INFORMATION SECURITY®

BUYER'S GUIDE TO Messaging Security

Messaging security options aren't clear cut any more. We'll help you decide when an on-premise solution is right for your organization, or when cloud-based SaaS is the way to go.

INSIDE

INFOSECURITYMAG.COM

SORT YOUR MESSAGING SECURITY CHOICES

MESSAGING SECURITY PRODUCT LISTING

SPONSOR RESOURCES

SORT YOUR MESSAGING SECURITY CHOICES

Companies face complicated buying decisions when it comes to buying messaging security, the most important being whether to go with an on-premise solution, a SaaS offering in the cloud, or both.

BY KAREN HOBERT AND DIANA KELLEY

PROTECTING MESSAGING SERVICES (e.g., email, instant messaging, texting) is an important part of any business messaging strategy. Vulnerabilities abound when you allow messaging traffic for delivery over the Internet. Messaging system administrators are charged with preventing data leaks, warding off system attacks such as spam, and guarding against malicious programs. Messaging security tools provide protection against spam and phishing, malware (both embedded and as attachments), as well as provide privacy policy enforcement (e.g., encryption for transport) to ensure compliance and data protection.

Choosing a solution requires looking at messaging security from two important aspects: the type of messaging security: perimeter security and message security; and the delivery of the service: on-premise or SaaS. As with any important security package, the choices depend on the individual business and what it feels it needs to protect. Although some messaging security solutions focus on other messaging traffic, many solutions that provide email security include modules for IM and other types of messaging traffic. Thus the scope of this guide will focus on email security although many of these concepts also apply to other types of messaging.

SORT YOUR MESSAGING SECURITY CHOICES

MESSAGING SECURITY PRODUCT LISTING

SPONSOR RESOURCES

MESSAGING SECURITY COMPONENTS

The best way to consider email messaging security is to look at it from two major functional aspects:

- **Perimeter security:** preventing incoming attacks and securing the hygiene of the messaging system, such as antivirus, antispam and antimalware protection.
- **Message security:** preventing the accidental or malicious release of information that would compromise user privacy or corporate data through message encryption, digital signatures, rules-based filtering and policy-enforced actions.

Most hosted services and on-premise solutions offer these basic functions: antispam and antiphishing; attachment scanning; and rules-based filtering. Additional features include: DRM policy enforcement; keyword scanning and blocking; encrypt on-send; tagging; digital signing; moving attachments to a secure repository; as well as archiving, message logging and journaling. Recent email platform updates include basic capabilities such as user generated whitelists and blacklists, administrator-managed policies that perform actions based on message contents (e.g., encrypt a message that contains personal data such as a Social Security number [SSN]), and auto-filtering to prevent virus and phishing attempts.

Email messages traverse many layers of the system to get to their destination, including in the cloud (over the Internet), gateway, network, service (e.g., email server, archive server), mailbox file, and email client. Messaging security tools can be applied to many parts of the system depending on business needs. In some cases the integrated messaging security capabilities of email platforms are enough for the needs of the business, however there are many reasons to extend messaging security beyond native email platform security tools. Third-party messaging security solutions can be used to secure messages as they traverse system layers.

Bottom Line: *Messaging security includes securing the messaging service from attacks as well as securing message content. Recent email platform upgrades now include perimeter and message security capabilities as native functionality. Message security enforced at different layers of the system is possible using third-party options. Organizations need to consider their messaging security requirements and where the system is most vulnerable.*

HOW TO DECIDE: ON-PREMISE VS. SAAS/CLOUD?

The messaging security market is robust with many vendors offering packages that support different aspects of messaging security. Some products are specialized for securing messages in support of specific industries, such as logging messages in an online service for legal verification of messages. Other packages focus on perimeter security or message security but not both. Whereas others support all messaging security features in different parts of the system, such as cloud-based perimeter security that filters out spam and malware before the messages cross the firewall.

Essentially there are three options for deploying messaging security: SaaS messaging security, on-premise messaging security, or a combination. Choosing one

SORT YOUR MESSAGING SECURITY CHOICES

MESSAGING SECURITY PRODUCT LISTING

SPONSOR RESOURCES

option over another is as varied as the needs of the company. Generally SaaS email security services focus on perimeter security services (although some offer message security as well) whereas on-premise solutions offer both perimeter and message security capabilities.

