

I D C V E N D O R S P O T L I G H T

The Time Is Now for Controlling Outbound Content

February 2006

Adapted from *Worldwide Outbound Content Compliance 2005–2009 Forecast and Analysis: IT Security Turns Inside Out* by Brian E. Burke, IDC #34260

Sponsored by SonicWALL Email Security

Information security solutions have traditionally focused on addressing external threats to corporate networks and endpoints — viruses, hackers, worms, trojans, spam, blended threats, and, most recently, spyware. In turn, enterprises have deployed an expanding array of perimeter security solutions to protect against external threats. Today, however, emerging threats to corporate security come from inside organizations. These threats arise from employees and partners who violate, either accidentally or intentionally, government and industry regulations or corporate policies and best practices designed to prevent loss or leakage of intellectual property and other confidential information. This document examines the threat environment for what IDC calls "outbound content compliance," or OCC, as well as other market drivers for OCC solutions, and shows how technology that monitors, secures/encrypts, filters, and blocks outbound content can play a key role in enforcing regulatory and corporate policy compliance in midmarket companies. The document also looks at the role of SonicWALL Email Security, a provider of email security solutions, in this strategically important market.

The Daunting Challenge of Insider Threats

For years, organizations have focused security efforts on external threats posed by the explosive growth of viruses, spam, blended threats, and spyware. The situation is beginning to change, especially in light of new information-intensive government and industry regulations that require organizations to protect the integrity of customer and employee personal information and corporate digital assets. Because noncompliance may result in substantial fines and executive liability, organizations are realizing that information leakage by insiders is a threat that can no longer be underestimated.

Addressing the insider threat, however, is turning out to be a complex challenge. The increasing use of corporate email, Web email, instant messaging, peer-to-peer (P2P) file sharing, and other channels for distributing data, along with the proliferation of mobile devices that allow employees to carry sensitive information outside the organization's boundaries, makes the control of outbound content a substantial challenge. Email remains the dominant form of electronic communication, and it is therefore the primary exit point of sensitive information and intellectual property. IDC believes email will remain the key business collaboration tool because of its ubiquity, user familiarity, offline capabilities, and integration with other business applications.

Outbound content compliance includes solutions that monitor, secure/encrypt, filter, and block outbound content contained in email, instant messaging, P2P file sharing, file transfers, Web postings, and other types of messaging traffic. OCC solutions play a key role in enforcing corporate

governance, which is defined by IDC as a combination of complying with both external regulatory requirements and internal corporate policies and best practices.

Public Governance Drivers

Government and industry regulations have placed unprecedented pressure on corporations to secure the use of their electronic communications. A wide range of communication channels available to employees, such as instant messaging, chat, Webmail, and P2P file sharing, represents a serious threat to customer information and can expose organizations to reputation, compliance, legal, and financial risks. Regulators now recognize electronic documents and messages as critical records of business and are mandating the proper management of these records.

Contrary to popular belief, regulatory compliance in the United States is mandated not only for firms in heavily regulated industries such as financial services, telecommunications, and pharmaceuticals. All United States-based businesses (both private and publicly listed firms) face a multitude of records management requirements. For example, organizations that manage patient health information, social security numbers, or credit card numbers are being forced by government and industry regulations to implement minimal levels of security to address leakage of personal information. The loss of confidential personal information can materialize into compliance infractions, lawsuits from customers and/or patients, potential identity theft, and significant and often irreparable harm to an organization's credibility and reputation.

Examples of pressing regulations and their potential penalties are as follows:

