



A DIRECTORY-DRIVEN APPROACH TO EMAIL SECURITY:

Using Directory Information to Optimize the Enterprise
Email Infrastructure.

Sendmail Directory™ and Sendmail DirSync™

May 2007

INTRODUCTION

The most common security threat to email and groupware is the relentless growth in unwanted email. New and improved methods for identifying and blocking spam have emerged but spammers are adapting with creative ways of getting bad mail through. With 70% of all enterprise data traveling within email and the percentage of bad to good mail racing past 85%, there's a major need to refine the process.

It's clear, traditional approaches like scanning, and reputation services alone are just not enough. To defend the email network effectively, enterprises need to apply additional intelligence to existing methods and policies.

This paper outlines how messaging directories provide a proven range of benefits that improve security and increase performance. These benefits include:

- Controlling message acceptance
- Routing mail accurately and efficiently
- Addressing regulatory compliance
- Enforcing complex corporate security policies
- Authenticating users and other security functions

This solution paper will demonstrate how Sendmail delivers these benefits by providing the only secure, scalable, and standards-based directory server that is tuned, secured and optimized for messaging.

HOW DIRECTORIES OPERATE.

In just a few years, email has arguably become the most important business communication tool. A directory server functions as a type of database. Unlike databases that are designed for processing hundreds or thousands of changes per minute — such as e-commerce Online Transaction Processing (OLTP) systems — directory servers are heavily optimized for read performance.

Directories are particularly useful for storing information which is accessed from many locations, but updated infrequently. Typical examples of data stored in directory servers includes:

- Employee phone book and organizational relationships
- External customer contact information
- User account information including passwords and group memberships
- Infrastructure services information: Network Information Services (NIS) maps, email aliases, etc.
- Configuration information for distributed software packages
- Public certificates and security keys

Most directory servers use an industry-standard protocol for accessing their data: LDAP. There are many commercial and open source vendors who offer directory server products. Some examples include: Microsoft Active Directory, Lotus Domino, Novell eDirectory, Netscape iPlanet/Sun One/Fedora Directory Server, and the Sendmail Directory Server. Directory data also can reside in relational databases and in flat text files.

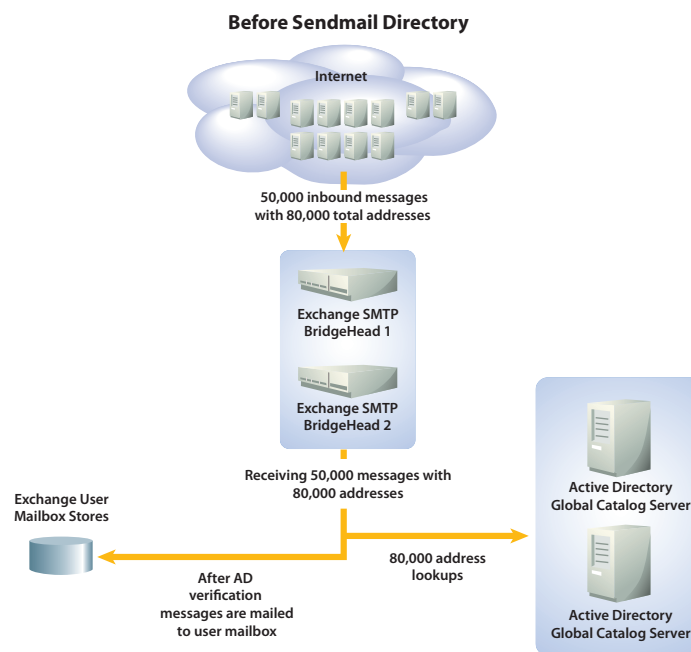
LDAP-based directory servers provide high performance, centralized management, and high levels of security when accessing or updating data, this includes options for delegated management of data.

Other non-LDAP directories do exist, including X.500, certain relational database, NIS. These directory options usually lack some of the benefits of LDAP-based solutions.

WHY IMPLEMENT DIRECTORY-DRIVEN EMAIL SECURITY?

