
April 19, 2002

Email Systems: Threats and Defense

Email systems provide hackers the easiest route to critical corporate data



1105 Sanctuary Parkway
Suite 450
Alpharetta, GA 30044
Tel: 877.448.8625
www.ciphertrust.com

About this White Paper

This White Paper presents an overview of the vulnerabilities of email systems, and how they pose security risks to your organization. The reader will gain an understanding of the very real threats resulting from email server “exposure,” virus, worm and trojan horse attacks, and other vulnerabilities inherent in an email system. The reader will also learn that protection from these risks exists in the IronMail security appliance.

Information Technology and Security Managers, and other executives concerned with protecting their email systems will want to read this document.

The Crowded Gateway	2
The Only Comprehensive Security Solution For Email Systems ...	3
IronMail Functions	4
<i>Secure the Gateway</i>	<i>5</i>
<i>Secure Your Communications</i>	<i>8</i>
<i>Secure Your Webmail Systems</i>	<i>9</i>
The Unified Policy Manager: Define and Enforce Global Email Policy	10
A Robust and Scalable Solution for the Enterprise	11
<i>High Performance</i>	<i>11</i>
<i>Reliability, Availability & Scalability</i>	<i>11</i>
<i>Logging, Reporting and Monitoring</i>	<i>12</i>
<i>Integrated Alert Manager</i>	<i>12</i>
<i>Easy to Deploy and Manage</i>	<i>12</i>
<i>Benefits of IronMail</i>	<i>13</i>

Applications: The New Battleground

Email systems provide hackers the easiest route to critical corporate data

For most companies, the corporate perimeter is secure. Firewalls, combined with a handful of other tools such as intrusion detection systems, have established a solid line of defense for corporate networks. In fact, firewalls have been so successful that most attackers have ceased trying to attack them.

“They [hackers] want access where they aren’t allowed and the firewall has limited their targets and made it difficult. So they have moved their attacks up to a place where firewalls can’t touch them — at the application layer.”

*Hurwitz Group,
December 2001*

Instead, hackers are shifting their attacks to areas unprotected by network security tools—applications. In particular, email is being widely exploited to disrupt and violate corporate networks.

The newest, most dangerous threats are not deterred by network firewalls or IDS. Multi-threat worms like Goner and Nimda exploited email to fly past firewalls and IDS without registering a blip. By focusing on the vulnerable email application, hackers are effectively bypassing network level defenses.

And attacks against email systems can lead to serious consequences. They can affect every part of your corporation, causing the loss of proprietary, confidential information, significant downtime and legal liability. *Information Week’s* 2001 security survey puts the loss of proprietary information due to security breaches in excess of \$45 billion, with 64% of corporations experiencing security breaches.

The rogue's gallery of email threats includes:

Viruses and Worms like Goner, Nimda, and I Love You. If not blocked at the gateway, viruses and worms can cripple a large organization in a matter of minutes, leaving your organization idle for hours or days and costing millions to clean up.

Attacks such as buffer overflows deliver harmful code to your email servers or end-user desktops with the intention of crippling them. Like viruses, these attacks can cripple your company, costing you time and money. But it could be worse...

Corporate Espionage is on the rise. Attacks such as password or operating system hacks may not be intended to simply cripple your systems. Espionage professionals use these tools to gain entry to your systems and steal confidential information. Having your confidential corporate information in the wrong hands could be fatal to your company.

Spam, or unwanted email, is overwhelming corporate networks. The Gartner group notes that some Spam campaigns are becoming indistinguishable from a denial of service attack. The cost? Lost IT resources and reduced employee productivity.

"Hacking has become a global blood-sport and each business to business link creates a new hole. No matter how vigilant you are gateways equal risk."

Liability costs are another consequence. When is a joke not a joke? Ask Chevron, which paid out over \$2 million in damages after being held liable when employees circulated an offensive email. Email liability risks ranging from pornographic, offensive messages to email containing confidential corporate information needs to be intercepted before it can enter or leave the organization.

