PROTECT YOUR EMAIL SERVERS

Guard the data and availability that enable business-critical communications
Guard the data and availability that enable business-critical communications

The Situation
The email server is a focal point of enterprise risk today, because most organizations implemented a secured email infrastructure initially, then adopted a “set it and forget it” approach in maintaining it. IT, with so many other high priority projects to address, may not look at the email server again until a problem is reported, such as a breach that can result in:

- **Loss of Information.** Hackers crave the valuable data stored in the email database. When hackers broke into the Epsilon email system, they captured email addresses and account context for customers of some of the largest organizations: Citibank, JPMorgan Chase, Capital One, Target, Walgreens, Home Shopping Network, and many more.

- **Downtime.** Breaches can also allow remote code execution that can result in denial of service (DoS), where business-critical email becomes unavailable for hours, days, or even weeks. If you are running Microsoft Exchange, you can find many known DoS exploits listed on the Microsoft Security Bulletin website (http://technet.microsoft.com/en-us/security/bulletin). These vulnerabilities can be found in the operating system where Exchange is installed, or Exchange itself. Hackers exploit these weaknesses through viruses, Trojans, worms, or even specially crafted emails.

To minimize the resources required to maintain email server security, enterprises need to consider ways to combat evolving security risks using solutions that provide more effective security.
Driving Concerns
Most organizations already have a multi-layered solution in place to protect their email servers: an email gateway solution stops threats at the perimeter, and server-based security protects their email servers. The problem many organizations have with this approach is not the design, but the solutions they choose to safeguard their email servers. Email security solutions that do not address the following concerns will be ineffective in providing enterprise-level security:

- **Outdated Protection.** Many email security solutions rely heavily on local intelligence to provide protection: antivirus definitions, antivirus engine updates, and updated threat dictionaries. The solution must pull down these updates on a very frequent schedule to protect against newer email threats. Some solutions can look for these updates from the security vendor as frequently as every 15 minutes. But what happens when a newer threat penetrates through to the email server before an update is provided?

- **Platform Disruption.** Patches secure the platform the email server is running on and the email server application itself from known vulnerabilities. Depending on the number of email servers you have in your environment and the regression testing you require, patch updates may take days, weeks, or even months to complete. To add complexity and risk to this process, how do you deal with critical patches that are issued outside normal patch cycles? These emergency patches are important from a security perspective, but can take just as long to deploy across all your email servers.

- **Operational Complexity.** If your IT organization used a multi-layer, multi-vendor approach to secure your email infrastructure, “situational awareness” is non-existent. When something important and time-sensitive comes along, you need every available resource to handle it. For instance, in the event email servers are compromised, silos of data, logs, and status dashboards must be manually correlated to determine where the breach occurred. Because each data set is separate, add more hours to diagnose which systems were affected, coordinate your remediation efforts, and demonstrate the systems are healthy again.

Solution Description
McAfee strongly recommends a unified multi-layered approach to effectively protect your email servers. The solution should employ proven technologies to secure the email infrastructure against both breaches and platform disruptions and significantly reduce operational complexity.

- **Perimeter-based security** should leverage real-time global threat intelligence to protect against malicious senders with negative reputations.
- **Server-based protection** should employ both heuristics and reputation for real-time defenses against viruses, spyware, buffer overflows, and other threats to the operating system and email server application.
- **Unpatched email servers** should be protected against unauthorized changes to critical system files, directories, and configurations.
- **A single console** should manage and report on all security solutions protecting the email servers.

Decision Elements
In order to provide strong protection for your email servers, it is important to understand the current solutions and processes safeguarding them.

- Have you ever had an email breach? If so, how long did it take to mitigate the issue?
- How do you manage patches on your email servers, including out-of-band patches? Do you feel confident that if a critical patch is not applied, your current solution provides adequate protection?
- Can you report and prevent unauthorized changes to your email servers?
- Can all of the components protecting your email servers report and be managed through one console?
Technologies Used in the McAfee Solution
McAfee products provide a multi-layered email security solution managed by a single console for the visibility and control needed to effectively protect against emerging email threats. The McAfee solution consists of McAfee® Email Gateway at the perimeter, with McAfee Security for Email Servers, McAfee VirusScan® Enterprise, McAfee Application Control, and McAfee Change Control on the email server itself. McAfee ePolicy Orchestrator® (McAfee ePO™) connects these systems for monitoring and reporting.

Global Threat Intelligence (GTI)

Email Security
- Reputation Filtering
- Antispam
- Antimalware
- Antivirus
- Application Enforcement
- Change Prevention
- Vulnerability Intelligence
- Exploit and DoS Protection

McAfee ePO

Real-time threat intelligence helps protect your email servers from breaking threats, while server-side controls limit the chance of downtime.