Promise of SaaS: reduce, re-use. SaaS-based services have become a popular option for many enterprises looking to reduce costs for IT services. Actually many customers have relied on hosted email perimeter security for some time and until recently, the only option for message content security was to purchase a third-party solution. Online spam and virus filtering services have grown to become reliable resources for protecting messaging systems from spam and other malicious email content. According to some reports, 90 percent to 95 percent of incoming traffic is crud (e.g., spam, phishing, malware). Stopping that traffic before it makes it to the internal message transfer agent (MTA) server not only improves the overall performance of the messaging service but also has a compliance impact; if the bad message never makes it to the internal network/server then the organization doesn't have to save it.

SaaS messaging security providers offer highly reliable services with up-to-date blacklists and virus tables. Pricing is a leasing model usually based on users or usage where customers pay for only what's used (not always a good deal, think about cellphone overage charges). One of the more attractive aspects of hosted services is that they can lower capital expenses for utilities, hardware, software and personnel. Not only are hosted services effective, but they can keep costs and capital expenditures under control.

SaaS messaging security providers offer highly reliable services with up-to-date blacklists and virus tables.

On-Premise benefits. Some organizations need more control or have strict policies for ensuring information privacy and preventing data leaks. Regulatory and business policies may require greater control over messages. On-premise messaging security solutions offer customers more granular control and options for securing their information and messaging systems than SaaS offerings. On-premise messaging security systems can mitigate insider threat by preventing breaches at various layers of the system. In some cases, overall cost for on-premise solutions may be lower than SaaS depending on the services used and whether native email platform security capabilities can support the business security requirements.

Weighing the pros and cons: on-premise vs.cloud. Overall, choosing a SaaS messaging security service over on-premise depends on how and where the security needs to be applied. If cloud-based filtering is most important, then a SaaS solution is likely a worthwhile option. If the organization needs more internal coverage as well as protection from external threats, on-premise options are a likely candidate. However, if a customer is looking to get the benefits of both cloud-based filtering and internal managed layers, then a hybrid of both SaaS message security and on-premises message security is probably the most beneficial combination for the organization.

SORT YOUR MESSAGING SECURITY CHOICES

MESSAGING SECURITY PRODUCT LISTING

SPONSOR RESOURCES

Bottom Line: *Message security delivery depends on what is of greatest concern to the organization. SaaS message security is best for filtering messages in the cloud, and preventing a lot of crud from entering the messaging system. On-premise message security systems offer more flexibility and options for controlling against internal threats. Many organizations use a combination on SaaS and on-premise message security services to get the most robust solution.*

LOGGING, ARCHIVING, REPORTING AND COMPLIANCE CONSIDERATIONS

Many regulations include protection requirements for information sent via email. The PCI-DSS requires encryption for cardholder data such as PANs (the 16 digit primary account number) sent in email or as an email attachment. Data breach laws, such as SB1386, and the recent HITECH Act offer "safe harbors" from notification if the information was encrypted. Messaging encryption is available as an integrated feature, or can be purchased as an add-on. Before purchase, consider what needs to be encrypted: email message content; file attachments; or both? Are there regulatory requirements for a certain type of encryption algorithm? And what kinds of policy controls need to be applied?

Mature messaging encryption solutions can encrypt based on individual or group sender and recipient, type of file, and by keyword or data type. For example, if the solution is configured to encrypt when SSNs are present, outgoing messages will be scanned for nine-digit numbers and encrypted if a match is detected.

Changes made to the Federal Rules of Civil Procedure (FRCP) in 2006 expanded legal discovery efforts to include electronic messaging.

Logging and archiving are a critical part of IT audit and compliance programs. Changes made to the Federal Rules of Civil Procedure (FRCP) in 2006 expanded legal discovery efforts to include electronic messaging. Organizations should look at the archival capacity of their proposed messaging solution. Consider the storage capacity of the product as well as the tools available to help search for and recover exchanges of interest. Retrieval and holds during an audit or legal e-discovery can be time limited—make sure the archival solution enables for multiple holds, fast searching, and recovery against the most common requirements: keywords; user; and date/time. Log data from the messaging system may also need to be archived for compliance purposes or as part of a larger security information and event management initiative.