Corporate directories hold valuable corporate information used to drive enterprise applications and control user access. This typically includes information such as user profiles, HR info, email aliases, forwarding information, reporting structures, security clearances, and administrative roles. The value of this information to the email network is significant when it can be securely accessed to:

Control the Perimeter Connection – Block connections from mail servers attempting to send email to invalid addresses. This reduces spam, conserves system resources and defends against directory harvesting attacks.



In this example, one connection represents 50,000 messages with 80,000 addresses. These inbound messages are about to impact the Microsoft Exchange and Active Directory environments.

Synopsis This solution paper describes the directory-based email security solutions of Sendmail, the first company to develop LDAP-compliant directory products specifically designed to optimize email processing. Sendmail's directory product is the most widely deployed messaging directory on the market today.



Mail Routing – Consolidate routing information from multiple groupware solutions and directories into a single, centralized directory. This information can be used to optimally route messages to intended recipients and mailstores.

Compliance – Implement policies based on sender and/or recipient directory attributes, for compliance with SOX, HIPAA, GLBA, NYSE 404 and SEC regulations. For example, one might implement a policy to archive all inbound messages to brokers, or to automatically encrypt messages containing identifiable health information.

Email Policy – Enable policy-driven email processing using the intelligence provided by the directory metadata. To adhere to corporate governance requirements, businesses might encrypt messages between executives, or scan outbound email for specific attachments (protect IP) or monitor for inappropriate language.

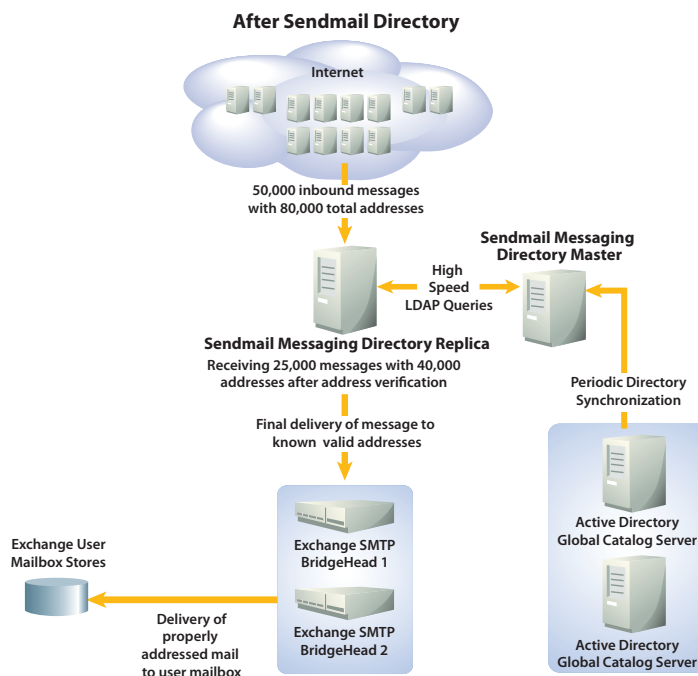
Authentication – Manage authentication of user accounts and access controls using the directory. This includes SMTPAUTH, quarantine, access to mailstores and administrative interfaces. In addition, Sendmail allows you to manage certificates or synchronize with an external PKI.

Protects the Messaging Infrastructure – Email networks are vulnerable to dictionary attacks, directory harvesting and connection flooding. With directory-driven email security, enterprises can turn away messages addressed to invalid recipients, even before the message is accepted, avoiding the need to scan for spam and viruses. This reduces system computing and network resources processing undeliverable mail.

Enterprises seeking to reduce their volume of unwanted mail need a secure and optimized messaging directory system, synchronized with all internal directory data, creating a high-speed centralized directory for address validation at the gateway.

