's sensitive information. Some questions that should be asked during this review include:

- What controls are in place to protect information in transit?
- Is any customer information stored by the service? If so, what information is stored and how is it protected?
- How are the provider's security controls tested? Do they perform routine network and web application scanning? Do they use penetration testing? Are the results of these tests made available to customers?
- Is data from multiple customers segmented or is it commingled? If commingled, what controls are in place?
- Are security controls audited on a regular basis? What standard is used for that auditing? Do customers have the right to review audit reports?

CDW: A Security Partner That Gets IT

Let CDW serve as your email security partner. Our team offers threat prevention strategies built using multilayer protection models designed to prevent malicious email attacks.

CDW's account managers and solution architects stand ready to assist your organization in every phase of a project as IT managers select and implement a suite of security tools that protect email both at rest and in transit.

We take a comprehensive approach to identifying and meeting the needs of every customer. Each engagement offers five phases to help achieve your security objectives. These phases include:

- An initial discovery session to understand your goals, requirements and budget
- An assessment review of your existing environment and definition of project requirements
- Detailed manufacturer evaluations, recommendations, future-environment design and proof of concept
- Procurement, configuration and deployment of the final solution
- Telephone support and product lifecycle support

In addition, CDW staff is available to perform both rapid and comprehensive security assessments custom tailored to reflect individual business needs. The comprehensive/rapid assessment can be either an internal or Internet assessment. Other assessments include:

- Internal network security
- Internet security
- Partner/extranet security
- PCI/HIPAA gap analysis assessment
- Data loss prevention assessment
- Incident response
- Social engineering
- Dial-access security
- Wireless network security

To learn more about CDW's security solutions, contact your CDW account manager, call 800.800.4239 or visit CDW.com/threat

TREND MICRO

Trend Micro Deep Security provides a server security platform that simplifies security operations while accelerating the ROI of virtualization and cloud projects. Tightly integrated modules expand the platform to ensure server, application and data security across physical, virtual and cloud servers and virtual desktops.

CDW.com/trendmicro

KASPERSKY lab

Kaspersky Endpoint Security for Business – ADVANCED boosts IT security and efficiency across your organization. It allows for safe web browsing from all devices. This security software helps you manage BYOD programs, one-to-one initiatives and more — all with one solution.

CDW.com/kaspersky

Symantec

Symantec Enterprise Solution provides multiple layers of protection to deliver strong data protection for mobile, endpoints and mail/web infrastructure. Symantec Enterprise Solution includes products protecting against malware, data loss and spam threats with endpoint security, drive encryption and system recovery.

CDW.com/symantec

SHARE THIS WHITE PAPER

CDW PEOPLE WHO GET IT