Building a better spam trap: Choosing the best defense for tomorrow's merging email threats

Organizations will need an integrated, multi-layered approach to defend against new and evolving email threats.

Abstract

The nature of spam is changing, incorporating a wide spectrum of email-borne attacks that can stifle productivity, infect corporate networks and undermine corporate reputation and regulatory compliance. In response, the nature of anti-spam defense is changing as well. Single-point solutions such as Sender IP Reputation should ideally represent only a single layer in a multi-layered defense.

Dell™ SonicWALL™ Anti-Spam/Email Security solutions apply an integrated multi-layered approach to protect organizations from inbound spam, phishing and email-borne malware, as well as from outbound data leaks and botnet transmissions.

The Evolving threat of spam

Over the years, spam has evolved from an annoyance to a serious threat to productivity and security. Inbound and outbound email threats continue to proliferate at exponential rates. Simultaneously, email-borne threats are also becoming more advanced. Increasingly, these more advanced threats blend spam, phishing, spyware, viruses, Trojans and other malware, into sophisticated blended attacks. As spam has evolved, traditional anti-spam systems have correspondingly evolved into more powerful and comprehensive email security solutions.

The expanding challenge

Inbound spam volume continues to increase significantly, with no signs of abating. For example, in 2005, an average of 30 billion spam email messages were sent daily. By 2010, that average has multiplied six times to 180 billion spam messages. Assuming the effectiveness of a company's spam filter had remained the same that equates to a six-fold increase in spam reaching inboxes over a five-year period.[1]

The incentive driving this global spam industry is profit. Despite its catastrophic impact on business productivity and network performance, and despite even high-profile prosecutions of spammers, spam still works. In response rate, but was still able to maintain a six-figure income by delivering tens of millions of emails a day[2]. In another case, a one-month spam campaign for an herbal supplement took in over half a million dollars in sales[3]. In "pump and dump" schemes, spammers buy stock, generate spam-bot mailing drives to pump up share volumes, and then dump the stock at a profit.

Coordinated industry efforts only temporarily stem this ever-growing tide. In 2008, for instance, industry pressure led to the upstream disconnection of the Internet Service Provider (ISP) McColo, causing an instant worldwide drop in spam by as much as 75%[4]. However, spam operations merely relocated to other ISPs, and spam volumes quickly recovered to their earlier levels.

Meanwhile, IT departments are left with having to allocate more resources to clean out swamped mailboxes, maintain key business communications and undo the damage done by newly emerging email-borne threats.

Multi-layered attacks

Spam is constantly getting more sophisticated because spammers are typically technically savvy and early adopters of innovative technology. For example, spammers created content-based tricks such as gibberish words and phrases, white-on-white text, tiny fonts, word salad, optical illusions and other advanced techniques in an attempt to deceive spam filters. More recently, spammers have focused their attention on IP reputation systems. As these types of systems have grown in popularity, spammers and hackers have increasingly focused their attacks on compromising legitimate mail severs at companies with good reputations, and cracking Web mail accounts at ISPs, such as Yahoo or Gmail. This allows spammers to avoid traditional IP reputation systems by sending bad

[1] SonicWALL Threat Research Team

[2] USA Today, May 2006
[3] Infoweek.com, August 2006
[4] [Washington Post, November 2008 [http://voices.washingtonpost.com/securityfix/2008/11/spam_volumes_drop_by_23_after.html]

mail from the servers of good businesses that have been compromised.

Phishing scams pose another significant threat. Distinct from spam, phishing emails are specifically created to imitate legitimate emails, often copying actual corporate communication. Billions of phishing emails are sent out every month, and these can lead to identity theft, security breaches, and financial loss and liability. Leveraging social engineering techniques to evade corporate security systems, criminals gain network access and steal confidential corporate data and financial assets. With the unwitting cooperation of an employee, network defenses such as firewalls, Intrusion Detection and Prevention systems and secure identification cards can become ineffective. Because phishing emails are designed to look like legitimate business correspondence, they consistently elude standard spam filters, and email policies alone are an insufficient defense. Phishing defense requires specific analysis, identification and handling.