- **The Health Insurance Portability and Accountability Act (HIPAA)** has two major objectives: making healthcare transactions simpler through the use of standards, common code sets, and unique health identifiers; and protecting the confidentiality of patients' health information. The act applies not only to healthcare service providers but also to all healthcare entities, including insurance companies and government agencies. The HIPAA Privacy Rule defines administrative, physical, and technical safeguards for covered entities (CEs), which include standards for keeping the privacy of Electronic Protected Health Information (ePHI). These standards deal with several requirements that are most relevant for OCC solutions, including the implementation of policies and processes on issues such as assigning and controlling access to ePHI; reporting incidents; keeping track of ePHI moving in, out, and within CEs; and securing the transmission of ePHI over networks. Noncompliance with the Privacy Rule requirements may carry criminal penalties of up to \$250,000 in fines and jail time of up to 10 years.
- **The Gramm-Leach-Bliley (GLB) Act** was passed to protect customer information maintained by (or on behalf of) financial institutions from loss, unauthorized access, or misuse. The GLB Safeguard Rule requires all financial institutions to "develop, implement and maintain a comprehensive written information security program that contains administrative, technical and physical safeguards" to protect customer "nonpublic information", or NPI, (e.g., account numbers and details, social security numbers, credit card numbers, and so on). It mandates different requirements for safeguarding NPI, including the establishment of access controls of IT systems on which NPI is stored; encryption of electronic records; and monitoring of systems to detect intrusion attempts and attacks. Noncompliance with the Safeguard Rule may carry severe penalties in fines and prison terms of up to five years for individuals.
- **The Sarbanes-Oxley (SOX) Act** was legislated in the United States in light of high-profile corporate scandals such as those of Enron and WorldCom. Defining new requirements regarding the financial management of publicly traded companies, the act is aimed at ensuring the integrity and the accuracy of reporting and preventing accounting errors and wrongdoings that may affect a company's shareholders and the general public. SOX lays responsibility on CEOs and CFOs, who must certify that their companies' financial reports are complete and do not contain any

inaccurate or misleading statements. Noncompliance may lead to fines of up to \$5 million for individuals and up to \$25 million for entities and prison sentences of up to 20 years. Section 404, which describes management's responsibility for establishing "internal control over financial reporting," is one of the key sections of SOX in terms of outbound content compliance. Under this liability, companies are required to "provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the registrant's assets that could have a material effect on the financial statements."

Many organizations are still struggling to understand these and other regulations that potentially affect their organizations and what that means from a business perspective. In today's increasingly information-intensive businesses, technology is becoming a key part of strategic compliance initiatives to ensure sustainability of compliance-related processes, mitigate risk, and manage ongoing costs.

Government and industry regulations are impacting the way organizations deal with information security and staffing in many different ways. Increased levels of network monitoring and reporting are very close to the top of the list of user concerns. IDC believes this is clearly driven by the pressure government and industry regulations have placed on corporations to secure the use of their electronic communications. We expect the risk of compliance infractions and lawsuits from customers and/or patients to continue to force organizations to implement network monitoring and reporting technologies.

Private Governance Drivers

The growing awareness of outbound content compliance has been recently catalyzed by a series of corporate scandals in which customer records, confidential information, and intellectual property were leaked. As the vast majority of cases demonstrate, however, such breaches are often not the result of malicious wrongdoing but rather employees who unknowingly put their companies at risk. These breaches may occur as employees send email messages that contain files or content they are not aware is confidential. Another example is employees delivering confidential files to their Web-based email boxes (or copying files to mobile devices) and thus exposing them to untrusted environments.

Protecting corporate intellectual property has also moved up the priority list of many IT departments. Organizations of various industry and company sizes are extremely concerned with protecting patents, trademarks, brands, trade secrets, designs, architectures, copyrights, algorithms, software code, hardware schematics, inventions, business processes, and many other corporate assets. Gone are the days in which intellectual property and corporate secrets were kept safe in locked cabinets behind guarded doors. Today, nearly all corporate information exists in electronic form, accessible to almost any employee.

Additionally, email has become the de facto filing system for much of this information, making it even more critical to protect the outbound flow of messages. The risks of inadvertent or deliberate disclosure of confidential information and intellectual property range from legal exposure to competitive disadvantage. Companies can risk losing serious dollars, for example, when design documents and source codes are posted to Internet message boards or emailed outside the organization.

Examples of such intellectual property loss include:

- In December 2004, Apple filed a lawsuit against three members of its Apple Developer Connection network who allegedly distributed a prerelease version of "Tiger," the company's next major Mac OS X release, through the P2P file-sharing network BitTorrent.

- In February 2004, portions of the Windows 2000 and Windows NT 4 source code databases were leaked, apparently by one of Microsoft's outsourcers for code development.
- In October 2002, an internal Dell Computer document regarding Dell's plan for entering the PDA market was leaked and posted on a French Web site.

