

SECURITY IN A HOSTED MICROSOFT® EXCHANGE ENVIRONMENT

INTRODUCTION

Hosted Microsoft® Exchange has become an increasingly popular way for organizations of all sizes to provide maximum email capability at minimum cost. “Always on” email access is certainly one of the advantages of a hosted Exchange solution. But it is not the only benefit. Due to the mission-critical role of email in organizations, the security advantages of hosted Exchange services compared with traditional on-premise email systems are increasingly seen as a compelling factor in their favor.

This white paper explores the role of security in a hosted Exchange environment. It examines the importance of email security. It highlights the security advantages of hosted solutions. Then It identifies the security-specific capabilities to consider in your evaluation and selection of a hosted Exchange provider. The paper concludes with an overview of the security features available from Integra Telecom and how they compare with other alternatives.

WHY SECURITY MATTERS

Email plays a critical role in today’s information-driven organizations. A breach in email security could produce significant commercial and legal ramifications. Consider an example in which your email system becomes infected with a highly destructive, virulent virus. Not only is your email system compromised. But, as with biological viruses, once the intruder begins circulating in other systems, the potential for mayhem is multiplied exponentially. As a result, a lethal email sent from your organization could infiltrate and infect the systems of multiple customers and partners. The virus could knock out your system and bring down a few others before the intruder is eliminated, the damage is contained, and systems are restored.

The commercial implications of such a security breach can be catastrophic: loss of business-critical systems and data, diversion of time and resources to restore operations, lost revenue and missed business opportunities. As if those effects weren’t damaging enough, consider the potential legal implications. In most cases, an organization can be held liable for losses suffered by a third party as a result of the infected email sent, albeit unintentionally, by you. If that third party happens to be a competitor, it might be more likely to exercise its legal right to sue for damages.

SECURITY ADVANTAGES OF HOSTED VS. ON-PREMISE EXCHANGE

Every IT organization shudders at the possibility of a breach in email security. But when one's entire business is built on providing secure, mission-critical communications capabilities, as it is with hosted Exchange providers, the stakes are even higher. For hosted Exchange providers, their entire business is predicated on their ability to offer a more secure email environment than their customers could deploy themselves on-premise. For this reason, providing ironclad security has become a key competitive differentiator for hosted Exchange providers. These organizations invest a great deal more in security measures than do most IT organizations.

At the core of every hosted Exchange provider's business are physical facilities that house the myriad of servers and network infrastructure required to serve their clients. These facilities

employ comprehensive physical security controls such as video surveillance, multi-factor employee authentication and other monitoring tools. It would be extremely cost prohibitive to replicate this level of physical security in data centers owned and operated by the typical organization. This is particularly true of small to midsize businesses that manage their email infrastructure on-premise.

In addition to the gamut of physical controls available, there are well-established, internationally recognized standards, such as the Statement on Auditing Standards (SAS) 70 and the Payment Card Industry (PCI) Data Security Standard, against which hosted Exchange providers can be audited. These audits provide an extra level of assurance beyond what is typically available in an on-premise email environment

SECURITY CAPABILITIES TO LOOK FOR IN A HOSTED EXCHANGE PROVIDER

When it comes to the selection of a hosted Exchange provider, there are plenty of options. In order to choose a provider that will best meet your organization's needs, a thorough review of their capabilities is essential. This is particularly the case when analyzing a provider's security capabilities. What follows is a list of the key areas each provider should be able to address with respect to their offerings.

FIREWALL, VPN, TRAFFIC MANAGEMENT AND INTRUSION DETECTION

A hosting provider's data center is designed to serve the email needs of multiple clients simultaneously. This multi-tenant environment requires vigilant security to protect unauthorized access to their clients' servers. Understand how your provider leverages firewall, virtual private networks (VPNs) and traffic management tools to safeguard against malicious attacks or unwarranted access. Intrusion detection systems (IDS) should also be in place as an added level of security beyond conventional firewalls.

PHYSICAL SECURITY

Physical security encompasses surveillance cameras, building perimeter security and employee access controls at each data center and company facility. The provider should have a clearly documented policy that governs how it treats your confidential account information, such as passwords and other credentials. The provider's dependence on Internet Service Providers (ISPs) is also important. Ask your provider how a denial-of-service attack, for example, launched on their ISP, would affect their service.