Backscatter or NDR (non-deliverable-return) spam are messages that look like returned emails that could not be delivered to their intended sender. Spammers spoof such messages, attempting to bypass the email security system.

Directory Harvest Attacks (DHAs) are exhaustive "brute force" attacks. DHAs bombard mail servers with emails sent to variations of possible email addresses to check which ones bounce and which are legitimate. The extensive volume of a DHA strains email infrastructures. In addition, DHAs acquire information on email addresses for the company to be used later in follow-up, targeted spam, virus and phishing attacks.

Denial of Service (DoS) attacks are malicious attempts to bring down email infrastructures. By sending an enormous volume of email traffic into an organization at a coordinated time, attackers attempt to overwhelm the network and email infrastructure, bringing email to a complete stop.

Outbound threats

Outbound threats are also becoming a top priority for IT administrators and CEOs, based upon fears of regulatory non-compliance and the leakage of sensitive intellectual property or confidential information. All organizations are faced with the challenge of meeting email compliance requirements, whether regulatory compliance from government legislation, such as HIPAA, GLBA, or SOX; industry standards; or corporate compliance, such as preventing offensive emails or protecting intellectual property.

Data leaks are not limited to malicious acts; most confidential data leaks are likely due to employee carelessness. With these various compliance requirements, encryption and archiving options alone are not enough. Organizations must have robust policy management and enforcement options to meet the range of compliance needs.

Additionally, as much as 25% of computers on the Internet are estimated to be infected with botnets or zombies[5], which can infect corporate mail servers and generate outbound attacks. A botnet is a collection of compromised computers (zombies) that run under a common control structure. A computer can become a zombie through downloading a virus or Trojan in the form of executable attachments to emails and downloads on Web sites.

Zombies are directed by a "botmaster" to send spam, phishing, viruses and other malware from the compromised system. Emails sent from zombie machines can appear to originate from the victim's computer and will steal computer resources to send the emails, which are often sent out in mass. These zombie machines can damage a company's reputation and require costly resources to purge the malicious code. There are an estimated 70 Million[6] to 150 Million[7] zombies active around the world. Infected companies face being blacklisted by their ISPs, and subsequently inability to send email.

The changing approach to anti-spam

A single-technology approach to anti-spam is no longer sufficient. No single analytic technique is enough to stop the constantly morphing forms of spam. Even multiple techniques, if they are not updated regularly, are not enough to keep spam at bay for long. Moreover, rigid scoring often ends up blocking email that users actually want to receive. Email security solutions now require a sophisticated blend of technologies focused on both inbound and outbound protection.

Conventional inbound methodologies

One recently adopted industry approach to anti-spam is Sender Identification (Sender ID). This technique authenticates the IP address of an external email server that is making an inbound connection to the network to see if it matches the domain name of the email sender. This assumes the sender has published a Sender Policy Framework (SPF) record and that the record is correctly set-up. There are two primary issues with this technique. First, spammers can create valid SPF records. Second, most companies do not like the restrictions Sender ID places their ability to have email sent on their behalf. For example, using a third-party vendor to send email messages to customers could cause an SPF failure.

Another inbound technique often attacked by spammers is Bayesian content analysis, which infers the

---

[5] Vint Cerf [http://news.bbc.co.uk/2/hi/business/6298641.stm]
[6] InformationWeek, October 2006 [http://www.informationweek.com/news/security/cybercrime/showArticle.jhtml?articleID=193105252],
[7] Vint Cerf [http://news.bbc.co.uk/2/hi/business/6298641.stm]

probability of an email being spam based upon combinations of specific individual words. Bayesian analysis can be a very powerful, but in practice, there is no universal definition for spam content, as each person has a different degree of tolerance and curiosity. Some companies try to train a Bayesian filter based on an organization's email. This opens the door to Bayesian poisoning attack by spammers who place "good" content in spam messages in an attempt to skew the Bayesian scoring system. So while Bayesian content analysis is an excellent technique, by itself is does not meet the challenge of defending against today's pervasive spammers.

