

STAMPing out Email Risk: Seven Technologies for Advanced Mail Protection

Table of Contents

Executive Summary	3
Introduction	3
Inbound Threats: This is Not Your Father's Spam	3
Global spam volumes and spam as a percent of all mail continue to grow	4
Enter the criminal element	4
Storm clouds on the email horizon	4
Outbound Threats: Sensitive Data Leakage	6
Email Security Today: Avoidable Risks Persist	7
Safety and Savings: You Can Have it All	7
Cost savings	7
Productivity gain	8
Tightening security, reducing cost	9
New delivery models	10
Summary	10
Stamp—McAfee's Seven Technologies for Advanced Mail Protection	10
Multi-protocol reputation-based protection	10
Global intelligence plus local knowledge	11
Complete content detection, both structured and unstructured	11
Robust encryption and other compliance actions with integrated policy	12
Integrated for inbound and outbound	13
Hybrid solution architecture	13
Enterprise-class scalability, stability, ease-of-administration, and reporting	13
Summary	14
McAfee Email Security Products	14
McAfee Email Gateway	14
TrustedSource	15
McAfee's hybrid delivery architecture	15
Conclusion and Next Steps	15
Endnotes	16

Executive Summary

Email is today's primary medium of business communications. As such, it presents a rich target for hackers, spammers, and malware owners, and a vulnerability to careless or malicious insiders. Regulators have noted the importance of email in the enterprise, and have issued email-specific rules and regulations regarding privacy and intellectual property protection and archiving. In September of 2008, McAfee commissioned the analyst firm IDC to survey¹ the state of email security at North American organizations with more than 500 employees. Given the threats and challenges we face, the results were dismaying. The survey revealed concern yet complacency, sub-optimal solution performance yet inaction.

This paper examines today's email threats, the current state of enterprise defenses, and plans to address emerging threats. Most importantly, it provides a technology blueprint for enterprise email security called STAMP—McAfee's Seven Technologies for Advanced Email Protection.

Introduction

Today's email threats are far more dangerous than yesterday's. On the inbound side, blended email and web attacks masterminded by profit-seeking criminals are now the norm. Spam is no longer about selling, it's about stealing. Attacks are targeted and fast moving. The perpetrators are more sinister, organized, and sophisticated. Orchestrated botnet armies strike globally and quickly go dormant. Harmful payloads morph continuously to evade signature-based defenses, and are more often delivered through an embedded web link rather than a direct file attachment. Every malicious email that penetrates the perimeter carries dramatically more risk than ever before.

On the outbound side, email is a primary egress point for sensitive and confidential information. More and more information is accessible to individuals within the organization, all of whom have email and web access. Combined with the temporary nature of the workforce, with contractors, consultants, and temporary workers continually coming and going, the risk of data leakage remains high. The potential costs of lost business, regulatory fines, lawsuits, and brand erosion can be staggering.

IT security professionals, meanwhile, must contend with the budget and cost pressures of an uncertain economy, line of business concerns, and changing priorities such as green computing and outsourcing. Security often takes a back seat.

The IDC survey sponsored by McAfee revealed both concern and complacency among IT professionals who manage email security for organizations in North America. Of the nearly 60 percent who were achieving sub-optimal inbound email security compared to best practices, only three percent were dissatisfied with that performance. And while almost 90 percent were very concerned about data leakage over email, less than a third had implemented a solution. In part, this inaction seems due to the lack of a framework for evaluating available solutions to select those that are both robust and cost-effective.

Drawing on customer experience, the IDC white paper, data gathered from TrustedSource™ (McAfee's global, multi-protocol reputation system), and third-party sources, this paper outlines today's email threats and explains why most existing email security solutions are inadequate. It then proposes a solution framework—McAfee's Seven Technologies for Advanced Mail Protection (STAMP).

Inbound Threats: This is Not Your Father's Spam

Spam is nearly as old as the Internet itself. As early as 1978, unsolicited marketing messages were being sent to APARANET users. These quickly evolved into USENET and MUDder postings.^{2,3} By the mid 1990s, spam was primarily an unsolicited email problem, and by 2005 email spam had reached over 50 billion messages per day.⁴ McAfee's TrustedSource research team tracks spam volume as it grows, and since 2005 it shows no signs of slowing down (see Figure 1). Spam volume now averages more than 159 billion messages per day—over 80 percent of all global email traffic.