EMPLOYEE SECURITY

Physical security shouldn't stop at the four walls of the provider's data center. It also pertains to the provider's employees themselves. For example, the provider should use thorough background checks on employees as part of the hiring process. Beyond the initial background checks, it is also important to understand the primary focus and experience level of security staff. Security should be maintained by dedicated and specially trained personnel rather than by the provider's general IT operations staff. Also, ask what role outsourced employees play in the provider's organization. While contracted employees certainly can provide excellent service, verify that they are held to the highest standards as well.

SAS 70 CERTIFICATION

Any hosted Exchange provider worthy of your consideration must demonstrate that it deploys adequate controls and safeguards when hosting or processing your organization's data. A widely recognized mark of service quality is the Statement on Auditing Standards (SAS) No. 70, Service Organizations. An audit based on this standard can demonstrate that a service organization has undergone an in-depth investigation of its control activities, including information technology processes. Developed by the American Institute of Certified Public Accountants (AICPA), SAS 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. In addition, the requirements of Section 404 of the Sarbanes-Oxley Act of 2002 make SAS 70 audit reports even more important to the process of reporting on the effectiveness of internal control over financial reporting.

Service auditors are required to follow the AICPA's standards for fieldwork, quality control and reporting. Identifying and evaluating relevant controls is generally an important step in the user auditor's overall approach. If a service organization provides transaction processing, data hosting, IT infrastructure or other data processing services to the user organization, the user auditor may need to gain an understanding of the controls at the service organization in order to properly plan the audit and evaluate control risk. The service auditor's report, which includes the service auditor's opinion, is issued to the service organization at the conclusion of a SAS 70 examination.

PCI COMPLIANCE

Compliance with Payment Card Industry Data Security Standards (PCI DSS) ensures that your payment information will never be accessed by unauthorized parties or shared with unscrupulous vendors. This is particularly relevant if you are processing credit card payments through your hosted environment. A hosted Exchange provider that complies with PCI DSS offers greater assurance that cardholder information will remain confidential.

EMAIL SECURITY

A true test of a hosted Exchange provider is how well it addresses email security and continuity. Email continuity is a standby email system that activates in the event of a mail server outage.

ANTI-VIRUS: The hosted Exchange provider must supply effective anti-virus protection. Check that the provider proactively scans for, detects and eradicates viruses before they affect your email service. Is there any additional cost to you for this protection? Also, check how frequently they update virus definitions. In most cases, providers' responsibility for anti-virus protection extends only to their hosted Exchange servers.

ANTI-SPAM: Effective spam protection saves network bandwidth and improves email performance. So ask what anti-spam protection is available from the provider. To what degree of granularity can users control their own spam settings, whitelists and blacklists? For administrators, compare what each provider offers in terms of flexibility and span of control across all spam settings.

CONTENT FILTERING: A provider should offer you the ability to decide what content is acceptable for business use and to filter out content that does not meet these specifications. This enables your organization to comply with company, state and federal communications regulations.

ENCRYPTION: Encryption of email protects confidential information by making it unreadable by unintended recipients. Depending on the nature of your business, the level of encryption offered may be a primary concern. At a minimum, the provider should offer message-level encryption as well as encryption of attachments to ensure the security of your organization's email.

SECURITY IN ACTION: INTEGRA TELECOM

Now that you have a sense of the key security capabilities to look for in your evaluation of hosted Exchange providers, let's take a closer look at how Integra addresses these requirements.

FIREWALL, VPN, TRAFFIC MANAGEMENT AND INTRUSION DETECTION

Integra uses multiple, redundant, enterprise-class firewall systems to prevent unwarranted intrusions and ensure only authorized users access your Exchange environment. This is a custom-built security system that integrates firewall, VPN and traffic management. Integra also uses an intrusion detection system (IDS) to detect malicious network traffic and computer usage that often cannot be caught by a conventional firewall. The system monitors for unusual traffic patterns and alerts system administrators of any suspicious behavior. IDS also can help prevent network attacks against vulnerable services, data-driven attacks on applications, host-based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware (e.g., viruses, Trojan horses, and worms).

PHYSICAL SECURITY

Each of Integra's seven world-class data centers (6 U.S.-based; 1 U.K.-based) adheres to the strictest standards in physical security. All data centers are closely monitored and guarded around the clock with sophisticated pan/tilt closed-circuit cameras for deterring and detecting suspicious activity. Secure access is strictly enforced using the latest technology, including electronic man-trap devices between lobby and data center, motion sensors and controlled ID key-cards. Security guards monitor every site entrance. Each data center is also served by multiple Tier-1 Internet providers. This eliminates the potential impact of a denial-of-service (DoS) attack on any one of Integra's Internet providers.