*Pricewaterhouse-
Coopers,
September 2001*

Content Exposure With email now the primary tool for business communication, protecting the privacy of messages is critical. Corporations need to be able to establish secure communications with remote offices and employees, partners, and customer.

The Crowded Gateway

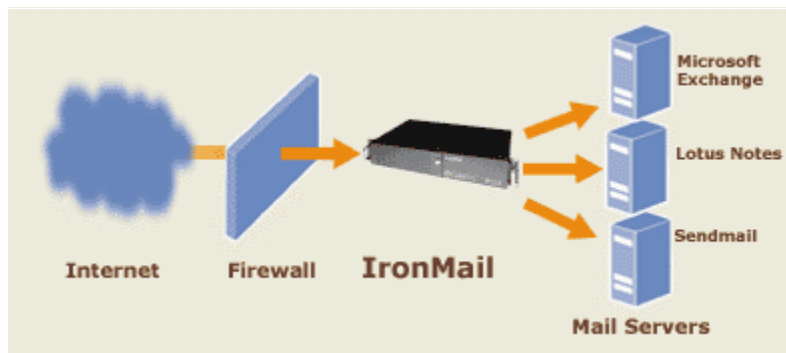
All of these threats require a response, and quite a few products aimed at addressing these threats exist. Most of these tools, including email proxies, virus scanners, content scanners, and encryption tools, require deployment at the Internet gateway. While this is the correct place in the network to address these problems, the traffic jam caused by all of these point solutions jockeying for space at the email gateway creates its own, new risks.

In fact, trying to deploy multiple solutions at the gateway, or on the mail server, can create significant additional risk to your network. While each solution may do a good job of addressing a specific issue, it likely also creates a new point of attack. For example, adding a virus-scanning package will most likely result in—you guessed it—less infections by known viruses. But the virus scanner software (not to mention the operating system it's running on) will be vulnerable to a wide variety of buffer overflows, denial of service attacks, etc., creating new vulnerabilities in your email system. Somehow, a way must be found to protect the entire email system. A different approach is needed...

CipherTrust approached this problem by taking a holistic view of the email system and providing corporations comprehensive protection from email risks. We provide an integrated solution, deployed at the gateway, which secures every aspect of the email system. The solution is **IronMail**, the secure email gateway appliance.

The Only Comprehensive Security Solution For Email Systems

IronMail, an all-inclusive email security appliance, sits at the mail gateway between your network firewall and mail servers. Every connection to your mail server(s) passes through IronMail.



IronMail is the first product designed to provide **application-level security** for email. What does this mean? It means that IronMail will not allow exploitation of vulnerabilities in your email systems or allow your email system to be used as a delivery vehicle for attacks.

“The IronMail appliance by CipherTrust is a comprehensive device to protect the corporate e-mail system from hacker attacks and other threats.”

Giga Information
Group,

Placed at the Internet **email gateway**, IronMail protects the entire email infrastructure, including all mail related servers. IronMail scrutinizes every connection and message received, ensuring that nothing harmful gets through, whether it is a buffer overflow, a self-propagating worm or a dirty joke.

IronMail **integrates** protection for the entire range of email threats seamlessly, ensuring the integrity of each defensive layer, and providing a manageable solution. Prior to IronMail, organizations deployed multiple point solutions in a piecemeal fashion to attempt to address the threat. As we mentioned, this approach creates more security holes, not less. Furthermore, effectively managing all of these solutions is quite difficult. IronMail, on the other hand, is easy to configure, manage and update.

IronMail is the only solution to fully address the needs of **enterprise** email security systems. Designed for complex, high volume environments, IronMail is based on a fully functional Messaging Engine, designed to parse and scan messages easily and quickly. IronMail enforces email policy across the organization, and supports integration with LDAP for group definitions.

IronMail allows you to configure alerts, reports and security responses within its simple, browser-based interface, and it can automatically update virus signatures every hour. The result is high performance, high security and high scalability.

