

How to Improve Network Security without Extra Staff or Busting Your Budget

Contents

Network Security: The "No-Win" Situation for Mid-Sized Companies.	2
You Will Get Stung.....	3
Why Existing Technologies Don't Work for Most SMBs	4
The Mid-Market Solution: Network Protection on Demand	5
Network Security and Compliance Made Easy	6
SaaS Approach Changing the Face of IT	7
About Alert Logic.....	9

Alert Logic, Inc.

1776 Yorktown, 7th Floor, Houston, TX 77056 | 877.484.8383 (toll free) | 713.484.8383 (main) | 713.660.7988 (fax) | www.alertlogic.com

Alert Logic and the Alert Logic logo are trademarks, registered trademarks, or service marks of Alert Logic Inc. All other trademarks listed in this document are the property of their respective owners.

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, ALERT LOGIC, INC. PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of Alert Logic, Inc., except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of Alert Logic, Inc. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. Changes or improvements may be made to the software described in this document at any time.

© 2010 Alert Logic, Inc., all rights reserved.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Invision Security and Alert Logic are trademarks or registered trademarks of Alert Logic, Inc. or its subsidiaries in the United States and other jurisdictions. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

Network Security: The “No-Win” Situation for Mid-Sized Companies

The responsibilities of network administrators and security managers at mid-size companies today can seem like an “no-win” situation. They are accountable for securing their organization’s network technologies with limited budgets and even more limited staff resources. Meanwhile, their network technologies are constantly evolving just as new and more deadly threats emerge almost daily. They must also create and maintain security policies and ensure that these policies are carried out to demonstrate regulatory compliance and avoid liability risks for their companies

Finding solutions to help manage these challenges creates another dilemma for IT directors and managers. The sheer number and variety of network security products and services can be overwhelming—not to mention the cost and effort of implementing these vendor offerings.

As described by eWeek columnist Larry Seltzer: “Just imagine if you were actually to implement all the security products that you can’t, of course, do without,” he says. “There’d be no money left for lunch, let alone the actual applications to do work with. And all of them create some new administrative burden for which you probably don’t have bandwidth... How can you sleep at night knowing you’re exposed due to your dereliction in not implementing these critical security systems?” ⁽¹⁾

However, throwing up your hands in frustration and doing nothing is not an option because the internal network security risks is simply too great.

You will Get Stung

A recent Information Week survey indicated that even though most IT professionals believe they have their security situation under control, recent incidents counter that assumption. One in particular – the so-called Zotob worm – spread to companies not through widespread Internet infections but rather through localized “explosions” inside business IT environments.

As one expert noted, “Organizations have been secured behind their ‘impenetrable’ firewalls, filtering all e-mails and stripping all executable content. Businesses felt secure and confident that no attack could reach them. The blow from the inside [from Zotob] was all the worse for being totally unexpected.” (2)

The bottom-line: Although many companies have invested in firewalls, anti-virus and other perimeter defenses, they remain more vulnerable than ever to targeted inside threats that have become more costly. Yesterday’s “blended threats” have become the “borderless” threats of today and tomorrow. And while security breaches at smaller businesses don’t grab headlines like those on Fortune 500 companies do, it does not mean they are any less devastating. As one major research firm indicates:

- 40 percent of SMBs who manage their own network security and use the Internet for more than e-mail will experience an Internet attack.
- SMBs that fail to incorporate security throughout their network will experience both a financial loss and a loss of reputation

Given these odds, mid-size businesses must develop and implement a plan to deal with security issues—inside as well as outside their network perimeters.

Why Existing Technologies Don't Work for Most SMBs

According to Forrester Research Inc., most companies secure their networks with point products from at least three different vendors. This leads to management complexity, increased costs, interoperability snags and a limited ability to enforce security policies. More recently, an additional category of point products emerged. Known as unified threat management appliances, they focus on perimeter security as the sole method for protecting networks. However, the reality for medium-size businesses is that network threats have swiftly evolved where they can easily bypass perimeter security solutions.

For example, firewalls fail to eliminate all threats because they cannot adequately detect all malicious traffic and miss attacks introduced by e-mail, roaming users or third-party connections. Traditional intrusion detection and prevention products fail to eliminate as many as 80 percent of network threats because they have to be “dialed down” to avoid generating too many false alarms. Finally, Security Event Management products, or SEMs, promise to eliminate false positives by correlating intrusion detection alarms with security log files, but they typically fail to include security knowledge that is built-in and constantly updated. This requires IT managers to develop their own rules when new threats emerge – a situation that no one has the resources to manage.

In reality, conventional network protection solutions are difficult to manage and costly to operate. They often come from different vendors (or from acquisitions by a single vendor) and prove incomplete and fragmented. Not only are these products time-consuming to install, but they also require IT personnel to monitor, fine tune and maintain them. Thus, the typical approach to network protection presents a cluttered and confused vendor landscape, offering scores of complex and fragmented products. These prove to be too costly and demand precious time, requiring a level of expertise that most small to mid-size companies simply cannot afford.

Given this frustrating dilemma, network administrators and security managers are seeking an additional layer of network protection that:

- Deals with threats from inside their networks
- Is designed to compliment perimeter defenses
- Leverages network security best practices, i.e. they don't have to reinvent the wheel
- Delivers proven technology that not only detects threats and exposures but also protects the network by shutting down threats quickly and effectively
- Offers a solution that is simple and affordable to deploy and maintain – without requiring extra staff or breaking their IT budgets

The Mid-Market Solution: Network Protection on Demand

Based on these needs, Alert Logic, based in Houston, Texas, has introduced an innovative network security solution that leverages a Software-as-a-Service (SaaS) platform to deliver on-demand protection to mid-sized companies. The Alert Logic solution is priced as a subscription service, eliminating the high cost and complexity of deploying and managing disparate network security point products.

