SECURITY IN A HOSTED EXCHANGE ENVIRONMENT

EXECUTIVE SUMMARY

Hosted Exchange has become an increasingly popular way for organizations of any size to provide maximum capability and at the same time control costs. In most organizations, it's no longer enough to provide 'always on' email access. The email environment must be protected with ironclad security. Despite a flurry of headlines that question the security of the 'cloud', hosted Exchange services have actually proven to be a more secure solution than their traditional on-premise email counterparts.

This white paper explores the role of security in a hosted Exchange environment. It examines why email security matters and the security advantages inherent in a hosted solution vs. on-premise. It then 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 Pinnacle Consulting and how they compare with other alternatives.

WHY SECURITY MATTERS

Given its business criticality, a breach in email security could have both commercial and legal ramifications. Consider the example in which your email systems are infected with a highly destructive, virulent virus. In addition to the infection of your own systems, the virus payload is delayed but destructive. As a result, an email sent from your organization manages to infect, say, a competitor or a customer, before the virus destroys your system.

The commercial implications alone could be catastrophic: loss of business critical systems and data; extensive time and resources required to restore your operations; lost revenue and missed business opportunity. As if those effects weren't damaging enough, there are the potential legal implications to consider. In most cases your organization could be liable for any loss suffered by a third party as a result of the infected email received from you, albeit 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.

THE SECURITY ADVANTAGES OF HOSTED VS. ON-PREMISE EXCHANGE

Whether hosted or on-premise, no IT organization relishes a breach in security. However, a hosted Exchange provider stands to lose a great deal more in the event their security is compromised. In a sense, their entire business is predicated on their ability to offer a more secure environment than their customers could deploy themselves on-premise. Security is actually seen as a key competitive differentiator for hosted Exchange providers. As such, they invest a great deal more in physical security than most IT organizations could ever afford.

At the core of every hosted Exchange provider's business are physical facilities that house the myriad of servers and network infrastructure required to service 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 datacenters owned and operated within the typical organization. This is particularly true of small to midsize businesses who manage their email infrastructure on-premise.

In addition to the gamut of physical controls available, there are well-established standards, such as SAS 70 and PCI, 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 is certainly no shortage 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 it comes to security. It is critical to go beyond the superficial buzz-word level features and thoroughly understand each 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.

MULTI-TENANT VS. DEDICATED 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 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

This encompasses everything from surveillance cameras, perimeter security, and employee access controls at each datacenter and company facility. The provider should have a clearly documented policy that governs how confidential information about your account, such as passwords and other credentials, are treated. The provider's dependence on internet service providers is also important. Ask your provider how a denial of service attack launched on their communications provider would impact their service.

EMPLOYEE SECURITY

Physical security shouldn't stop at the four walls of the provider's datacenter. It also pertains to the provider's employees themselves. For example, how thorough are the background checks each employee is subjected to as part of the hiring process? Beyond the initial background checks, it's important to understand the primary focus and experience level of staff dedicated to the security. Is security maintained by dedicated and specially-trained personnel or does that responsibility fall on the shoulders of the provider's general IT operations staff? What role do outsourced employees play in the provider's organization?

SAS 70 CERTIFICATION

Any hosted Exchange provider worthy of your consideration must demonstrate that they have adequate controls and safeguards when they host or process your organization's data. Widely recognized as a mark of service quality, a Statement on Auditing Standards (SAS) No. 70, Service Organizations, audit shows that a service organization has been through 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.

Email security

A true test of a hosted Exchange provider is how well they address email security and continuity. Ideally, this should involve a comprehensive approach that protects against both viruses and spam.

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? In most cases, providers' responsibility for anti-virus protection extends only to their hosted Exchange servers. What is your obligation to protect end-user client devices in your organization?

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 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 filter out content that does not meet these specifications. This enables your organization to comply with company, state and federal communications regulations.

Encryption: 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 your organization's email is secure.