Loss of Customer Records and Confidential Information

A privacy failure, even a merely perceived failure to protect customer data, can result in loss of consumer trust, affect customer retention, and cause significant damage to brand and company reputation. Online privacy practices must be consistent with offline irreparable damage to brand, reputation, consumer retention, and customer-focused business strategy.

Customer records and/or confidential information have been leaked in several high-profile incidents, including:

- Data collector ChoicePoint mistakenly gave private information on 145,000 U.S. residents to identity thieves. ChoicePoint reached an agreement in February 2005 with 19 state attorneys general to tell the 145,000 potential victims that identity thieves may have gained access to personal information such as social security numbers and credit reports.
- In September 2004, a former help desk employee at Teledata Communications pleaded guilty to a scheme to steal and sell 30,000 customers' consumer credit reports.
- In June 2002, parts of Cisco's quarterly report were leaked via email, which forced the company to publish the report ahead of its scheduled financial release.

Although in some cases email usage policies were established, violations still occurred, which demonstrates that policies alone are not enough. Organizations are realizing that to prevent such incidents from happening, dedicated solutions that provide better control and enforcement mechanisms over electronic communications are becoming essential.

What to Do About OCC

IDC demand-side research indicates a growing concern with internal security threats in companies of all sizes — which isn't surprising. In fact, several data points lead IDC to believe that internal security threats will continue to rise:

- According to the latest CSI/FBI *Computer Crime and Security Survey*, 80% of respondents reported security incidents involving insider abuse in 2004 (up from 64% the previous year).
- According to IDC's 2004 *Security Survey*, 31% of organizations have terminated employees or contractors for internal security violations.
- According to IDC's 2005 *Security Survey*, employees following security policies was rated as the second-highest security challenge that organizations will face over the next 12 months.

Despite these market drivers, however, there remains an OCC adoption lag among some segments of the market. The largest challenges to adoption are limited resources and budgets and unawareness of the problem. IDC believes that outbound content compliance is a key organizational governance and control issue and must be managed from the top of the organization and incorporated in all long-term compliance strategies — regardless of company size.

We strongly urge companies to focus on implementing solutions that address a broad spectrum of needs, including:

- Controlling access to and usage of confidential and sensitive information
- Preventing confidential and sensitive information from leaving an organization
- Protecting documents outside the corporate firewall
- Ensuring compliance with government and industry regulatory requirements such as GLB, HIPAA, and SOX
- Educating users about their responsibility in reducing and preventing the unwanted leakage of risky information
- Enforcing policies around content creation, editing, sharing, publishing, and distribution

Specific actions companies should take to address the challenges of email compliance include the following:

- Design and document policies and controls in specified business areas such as privacy, security, and finance
- Automate compliance processes that are repeatable in nature and integrate those processes into day-to-day activities when possible
- Ensure and certify the accuracy of information as well as identify/resolve exceptions that indicate possible noncompliance
- Establish and adhere to strict requirements for information access and record retention
- Protect the long-term integrity and availability of retained information from isolated IT system failures, local outages, or regional disasters

As a starting point for developing policies and controls specific to email content, organizations should answer the following questions:

- How can we determine if an email contains personal, proprietary, or other nonpublic information?
- How do we monitor for such information leaving the organization?
- What actions do we want to take to either prevent or protect these outgoing messages?

Considering SonicWALL Email Security

SonicWALL Email Security is a leading provider of email security and compliance solutions that protect organizations against threats such as spam, phishing, and viruses; identify and enforce regulatory and corporate compliance policies; and enable consolidation of email infrastructure.

SonicWALL Email Security protects more than 1,700 enterprise customers, including HealthEast Care System, Heidrick & Struggles International Inc., OfficeMax, Pier 1 Imports, SAP, and Wyndham International.

SonicWALL Email Security offers the following OCC products:

- SonicWALL Email Security Gateway is available as an appliance or software and enables businesses to establish compliance policies and provides the power to easily enforce these policies across an organization or specific groups in addition to providing inbound threat protection.