Conventional outbound methodologies

It is just as important to monitor and control outbound email as inbound email. Unfortunately, many small and midsize businesses choose to forego deploying outbound email protection. This carries with it the highest risk of compromise of private or proprietary information. To lower that risk, many organizations have established and communicated written email usage policies. While these written policies are a step in the right direction, best practice is to automatically analyze and enforce outbound email polices in order to ensure compliance with internal and external regulations.

The Dell SonicWALL advantage

While most businesses now have some type of anti-spam protection, many still struggle with limited effectiveness against emerging email threats, and a total cost of ownership much higher than they expected.

The Dell SonicWALL Email Security Series is available as a hardware appliance, virtual appliance or software addresses the challenges of today's email threats with a multi-layered defense for both inbound and outbound security, engineered to minimize administrative overhead for a lower total cost of ownership.

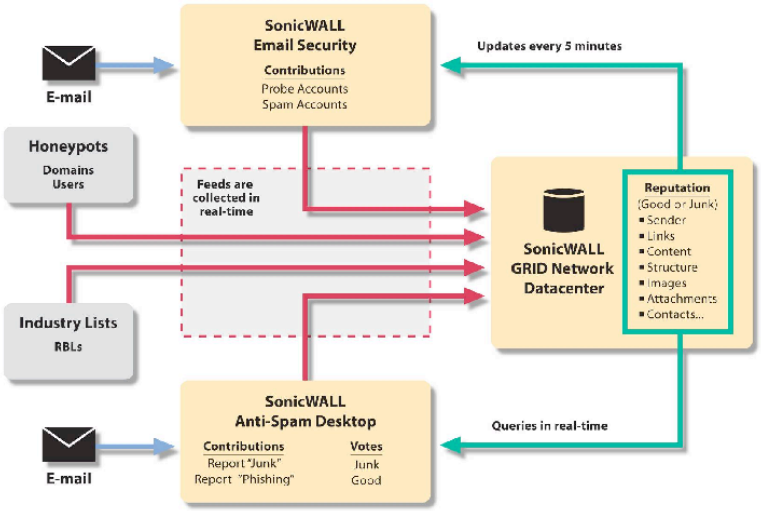
Multi-layered inbound protection

Dell SonicWALL takes spam management beyond arbitrary scoring by applying cross-analysis techniques that uniquely identify the sender, analyze the content and apply a collaborative review to every email. Dell SonicWALL Email Security delivers industry-leading spam, phishing and virus-laden email protection with an integrated multi-layered defense suite, including the Dell SonicWALL GRID Network, Dell SonicWALL Advanced Reputation Management (ARM), Dell SonicWALL Advanced Content Management (ACM), Dell SonicWALL GRID Anti-Virus™ (GRID AV) and a host of other layered defenses.

The Dell SonicWALL GRID Network

The Dell SonicWALL Global Responsive Intelligent Defense (GRID) Network™ collaboratively gathers, analyzes and vets cross-vector threat information from millions of business-oriented sources around the world in real time. This data is then correlated to develop reputation scores known as GRIDprints. GRIDprints not only include current reputation information on Sender IP addresses, but also all significant components of the message, including message structure, content, embedded URLs, images, attachments and other factors.

This reputation-based threat protection information is then distributed securely, anonymously and in real time to improve the overall effectiveness of Dell SonicWALL security solutions. Due to the distributed nature of this network and the use of multiple different data sources, the evaluation from one contributor can be vetted against multiple other contributors, allowing the GRID Network's collaborative filtering process to be highly accurate and fully self-correcting. Unlike competitive solutions that leave businesses vulnerable by taking an hour or longer to update with the latest attack information, every Dell SonicWALL Email Security solution receives GRIDprint updates of reputation-based threat protection information from the GRID Network in real time.