Global spam volumes and spam as a percent of all mail continue to grow

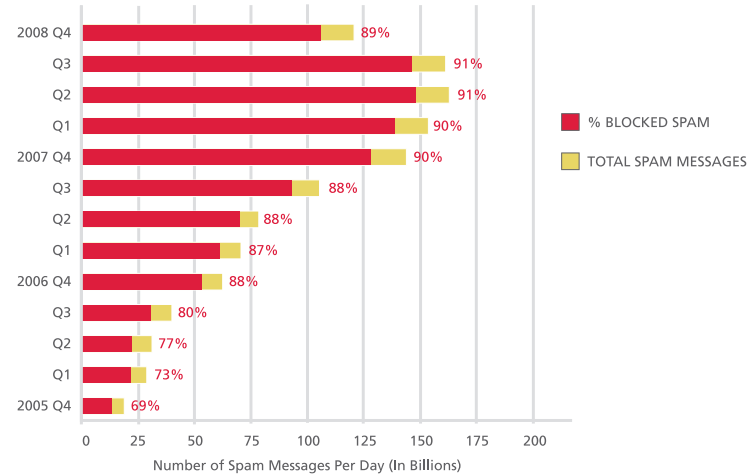


Figure 1: Spam continues to grow. (Source: McAfee TrustedSource.org)

Enter the criminal element

If volume were the only difference in today's spam, then the threat would be fairly well defined and benign. While every unwanted email has bandwidth and productivity costs, the real threat now lies in the motive and sophistication of today's spammers. Thrill seekers and marketers have now been joined by organized, profit-seeking criminals. The difference between spam today and yesterday is shown in Table 1. McAfee now estimates that as much as 20 percent of all spam either carries or links to malware attacks.

	The Classic Era (1995 to 2007)	Storm Era (2007 - onward)
Payload	Embedded	Linked
Motive	Marketing and scams	Theft of info and resources
Organization structure	Individuals or small groups	Organized cyber criminals
Effectiveness of signature-based defenses	High	Low
Key techniques	Volume	Volume and social engineering

Table 1: Spam, then and now!

Storm clouds on the email horizon

Perhaps no single example better illustrates the new severity of spam threat than the infamous Storm botnet. Storm has been studied in depth by many, including McAfee. (For a complete analysis of Storm, see McAfee's white paper: *Storm: The First Comprehensive Solution for Internet Fraud.*)

The Storm botnet first appeared as a series of emails that enticed users to click on an embedded executable posing as a video about the storms then ravaging Europe. The executable then turned their machine into a bot. For a while, Storm continued to embed files linked to current events. An example is shown in Figure 2.

White Paper STAMPing out Email Risk: Seven Technologies for Advanced Mail Protection

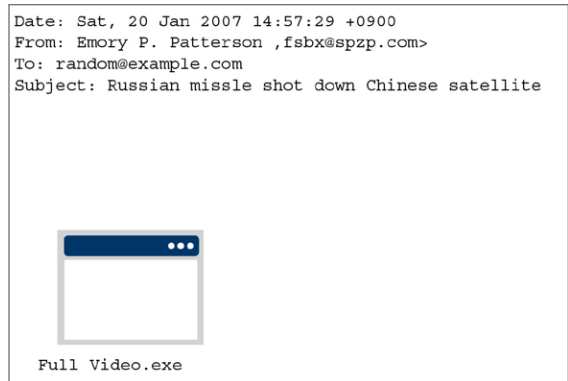


Figure 2: An early Storm spam message

While this may seem crude, the Storm masterminds quickly evolved both the techniques and the social engineering used to bait users. A later, more polished example is shown in Figure 3 below.

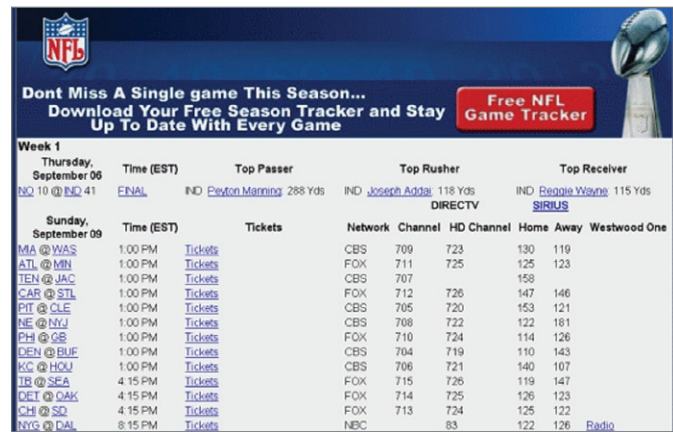


Figure 3: Later Storm messages show much greater design and sophistication.