DEDICATED SECURITY STAFF AND EMPLOYEE CONTROLS

Integra offers a dedicated, full-time security staff, led by a Certified Information Systems Security Professional (CISSP) analyst. Every employee, regardless of his or her role, undergoes a rigorous background check. Employee access to passwords, encryption keys and electronic credentials is also strictly controlled. Access to servers is restricted to a limited number of authorized engineers.

EMAIL SECURITY AND CONTINUITY

Integra offers a full suite of products that provides customers with secure and always available email:

ANTISPAM: All hosted Exchange accounts from Integra include SpamStopper™ or SpamStopper™ Pro, our advanced antis spam software, at no additional cost. Based on SpamAssassin email spam-filtering software and customized for our hosted Exchange environment, Integra SpamStopper runs in a separate server cluster, outside the Exchange servers, for maximum performance. SpamStopper provides:

- » **Content filtering:** Content filtering offers server-side protection against bad headers and suspect attachments. This also enables customers to comply with acceptable business-use policies, as well as with company, state and federal communications regulations.
- » **Company-wide whitelists and blacklists:** Customers can define in detail which senders should always or never be allowed, both at the mailbox level and across the account at the administrator level.
- » **Microsoft® Outlook® integration:** End users can control their personal whitelists and blacklists directly from their Outlook settings.
- » **Flexibility:** Administrators can manage all spam settings, and users get mailbox-level whitelist/blacklist control.
- » **User-defined sensitivity:** Customers can refine spam sensitivity levels according to their company's email usage.

ANTIVIRUS: Integra integrates VirusStopper comprehensive managed antivirus protection into all Exchange mailboxes, at no extra charge. This advanced software resides on Linux-based clustered servers, which receive all messages before they enter the Exchange environment. It then scans for and automatically deletes any messages that are detected to contain viruses. All viruses are deleted before reaching the Exchange environment. Integra's antivirus protocol catches 99.999 percent of all viruses that could potentially infiltrate and harm your mailboxes and Exchange environment. The virus databases are updated multiple times per day, and Integra continuously manages the antivirus software and virus definitions. In addition to the server-based antivirus software that Integra provides, clients are advised to install and maintain up-to-date, anti-virus software on all end-user computers.

DATA REPLICATION: Besides running regular backups, Integra replicates Exchange 2010 data in real time from one set of premium hardware to another. This protects the critical information your business keeps within Exchange, even in the event of hardware failure or database corruption. It also enables Integra to rapidly restore the full functionality of your Exchange environment should an issue occur.

ENCRYPTED EMAIL: Email between mailboxes on Integra's system is natively encrypted. Native encryption Clients can also use Integra's Encrypted Email solution to communicate externally with military-grade encryption of email and attachments. Integra's policy-based Encrypted Email easily encrypts emails based on company-wide rules and policies that clients set up and manage—all without disrupting day-to-day workflow. All email content and attachments are automatically scanned to detect whether the message warrants encryption before being sent. Policies can be configured to encrypt and send, return to sender or delete messages with insecure content. This option reduces human error and minimizes the risk of security breaches. If clients need end-to-end encryption, Integra also offers user-level Encrypted Email, which encrypts emails from the desktop client, and can be used to encrypt intra-company and confidential communications. Both Encrypted Email solutions are backed by a globally recognized Certificate Authority. Standards-based technologies are used, such as Public Key Infrastructure (PKI), S/MIME, and X.509 certificates, to establish confidentiality, message integrity and user authentication.

CONCLUSION

The latest software and fastest servers housed in the most state-of-the-art data centers mean little if your users cannot send and receive email securely. Hosted Exchange providers turn security concerns into a distinct advantage by investing in comprehensive physical security controls that comply with strict, internationally recognized and audited standards. Not all hosted Exchange providers are equal, however. Conducting a thorough review of capabilities using the criteria discussed in this white paper will help you choose a provider to best meet your organization's needs for security as well as performance and service.



About Integra Telecom

Integra Telecom, Inc., connects business by providing business-grade networking, communications and cloud solutions to thousands of business and carrier customers in 11 Western states, including Arizona, California, Colorado, Idaho, Minnesota, Montana, Nevada, North Dakota, Oregon, Utah and Washington. The company owns and operates a nationally acclaimed best-in-class fiber-optic network consisting of a 5,000-mile high-speed long-haul fiber network and a 3,000-mile metropolitan access network including more than 1,700 fiber-fed buildings.

Contact Us

Integra Telecom
1201 NE Lloyd Blvd., Suite 500
Portland, OR 97232
1-866-INTEGRA
www.integratelecom.com