SECURITY IN ACTION: PINNACLE CONSULTING

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 Pinnacle Consulting addresses these requirements:

MULTI-TENANT PLATFORM SECURITY

Pinnacle Consultinguses multiple redundant, enterprise-class firewall systems to prevent unwarranted intrusions and ensure only authorized users access your Exchange environment. This is a purpose-built security system that integrates firewall, VPN and traffic management. We also use 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 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 Pinnacle Consulting's seven world-class datacenters (6 US-based; 1 UK-based) adheres to the strictest standards in physical security. Each datacenter is closely monitored and guarded 24x7x365 with sophisticated pan/tilt closed-circuit TVs. Secure access is strictly enforced using the very latest technology, including electronic man-trap devices between lobby and datacenter, motion sensors and controlled ID key-cards. Security guards are stationed at every entrance to the site. Each datacenter is also serviced by multiple Tier-1 Internet providers. This eliminates the potential impact of a Denial of Service (DoS) attack on any one of our Internet providers.

SAS 70 Audit Report Contents	Type I Report	Type II Report
Independent service auditor's report (i.e. opinion)	Included	Included
Service organization's description of controls	Included	Included
Information provided by the independent service auditor; includes a description of the service auditor's tests of operating effectiveness and the results of those tests	Optional	Included
Other information from the provider (e.g. glossary of terms).	Optional	Optional

DEDICATED SECURITY STAFF AND EMPLOYEE CONTROLS

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

SAS 70 TYPE II CERTIFICATION

Pinnacle Consulting is SAS 70 Type II certified. This is far more rigorous than Type I certification, which looks for effective controls and processes but does not test for actual use or implementation. Type II requires an independent auditor to validate, in their opinion, that the controls and processes in use are effective over its one year evaluation period. Pinnacle Consulting is also audited company-wide, not just at the datacenter level.

PCI COMPLIANCE

Pinnacle Consulting has passed the strict testing procedures necessary to be compliant with the PCI Data Security Standards (PCI DSS). This ensures that your payment information will never be accessed by unauthorized parties or shared with unscrupulous vendors.

EMAILSECURITY AND CONTINUITY

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

- **Antispam**: All Pinnacle Consulting Exchange accounts include SpamStopper™ or SpamStopper Pro, our advanced antispam software, at no additional cost. Based on Spam Assassin and customized for our Exchange hosting environment, Pinnacle Consulting's SpamStopper runs in a separate server cluster, outside the Exchange servers, for increased performance. SpamStopper provides:
    - **Content filtering**: This provides server-side protection against bad headers and suspect attachments. This also enables customers to comply with acceptable business use policies, company, state and federal communications regulations
    - **Company-wide white and black lists**: 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.
    - **Outlook integration**: End users can control their personal white and black lists directly from Outlook.
    - **Flexibility**: Administrators can manage all spam settings and users get mailbox-level white/black list control.
    - **User-defined sensitivity**: Customers can refine spam sensitivity levels according to their company's email usage.
- **Antivirus**: Pinnacle Consulting provides VirusStopper, comprehensive managed antivirus protection of all Exchange mailboxes, free of 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 ever reaching the Exchange Environment. Our 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 Pinnacle Consulting continuously manages the antivirus software and virus definitions. In addition to the server-based antivirus software Pinnacle Consulting provides, clients are advised to install and maintain up-to-date, anti-virus software on all end-user computers.

- **Data Replication**: In addition to running regular backups, Pinnacle Consulting 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 Pinnacle Consulting to rapidly restore the full functionality of your Exchange environment should an issue occur.

- **Encrypted Mail:** Email between mailboxes on our system is natively encrypted. Clients can also use our Encrypted Email solution in order to communicate externally with military-grade encryption of email and attachments. Our 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, 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 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.

The latest software and fastest servers housed in the most state-of-the-art datacenters mean nothing if your users can't send and receive email securely. In your search for the hosted Exchange provider that will best serve your organization's needs, be sure to give security the appropriate attention it deserves.