A GUIDE TO

Security and privacy in a Hosted Exchange environment

What's inside this white paper:

- A two-page checklist for comparing the security of hosted Exchange providers
- Definitions for each element of hosted Exchange security
- Explanations of how Intermedia addresses each element of hosted Exchange security

INTERMEDIA
The Business Cloud™

For more information:

CALL US	EMAIL US	ON THE WEB
800.379.7729	**security@intermedia.net**	**intermedia.net**

Executive Summary

When it comes to deploying Microsoft Exchange, businesses are turning to the cloud in increasing numbers. That's because the cloud enables them to extend fully featured Exchange functionality without investing capital into extensive on-premise hardware and software deployments.

But not all clouds are created equal. As you consider hosted Exchange providers or even on-premise deployments, it's critical to look beyond functionality and pricing to elements such as onboarding, support, back-end architecture and—perhaps most importantly—security.

There are many elements of hosted Exchange security, and a good hosted Exchange provider will excel at all of them. A good provider will also constantly evaluate and update their security tools and processes. This is especially important if you plan to integrate mobile devices into your Exchange environment, because mobile technology changes at an extremely fast rate; you'll be relying on your provider to ensure the security of your environment keeps pace.

This white paper helps you make an informed decision about provider security. It's divided into three parts:

- **Part One: Exchange Security Checklist.** This easy-to-use checklist lets you contrast the security offerings of hosted Exchange providers (as well as on-premise deployments).
- **Part Two: Exchange Security Definitions.** This section defines and explains each of the hosted Exchange security elements that are included in the checklist.
- **Part Three: Our Company's Exchange Security.** This section describes how Intermedia addresses each of these elements in its business cloud.

Why does security matter?

A breach in email security can have both commercial and legal ramifications. Consider the example in which your email systems are infected with a highly destructive virus. In addition to infecting your own systems, a malware-infected email could infect a customer, a partner, or even a competitor. If the malware payload is delayed, you might spread the infection even before it compromises your own system.

The commercial implications alone could be significant. They could include loss of business-critical systems and data, extensive time and resources required to restore your operations, and lost revenue and missed business opportunities.

Worse, though, is that your organization could be liable for any loss suffered by a third party as a result of the infected email, even if it was spread unintentionally. If that third party happened to be a competitor, they would be even more likely to exercise their legal right to sue for damages.

Why Hosted Exchange is more secure than an on-premise deployment

A hosted Exchange provider's viability in the marketplace rests in part on its ability to offer a more secure environment than customers could typically achieve on their own. This means that few businesses stand to lose as much in a security breach.

As such, the hosted Exchange provider will invest a great deal more in security than their customers could typically afford in an on-premise deployment.

This is especially true for physical security. At the core of every hosted Exchange provider's business are physical facilities that house their servers and network infrastructure. These datacenter facilities employ comprehensive physical security controls such as video surveillance, multi-factor employee authentication and other monitoring tools. It would generally be cost prohibitive for a small or medium-sized business to replicate this level of physical security in their on-premise email infrastructure.

In addition to physical controls, the best hosted Exchange providers will spotlight their security capabilities by having them measured against a well-established auditing standard (such as SSAE 16 Type II, PCI, or especially SOC 2 Type II). These audits confirm that the provider's security and data protection meet standards that are far more stringent than what a business could typically achieve with their own on-premise environment.

Part I: checklist for comparing exchange providers (page 1 of 2)

This checklist makes it easy to compare the security offerings of potential hosted Exchange providers. (Each of these elements of security is defined in detail on the following pages.)

