



# **Best Practices for Securing Exchange Email**

Delivering enterprise-level security to small, medium and large businesses through email hosting

## Table of Contents

Executive summary .....	3
The benefits and threats of corporate email.....	3
Combating the email threat, effectively and affordably .....	4
Best practices for hosted Exchange email providers .....	5
People: addressing the weakest link .....	5
Background checks .....	5
Employee roles.....	6
Certifications and training.....	6
Processes: providing a systematic approach .....	6
Key processes and procedures.....	6
Procedural best practices.....	6
Technology: providing a state-of-the-art defense .....	7
Strong perimeter defense.....	7
Encryption .....	8
Physical data center .....	8
Choosing the top-ranked hosted email provider: USA.NET.....	9
People: Committed, reliable, experienced personnel .....	9
Processes: Tested, industry-standard procedures .....	9
Technology: Best-of-breed technology and partners.....	9
Summary: multi-layered, end-to-end email security for organizations of all sizes .....	10

## Executive summary

Email is an essential business tool for organizations of all sizes. Yet it is also the easiest way for hackers, spammers, and other malicious threats to penetrate and disrupt business operations. End-to-end security is as vital to today's businesses as email itself. For small, medium and even large-sized companies looking for robust, secure email they can afford, outsourcing to an experienced Microsoft Exchange Hosted Service Provider is the ideal solution. Companies can achieve maximum benefit only by identifying a truly qualified provider—one that implements best-of-breed technology and follows best practices for email security comprising deep expertise in people, technology, and processes.

## The benefits and threats of corporate email

For the majority of today's businesses, email has become an indispensable productivity tool. The figures alone reflect email's value: corporate mailboxes worldwide, numbering approximately 357 million in 2005, are predicted to reach a staggering 465 million by 2009<sup>1</sup>. Email injects speed, efficiency, and cost-effectiveness into employee communications. But there's a rub: it is also one of the primary avenues by which hackers can infiltrate corporate networks. Gartner projects that by the end of 2007, targeted attacks using professional-grade malware will have infected 75 percent of enterprises<sup>2</sup>. Many of these attacks will be launched through email.

Spam. Viruses. Trojans. Phishing attacks. These are just a few of the changing email-borne threats that can choke network activity or lead to debilitating loss of proprietary data. Spam, for example, has become infamous in recent years for congesting corporate mailboxes. It has also been responsible for more destructive activity: flooding recipients with links to web sites that host viruses and other malware. In spring 2007, spam emails depicting various celebrities lured users to a web site hosting a fatal zero-day vulnerability. Later in the year, a wave of mass-mailed "Storm" malware accounted for tens of thousands of infected PCs by directing users to web-hosted exploits—and making user computers drones in a Peer-to-Peer (P2P) botnet.

Similar to large enterprises, today's small and medium-sized businesses (SMBs) are supporting increasing numbers of remote employees, mobile devices and online availability of greater volumes of corporate data. For organizations like these with limited security budgets, email-borne threats are cause for serious alarm. Further complicating matters is the additional financial burden of complying with stringent government requirements—Sarbanes-Oxley(SOX), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), and others—that legislate the storage and transmission of sensitive data. Grappling with scarce resources, how can today's SMBs continue to reap the benefits of email while avoiding its potentially devastating pitfalls?

---

<sup>1</sup> The Radicati Group, Inc., 2006

<sup>2</sup> Gartner Research, 2007

## Combating the email threat, effectively and affordably

Most large enterprises have the financial resources to implement and maintain comprehensive in-house email security. But SMBs often lack the resources to deploy an in-house email server and its accompanying security solution. Many smaller companies feel that their only option is to implement single-point solutions such as standalone firewalls, anti-spam software, or intrusion detection systems. While these kinds of solutions do provide a certain measure of email security, they simply can't offer the same kind of protection against blended email threats as enterprise-grade, end-to-end security solutions that effectively utilize best of breed technologies.