Key Technology

Messaging Engine

IronMail is based on our patent-pending Messaging Engine. The Messaging Engine actually contains most of the functions of a full mail server engine, but it has been streamlined and optimized for IronMail. Designed for high-volume, enterprise environments, the Messaging Engine is designed to parse and scan messages within our unique queuing architecture, easily and quickly. The Messaging Engine allows true store and forward of messages as well as an onboard message store for quarantined mail. The result is a robust solution offering high performance, high security and high scalability.

IronMail Functions

IronMail combines hardware and pre-loaded and pre-configured software in an integrated appliance to provide a total security solution for your email system. IronMail addresses the three risk areas of email systems – the gateway, communications and webmail systems.

Secure the Gateway

The first step to achieving email security is control of the gateway. Controlling the gateway means scrutinizing every connection and message received. It means allowing nothing harmful to get through, whether it is a hacker exploit, a self-propagating worm or a dirty joke. It means identifying and stopping threats targeted at the security devices, the mail servers and the message recipients.

The range of threats targeted at email systems makes control of the gateway difficult. IronMail achieves this in two steps. First, it fortifies your email systems against attacks. Second, it screens every message for threats. IronMail ensures that only legitimate, non-threatening messages are allowed past the gateway.

Fortify

“Enterprises should, in 2002, begin planning for implementing application-specific firewall functions.”

*Gartner Group,
January 2002*

IronMail’s Mail-Firewall technology acts as an application-specific firewall, allowing only valid and safe connections to your email servers. Mail-Firewall’s capabilities include:

- Identifying and throttling denial of service attacks directed toward your mail server.
- Identifying and modifying messages and commands that fail to comply to Internet mail standards, in order to prevent buffer overflow attacks directed at internal servers.
- Proxying of SMTP, SMTPS, POP, POPS, IMAP and IMAPS to ensure that no direct connections are made to your mail server.
- Defense against exploits such as Malformed MIME headers via our Application Inspection Engine.
- Authentication of every connection to detect threats such as hijacked servers.
- Blocking unauthorized mail relays to prevent your corporate server from being exploited by a Spammer.
- Routing mail to multiple internal servers.

Additionally, IronMail's Mail-IDS, the industry's first, email-specific intrusion detection system (IDS), acts like a video camera to proactively monitor your mail servers 24 hours a day. IronMail detects suspicious, mischievous or unauthorized activities. Upon detection, it can notify security managers of impending threats or terminate specific connections to thwart attacks. Mail-IDS's capabilities include:

“IronMail is a product worth evaluating simply for its email firewall and email intrusion detection abilities.”

*Giga Information
Group,
January 2002*

- Identification and prevention of email-specific attacks such as password cracking or mail bombs.
- Measuring and reporting on end-user password strength.
- Monitoring and reporting on telltale signs of attack reconnaissance such as port scans.
- Detection and prevention of threats such as dictionary attacks which attempt to gain access to accounts by trying multiple usernames with simple, likely passwords.
- Verification of IronMail application and file system integrity to thwart attempts to implant Trojan horses or back doors.

Message Screening

Once IronMail has determined that a connection is legitimate, it then scans the contents of every message for known and potential threats. IronMail can identify and handle all manner of threats, sensitive content and liabilities.

IronMail protects email systems against both known and unknown viruses. It scans and detects known viruses by integrating anti-virus technology from Sophos™.

Key Technology

Application Inspection Engine

Current mail proxies do little to protect email systems. While a mail proxy can determine if an email command is a legitimate command, it has no understanding of the information that follows the command. Our Application Inspection Engine examines each message within the context of each mail command and its parameters, providing a level of protection not found in any other email security product. The Application Inspection Engine is capable of blocking difficult to identify attacks such as Malformed MIME and MIME header overflow, ensuring the highest level of threat resistance.

IronMail ensures timely virus detection with updates offered hourly and executed automatically. To address the more difficult issue of protecting against unknown or potential viruses, IronMail employs several tools, including attachment type scanning and keyword filtering. IronMail can be configured to block, hold, alter or quarantine suspect messages, based on the specific attachment type or keyword.