At its peak, the Storm botnet is estimated to have reached 10 million nodes. With the closure of several vulnerabilities, some believe the Storm threat is over. Others expect that Storm will either reemerge or be replaced by newer botnet armies like Nugache.⁵ In fact, Storm reappeared in July 2008 with an email about the “Amero” currency replacing the US dollar.⁶ Regardless, Storm provides a blueprint to understand the goals and techniques of the emerging criminal threat. It was groundbreaking in many ways including⁷:

- *Network stealthiness*—Storm used sophisticated network techniques to hide sender identity
- *Resilience*—Storm pioneered distributed P2P command and control and other techniques to stop shutdown attempts by researchers
- *Patience*—Storm was not always on the attack; it spent long quiet periods perfecting its next attack
- *Multi-vector infection mechanism*—Storm augmented traditional email-laden viruses with blended web and email attacks
- *Social engineering*—Storm continuously innovated new social engineering attacks
- *Transformation*—Storm’s malware morphed continuously to avoid signature-based defenses
- *Self-defense*—Storm pioneered the use of automated offensive self-defense mechanisms, launching distributed denial of service (DDoS) attacks against researchers analyzing the botnet
- *Spam innovations*—Storm was responsible for a number of new innovations in the delivery of spam, including PDF and Excel-based spam

The Storm phenomenon proves the sophistication and resourcefulness behind the new blended mail and web spam threats.

- *Desktop stealthiness*—Storm used new techniques to avoid causing noticeable degradation of performance on infected machines
 - *Modularity*—Storm attack components were modular and segmented
- Storm epitomizes the sophistication and resourcefulness behind new blended mail and web spam threats. It shows how today's spammers can survive, propagate, and elude detection by conventional defenses and how spam has evolved from nuisance to criminal enterprise. While much attention has been paid to the non-email pieces of the Web 2.0 threat, Storm also shows that the IT security war started with and ends with effective spam defenses. In this era, it's no wonder that despite the investment of billions in email security solutions, spam volumes continue to rise and IT security administrators continue to lose sleep.

Outbound Threats: Sensitive Data Leakage

Data leakage has been a popular topic in recent years. Advocacy, industry, government, and news organizations have chronicled many leaks and breaches, including a 2006 incident in which the Republican National Committee inadvertently emailed donor names and social security numbers to a New York Sun reporter. In a more recent example (July 2008), a departing employee at the California Department of Consumer Affairs emailed 5,000 personnel files to her Yahoo! account, complete with employee names and social security numbers.

Employees, contractors, and other insiders have increased access to confidential information that is easily compromised through email and web communications. Many workers use email as a de facto filing system, using email folders to retain important files on the mail server. New reports confirm the increasing difficulty of protecting sensitive data⁸.

- 263 major privacy breaches occurred between January and mid-October 2008
- The FTC estimates that as many as 9 million Americans have their identities stolen each year
- Over 244 million data records of U.S. residents have been exposed due to security breaches since January 2005

In early 2008, IDC predicted that, "Most of these leaks will be accidental, but we expect a rising number of carefully managed attacks by sophisticated crime syndicates."⁹ Figure 4, from a five-year study by Verizon¹⁰, shows that personally identifiable information (PII), especially payment card data, is the primary type of data lost in a data breach.

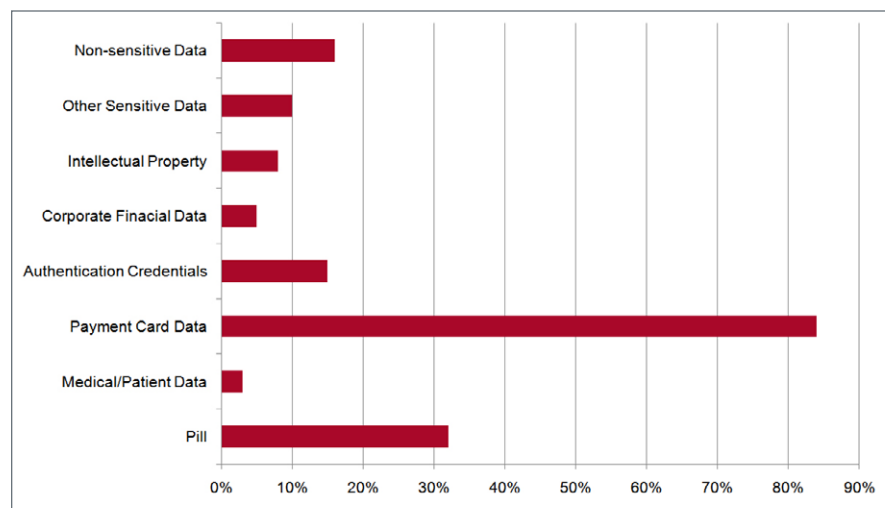


Figure 4: Data breaches focus on personal and payment data. (Source: Verizon 2008 Data Breach Investigation Report)

Email Security Today: Avoidable Risks Persist

How has enterprise email security adapted to the increasing volume and severity of inbound and outbound threats? IDC research both confirmed and confounded reasonable expectations. Among the survey findings:

- The vast majority of IT professionals expressed very high levels of concern around the principal vectors of inbound email attack, including:
 - » Email with malicious links embedded (83 percent)
 - » Mail with malicious attachments (86 percent)
 - » Email-based phishing exploits (83 percent)
 - » mail-based botnet recruitment (74 percent)
 - » Email spam (78 percent)
 - » Email-related data leakage (77 percent)
- Many respondents reported multiple email security breaches within the past year
- Despite high levels of concern and high frequency of attack, more than 60 percent of respondents reported spam detection rates of 95 percent or less, and just 11 percent reported 99 percent effectiveness—today’s consensus benchmark for best practice performance
- Amazingly, of the 60 percent currently achieving less than 95 percent spam detection effectiveness, only three percent expressed dissatisfaction with their current solution
- Many respondents reported incidents of both accidental and deliberate leakage of sensitive and proprietary information via email
- Although nearly 80 percent of the responding organizations were extremely or very concerned about email information leakage, only 28 percent had implemented a DLP solution
- While 79 percent of survey respondents agreed that an integrated solution for inbound and outbound email security reduces licensing, support, and administrative costs, many organizations still reported using separate solutions

Why do organizations have such low expectations? Either they don’t believe they can cost-effectively get better results or they don’t understand the benefits of doing so. If we assume that 11 percent of enterprises can achieve better than 99 percent effectiveness across all size segments, then it is possible for everyone to do so. Is it, however, worthwhile? A simple ROI model says “yes”—resoundingly.

Safety and Savings: You Can Have it All

The model shown below in Table 2 demonstrates two cost savings and one productivity gain from the implementation of a best-in-class solution that raises an organization’s inbound effectiveness to 99.5 percent, and the catch rate of connection layer blocking^{12, 13} to 80 percent or above.

Cost savings

The first way to reduce costs is to reduce malware infection and associated cleanup. McAfee estimates that about 40 percent of spam contains malware or links to malware. Industry estimates of direct and indirect cleanup costs exceed \$10,000 per infection incident. By combining these statistics with typical malware catch rates and user behavior, it is possible to calculate the reduction in malware cleanup costs from improved inbound spam effectiveness.

The second way to reduce costs is to reduce archiving and bandwidth expenses. When messages are blocked with connection layer technologies such as reputation and recipient validation, no connection is made with the email server. This saves bandwidth and eliminates the costly burden of archiving spam for up to seven years¹⁴, because the unwanted email is never accepted. Solutions with connection control technologies block 80 percent or more of bad email, yet the IDC research showed that only 13 percent of responding companies reach these levels of performance and 41 percent have not even implemented this technology.

Productivity gain

The model also demonstrates that users can gain additional productivity by reducing the amount of time they spend opening, identifying, and deleting spam messages.

Table 2 (on page 9) shows that for a 1,000-person organization currently at 95 percent overall spam blocking effectiveness and 60 percent connection layer catch rates, the total cost savings of implementing a more efficient and effective solution is over \$270,700 annually. The total ROI for this solution, based on a cost of \$30 per user per year, is over 1,800 percent.

Tightening security, reducing cost

Organizational Assumptions	
Average number of "good" email messages received by a corporate user a day	50
Percentage of "good" email users receive from outside the gateway	20%
Spam filtering accuracy percentage with current solution	95%
Connection layer blocking effectiveness percentage with current solution	50%
Number of users in organization	1000
Average fully burdened end-user costs annually	\$100,000
Costs/user/year with current solution	\$15
Industry Assumptions	
Percentage of global email that is "bad" (that traverses the Internet)	80%
Spam filtering accuracy with best-in-class solution	99.5%
Connection layer blocking effectiveness percentage with best-in-class solution	80.0%
Percentage of spam containing malware or links to malware	20%
Malware cleanup cost per infection	\$100.00
User time to open, process, and delete spam (in seconds)	30
Archiving cost per 20kb message delivered	\$0.005
Bandwidth cost per 20kb message delivered	\$0.005
Costs/user/year for best-in-class solution	\$30.00
Calculations	
"Good" emails per user per day from outside the gateway	10
Total "good" email delivered from outside the gateway daily	10,000
Total emails attempted to be delivered from outside the gateway	50,000
Total daily spam emails attempted to be delivered	40,000
Total daily spam messages delivered with current solution (95% spam filtering accuracy)	2,000
Total daily spam messages delivered with best-in-class solution (99.5% spam filtering accuracy)	200
Additional daily spam messages stopped at connection layer with best-in-class solution	12,000
Daily spam messages not delivered to users with best-in-class solution	1,800
Daily malware-laden spam messages not delivered to users with best-in-class solution	360
Daily malware infections avoided with best-in-class solution implementation total	2.0
Productivity loss per opened spam	\$0.40
Total incremental solution costs (based on \$15K for current solution and \$30K for best-in-class solution)	\$15,000
Hard Cost Savings	
Malware cleanup costs avoided	\$52,000
Connection layer reduced bandwidth and archiving costs	\$31,200
Total Hard Cost Savings	\$83,200
Hard Cost ROI	555%
Productivity gains	\$187,500
Total Cost Savings (Hard costs plus productivity gains)	\$270,700
Total ROI	1,805%

Table 2: ROI model for a 1,000-person company.