Today, more and more SMBs and a surprising number of enterprises are beginning to migrate toward hosted email providers—particularly those offering Microsoft Exchange hosting. Exchange email hosting provides all sized businesses with a high-caliber, scalable email solution at an affordable cost. Whether a company is expanding or downsizing; has 5,000 users or 15, it only pays its email host for the resources it actually uses on a monthly basis. And it benefits from enterprise-grade email functionality that could never be achieved through single-point solutions.

As an increasing number of SMBs explore solutions offered through hosted Exchange providers, they are realizing that enterprise-grade email functionality and enterprise-level email security do not always go hand in hand. As we'll examine in the next few sections, it is critical that all size groups, SMBs and large enterprises with multiple locations, select an Exchange email provider that follows best security practices—both within its own organization and across its email offering.

## Best practices for hosted Exchange email providers

Iron-clad email security requires far more complexity than a one-time technology implementation. To provide the end-to-end security required by today's growing businesses, an information security program must comprise multiple, overlapping layers of security. An ideal security program involves a finely tuned 'information security triad' consisting of expertise in the areas of *people*, *processes*, and *technology*. Only through excellence in each of these areas can an email host proactively mitigate the risks inherent to the ongoing operations of its customers.



### ***People: addressing the weakest link***

An email host is only as good as the people it employs. Companies place a great deal of faith in the ability of their vendor's staff to maintain the strictest standards of data privacy and security. Yet people—sometimes unpredictable, often resistant to change—are traditionally the weakest link in the chain of security technology. Companies entrusting their assets to another organization must ensure that the host company's staff is flexible, highly talented, and thoroughly trustworthy. Here are some of the ways a qualified vendor ensures the quality and reliability of its people:

#### **Background checks**

Best practices dictate that vendors take the 'people' aspect of security very seriously. Top-notch vendors require that their employees pass extensive background checks, which include verification of former employment and cross-checking through secondary references. A basic check includes SSN verification, address history, and a search of county records for felonies and misdemeanors. Basic

background research should also include verification of certifications for technical personnel and a review of credit history for employees working in finance departments.

### **Employee roles**

Trusted vendors set strict rules regarding roles and responsibilities by granting employees access only to areas of customer systems that are pertinent to their duties. This helps limit the risk of compromise, even if it is unintentional. A secondary aspect of employee-related rules should include a no-tolerance policy on the viewing of private customer data.

### **Certifications and training**

A trusted vendor ensures that its employees keep pace with ever-evolving security technology by requiring up-to-date certifications and providing continuous training. Some of these certifications include MCP, MCP+1, MCSE NT/Windows, A+, Citrix, BlackBerry, CCSE, CCSA, CCNA/CCDA, CCNP/CCDP, CISSP, MSP, LPI, HP-UK, ITIL, Microsoft Hosting, and Mobility certification.

High-caliber email hosts that place value in their employees can generally boast of a low employee turnover, with an average worker longevity of three to five years. The higher the employee longevity factor, the more deeply a vendor can embed workers into its processes to ensure continuity in the event of an employee role change.

### ***Processes: providing a systematic approach***

Top-tier hosting companies adhere to well-defined, heavily tested processes and procedures that bring consistency and structure to email security. Processes should be established and thoroughly documented for every aspect of the operation, from firewall configuration to facility access. The advantage of well-documented, strictly followed processes is repeatability: they help personnel minimize errors through consistent performance of tasks, even when staff changes.

### **Key processes and procedures**

Privacy and data classification procedures are particularly important for a vendor to adhere to. A hosting company should show documentation of carefully conceived processes that describe how and to whom they grant system access.

Another essential process is continual auditing—when a system is built, when significant changes are made, and on a quarterly or even monthly basis. This enables the company to compare a ‘snapshot’ of the system against the ever-changing list of system threats and to ensure compliance with best practices for security, privacy, and operational controls. The best vendors supplement their internal auditing practices with third-party audits. By seeking system validation from independent auditors, such as Microsoft or Deloitte and Touche LLP, for example, hosting companies can solidly demonstrate that they are adhering to rigorous, industry-accepted security practices.