IronMail offers several tools to stem the Spam tide. Real-time Blackhole List support allows administrators to block communications from known Spammers. Reverse Domain Name System checking blocks access for hijacked servers. Keyword searching blocks, reroutes or quarantines messages based on keyword matching. Exception lists for RBL and reverse DNS checking ensure that administrators can override these tools for specific

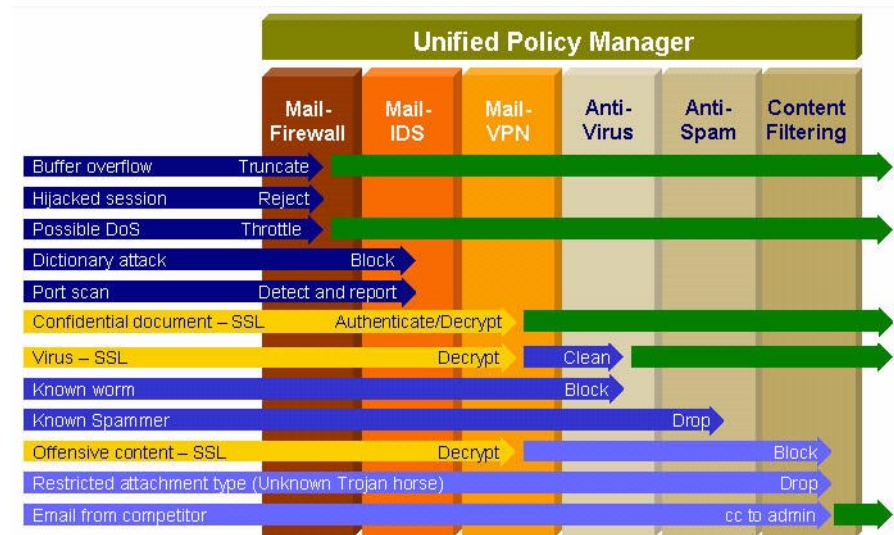
domains or IP addresses. In addition, IronMail can learn to identify patterns of Spam propagation via our Anomaly Detection Engine, allowing administrators to continually improve Spam blocking.

IronMail's content filtering features allow you to screen your email for questionable content. IronMail can perform keyword searches in the message headers, message body and text attachments. IronMail can also filter based on other characteristics such as message size and message type. IronMail gives you the options to block, hold or quarantine messages based on message characteristics. The result is administrator control over content flowing in and out of the organization through email.

Key Technology

Anomaly Detection Engine

The threats to email systems will continue to evolve, becoming more sophisticated and complex. To ensure protection against the next generation of attacks, IronMail now includes our heuristics-based Anomaly Detection Engine. This patent-pending technology monitors all events as the email traffic flows in and out and makes decisions based on a set of heuristics to determine malicious behavior. The engine can detect events like the Nimda or Melissa virus outbreaks before the virus signatures are known. It can detect Spam propagation or denial of service teltales. With the Anomaly Detection Engine, IronMail is fighting the threats of tomorrow, today.



Securing the Gateway: *Just a few examples of how IronMail scrutinizes incoming communications for threats of all kinds, and then terminates or neutralizes the threat. Only safe, legitimate messages (green arrows) are allowed to continue on to the mail server.*

Secure Your Communications

Once your gateway is secure, the next step is securing your communications beyond the gateway to include your external users, partners, clients and others. IronMail achieves this with our Mail-VPN feature.