Organizations moving to newer and more-effective solutions can realize additional efficiencies. In addition to inbound security paybacks, companies can also achieve a reduction in the risks of outbound data leakage, as well administrative costs savings and flexibility gains through vendor consolidation.

New delivery models

Not surprisingly, respondents also reported that new and emerging delivery models are part of their plans going forward. More than a third of respondents plan to deploy virtual security appliances in the next year. Over half believe that a hybrid solution approach, combining a hosted solution with an on-site appliance will deliver the best email security for both inbound and outbound threats. Interestingly, only 11 percent see hosted-only solutions as optimal. Whether driven by the promise of green computing or cost pressures, organizations are clearly looking to improve the delivery efficiency of email security solutions. While lowering costs and increasing efficiency, organizations must be sure to maintain or improve their overall security posture.

Summary

Even in today's challenging economic times, executives recognize the criticality of email security, and organizations are willing to invest in new solutions. 96 percent of respondents said that their organization's senior management understood the importance of email security, and nearly 60 percent anticipated increased spending on email security solutions.

In summary, organizations, despite the costs and risk, are satisfied with sub-optimal inbound security and have not widely implemented sufficient outbound security. They have too many solutions in place and have the opportunity to consolidate providers. Lastly, they are planning on implementing new service delivery models aggressively.

Before rushing into solution replacement and consolidation, it is critical to understand the gap between solutions that deliver sub-optimal effectiveness and higher administrative costs and solutions that are comprehensive, highly integrated, extremely effective, and extraordinarily manageable. McAfee has analyzed this gap and identified Seven Technologies for Advanced Mail Protection (STAMP). This paper explores these STAMP technologies in. McAfee recommends that enterprises evaluate solutions based on their ability to deliver these capabilities when considering new email security solutions.

STAMP—McAfee's Seven Technologies for Advanced Mail Protection

Email security is a mature technology. Many basic functions, such as secure message transfer agents (MTAs) that protect against intrusion, denial of service (DOS), and directory harvest attacks (DHA), are well understood. However, as we have seen from above, many of the solutions deployed today are not fit for today's threats and business environment. In order to cost-effectively protect an organization from today's inbound and outbound email risks, email security solutions must have the following capabilities:

- Multi-protocol, reputation-based protection
- Global intelligence plus local knowledge
- Complete content detection, both structured and unstructured
- Robust encryption and other compliance actions, with integrated policy
- Integrated inbound and outbound protection
- Hybrid solution architecture
- Enterprise-class scalability, stability, ease of administration, and reporting capabilities

Each of these capabilities is discussed in more detail in the following section.

Multi-protocol reputation-based protection

Similar to a credit score that evaluates financial behavior (the number of loans taken out, late payments, loan defaults, and others), reputation services assign a numerical score to Internet entities based on their cyber behavior (have they sent out millions of messages at once, associated with a known phishing site, hosted malware, or others). These scores allow security administrators to determine whether or not connections to and from these entities should be allowed.

The primary shortcoming of many reputation services is that they only evaluate IP addresses. All too often, that evaluation is superficial. Some services only provide a score of +10 to -10, giving administrators no details on how the solution arrived at that score. Can you imagine applying for a mortgage and only getting a credit score of +8 without getting an explanation?

A truly mature and sophisticated reputation service scores multiple types of Internet entities, then correlates them to form a granular and precise picture. As you evaluate reputation services, look for scores that provide a wide range of factors and actually explain those factors. It is possible that a negative score could be based on criteria that aren't relevant to your particular set of circumstances.

Global intelligence plus local knowledge

While intelligence of what happens around the Internet world is very useful, it may not be relevant to you. That's why mature security solutions marry global intelligence with local knowledge. For example, some organizations consider e-newsletters to be spam. Others have more flexible policies and allow their users to receive e-newsletters. Some block email with public web domains (Hotmail, Gmail, Yahoo, AOL, etc.) while others allow this traffic.

The best defense-in-depth strategy is to combine global and local criteria for a customized and effective email security solution. When used effectively, blocking spam is simple. Over 80 percent of spam can be blocked based solely on global reputation services. The addition of local knowledge should catch an additional 19.5 percent of spam. The right combination easily provides an overall spam block rate of 99.5 percent or better.