### **Procedural best practices**

To achieve the 99.9% uptime and robust security that customers have come to expect, email hosting companies must closely align their operational procedures with best practices followed by big technology partners such as Cisco and Microsoft. Some examples of best-practice operational processes include:

- Patches and hotfixes should always be tested in a lab environment that mimics the production environment prior to rollout.
- Customer data should be backed up to tape and stored offsite—and restored only when the customer follows the proper sequence of events.
- Customers must follow proper procedures to report a lost device before the vendor can remotely deactivate and wipe the device.

### ***Technology: providing a state-of-the-art defense***

Arguably, the most critical component of an email security program is a vendor's technology which helps lock down corporate assets by recognizing and thwarting mail-borne threats. To ensure comprehensive protection against malicious activities, a qualified vendor should employ state-of-the-art, rigorously tested technology with the following features.

#### **Strong perimeter defense**

Security threats typically access an organization through the front door via inbound email. A top-tier vendor should focus heavily on email security with baseline protection. Strong perimeter defense for email includes addressing security issues at every level within an organization (physical, network, servers, applications and users); auditing servers prior to being put into the production environment to ensure that changes introduced do not reduce the security level of the infrastructure; regularly and documented audits of the environment helping to ensure that the risk levels to the organization are within acceptable levels; multiple layers of firewall and filtering protection restricting access to critical data from unauthorized sources; and Intrusion Detection Systems/Intrusion Prevention Systems restricting system and network access from malicious activities. Top-tier email security also includes:

- Centralized log servers enabling system administrators to view all security logs from one system, increasing the probability of daily review of log files throughout the environment.
- Best practices for network devices including both hardware and software configurations
- Secure mobility technology such as Triple DES or AES, remote disabling of lost devices, mandatory passwords, idle lock, and wiping of device after a set number of incorrect passwords.
- Host Security – best practices for securing multi-tenant environment, including secure server builds, Active Directory Group Policies, daily audit log review.

An email host should also offer a variety of value-added defensive components that help regularly patrol and strengthen the network, such as anti-virus and anti-spyware solutions to stop malicious code before it enters the organization, as well as anti-spam solutions limiting the number of unwanted emails in your user's inbox. Additional value-added security components include:

- Inbound and outbound content filtering which helps minimize the risk of confidential data being sent in and out of the organization.
- Provisioning tools for delegation of email administration as well as logging and reporting of such administration.
- Active Directory – best practices for securing multi-tenant environment, including group policies.

## Encryption

As more and more companies conduct global transactions, the boundaries of their perimeters increase—thereby widening their vulnerability to greater numbers of untrusted networks. Strong encryption helps significantly reduce the risk that an untrusted party will have the ability to eavesdrop on communications or obtain proprietary company information.

The most secure email hosts utilize a robust blend of encryption solutions including a Virtual Private Network (VPN), which shields your corporate network from unauthorized access to data through an established encrypted tunnel allowing access to network resources; standard and enforced Transport Layer Security (TLS); and the following:

- Public Key Infrastructure (PKI)
- Encrypted email capability
- Key management and recovery
- Secure Socket Layer (SSL)
- Internet Protocol Security (IPSEC)

Top level email hosting providers employ not only industry best messaging specialists, but have seasoned and knowledgeable network professionals on hand to assist with the complex connectivity issues facing organizations today. Such issues include technical knowledge of a wide number of firewall, VPN, wireless and other network related solutions on the market and how those solutions will integrate into the messaging solution.

## Physical data center

The location, layout, and physical security at an email host's data center are just as important as its logical security. Companies that choose a vendor that resides in a Tier 1 or 2 data center are getting minimal physical asset protection and toleration of up to 28.8 hours of downtime per year. A more thorough option is to select a host in a Tier 3 or Tier 4 facility.