McAfee Email Gateway
McAfee Email Gateway (MEG) stops email threats at the perimeter, utilizing proven technologies to protect organizations against both known and emerging message-based threats. Unlike competitors that rely heavily on local intelligence to provide protection, MEG combines real-time McAfee Global Threat Intelligence (GTI) and local intelligence to stop threats before they can get to your email servers. GTI continuously monitors and characterizes Internet traffic through a network of sensors in 82 countries, and performs connection level drops on messages received by senders with bad IP, domain, or URL reputation data.

McAfee Security for Email Servers
When it comes to providing security for all the areas that may be affected by an email infection, you should always start with the source—your email servers. McAfee Email Security for Servers is designed specifically to protect against breaches of the email server application and the sensitive data stored within the email database. It checks incoming and outgoing email messages for viruses, worms, Trojans, and other malware. Additionally, it will scan all internal emails to block a worm propagating internally. Using cloud-based McAfee Global Threat Intelligence, McAfee sends a fingerprint of any suspicious file for instant reputation analysis at McAfee Labs. If the fingerprint is identified as known malware, an appropriate response is sent back in milliseconds to block or quarantine the file.
McAfee VirusScan Enterprise
With McAfee VirusScan Enterprise (VSE) installed on your email servers, you can proactively stop and remove threats to the operating system, extend coverage for new security risks, and reduce the cost of managing outbreak responses. Even without an update, it stops zero-day threats and reduces the window of vulnerability—the time between the discovery of a vulnerability and when its fixes are deployed. Plus, you have the flexibility to detect and block malware based on your business needs: on access, on demand, or on a schedule. VSE is critical to protect the operating system on which the email application runs.

McAfee Application Control
McAfee Application Control offers an effective way to block malicious code and unauthorized applications from executing. Administrators define a standard list of which processes and applications are allowed to run on email servers, and a dynamic trust model allows controlled, automated updating of software by trusted updaters. In situations where an email server is not patched with critical updates, McAfee Application Control provides a virtual barrier from remote code executions that can result in attacks like DoS or theft of information. It can also protect legacy email systems where patches are no longer available from the vendor.

McAfee Change Control
McAfee Change Control provides continuous detection of changes made across all email servers, such as out-of-band configuration changes. Unlike scan-based solutions that take snapshots of the state of a system and compare them, McAfee Change Control continuously tracks and validates every attempted change in real-time and allows changes only through approved change management processes.

McAfee ePolicy Orchestrator
At the heart of the email security solution, McAfee ePolicy Orchestrator (McAfee ePO) consolidates and centralizes management using a single integrated management platform. McAfee ePO software provides flexible, automated management so organizations can identify, manage, and respond to email breaches quickly. You can define how McAfee ePO directs alerts and responses based on the type and criticality of security events in your environment, as well as create automated workflows to quickly remediate open issues.
Impact of the Solution
The recommended McAfee solutions for protecting email servers provide a unified multi-tiered approach for securing your architecture. We replace the inadequacies of a multi-vendor approach with:

• Real-time visibility and analytics, as well as unique predictive capability enabled by McAfee Global Threat Intelligence
• An integrated security management platform that automates deployment, updates, and reporting, giving your organization unprecedented visibility into your entire email security posture
• Layers of scanning to detect and clean malware and protect your files from viruses, worms, rootkits, Trojans, and other threats

With McAfee safeguarding your email servers, organizations can reduce risk and achieve operational efficiencies – all while protecting what is most important: your email server data and uptime.
Additional Resources
www.mcafee.com/emailgateway
www.mcafee.com/emailservers
www.mcafee.com/virusscan-enterprise
www.mcafee.com/appcontrol
www.mcafee.com/changecontrol
www.mcafee.com/epo
www.mcafee.com/gti

Optimal Email Security Solution Brief

For more information about the Security Connected Reference Architecture, visit:
www.mcafee.com/securityconnected
About the Author

John Kim is a Sales Engineer located in Texas. He has over 17 years professional experience in Information Technology and has worked for companies like Citigroup, Bank of America, and Microsoft. In his role at Citigroup, he was a Senior Engineer responsible for providing email security for one of the world's largest Exchange deployments. Throughout his career, he also gained experience in many areas of technology: Software Infrastructure Life Cycle (SILC), Software Development Life Cycle (SDLC), Project Management, IT Audit, IT Business Recovery, Security Engineering, and Sales Engineering.