Security Element	On-Premise or Cloud Exchange Provider	Intermedia's Hosted Exchange
Multi-tenant platform security	□ ______ □ ______	✓ Redundant, enterprise-class firewalls ✓ Multiple Intrusion Prevention Systems (IPS) employed (host and network)
Physical Security	□ ______ □ ______ □ ______	✓ Closed-circuit TV ✓ Secure access policies ✓ Security guards
Employee security	□ ______ □ ______ □ ______	✓ Background checks ✓ Two-factor authentication and role-based access control ✓ Restricted server access
Redundant Internet service providers	□ ______	✓ Multiple Tier-1 Internet providers
Authentication and access	□ ______ □ ______	✓ Stringent caller identification procedures ✓ Admins have control over access
Dedicated security staff and monitoring	□ ______ □ ______	✓ Employs dedicated, full-time certified security staff ✓ Team monitors all aspects of security
Privacy	□ ______ ______ ______	✓ Registered with the US Dept. of Commerce's Safe Harbor program, meeting their privacy requirements
Audit reports	□ ______ □ ______ □ ______	✓ SOC 2 Type II audited ✓ Audit applies company-wide, not just at the datacenter level ✓ Audited against all five trust service principles
PCI Compliance	□ ______	✓ Payment processing system is PCI compliant

Part I: Checklist for comparing Exchange providers (page 2 of 2)

Continued from the previous page.

Security Element	On-Premise or Cloud Exchange Provider	Intermedia's Hosted Exchange
Anti-spam and anti-virus	□ ____________ □ ____________ □ ____________	✓ McAfee Basic/Advanced Email Protection included with every mailbox ✓ Shields you from spam & viruses ✓ Advanced Email Protection offers granular control over security settings
Email Data Loss Prevention	□ ____________ □ ____________ □ ____________	✓ Intermedia offers McAfee Email Data Loss Prevention ✓ Filters outgoing email for spam, viruses, credit card info, corporate info, etc ✓ Prevents users from sending sensitive content
Email Continuity	□ ____________ □ ____________	✓ Intermedia offers McAfee Email Continuity ✓ Provides redundant email access for total peace of mind
Protection for mobile devices	□ ____________ □ ____________ □ ____________ □ ____________	✓ Admin can set security and message management policies for mobile devices ✓ Remotely wipe mobile devices ✓ Deactivate devices remotely ✓ Set policies account-wide or per user
Data replication	□ ____________ □ ____________ □ ____________	✓ Runs regular backups ✓ Replicates data in real time ✓ Maintains two copies of data
Encryption	□ ____________ □ ____________ □ ____________ □ ____________	✓ Encrypted Email solution offered for greater protection ✓ Can be deployed at the account level or the user level ✓ Standards-based encryption (PKI, S/MIME, X.509) ✓ Transport layer encryption via SSL from client to server

Part II: Elements of security in a Hosted Exchange environment

To help you evaluate a potential provider's security capabilities, this section provides a list of key elements of hosted Exchange security. Any provider should be able to clearly articulate how they meet each of these standards.

Multi-tenant platform security

A hosting provider's datacenter is designed to service the email needs of multiple clients simultaneously. This multi-tenant environment requires vigilant security to protect against unauthorized access between accounts.

You should ask your provider how they leverage firewalls, virtual private networks (VPNs) and traffic management tools to help safeguard against malicious attacks (such as DDoS) or unwarranted access.

Intrusion protection systems (IPS) should also be in place as an added level of security beyond conventional firewalls.

Physical security

A hosted Exchange provider's datacenter should be physically protected. Physical security elements encompass surveillance cameras, perimeter security, employee access controls at each datacenter and company facility, and more.

Employee security

A provider's vigilance for security should extend to employees themselves. A few questions you should ask: how thorough are their employee background checks? What is the primary focus and experience level of the security staff? Is security maintained by dedicated and specially trained personnel, or by the provider's general IT operations staff? What role does outsourcing play in the service provider's organization and service offerings?

Redundant internet service providers

A hosted Exchange provider's dependence on Internet service providers is important. Ask your potential providers how a Distributed Denial of Service (DDoS) attack targeted against their infrastructure would impact their service, and ensure they have proper mitigation technologies in place to switch providers seamlessly if one should become unavailable.

Authentication and access

A provider should have clearly documented policies that govern how confidential information about your account (such as passwords and other credentials) are treated. For example: how do they verify the identity of callers who request phone support for your account?