Mail-VPN secures messages while they are in transit over the Internet, with no client interaction, using SSL technology. Mail-VPN can create secure tunnels to other mail servers or other IronMail units as well as end-users such as remote employees and telecommuters. Mail-VPN capabilities include:

- Guaranteed secure delivery by domain to create trusted networks of partners, remote offices and customers.
- Interoperability with SSL (Secure Sockets Layer) enabled mail servers such as Microsoft Exchange and Lotus Notes.
- Protection for remote employees (such as “road warriors” and telecommuters) to send or receive messages securely via SMTPS, POPS or IMAPS using the email client of the user’s choice, including Microsoft Outlook, Outlook Express, and Netscape Messenger.
- Encryption of passwords, message contents and message headers.
- Authentication of remote mail servers using VeriSign® digital certificate technology.
- Hardware-based cryptographic acceleration to deliver high throughput.
- Message relay for authenticated users, such as a field rep sending an email to a client, without fear of unauthorized relay.

Key Technology

Securing Email Using SSL

SSL is widely known as the technology that allows companies like E*Trade to conduct millions of dollars a day in transactions securely over the Internet. However, SSL is not specifically tied to web traffic (HTTP). SSL is a transport-layer protocol developed to secure TCP/IP-based protocols such as Internet Message Access Protocol (IMAP), Post Office Protocol (POP), and, of course, HTTP. By applying SSL technology to email, secure email becomes as easy to secure as web browsing.

“By year-end 2002, 80 percent of enterprises will implement browser-based e-mail, independent of e-mail systems.”

*Gartner Group,
December 2001*

Secure Your Webmail Systems

As email has become an integral part of both work and personal life, end-users are demanding access to their work email account even when away from the office. Most of this demand is for “webmail” systems such as Microsoft Outlook® Web Access (OWA) and Lotus iNotes. OWA and iNotes extend the messaging capabilities of Microsoft Exchange and Lotus Notes by offering access to corporate email accounts from any Internet browser. However, a growing list of security vulnerabil-

ities has kept security and e-mail administrators from offering OWA and iNotes to end-users. For instance, the Nimda worm attack in September 2001 exploited no less than 16 different flaws in Microsoft's Internet Information Services (IIS), the underlying web server technology for OWA.

IronWebMail is a module of IronMail that deals specifically with securing OWA, iNotes and other similar systems. It combines elements of both a secure email and a secure web solution to allow corporations to address the unique security demands of OWA and iNotes. IronWebMail confirms that every connection to your webmail server is legitimate and safe and scrutinizes the content for threats and attacks. IronWebMail's capabilities include:

- HTTP and HTTPS proxy to scrutinize and control all connections to the webmail server.
- Enforcement of protocol standards for formatting and compliance to prevent buffer overflow attacks.
- Detection and blocking of known threats including malicious code via an Intrusion Detection System that scrutinizes each request to the webmail systems against a signature database.
- Intelligent HTTP request checking to protect against "data driven" attacks such as hex encoding exploits, double hex encoding exploits and directory traversal attacks.
- Masking the webmail server to eliminate attacks targeted at IIS or other webmail systems.
- Strong Client Authentication to provide an additional layer of authentication at the gateway level.
- Full administrator control to allow administrators to tailor buffer lengths, IDS signatures, and other characteristics to their specific needs.

The Unified Policy Manager: Define and Enforce Global Email Policy

In order to manage the complexity of email security, IronMail incorporates a unified policy manager capable of defining, monitoring and enforcing email policy across the enterprise email infrastructure. Using our flexible rule-based engine, corporate policy for both inbound and outbound messages is defined using our simple browser-based interface. Rules can be defined and enforced for specific groups

either on IronMail or through LDAP or Microsoft Active Directory®. The unified policy manager can configure policy based on almost any characteristic or threat. For example:

- Define and enforce a consistent policy across anti-virus, anti-Spam, content filtering, Mail-Firewall, Mail-IDS and Mail-VPN.
- Block, reroute or blind copy mail messages from competitor's domains.
- Block or deliver large messages at off-peak hours to avoid network congestion.
- Block or reroute messages encrypted using S/MIME or PGP unless the user is not authorized to use these technologies.
- Integrate with LDAP or Active Directory or define user groups onboard, in order to enforce rules by group.
- Designate that email to a specified domain must be encrypted to guarantee secure delivery to partners, remote offices and customers.

