GFI White Paper

Email security: The performance, protection and choice SMBs deserve

GFI®

Contents

Overview 3

Common email security roadblocks 3

The email security checklist 3

Complete protection, day in and day out 4

On-premise email security 4

Online email security 4

Make the choice that's right for you 4

Overview

Email security threats don't discriminate. Whether you're an organization with 50 employees or a global corporation with 50,000, the reality is that spam and viruses can wreak havoc on your business, drain users' productivity and take a major toll on IT resources. SMBs need to make sure they are armed with the best security solutions available – demanding enterprise-class protection paired with fast deployment, ease of management and flexible configuration options. And, all at a price they can afford.

The growing volume of malicious messages is driving organizations to extend security measures to the perimeter – adding layered protection either at the gateway or in the cloud. For SMBs, choice matters. You deserve a solution that performs seamlessly with your email infrastructure today and can be delivered in a model that works for you – via a hosted online solution, on-premise solution or a hybrid of these options.

Are you getting the email security that you deserve?

Common email security roadblocks

Deploying point solutions may have been a quick and easy way to put security measures in place, but you've likely since discovered that the added risk and complexity greatly outweigh the reward.

Do you want to prevent future virus attacks? Or, simply decrease the onslaught of spam? If concerns around your current email security solutions are keeping you up at night, you're not alone. When it comes to administrator headaches, here are some common SMBs email security roadblocks:

- Excessive bandwidth consumption due to high volumes of junk mail
- Email delays due to high volumes of inbound spam
- Lost emails and inability to send/receive emails when the mail server is offline
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
- Ineffective spam detection
- Inefficient or limited user-based quarantine controls
- Excessive time spent managing daily spam digests
- Negative impact on network and mail servers – want to offload spam and virus filtering demands
- Sound familiar? Find out how to eliminate these pain points and make your email security solution work for you.

The email security checklist

If you're ready to take your email security infrastructure to the next level, you want to be confident that you select a solution that meets your security needs of today, and tomorrow. Whatever solution you choose, you should require the following of your go-to vendor:

- Spam filtering: Are inbound and outbound spam attacks stopped with a minimum of 99% effectiveness?
- Antivirus protection: Does the solution deliver stellar defense against viruses, trojans, spyware and other malicious threats?
- Global attachment filtering: Is there built-in and/or customizable support for filtering varied attachment types?
- Simple administration: Do administrators have anywhere, anytime access and control via a web-based interface?
- Global disclaimers: Can you easily create rules for global disclaimers for outbound emails?
- Rapid deployment: Is the solution able to be up and running instantly, delivering immediate results?
- System compatibility: Is the solution easily integrated with any email infrastructure and/or operating system?

- Reporting: Is there a wide-range of pre-defined reports which can be customized by system, group or user?
- Scalability: Will the solution cost-effectively grow as your organization's employee base and infrastructure grow?

Complete protection, day in and day out

At GFI, we've built a business on delivering powerful, award-winning solutions specifically designed for SMBs. We pride ourselves on providing products that are built on world-class technology, are easy to use and make your job easier. The GFI email security solutions meet all three criteria – and more.

The GFI email security solutions deliver complete email protection, defense and continuity– within minutes. The product line was created to help address SMBs' needs for more comprehensive functionality, ease of use and deployment flexibility – providing the performance and choice you deserve. The GFI email security solutions give you the flexibility to choose the deployment option that's best for you – whether a hosted online solution, on-premise solution or a hybrid of these options.

On-premise email security

Commercial-grade hardware or VMware virtual Linux-based appliance, MailEssentials Complete Appliance™ provides layered protection at the gateway. Powered by the world-class Cloudmark™ anti-spam engine and the VIPRE® Antivirus engine, you benefit from proven technology built on server-class hardware. A true plug-and-play solution, MailEssentials Complete Appliance delivers unrivaled detection right out of the gate – and gets you up and running in less than 15 minutes.

Online email security

Comprehensive security delivered via a hosted online solution. MailEssentials Complete Online™ delivers layered security and anti-spam/antivirus functionality, which can be implemented as a replacement for existing anti-spam/antivirus solutions or as part of a layered hybrid deployment with an on-premise solution. MailEssentials Complete Online delivers proven anti-spam and antivirus detection, combined with attachment filtering, email continuity and optional email archiving to safeguard your mission-critical communications.

Make the choice that's right for you

With the proliferation of spam and viruses showing no signs of reprieve, you deserve an email security solution that keeps threats at bay, keeps users productive and keeps your business up and running – simply and reliably. Don't settle for anything less.

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com

For a full list of GFI offices/contact details worldwide, please visit http://www.gfi.com/contactus

GFI 2369 oct11

Disclaimer

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.