The GRID Network is unique in that it applies information from only its own business-focused sources, unlike other solutions that rely upon rented or purchased lists from consumer-focused ISPs. The GRID Network's initial purpose was to provide Dell SonicWALL Email Security and Dell SonicWALL Anti-Spam Desktop solutions with dynamically up-to-date email component reputation analysis. Building upon this successful foundation, Dell SonicWALL has actively developed and expanded the breadth of the information shared over the GRID Network, and has integrated the entire range of Dell SonicWALL solutions—including Unified Threat Management (UTM), anti-virus, anti-spyware, intrusion prevention, content filtering and application firewall defenses—that contribute to and take advantage of this global threat monitoring. For Dell SonicWALL Email Security, the GRID Network's GRIDprints provide the cornerstone for Dell SonicWALL's Advanced Reputation Management and Advanced Content Management email security defenses.

Dell SonicWALL Advanced Reputation Management (ARM)

Dell SonicWALL Email Security solutions block up to 99% of junk email. Its first line of defense is Dell SonicWALL ARM, which blocks up to 80% of junk emails at the connection level, before they can even enter the email server and degrade performance. What's more, ARM's aggressiveness is fully customizable, and Dell SonicWALL Email Security solutions log all actions, so the IT administrator retains complete control. Utilizing more than only Sender IP Reputation, ARM also applies Dell SonicWALL GRIDprints and Bounce Address Tag Validation (BATV) for NDR messages, as well as DoS and DHA protection. ARM does not put any size limits on what can be scanned. Administrators can customize GRIDprint settings, and initiate centralized management and reporting across multiple systems to reduce the chance of email-borne threats entering the network.

Dell SonicWALL Advanced Content Management (ACM)

After ARM eliminates up to 80% of spam at the connection level, any remaining email is analyzed and filtered by ACM, using more than a dozen comprehensive layered techniques including comprehensive Adversarial Bayesian™ analysis, which includes advanced text and image parsing engines; lexicographical distancing; image analysis (white-on-white, teeny fonts, etc.); gibberish detection; and corporate or user allow/block lists. ACM scans content in every significant email component (body, subject, attachments, etc.) to assure compliance with corporate policy, and can block or re-route non-compliant emails to appropriate LDAP-based groups or individuals.

Dell SonicWALL GRID Anti-Virus

Dell SonicWALL GRID Anti-Virus leverages Dell SonicWALL's anti-virus and anti-spyware technology to deliver inbound and outbound anti-virus and anti-spyware scanning in email security solutions. Using the dynamically updated GRID Network and its extensive list of malware signatures, GRID AV automatically blocks the most common threats as well as prevents Time Zero attacks. GRID AV prevents users from downloading spyware and stops any existing spyware from being disseminated via email systems. GRID Anti-Virus can be further augmented by optional anti-virus subscriptions from McAfee® or Kaspersky Lab® for layered defense and added capability for outbound protection against email-borne viruses.

Dell SonicWALL Time Zero Anti-Virus

Dell SonicWALL's breakthrough Time Zero anti-virus technology provides predictive virus defense complemented with responsive techniques to stop viruses as soon as they emerge. With Dell SonicWALL Time Zero anti-virus technology, emails potentially containing new viruses are identified and safely quarantined.

Dell SonicWALL Anti-Phishing

Dell SonicWALL Anti-Phishing includes header analysis with Sender ID and GRIDprint evaluation. Leveraging Dell SonicWALL's expertise and success with Adversarial Bayesian™ for anti-spam, Anti-Phishing incorporates a unique and patented Bayesian Fraud™ analysis into its content analysis. Developed from an extensive database of phishing and fraud samples collected from the GRID Network and vetted by the Dell SonicWALL Threat Research Team, Bayesian Fraud content analysis differentiates and isolates phishing fraud from spam during the filtering process, unlike most other solutions. The Dell SonicWALL Threat Research Team discovered that if a phishing email were placed in the same folder as a user's spam email, the user would move the phishing email to their inbox approximately 10% of the time, even though the email was indeed a phishing email. The same research demonstrated that if phishing email is marked as a phish and placed in a "phish" folder, then users would move the phishing email to their inbox less than 0.5% of the time.