If your company has a spoliation policy in place that calls for deletion of logs or email conversations after a certain time, look for a solution with complete wipe-out capabilities. Consider what kind of reports will be required and review how flexible the solution is. Are pre-formatted templates for common reporting available? How customizable is the reporting tool? For example, auditors may want to see data leak report that shows no personal health information (PHI) was sent out of the organi-

SORT YOUR MESSAGING SECURITY CHOICES

MESSAGING SECURITY PRODUCT LISTING

SPONSOR RESOURCES

zation via email or the CIO may want to see usage statistics during a network resizing exercise—can the reporting be adjusted easily for these user needs?

A special consideration for the off-premise solutions—what kind of reporting is in place regarding access to their data center and messaging servers? Are there physical controls such as badge access and cameras? Are unique IDs and hierarchical administrative duties in place? Are logs protected with encryption, file integrity monitoring, and tamper proofing/tamper evidence protection? What is the SaaS providers' policy for producing log and archive data to the company or its agents? Make sure the provider shows proof of the exact certifications they have received to ensure they match the regulatory requirements of the business. The off-premise solution should meet or exceed all compliance and reporting requirements of an in-house one.

Bottom Line: *Email communications are the lifeblood of today's business. Legal and regulatory policies and standards require organizations to protect, archive, and report on email activity. Look for solutions that provide policy-based encryption and robust activity logging. Reporting often serves many different groups; make sure the messaging solution can provide the reporting the business needs. Finally, don't forget compliance and protection needs when opting for an off-premise solution. Confirm that the provider has appropriate logging, access control, and monitoring in place.*‣

Karen Hobert is an IT industry research analyst who focuses on communication, collaboration, content management, and social software technologies. She offers over 20 years of hands-on and market expertise to enterprises planning, designing, and deploying shared information systems.

Diana Kelley is founder of consultancy SecurityCurve and former vice president and service director for the security and risk management strategies service at Burton Group.

SORT YOUR MESSAGING SECURITY CHOICES

MESSAGING SECURITY PRODUCT LISTING

SPONSOR RESOURCES

VENDORS

Messaging Security

Here is a representative list of some vendors offering messaging security products that are either on-premise or offered as a service. Compiled by SearchSecurity.com editors

Aladdin Knowledge Systems
www.aladdin.com

AppRiver
www.appriver.com

Astaro Networks
www.astaro.com

Barracuda Networks
www.barracuda.com

BitDefender
www.bitdefender.com

WatchGuard (BorderWare)
www.borderware.com

CA
www.ca.com

Cisco Systems (IronPort)
www.ironport.com

Clearswift
www.clearswift.com

Clearwell Systems
www.clearwellsystems.com

Cloudmark
www.cloudmark.com

ESET
www.eset.com

eSoft
www.esoft.com

Fortinet
www.fortinet.com

F-Secure
www.f-secure.com

GFI
www.gfi.com

Google (Postini)
www.google.com/postini

Gordano
www.gordano.com

IBM Internet Security Systems
www.iss.net

Mailprotector
www.mailprotector.net

Marshal8e6
www.m86security.com

McAfee
(Secure Computing, SafeBoot)
www.mcafee.com

MxLogic (McAfee)
www.mxlogic.com

MessageGate
www.messagegate.com

MessageLabs (Symantec)
www.messaglabs.com

Microsoft
www.microsoft.com

Microworld
www.mwti.net

Mirapoint
www.mirapoint.com

MXLogic (McAfee)
www.mxlogic.com

PGP
www.pgp.com

PineApp
www.pineapp.com

Process Software
www.process.com

Proofpoint
www.proofpoint.com

RedCondor
www.redcondor.com

Sendmail
www.sendmail.com

Sigaba
www.sigaba.com

Somansa
www.somansatech.com

SonicWALL
www.sonicwall.com

Sophos
www.sophos.com

St. Bernard Software
www.stbernard.com

Sunbelt Software
www.sunbeltsoftware.com

Symantec
www.symantec.com

Trend Micro
www.trendmico.com

Tumbleweed (Axway)
www.tumbleweed.com

Vircom
www.vircom.com

Voltage
www.voltage.com

Webroot
www.webroot.com

Websense
www.websense.com

ZixCorp
www.zixcorp.com

SORT YOUR MESSAGING SECURITY CHOICES

MESSAGING SECURITY PRODUCT LISTING

SPONSOR RESOURCES

TECHTARGET SECURITY MEDIA GROUP

INFORMATION SECURITY®

EDITORIAL DIRECTOR Kelley Damore

EDITOR Michael S. Mimoso

SENIOR TECHNOLOGY EDITOR Neil Roiter

FEATURES EDITOR Marcia Savage

ART & DESIGN
CREATIVE DIRECTOR Maureen Joyce

COLUMNISTS
Jay G. Heiser, Marcus Ranum, Bruce Schneier

CONTRIBUTING EDITORS
Michael Cobb, Eric Cole, James C. Foster, Shon Harris, Richard Mackey Jr., Lisa Phifer, Ed Skoudis, Joel Snyder