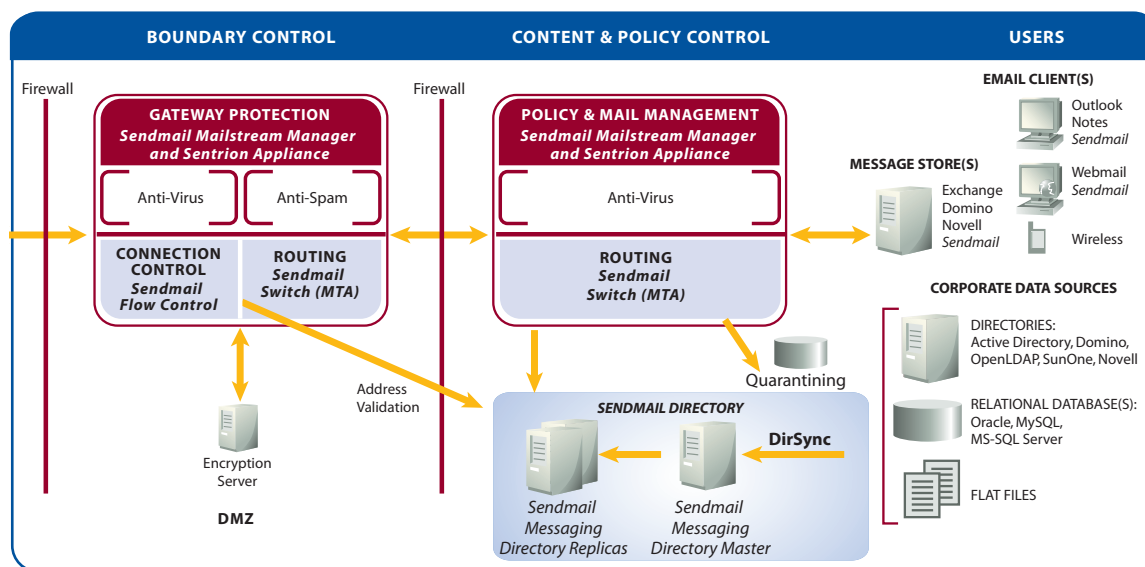
Directory-driven email security delivers a significant ROI:

- Reduce email traffic by only accepting email for valid recipients



With Sendmail Directory in place, unwanted messages are dramatically reduced (typically by 50%) at the gateway, resulting in a significant reduction in network bandwidth, CPU load for scanning, and storage requirements. With Sendmail in front of them, Exchange and Active Directory are protected and operate more efficiently.

- o 50% reduction in mail volume
- o Corresponding reduction in network bandwidth
- o Reduced CPU load when scanning for spam and viruses
- o Less storage required for archiving or queuing of unwanted messages
- Lower load on groupware systems
 - o Fewer queries to locate message recipients within the organization
 - o Eliminate outbound bounce messages from mailstores
 - o Increased performance and reliability of groupware mailservers
- Implement powerful policy controls for regulatory and corporate compliance
 - o Selective archival and routing based on groups and roles
 - o Secure delivery of inbound/outbound mail based on roles, customer type, etc.
 - o Custom handling instructions for specific types of mail



Sendmail Directory and DirSync (shaded) are key parts of Sendmail directory-driven email security. The architecture delivers a proven, standards-based, and secure method of weaving intelligence into the email security infrastructure. Other Sendmail products that integrate with Directory are listed in italics.

THE SENDMAIL SOLUTION FOR DIRECTORY-DRIVEN EMAIL SECURITY.

Sendmail Directory and Sendmail DirSync

Sendmail Directory is a comprehensive, standards-based directory solution. It is the most widely deployed commercial LDAP directory specifically designed and tuned for the enterprise email infrastructure. Sendmail has devoted over seven years of development and significant experience gained in hundreds of customer deployments perfecting this solution.

Sendmail Directory centralizes users, alternate email addresses, groups, mail distribution lists, administrative groups and policy-related information into a centrally managed data repository. Directory provides this information to email servers across the enterprise to add intelligence to gateway security, routing, and policy enforcement.

The Directory server environment consists of the Sendmail Messaging Directory Master (SMD Master) and Sendmail Messaging Directory Replica (SMD Replica). The SMD Master and Replica servers securely provide directory data for utilization throughout the entire email network. Updates from the corporate directory occur on the SMD Master, with SSL-secured, one-way replication happening in real time to each of the SMD Replica servers.