Dedicated security staff and monitoring

Who is in charge of the provider's security? Is there dedicated security staff, or is the staff's attention split between multiple elements of the providers' business? In either case, which elements of security does the provider's staff monitor—and which ones, by implication, are left for you to monitor?

Privacy

The US Department of Commerce has established clear privacy guidelines under their Safe Harbor program. Ask a provider for details about how they meet the requirements of this program.

Audit reports

Any hosted Exchange provider worthy of your consideration must demonstrate adequate controls and safeguards for your organization's data. One widely recognized mark of service quality is the Service Organization Controls (SOC) 2 Type II audit report. This report attests that a service organization has undergone in-depth identification and testing of its control activities, including information technology and security processes.

Developed by the American Institute of Certified Public Accountants (AICPA), SOC 2 Type II provides 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. It differs significantly from a SOC 2 Type I audit report because in that report the controls are only stated—not tested. (In other words, Type II is much more stringent.)

SOC 2 Type II also contrasts markedly to the older SAS 70 as well as the newer SSAE16 reports. In those reports, the service organization defines the criteria for their audit. In the SOC 2 Report, the service organization uses pre-defined control criteria. These "trust service principles" include:

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy

SOC 2 Audit Report Contents	Type II Report	Type I Report
Independent service auditor's report (i.e. opinion)	✓	✓
Service organization's description of controls	✓	✓
Independent service auditor tests operating effectiveness and describes the results of those tests	✓	✗

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 SOC 2 Type II examination. It is typically available for you to examine, subject to a Non-Disclosure Agreement.

PCI compliance

Compliance with Payment Card Industry Data Security Standards (PCI DSS) helps ensure that our payment information will not be accessed by unauthorised parties or shared with unscrupulous vendors. This is particularly relevant if the hosted Exchange provider is processing credit card payments.

Email security and continuity

A true test of any hosted Exchange provider is the tools they use address email security. Ideally, they should demonstrate a comprehensive approach that protects against both viruses and spam as well as encrypts your email, if necessary. Your provider should offer you a number of services, including:

- **Anti-spam.** Effective spam protection saves network bandwidth and improves email performance. What anti-spam protection is available from your provider? To what degree of granularity can users control their own spam settings and white/black lists? For administrators, compare what each provider offers in terms of flexibility and the control they offer across all spam settings.
- **Anti-virus.** How effective is the provider's anti-virus protection? How do they proactively scan for, detect and eradicate viruses before they impact your email service? Is there any additional cost to you for this protection? How frequently are virus definitions updated?
- **Email Data Loss Prevention.** Email makes it all too easy for employees to send sensitive content. The consequences of errant emails—whether they're innocent or intentional—can harm a company's prestige, shatter customer confidence and even result in regulatory fines or financial losses. What tools does your provider offer to filter outgoing email to prevent users from sending spam, viruses, credit card numbers, social security numbers, and other sensitive corporate information?
- **Email Continuity.** Proper business continuity planning must include the creation of redundant paths to mission-critical services. Since email is widely considered to be the most critical element of business communications, it's vital that you establish a redundant path for sending and receiving messages. Does your provider offer this service?
- **Protection for mobile devices.** In some cases, a provider's anti-virus protection extends only to their hosted Exchange servers. When that's the case, what obligation does that create for you to protect end-user client devices in your organization?
- **Data replication.** How does a potential provider back up your data to guard against corruption or other threats to data integrity and business continuity?
- **Encryption.** Depending on the nature of your business, the level of encryption your provider offers may be a primary concern. At a minimum, the provider should offer message-level encryption as well as encryption of attachments to ensure your organization's email is secure.

Part III: How Intermedia ensures Hosted Exchange security

Now that you understand the key security capabilities to seek in a hosted Exchange provider, let's take a closer look at how Intermedia addresses these requirements.