Alert Logic's unique SaaS platform delivers solutions on-demand – featuring rapid deployment, zero maintenance and no hardware or software costs. Our solution provides intrusion protection, vulnerability management and IT compliance automation that enables businesses to detect and contain network threats, discover and correct vulnerabilities and helps ensure compliance with policies and regulations. As a result, Alert Logic customers benefit from easy, effective and affordable network protection.

Network Security and Compliance Made Easy

In developing these solutions, Alert Logic has responded to the needs of mid-sized businesses, such as GSI Commerce in King of Prussia, Pennsylvania. Overseeing hundreds of servers across their two datacenters, GSI enables retailers, branded manufacturers, entertainment companies and sports organizations to operate e-commerce businesses.

Wyman Lewis, Director of Information Security for GSI, points out that Alert Logic's on-demand solution provides a critical component in demonstrating compliance with the PCI Data Security Standard. Supported by major credit card issuers, including VISA, MasterCard, American Express and Discover, PCI-DSS provides guidelines and requirements for safeguarding sensitive customer and transaction data.

"Compliance with PCI-DSS is an absolute must for our business," Lewis emphasized. "Part of our IT systems audit includes a requirement that we have security controls in place for our intrusion defense systems and that we can demonstrate that we monitor these systems around the clock," he said. "Using Alert Logic's managed threat defense solution in conjunction with our other security measures helped us to demonstrate compliance with PCI and pass our audit."

SaaS Approach Changing the Face of IT

According to the IT research firm Gartner, the emergence of Software-as-a-Service solutions is an important evolutionary step forward in IT application architectures. “The dysfunction of the client/server era is driving alternative approaches to IT. SaaS is the most apparent alternative. There is now a widespread consensus among the movers and shakers of the IT industry that SaaS is an important and meaningful issue.” (3)

For example, the Philharmonic Center for the Arts in Naples, Florida, is a non-profit, donation-driven organization. But they knew that any security incident would be extremely detrimental to the center’s image and livelihood. “People who donate their money expect a certain amount of discretion. A security incident would look very bad,” said Anthony Garmont, the Philharmonic Center’s network administrator.

Because of limited personnel resources, Garmont required a solution that was easy to deploy and manage. Alert Logic’s SaaS-based model offered a unique combination of low cost and low management overhead. “We didn’t have the resources to deploy the solution and keep it running. We required a hosted solution and a threat monitoring service,” he said.

Another customer, the Harris County Hospital District in Houston, Texas, spends about \$600,000 to \$700,000 annually on their IT security staff, roughly double what it spent five years ago, according to CIO Tim Tindle. The sophistication and expense of their technology has increased as well, and Tindle has been working hard to find ways to save the district money. At his direction, Harris County began outsourcing its intrusion-detection needs to Alert Logic rather than manage them in-house. By relying on Alert Logic’s Network Protection On-Demand, Tindle estimates that his organization has saved up to \$900,000 per year. (4)

With the introduction of Alert Logic’s SaaS platform for network security, there is no reason to incur the cost and hassle of hardware and software to gain the extra internal security that mid-size businesses need to protect their networks. Alert Logic’s SaaS platform is designed for rapid deployment, zero maintenance and maximum ease of use for our customers and partners.

Alert Logic customers simply deploy an appliance that plugs into a network switch – no agents to deploy on desktops, servers, or endpoints of any type. In addition to the appliance, all other Alert Logic solution components, such as the management portal, reporting engine, historical data repository and configuration data, all reside in the Alert Logic data center, not on the customer network. All you need to access the application is a web browser. As a result, virtually no customer time is spent deploying, configuring, maintaining or upgrading our solution.

The Alert Logic SaaS delivery platform consists of three major components which enable previously unheard of levels of ease and effectiveness:

- The **network appliance** is responsible for monitoring network traffic for suspicious behavior, scanning network assets for vulnerabilities, passing threat and vulnerability related data to our data center for further analysis and initiating defensive actions to block or contain confirmed threats.

- The hosted software in our data center analyzes, correlates and archives threat and vulnerability information from all appliances across all Alert Logic customers around the globe. It supplies all real-time and historical trending and reporting via the customer web portal that is accessible from any browser.
- The Security Operations Center is staffed by certified security experts who can provide optional professional services to extend the value of our solutions. Optional services include 24x7 network threat monitoring where our security analysts monitor your network for security threats, notify you when incidents occur and help you take prompt, effective defensive actions.



About Alert Logic

Alert Logic's patented solutions are the smartest choice for over-regulated businesses with underfunded IT departments to secure networks and ensure compliance. Its cloud-powered managed solutions combine intrusion protection, vulnerability assessment, log management and 24x7 threat surveillance, and are designed to maximize revenue and profit opportunities for service providers and hosting partners. Enterprises experience a solution that addresses network security and compliance requirements at a low price point, with little dependency on IT resources. Alert Logic is based in Houston, Texas and was founded in 2002. More information about Alert Logic can be found at <http://www.alertlogic.com>.

[CONTACT US](#)

References:

- (1) Larry Seltzer, eWeek Security Center Editor
- (2) "The Threats Get Nastier: Information Security Survey" InformationWeek, August 29, 2005
- (3) Gartner SMB Spending Report, 2005
- (4) Healthcare IT News, "Outsourcing Security Saves Texas Hospital \$1 Million", June 1, 2006