Tier 4, the highest-rated facility, offers a layered, secure data defense model comprised of power redundancy through separate power grids with automatic failover; redundant backbone for cabling infrastructure; gated, badged access to the facility parking area; access to and within the building controlled with biometric readers and single-person entryways; and live, 24x7x365 onsite CCTV monitoring of the parking area, building entrances, and interior areas of the building. Tier 4 facilities also include:

- Caged off floor space accessible only to vendor employees
- Proactive monitoring of power and ambient air temperature inside the cages
- Tolerance of no more than 0.4 hours of downtime per year
- Gaseous fire suppression that enable automated response in the case of a fire
- Facility location in an area with a low occurrence rate for natural disasters

Top-tier email hosts strive to align the caliber of their data center security with that of other security technologies to ensure that both physical and logical threats are addressed.

## Choosing the top-ranked hosted email provider: USA.NET

Ranked by The Radicati Group as the leader in hosted security for email communications<sup>3</sup>, USA.NET offers a broad selection of hosted, customizable, affordable email services ranging from basic webmail to hosted Microsoft Exchange. USA.NET specializes in helping companies with traditional in-house IT departments outsource their messaging as a strategic element in business transformation.

Focused exclusively on hosted email services, USA.NET protects its customers' core data assets by utilizing the information security triad—the most effective blend of people, processes, and technology available today in a hosted solution.

### ***People: Committed, reliable, experienced personnel***

USA.NET firmly believes that its people are the key to its success and to the success of its customers. The company hires only the brightest and most reliable talent, as verified through comprehensive background checks performed by an independent investigative organization. The background check includes criminal history, employment references (including secondary referrals), and motor vehicle records. In addition, professional license/certification verification is performed for technical personnel, while credit history is reviewed for finance personnel.

USA.NET strongly encourages employee growth by supporting in-house and external training and lab time to earn additional certifications. Its commitment to staff—through training dollars, benefits, and flexibility—has earned the company loyal employees whose tenure averages five years. High employee retention means that company processes run more smoothly and are not adversely impacted by occasional changes in staff.

### ***Processes: Tested, industry-standard procedures***

Over 15 years in the industry has enabled USA.NET to develop and test security processes, audits, and operations that align with the best practices of government agencies and large organizations. The company fulfills SANS security requirements and is the only email host that is Microsoft Gold Certified and SAS 70 Type II audited. This reflects its well-documented processes and ability to deliver security procedures as promised. USA.NET follows best practices for vulnerability management operations such as patch management, performing heavy testing in an operational readiness lab to minimize issues during rollout. By adopting the best practices used by partners like Microsoft and Cisco, USA.NET gets stronger support from these organizations and can pass that on to its customers.

### ***Technology: Best-of-breed technology and partners***

USA.NET secures inbound and outbound email through multi-layered protection involving premium anti-spam, anti-virus, and email encryption technologies. It reinforces logical data security with the physical security of a Tier 4 data center boasting a fully redundant architecture, state-of-the-art access control, live monitoring, on-site personnel, and a Denver location with an extremely low probability for the occurrence of natural disasters. USA.NET works with leading technology partners like Microsoft, HP, Cisco, Check Point, F5, Symantec Brightmail, and Trend Micro to create custom, interoperable systems and devices that ensure the integrity of customer data. USA.NET's premier support with these technology partners further ensures best-of-breed email security for our customers.

---

<sup>3</sup> The Radicati Group, Inc., 2006

**Summary: multi-layered, end-to-end email security for organizations of all sizes**

For SMBs and large enterprises seeking secure, affordable Exchange email hosting, USA.NET offers a comprehensive blend of best security practices and best-of-breed technology. Ranked by the Radicati Group as a Top Player in the hosted business email market<sup>4</sup>, USA.NET believes that security is a multi-layered, continuous process.

Many companies continue to take risks every day by utilizing a single-point, single-setup solution or going with lower-tiered hosted email vendor. USA.NET, a top-tiered provider host, helps SMBs and large businesses, including United Airlines, Farmers Insurance, Realogy, Intertek and others, address all aspects of risk with an affordable, multi-point solution that reacts swiftly to today's ever-changing threat landscape.

---

<sup>4</sup> The Radicati Group, Inc., 2006