Multi-tenant platform security

Intermedia uses multiple redundant, enterprise-class firewall systems to help prevent unwarranted intrusions and to help ensure only authorised users access your Exchange environment. This purpose-built security system integrates firewall, VPN and traffic management.

We also run multiple intrusion protection systems (IPS) (both host and network) to help detect and deter 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. IPS can also 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 Intermedia's datacenters adheres to strict standards in physical security. Each datacenter is closely monitored and guarded 24/7/365 with sophisticated pan/tilt closed-circuit TVs. Secure access is strictly enforced using the latest technology, including electronic man-trap devices between lobby and datacenter, motion sensors and controlled ID key-cards. Security guards are stationed at the entrance to each site.

Employee security

Every Intermedia employee, regardless of role, undergoes a rigorous background check. Employee access to passwords, encryption keys and electronic credentials is strictly controlled using two-factor authentication and role-based access control. Access to servers is restricted to a limited number of authorized engineers and monitored regularly.

Redundant internet service providers

Each of our datacenters is serviced by multiple Tier-1 Internet providers to mitigate the potential impact of a Denial of Service (DoS) attack on any single provider.

Authentication and access

Intermedia has established a number of stringent policies and procedures to authenticate a caller's identify during support and service calls. These policies and procedures help protect confidential information belonging to your account and to your users by helping to ensure that only authorised members of your team are given access to our services. In addition, our online control panel enables administrators to fully control access to services and administrative functions.

Dedicated security staff and monitoring

Intermedia employs dedicated, full-time security staff who are certified in all disciplines of information security. This team is involved with all aspects of security, including log and event monitoring, incident response, managing intrusion detection systems (both host and network), perimeter defense, service and architecture testing, and source code reviews.

Privacy

Intermedia is registered and certified with the US Department of Commerce for privacy under the Safe Harbor program. This stringent set of requirements helps ensure that any certified provider has established an in-house program, identified a privacy officer, met all the provisions for proper disclosure of its privacy practices, and offers mechanisms for feedback, opting out, and dispute resolution.

Audit report: SOC 2 type II certification

Intermedia has a SOC 2 Type II audit report from an independent auditor who has validated that, in their opinion, our controls and processes were effective in assuring security during the evaluation period. Intermedia is audited company-wide, not just at the datacenter level. Additionally, while some service providers may only choose to be audited against one or two of the five trust service principles (security, availability, processing integrity, confidentiality and privacy), Intermedia has been audited against all five.

PCI compliance

The payment processing system utilized by Intermedia has passed the strict testing procedures necessary to be compliant with the PCI Data Security Standards (PCI DSS). This helps ensure that your payment information will not be accessed by unauthorised parties or shared with unscrupulous vendors.

Email security and continuity

Intermedia employs a full suite of tools to help protect against spam and viruses and encrypt your emails. These include:

- **Anti-spam and anti-virus.** McAfee Email Protection helps eliminate spam and viruses before they reach your users' mailboxes. Powered by the global leader in IT security, this service is bundled with every mailbox to help identify, quarantine and block suspicious email.

  McAfee's multilayered protection helps give peace-of-mind and lets your users and IT administrators focus on more strategic activities. It offers:

  - Patented spam blocking with 20+ separate filters, multi-language and image capabilities that block 99+% of spam
  - Industry-leading, signature-based antivirus engine
  - Automated 24x7 threat monitoring and updates as McAfee's experts detect new threats
  - Proprietary worm detection that intercepts zero-hour mass mailings
  - Content and attachment filtering that intercepts malicious and sensitive content
  - Protection against email-based attacks such as denial of service, directory harvest, email bombs and channel flooding
  - Gray mail and bulk mail filtering to reduce clutter from unwanted newsletters and sales messages
  - Daily report of quarantined messages that helps end users spot false-positives

Features that are available in McAfee Advanced Email Protection include:

- Granular control over how emails are handled based on spam score (inbox, junk box, deletion)
- Content filtering based on predefined or custom-built criteria
- McAfee ClickProtect for inspecting URLs that a user clicks before allowing the page to load, which is especially helpful for protecting mobile device users against phishing attacks
- Admin control over white lists and black lists to customize your filtering policies
- End-user management over individual white lists, black lists, reporting and other settings
- Control over the level of threat protection to balance usability with security
- The ability to set policies based on user groups
- Message audit capabilities to find message disposition information as well as blocked IP addresses
- User activity reports to spot trends in users' inbound and outbound emails.