- SonicWALL Email Security Compliance Module provides unique tools for enabling compliance, including predefined and custom record matching, compliance dictionaries, and predefined compliance policies and reports.
- SonicWALL Email Security PGP Appliance E500 enables powerful and easy-to-deploy gateway-to-end-user encryption.
- SonicWALL Email Security provides archiving offerings through both on-box SonicWALL Email Security archiving and off-box archiving through its partnership with AXS-One.

SonicWALL Email Security OCC products provide:

- **Streamlined manageability** creates powerful inbound and outbound policies easily through SonicWALL Email Security's Web-based administrative interface. The multilingual centralized management console enables unified administration of all systems, delegation of responsibilities, and at-a-glance reporting.
- **Intelligent identification** effectively identifies possible compliance violations and confidential emails through rigorous content analysis of messages applied to specific LDAP-based roles, groups, or senders.
- **Monitoring and reporting** allow administrators to inconspicuously view compliance violations via notification emails, approval boxes, blind copy to administrators, and compliance reports.
- **Integrated remediation** utilizes a range of remediation options once noncompliant or confidential email has been identified. Remediation options include:
 - **Stop/review/notify.** Messages can be stopped or placed in an approval box pending review. Senders or administrators can be notified of violations.
 - **Archive.** All or selected messages can be archived either within SonicWALL Email Security Gateway or routed to a corporate email archive.
 - **Encryption.** STARTTLS SSL-for-email secures email between business partners. SonicWALL Email Security partnerships with PGP and Voltage provide a unified solution for secure email delivery to seamlessly encrypt, decrypt, and digitally sign confidential email messages.

SonicWALL Email Security recently announced new compliance features for intelligent identification and integrated remediation options to SonicWALL Email Security Gateway for businesses to meet the increasing challenges of compliance requirements, whether they are corporate governance or regulatory compliance measures such as HIPAA, GLBA, and SOX.

SonicWALL Email Security enables business enterprises to achieve critical inbound and outbound email compliance and preserve corporate security — without complexity and without requiring another separate appliance. These features should appeal particularly to organizations with budget and resource constraints.

Challenges

To continue its success, however, SonicWALL Email Security must work to address certain key misconceptions in the market. The publicity around SOX and the rest of the SEC and NASD regulations, for example, has generally crowded out the message that regulatory compliance permeates both publicly listed and private companies. SonicWALL Email Security's messages should focus on the following:

- The need for user firms to have content compliance policies in place because regulations not only cover financial reporting and auditing requirements but also cut across industries (e.g., OSHA and ADA) and records retention requirements that may span 2 to 30 years
- The continuing need to raise awareness that even private firms have to comply with financial reporting and the associated record retention requirements
- The fact that in litigation and email discovery, email is not necessarily admissible in court and must pass the requirements to the "hearsay rule" on evidence

Conclusion

IDC believes that outbound content compliance will be a strong growth area over the next five years, driven by several different convergent forces. But the bottom line for midmarket firms is, OCC is needed for good governance in both the public and private arenas.

In addition to normal budgetary constraints, however, the greatest challenge to companies in terms of protecting customer records, confidential information, and intellectual property will come from unstructured content. Electronic documents, emails, instant messages, and other digital content are either covered today or will soon be covered under one or more regulations and can certainly be included as part of evidence discovery.

Although financial, employee, and customer records are usually safe in a secure database, unstructured content is frequently scattered across hundreds or even thousands of email and file servers. Unlike the records managed in the database, this unstructured content is typically not well organized, not easily found, controlled only under ad hoc security and access control policies, and generally not maintained in a way that provides any kind of context for the embedded information.

Whether with regard to regulatory compliance or discovery, the unstructured content in midmarket companies represents a time bomb waiting to go off. To the extent that solutions from SonicWALL Email Security help diffuse this time bomb, the company should enjoy continued success.

A B O U T T H I S P U B L I C A T I O N

This publication was produced by IDC Go-to-Market Services. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Go-to-Market Services makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

C O P Y R I G H T A N D R E S T R I C T I O N S

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the GMS information line at 508-988-7610 or gms@idc.com. Translation and/or localization of this document requires an additional license from IDC. For more information on IDC visit www.idc.com. For more information on IDC GMS visit www.idc.com/gms.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com