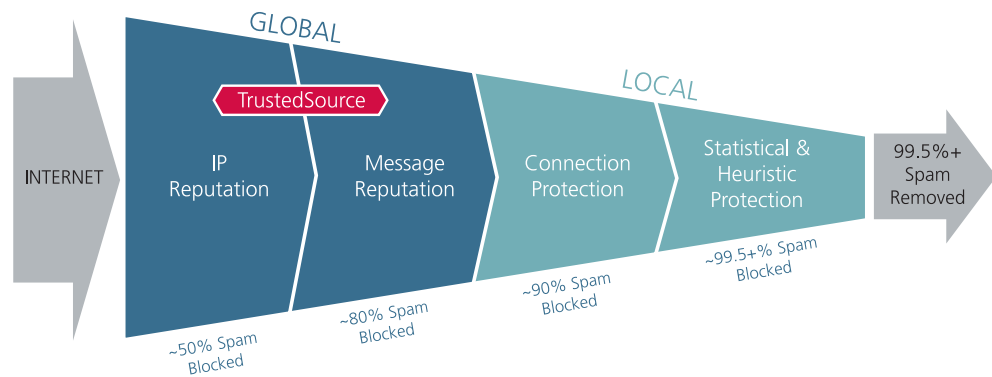


Figure 5: Global intelligence plus local knowledge results in better than 99 percent spam blockage.

Complete content detection, both structured and unstructured

Data leakage is one of the biggest security problems facing companies today. Protecting intellectual property as well as regulated data has boardroom-level attention. The technology to do this, however, is extremely complex. Because most data-in-motion security products can only do keyword matching, it's far too easy for spammers to disguise words by replacing them with something that is visible to the human eye, but not to the computer. For example, the word Viagra can be hidden in a number of creative ways:

- \ / i a g r a
- V1agra
- Vi@gr@
- Y agra
- V/i/a/g/r/a
- Vi?agr?

These are just six possible variations. In actuality, this six-letter word can be represented in more than 600,426,974,379,824,381,952 ways¹⁵.

Structured data (like social security or credit card numbers) follows predictable patterns, but unstructured data can be almost anything. The right solution provides the same defense-in-depth logic that we already rely on to uncover both structured and unstructured data as it moves within and outside the enterprise. Many regulations such as HIPAA and PCI DSS lend themselves to keyword matching, and the right solution should provide extensive dictionaries for all major U.S. regulations out of the box, as well as regular updates. In addition, advanced technologies should work together to discover all types of sensitive data before they can leave the enterprise. These technologies can include:

- *Fingerprinting*—uniquely identifies sensitive documents, so that portions or the entire document can be tracked
- *Advanced lexical analysis*—scrutinizes not just words, but phrases, non-consecutive words, and words that appear in proximity to each other, so that it can detect matches in content even with misspelled words, reordered sentences and paragraphs, or broad word replacements
- *Clustering of like documents*—looks at the contents of a message or attachment and compares them to known documents which have been identified as a type of document that should be protected
- *Advanced content analysis*—searches for combinations of expressions that when used together could constitute a violation, but used individually would not

Robust encryption and other compliance actions with integrated policy

SOX, HIPAA, PCI DSS and other regulations require sensitive information to be encrypted as it moves inside and outside the enterprise. The best and most reliable place to make the encryption decision is at the gateway. This eliminates the possibility of human error exposing the enterprise to non-compliance risk.

Two basic types of encryption are acceptable, depending on the nature of the content and the nature of the communications:

- Gateway-to-gateway—encrypts messages while in transit from one corporate gateway to another
- Gateway-to-user—encrypts messages intended for end-users who do not have encryption/decryption capabilities

The right email security solution should support both types, and provide flexible, policy-based selection of the appropriate method. The most flexible solutions should provide each of the following options for gateway-to-gateway encryption:

- SSL/TLS—uses SSL/TLS (Secure Sockets Layer/Transport Layer Security) to create a secure “tunnel” to the recipient server or client
- S/MIME—employs S/MIME (Secure Multipurpose Internet Mail Extensions) to encrypt messages and send them securely
- OpenPGP—uses PGP (Pretty Good Privacy) to encrypt the message and send securely

Gateway-to-user encryption options should include:

- Email push—sends user the encrypted message and prompts for a password to decrypt the message
- Email pull—holds encrypted email in a secure, web-based mailbox for the user to retrieve using a password
- Strong industry recognized solution for encryption at the desktop and gateway

The combination of the ability to discover sensitive content in motion and applying policy-driven encryption provides a complete outbound data protection solution, as shown in the following figure.