Within the Sendmail Directory environment, only data required for messaging is accessible

on the SMD Replica servers. Under this configuration, the corporate directory information is never within direct reach of email servers, or the Internet, and is always kept secure.

AUTOMATED DIRECTORY SERVER MANAGEMENT: SENDMAIL DIRSYNC

For companies that already have one or more sources of user information, Sendmail DirSync can be added to a Sendmail Directory implementation. DirSync provides automatic synchronization of the data in the Sendmail Messaging Directory Master (SMD Master) using the information from one or more data sources.

Supported data source connectivity includes directory servers such as Microsoft Active Directory, Lotus Domino, Novell eDirectory, Netscape iPlanet/Sun One/Fedora Directory Server, Open LDAP, and virtually any other standards-compliant LDAP v3 directory server.

DirSync is also able to pull data from NIS, relational databases and text file sources.

DirSync automates complex directory functions, eliminating the need for extensive directory synchronization expertise. With DirSync there are no new tools for systems administrators to learn or use. When changes are available, from any of the data sources, DirSync will use that information to update the SMD Master either selectively or in batch mode.

The Sendmail Directory Architecture Advantages:

- Tuned for optimal performance in email environments
- SSL-secured connections for replicating from master to replica servers
- Automatic synchronization from the widest set of structured and unstructured data sources
- Directory servers are pre-configured with access controls to protect sensitive data
- Extremely lightweight and scalable, proven at customer sites ranging from 300 to 2 million users
- Flexible configuration supports additional usage beyond messaging environments
- Real time replication from the centralized directory to the SMD Master to the SMD Replica servers
- Powerful data validation to ensure the highest possible data integrity



Without changing existing tools and processes, DirSync allows information stored in non-standard formats to be used to provide mail validation and routing information for the email environment. Example: taking user information from an Active Directory source and mapping the mail server information stored there to industry-standard DNS names for email delivery.

DirSync can also auto-provide alternate email addresses in a number of ways. DirSync can automatically combine first and last names to provide First.Last@domain addresses, with automatic duplicate addresses detection and validation and reporting. DirSync can also provide alternate domain email addresses, which can be extremely useful during corporate mergers.

The Sendmail directory-driven email security environment is designed to be flexible and easy to administer. To augment and validate the directory information being supplied by DirSync, Sendmail Directory provides the Sendmail LDAP Console, a complete set of administrative interfaces to create, edit, delete, and manage contents of a directory server.

SENDMAIL DIRECTORY LEVERAGES BEST PRACTICES IN ENTERPRISE SECURITY

The LDAP protocol was designed with security in mind, but it is up to each directory server vendor (or application developer) to implement

that security. By default, access to any directory server for information is only as secure as that directory server's 'typical' configuration.

While many enterprises see the benefits of integrating directory information into the email infrastructure, most have concerns about the ability to access directories securely and efficiently without compromising confidential data or exposing the entire directory to an organized attack. By leveraging best practices in email security, Sendmail addresses the following security concerns:

Directory Access from the DMZ into the Groupware Environment – Data in the directory environment is secured by a robust set of access controls and by the server topology. The Sendmail master and replica directories are configured with one-way synchronization, so the groupware network is never within reach of hosts in the DMZ or the Internet.

Component Parts of Sendmail Directory:

Sendmail Messaging Directory Master (SMD Master & Replicas) – Provides centralized directory information from backend sources, optimized and secured for enterprise messaging. SMD uses SSL-encrypted directory connections for secure replication. This directory product is extremely lightweight compared to other directory server solutions, using up to 100 times less memory and disk space per machine.

Sendmail LDAP Console – An extensible, delegated administrative Web GUI used to manage domain, account, email distribution list, and administrative data within the directory.

Sendmail Authentication Proxy – Ties SMD Master and Replicas to Kerberos or non-Sendmail directory servers for pass-through authentication purposes.

MTA Enablers – Automatically manages the configuration of routing MTAs to dynamically change email acceptance and routing functionality when domains are added to or removed from the directory.

Mailstore Enablers – Manages all aspects of the Sendmail mailstore environment based on directory information. This is used to drive account provisioning and removal, quota management based on classes of servers, and message aging and retention policies (e.g., SOX compliance).