Multi-layered outbound protection

In addition to full inbound protection, Dell SonicWALL Email Security also applies Outbound Threat Management (OTM) and Compliance Defense Management to provide complete inbound and outbound protection on the same system.

Dell SonicWALL Outbound Threat Management (OTM)

Dell SonicWALL OTM combines anti-zombie, anti-spam, anti-virus and time-zero protection services to scan all outbound email to ensure it is both legitimate and virus-free.

OTM provides robust anti-zombie defense by identifying and blocking zombie-generated email and alerting the administrator to potentially infected machines. Dell SonicWALL's multiple-diagnostic approach, combined with flexible response options,

enables enterprises to prevent zombie damage while allowing the company to send legitimate outgoing emails. Dell SonicWALL zombie detection employs multiple indicators to locate these dangerous machines and stop the transmission of email threats. These indicators include machines sending out spam, phishing or virus emails; emails sent from addresses not in the company's LDAP address list; and high email volumes sent from individuals or corporate-wide.

The administrator can select how to respond to actions flagged as zombie machine indicators. For example, the email messages can be deleted or quarantined, or an alert can be sent to a designated recipient. If "Outbound Safe Mode" is initiated, Dell SonicWALL Email Security sends alerts every 30 minutes, prevents dangerous attachments from being sent, and can optionally delete or quarantine outbound messages with potentially dangerous attachments (e.g., executable program files).

Dell SonicWALL solutions also have the ability to apply optional dual-engine anti-virus technology from partners McAfee and/or Kaspersky to both inbound and outbound emails to ensure that dangerous attachments are not being sent from within the company. This both keeps the network safe and enables the organization to maintain a reputation of safe outbound email.

Dell SonicWALL Compliance Defense Management

Dell SonicWALL Compliance Defense Management combines Dell SonicWALL's built-in policy engine and compliance services to identify, route and report on compliance-related information entering or leaving the organization via email. The extensive Compliance Defense Management tool set includes compliance dictionaries, Record-ID Matching, compliance reports, archiving, encryption and approval boxes with alerts.

Compliance Defense Management eases the burden of becoming compliant by delivering a host of flexible, easy-to-use features that enable organizations to meet both external (e.g., PCI, SOX, HIPAA) and internal (e.g., intellectual property policy) requirements. By intelligently identifying emails that violate compliance policies, providing monitoring and reporting and applying multiple enforcement actions, Compliance Defense Management delivers a powerful framework for driving compliance initiatives.

Compliance Defense Management offers a host of features, applying multiple techniques to help ensure comprehensive compliance:

Record-ID Matching searches for predefined patterns (e.g., social security numbers, bank routing numbers, credit card numbers, etc.,) for easy-to-use Web-based, UI-enabled custom record searches.

Attachment Scanning looks for content within attachments (e.g., Word, PowerPoint, PDF and over 300 other file types) to ensure sensitive data does not leave within attachments.

Predefined policies provides common compliance setups.

Predefined dictionaries help in handling health or financial records to monitor for regulatory (e.g., HIPAA, SOX, GLBA, etc.) violations and, used in conjunction with Record ID Matching, ensure the protection of confidential information and prevention of sensitive data leaks.

Approval boxes allow viewing and approval of emails that potentially violate compliance policies before they leave the organization.

Email archiving is available for both inbound and outbound email traffic on the same server or appliance. Additionally, organizations can route emails that match a specific policy to an external archive.

Encryption routing directs emails that match a specific policy to an encryption/decryption server. Coupled with Transport Layer Security (TLS), a free standards-based gateway-to-gateway encryption protocol, Dell SonicWALL Email Security ensures the secure communication of confidential information.

Compliance reporting enables organizations to monitor and report on compliance-related email traffic.