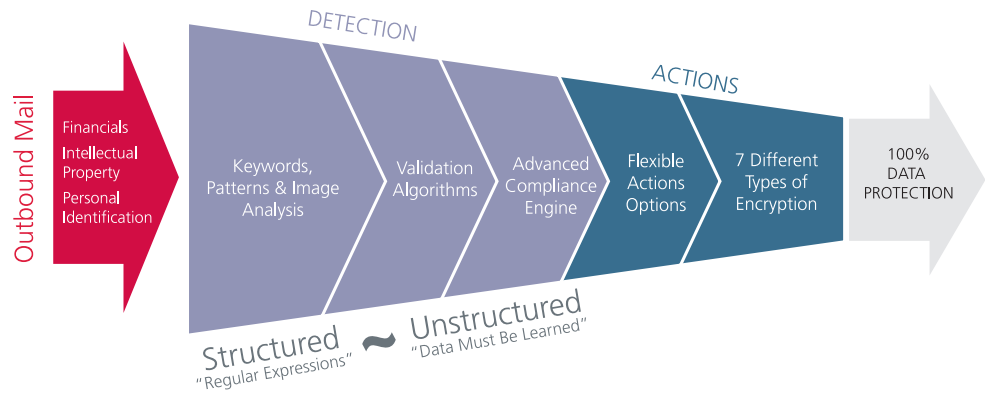


Figure 6: Data leakage is prevented by combining detection with encryption.

Integrated for inbound and outbound

Email security management shouldn't be made more complex by the need for separate products to secure inbound and outbound email. Comprehensive solutions should provide integrated inbound and outbound security in one easy-to-deploy-and-manage product.

Hybrid solution architecture

A hybrid delivery architecture is a technical and business architecture that provides flexible and reliable delivery, portability and hybridization of security services across hosted, virtual, and appliance platforms. It allows IT security staff to efficiently protect their organizations against today's emerging and morphing threats, while taking advantage of the strengths of all three delivery platforms. Hybrid delivery architectures should be built on six key design pillars:

- Availability of integrated hardware/software, virtualized and hosted service-delivery platforms
- Fully portable and proactive security services
- Hybrid: service deployment-enabled, allowing the splitting of services across delivery platforms
- Unified service offerings and pricing
- Common policy definition and administration
- Unified reporting

Enterprise-class scalability, stability, ease-of-administration, and reporting

The best technology in the world won't solve any problems at all if it can't be managed easily and effectively. The right email security solution should empower email administrators to deliver ROI and investment protection without compromising security or compliance requirements, and then be able to prove it through extensive reports and forensic capabilities. A solution must:

1. Be easy to implement and maintain
2. Scale with organizational needs and growth
3. Provide stability at very high levels of availability
4. Automatically maintain effectiveness without administration
5. Provide out-of-the-box, extensible logging and reporting

Summary

Combining these seven technologies provides significant benefits against a wide variety of threats and attacks. The following table summarizes these technologies and what they can provide to your enterprise.

Benefits of seven advanced technologies

Technology	Benefits	Type of Threats Eliminated
Multi-protocol, reputation-based protection	<ul style="list-style-type: none"> • Zero-hour protection • Reduces bandwidth • Reduces unnecessary archiving costs • Eliminates the need for additional email servers • Lowers the impact of email spikes due to spam 	<ul style="list-style-type: none"> • Malware • Phishing • Viruses • Trojans • Spyware • Currently Unknown Attacks
Global intelligence plus local knowledge	<ul style="list-style-type: none"> • > 99.5% effectiveness • Zero-hour protection • Efficient system processing • Stops threats at the earliest possible juncture 	<ul style="list-style-type: none"> • Spam containing blended threats • Harmful attachments • Inappropriate content • Policy violations • Denial of Service attacks
Complete content detection, both structure and unstructured	<ul style="list-style-type: none"> • Stops intentional data leaks before they happen • Stops unintentional misuse before data can leave the enterprise • Educates users on correct policies and usage • Automatically notifies security and compliance officers 	<ul style="list-style-type: none"> • Data leakage • Policy violations • Inappropriate content (inbound or outbound) • Intentionally obfuscated protected data • Unintentional data misuse
Robust encryption and other compliance actions with integrated solution	<ul style="list-style-type: none"> • Enforces compliance even when employees don't remember or know • Lowers risk of theft 	<ul style="list-style-type: none"> • Sensitive data stolen in transit • Policy violations • Compliance violations
Integrated inbound and outbound solution	<ul style="list-style-type: none"> • Operational, cost, and administrative efficiencies • Integrated reporting 	
Hybrid solution architecture	<ul style="list-style-type: none"> • Increases business agility and flexibility • Provides best utilization of resources and budgets • Eliminates risks even from sites without security expertise • Complies with green initiatives 	
Enterprise ready (scaling, stability, ease of administration, and reporting)	<ul style="list-style-type: none"> • Cost effectiveness • Improved ROI • Robust compliance reporting 	