- **Email Data Loss Prevention.** McAfee Email Data Loss Prevention filters outgoing email to ensure sensitive information or undetected viruses don't leave your users' outboxes. Using McAfee's web console, your administrators can:
    - Filter content using keywords to spot credit card numbers, social security numbers, profanity and more
    - Control document types by size, media type, binary content and file integrity
    - Set policies to block certain file formats or very large files that monopolize bandwidth
    - Prevent viruses, worms, and other malicious content from infecting recipients
    - Define policies by individuals, groups or universal coverage
    - Define actions that include blocking, tagging or quarantining for administrator review
    - Monitor activity and run queries to track email disposition
    - Rely on built-in transport layer security (TLS) encryption for secure organization-to-organization communications

- **Email Continuity.** McAfee Email Continuity offers redundant email access for peace of mind beyond Intermedia's 99.999% uptime guarantee. It gives users a redundant path for sending and receiving email, even if they can't connect to their Exchange server. This includes:
    - A web portal within McAfee's cloud for sending and receiving email
    - Additional redundant administrator tools for monitoring email activity, suspending incoming mail flow, and setting policies for email spooling priorities and notifications
    - The peace of mind of enterprise-grade redundancy. McAfee's datacenters are geographically isolated ISO 27001-certified with active-active redundant hardware at all network layers.
    - A way to completely avoid downtime during your provider's late-night planned maintenance windows

- **Protection for mobile devices.** Our administrator control panel allows you to set security and message management policies for your mobile devices with one integrated view.
  - If a user's mobile device is lost, stolen or otherwise compromised, you can use our control panel to perform a remote wipe that removes critical company data
  - You can also use our control panel to deactivate devices so they no longer receive emails
  - You can set custom account-wide policies or apply custom policies for selected users
- **Data Replication.** In addition to running regular back-ups, Intermedia replicates Exchange data in real time from one set of premium hardware to another. This helps protect the critical information your business keeps within Exchange, even in the event of hardware failure or database corruption. It also enables Intermedia to rapidly restore the full functionality of your Exchange environment should an issue occur.
- **Encryption.** For high degrees of encryption, you can use our Encrypted Email solution to communicate externally with military-grade encryption of email and attachments.
  - Encrypted Email easily encrypts emails based on company-wide rules and policies that clients set up and manage. It does so without disrupting day-to-day workflow.
  - Email content and attachments are automatically scanned to detect whether the message warrants encryption before being sent. You can configure policies 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 you need end-to-end encryption, we also offer user-level Encrypted Email, which encrypts emails from the desktop client, and can be used to encrypt intra-company and confidential communications.
  - Both of our encrypted email solutions are backed by a globally recognized Certificate Authority. They use standards-based technologies—such as Public Key Infrastructure (PKI), S/MIME, and X.509 certificates—to establish confidentiality, message integrity and user authentication. They also include transport-layer encryption via SSL from client to server.

Conclusion

Many hosted Exchange providers will advertise the latest software, the fastest servers, and the most advanced datacenters. But in order for you to trust this critical business tool to their cloud, their services must be backed up by the highest levels of security.

As you search for a hosted Exchange provider that best matches your organization's needs, be sure to give security the priority it deserves.

If you have any questions about Intermedia security levels or processes, don't hesitate to ask. You can contact us any time at **800.379.7729** or by emailing **security@intermedia.net.**

INTERMEDIA
The Business Cloud™

For more information:

CALL US	EMAIL US	ON THE WEB
800.379.7729	**security@intermedia.net**	**intermedia.net**