A Robust and Scalable Solution for the Enterprise

High Performance

IronMail has been designed from the ground up to meet the performance and scalability needs of the largest enterprise mail environments. Our Messaging Engine allows IronMail to meet the performance needs of the most demanding corporate environments. In addition, IronMail provides hardware-based cryptographic acceleration to ensure high performance when encrypting with SSL and to offload encryption overhead from the mail server.

Reliability, Availability & Scalability

As an integrated security appliance, IronMail is designed and optimized to provide the reliability, availability and scalability required by medium to large enterprises.

- Reliable, redundant components such as hot-swappable, hot-spare mirrored RAID, dual redundant power supplies, and error correcting code (ECC) memory.
- High availability configurations to ensure zero downtime.

“The IronMail solution is transparent to users, email client and server agnostic, and potentially a valuable addition to an enterprise’s defense-in-depth email security.”

*Information Security
Magazine,
October 2001*

- Clustering support for scalability to meet the needs of the highest throughput environments.

Logging, Reporting and Monitoring

IronMail provides superior visibility into your email system and security with detailed, easy to understand logs. The daily reports give insight into email usage and traffic patterns, scan results, compliance with corporate email policy, and anomaly and intrusion monitoring data. IronMail logs can be exported or automatically redirected to a central log server for analysis using standard reporting tools. This also serves as a comprehensive log database for proactive threat analysis and forensic analysis. IronMail also provides access to message queues and quarantine queues for management of exceptions and immediate access to forensic data.

Integrated Alert Manager

IronMail allows real-time notification on a wide range of security and operational issues via a pager or email. The alert manager allows administrators to configure which alerts trigger a given action based on the needs of their environment. It can integrate with leading network management systems such as NetCool®, Tivoli™ and HP OpenView™, based on the SNMP protocol.

Easy to Deploy and Manage

Designed as a true appliance, IronMail can be installed and configured in minutes. No software needs to be added to your mail servers or email clients. Key features include:

- Intuitive, secure, browser-based graphical interface for administration and management.
- Secure remote management with optional strong client authentication.
- Automated and secure update management, with updates as frequent as hourly.
- Multi-user administrator access to allow multiple administrators to be defined, with each user given access to a subset of the interface.

“We were planning to implement three separate products to secure our e-mail infrastructure, but IronMail provided a single, integrated solution that met our e-mail security needs. IronMail fortified our e-mail systems at an affordable cost, with no hassle.”

*John Warren, Internet
Technology Manager,
ESCO Corporation,*

Benefits of IronMail

Protect confidential corporate information from intruders and competitors.

IronMail ensures that your email servers and other associated business servers are safe from the threat of hackers, competitors or disgruntled employees. This enables you to protect your most valuable assets and maintain your competitive edge.

Ensure uptime and increase productivity by eliminating viruses and Spam.

Slam the door on viruses, worms, Trojan horses, Spam, or any other intrusion that can interrupt your normal business operations. IronMail eliminates downtime of your mail systems and maintains employee productivity.

Provide privacy for email messages in-transit over the Internet.

IronMail ensures that whether you are sending financial transaction data, product plans, or employee records, your email messages cannot be snooped or altered by intruders. IronMail allows you to create a trusted network of internal and external users, partners and customers.

Reduce corporate liability by monitoring and enforcing email policy.

Define, monitor and enforce corporate email policy in a unified, integrated fashion to ensure a comprehensive email security environment. IronMail gives you to control over your email infrastructure.

Plug and protect your email systems.

The IronMail appliance can be easily and rapidly plugged into your existing email and security infrastructure to provide immediate protection. Save time and money and secure your email infrastructure.

Attractive Return on Investment

Email is mission critical. It often contains highly proprietary and confidential information. You can't afford to have your email servers hacked or brought down by intruders, viruses, worms, or Trojan horses, or to have your servers used as conduits for questionable, inappropriate content. IronMail protects corporations against these business risks, provides a cost-effective solution with a very attractive return on investment and gives you peace of mind.