TECHNICAL EDITORS
Greg Balaze, Brad Causey, Mike Chapple, Peter Giannacopoulos, Brent Huston, Phoram Mehta, Sandra Kay Miller, Gary Moser, David Strom, Steve Weil, Harris Weisman

USER ADVISORY BOARD
Edward Amoroso, AT&T
Anish Bhimani, JPMorgan Chase
Larry L. Brock, DuPont
Dave Dittrich
Ernie Hayden, Seattle City Light
Patrick Heim, Kaiser Permanente
Dan Houser, Cardinal Health
Patricia Myers, Williams-Sonoma
Ron Woerner, TD Ameritrade

SEARCHSECURITY.COM
SENIOR SITE EDITOR Eric Parizo

NEWS EDITOR Robert Westervelt

ASSOCIATE EDITOR William Hurley

ASSISTANT EDITOR Maggie Wright

ASSISTANT EDITOR Carolyn Gibney

INFORMATION SECURITY DECISIONS
GENERAL MANAGER OF EVENTS Amy Cleary

EDITORIAL EVENTS MANAGER Karen Bagley

VICE PRESIDENT AND GROUP PUBLISHER
Doug Olender

PUBLISHER Josh Garland

DIRECTOR OF PRODUCT MANAGEMENT
Susan Shaver

DIRECTOR OF MARKETING Kristin Hadley

SALES MANAGER, EAST Zemira DelVecchio

SALES MANAGER, WEST Dara Such

CIRCULATION MANAGER Kate Sullivan

ASSOCIATE PROJECT MANAGER
Suzanne Jackson

PRODUCT MANAGEMENT & MARKETING
Corey Strader, Jennifer Labelle, Andrew McHugh

SALES REPRESENTATIVES
Eric Belcher ebelcher@techtarget.com

Patrick Eichmann peichmann@techtarget.com

Jason Olson jolson@techtarget.com

Jeff Tonello jtonello@techtarget.com

Nikki Wise nwise@techtarget.com

TECHTARGET INC.
CHIEF EXECUTIVE OFFICER Greg Strakosch

PRESIDENT Don Hawk

EXECUTIVE VICE PRESIDENT Kevin Beam

CHIEF FINANCIAL OFFICER Eric Sockol

EUROPEAN DISTRIBUTION
Parkway Gordon Phone 44-1491-875-386
www.parkway.co.uk

LIST RENTAL SERVICES
Julie Brown
Phone 781-657-1336 Fax 781-657-1100

REPRINTS
FosteReprints Rhonda Brown
Phone 866-879-9144 x194
rbrown@fostereprints.com

TechTarget
The Technology Media ROI Experts

INFORMATION SECURITY (ISSN 1096-8903) is published monthly with a combined July/Aug., Dec./Jan. issue by TechTarget, 117 Kendrick St., Suite 800, Needham, MA 02494 U.S.A.; Phone 781-657-1000; Fax 781-657-1100.

Proofpoint, Inc.

proofpoint™

See ad page **2**

- Gartner positions Proofpoint in the Leaders quadrant in the 2008 Magic Quadrant for Email Security Boundaries
- Learn more about Proofpoint Encryption, Proofpoint's easy-to-deploy and easy-to-use policy-based email encryption solution.
- Learn how Proofpoint MLX technology provides unrivalled defense against spam.

SORT YOUR MESSAGING SECURITY CHOICES

MESSAGING SECURITY PRODUCT LISTING

SPONSOR RESOURCES

About Proofpoint, Inc.

Proofpoint secures and improves enterprise email infrastructure with solutions for email security, archiving, encryption and data loss prevention. Proofpoint solutions defend against spam and viruses, prevent leaks of confidential and private information, encrypt sensitive emails and archive messages for retention, e-discovery and easier mailbox management. Proofpoint solutions can be deployed on-premises (appliance), on-demand (SaaS) or in a hybrid architecture for maximum flexibility and scalability. For more information, please visit http://www.proofpoint.com