Superior manageability

Dell SonicWALL Email Security makes comprehensive email security easy to deploy, manage and own. Using the 5-step Quick Configuration option, Dell SonicWALL Email Security can be installed and operational in under an hour. While the email security solution is simple to install using default configurations for basic needs, it is flexible enough to support many advanced security techniques, including advanced configurations and tailored policy management for regulatory compliance. Dell SonicWALL Email Security also eases management by automating routine tasks such as end-user spam management, LDAP and status reporting.

Dell SonicWALL Policy Management

Dell SonicWALL Policy Management enables organizations to implement email management rules easily for both inbound and outbound email. Dell SonicWALL's easy-to-use Web-based administrative interface allows administrators to implement single or multi-action email policies. Policies can regulate inbound and outbound email traffic, scan all message components for specific criteria or content, and initiate a variety of corresponding actions (e.g., bounce, route to, notify, etc.). These policies can be applied company-wide or to specific users or LDAP-based groups. Administrators can then monitor the impact of a particular policy by placing all emails that match the policy in a named Approval Box for review.

End-user spam management

Dell SonicWALL's Junk Box Summary provides employees with a single email that summarizes all of their quarantined spam, virus and phishing emails. It also includes single-click access to "unjunk" message types permitted by IT, delivering them to the employee's inbox and allowing the senders to be added to the user's personal allowed list. This summary email ensures that employees never miss a legitimate message and never need to contact IT to find the message. Users can preview messages in "safe mode," which prevents the user from seeing offensive content and will not allow the execution of Java, JavaScript or any other potentially malicious code.

Employees are also provided a personal Junk Box, which they can access through a simple Web interface. From here, users can search, sort, and review email determined to be junk. Then, with a single-click of the unjunk option, users can have mail delivered seamlessly to their inbox and have the sender added to their personal allowed list. The Junk Box itself is kept at the perimeter—off the email server—decreasing risk and load.

The Dell SonicWALL Email Security administrator can also enable end-user access to a Junk-Button for Outlook plug-in. If allowed, a user can download this lightweight Outlook plug-in and install it in less than a minute. The Junk Button will display whenever Outlook is running and, when used, will not only remove the selected spam message from the user's inbox, but also send the user's "junk" vote immediately and anonymously to the Dell SonicWALL GRID Network, collaborating in a global-community-based solution to stopping spam.

Judgment details for system tuning

Dell SonicWALL Judgment Details ease administrative troubleshooting by clarifying categorization actions to explain why a specific message was classified as spam, likely spam or non-spam. This feature allows administrators to fine-tune their system to block spam while minimizing false positives. In the rare case of a false positive or false negative, the administrator can use the judgment details to provide a detailed explanation as to why a specific email was or was not blocked.

Multi-LDAP support

Dell SonicWALL Email Security provides Multi-LDAP and User List support to provide a flexible solution for distributed organizations or managed service providers (MSPs). These types of deployments typically need to connect to multiple LDAP servers, or have a User List of valid users for a given domain where LDAP services are not available. Dell SonicWALL Email Security dynamically synchronizes with existing LDAP servers, ensuring any modifications made by administrators are automatically reflected in Dell SonicWALL's filtering activity in real time. Dell SonicWALL synchronizes with nearly any corporate directory, including Exchange 5.5, Active Directory, Lotus, iPlanet and OpenLDAP.

Status Reporting

Dell SonicWALL offers comprehensive, detailed status reporting on spam, phishing, email-borne malware attacks and compliance management activity, along with automated alert and feedback tools. These features enable administrators to be kept aware of threat trends, make necessary security modifications, and report findings to regulatory auditors, executive staff or third-party security providers.

Conclusion

As email-based threats grow more numerous, more sophisticated and potentially more harmful, conventional single-point solutions alone have become less effective. A more sophisticated, multi-layer defense is required to combat the emergence of new blended forms of spam and other email-based attacks. Applying seventh-generation technology and dedicated research and development, Dell SonicWALL's award-winning Anti-Spam/Email Security solutions deliver comprehensive multi-layered protection, while streamlining administration to lower total cost of ownership.