McAfee Email Security Products

McAfee Email Gateway

McAfee Email (*formerly IronMail*) provides total email protection, providing integrated inbound protection from email-borne threats, outbound protection from data leakage, and administrative empowerment for email administrators. McAfee Email Gateway combines local information from the network with TrustedSource global intelligence to achieve over 99 percent spam detection accuracy and provide the most complete protection against inbound threats and malware. For regulatory compliance and data leakage prevention, the solution includes advanced compliance with the most sophisticated scanning technology for detecting sensitive information accompanied by the most granular, flexible administrative actions that include six different encryption techniques. The integrated solution can be centrally managed, combining inbound and outbound Internet email through one solution and one console with enterprise-class reporting and logging capabilities.

Total inbound protection maximizes user productivity and service uptime.

- 99 percent + spam detection accuracy
- Real-time zero-hour threat prevention
- Spam surge protection
- Denial of Service attack prevention

Total outbound protection eliminates information loss over email, without stopping business.

- Complete data loss prevention (DLP): Privacy and intellectual property content detection and data leak prevention
- Policy-enforced email encryption

Total administrative flexibility empowers you to deliver the best possible email protection and prove it!

- Inbound and outbound policy configurable to YOUR business needs
- Flexible deployment architecture
- Extensive reporting and dashboards

TrustedSource

McAfee's TrustedSource™ global multi-protocol reputation service is the first of its kind. It evaluates thousands of different criteria and delivers reputation scores in the range of +180 to -180, complete with supporting context. Administrators can precisely tune security to their exact requirements. TrustedSource also evaluates multiple types of Internet entities, and correlates analyses before scoring. TrustedSource assigns scores to each of the following:

- Senders
- Messages
- Images
- Attachments
- URLs
- Domains
- Malware

McAfee's hybrid delivery architecture

While other vendors have announced availability of solutions on multiple platforms, only McAfee offers flexible and reliable delivery, portability, and hybridization of security services across hosted, virtual, and appliance platforms.

Find out more about McAfee's Hybrid Delivery Architecture by reading the white paper *The McAfee Hybrid Delivery Architecture: An IT Executive Overview*.

Conclusion and Next Steps

Too many organizations rely on sub-optimal email security solutions today. The cost of inaction is increased risk of successful attack, potential data leakage, failed compliance audits and wastefully high costs. Organizations must update their email security solutions to ensure safety, flexibility, and cost effectiveness. McAfee recommends that organizations look for the seven key STAMP capabilities when moving to next-generation email protection. McAfee's Email Gateway (*IronMail*) product line, powered by TrustedSource, delivers these seven key technologies. It provides a complete customer solution that fully addresses today's enterprise email threats, vulnerabilities, and risks.

For more information on McAfee STAMP, McAfee Email Gateway, and other McAfee solutions visit www.mcafee.com.

To learn about your own organization's global email and web reputation, try our free reputation reporting service, Domain Health Check at www.securecomputing.com/dhc/.

Endnotes

1. Securing Email Against Today's Threats: A Wake-Up Call on the Benefits of Comprehensive Messaging Security, IDC document number 214837, October 2008
2. [http://en.wikipedia.org/wiki/Spam_\(electronic\)#History_of_Internet_.22spam.22](http://en.wikipedia.org/wiki/Spam_(electronic)#History_of_Internet_.22spam.22)
3. <http://www.templetons.com/brad/spamterm.html>
4. http://en.wikipedia.org/wiki/E-mail_spam
5. For an overview of competing claims and opinions of Storm's future, see: http://en.wikipedia.org/wiki/5._wiki/Storm_botnet
6. <http://www.offensivecomputing.net/?q=node/799>
7. Storm: The First Comprehensive Solution for Internet Fraud, www.mcafee.com
8. Sources: <http://www.privacyrights.org/index.htm> and Federal Trade Commission
9. Worldwide Security 2008 Top 10 Predictions: Security's Troublesome Twins, Crime, and Compliance, Ride the Web to Drive 2008 Trends, IDC document number 210400, January 2008
10. Verizon 2008 Data Breach Investigation Report
11. Securing Email Against Today's Threats: A Wake-Up Call on the Benefits of Comprehensive Messaging Security, IDC document number 214837, October 2008
12. See Money: Monetary Savings on Network Edge – Year after Year, <http://www.securecomputing.com/pdf/MGS-Monetary-download.pdf>
13. Connection layer blocking refers to techniques that operate at the connection layer by analyzing initial content such as mail header and recipients
14. Seven Design Requirements for Web 2.0 Threat Prevention white paper: <http://www.securecomputing.com/SWAT/>
15. Source: <http://cockeyed.com/lessons/viagra/viagra.html>