Managing Multiple Directories in Multiple Locations.

Corporate mergers, acquisitions and restructurings have a significant impact on directory infrastructures. Disparate domains, directory products, and geographic distribution across an organization present an administrative challenge. DirSync helps consolidate data from multiple directory sources, providing a means to move data from multiple sources/locations into a single location. DirSync is capable of pulling information from any LDAP-compliant data source and adapting it to the standard format, and there is no need to reconfigure existing directory servers.



Directory Access Slows the Groupware Environment – All directory updates occur in batch mode, and lookups happen between the messaging environment and the Sendmail Messaging Directory Replica servers. Because of these access controls there is no impact on groupware performance.

Additional Hardware for Dedicated Servers – Sendmail Messaging Directory Replicas do not require dedicated servers. The Directory Services environment is optimized specifically for messaging and is lightweight, up to 100 times less than typical directory servers. SMD servers are designed to run on machines that also run the Sendmail MTA, or on the Sendmail Sentrion email gateway security appliance.

Administrative Concerns to Manage Data and Tools – Sendmail Directory uses DirSync to automatically populate directory server information from the corporate directory source into the Sendmail directory server environment; there is never a new interface or tool to learn.

Complexity of Reconfiguring the Sendmail Existing Backend Directory Environment – Directory is preconfigured and optimized for messaging environments. Because the email environment does not directly contact the groupware directory servers, there is no need to reconfigure that environment with access controls or additional indexing information.

Two Way Synchronization With Active Directory or Other Directory Servers – As a default other email security vendors provide two-way synchronization. If one server in their directory

environment is compromised, an intruder can maliciously alter the data stored throughout the directory environment. With the Sendmail solution, mail servers only talk to Sendmail Messaging Directory Replicas, which use one-way master-to-replica synchronization. Data pollution is not possible, and the corporate directory is always secure and out of reach.

With directory-driven email security, enterprises leverage a proven and secure method of integrating security throughout the email infrastructure. Sendmail Directory is the only directory server environment preconfigured for high performance and complete security in an email environment.

KEY PRODUCT FEATURES THAT ENABLE DIRECTORY-DRIVEN SECURITY.

Standards-compliant and Interoperable

Sendmail Directory is a true LDAPv3 directory server based on open industry standards, enabling deployment in any environment where applications use standards-based protocols to access directory servers.

Sendmail works with: Microsoft Active Directory, Lotus Domino, Novell eDirectory, Netscape iPlanet/Sun One/Fedora Directory Server, Open LDAP, and virtually any other standards-complaint LDAP v3 directory server.

Centralized Messaging Data Repository

Sendmail Directory provides a single-source repository to improve the integrity and reliability of data, and allows administrators to easily automate provisioning tasks and provide users a single, self-service interface. This enables IT to focus less time on user maintenance and more time on strategic issues. Companies with multiple directory environments can realize significant benefits from a single repository of messaging information.

High Availability and Reliability

Sendmail Directory is a secure, lightweight, high performance, LDAP-compliant, directory environment. It is designed to enable security and performance throughout the email infrastructure. As updates to directory information occur on the Directory Master, real-time push-based replication securely sends the changes to the replica servers.

This architecture is designed to scale to geographically distributed environments, and is capable of providing the redundancy necessary to withstand large-scale network outages and catastrophes.

Advanced Authentication Support

Allows enterprises to store provisioning and routing data in the directory; validate authentication credentials against Kerberos, or any non-Sendmail LDAP Directory Server.

When using Directory with DirSync to synchronize data in some environments, passwords can be pulled directly into the Sendmail LDAP environment. In other instances (including Active Directory, Domino, and Kerberos environments) password synchronization is not possible. For these situations Directory provides an automatic pass-through authentication request to the corporate authentication source. This is far superior to competitive solutions which require special plugins and tools that run on the corporate servers.

Supports Multiple Internal Email Environments

When there are multiple mail servers within the enterprise, mail routing is unpredictable. Directory, together with DirSync, solves this problem, automatically, providing updates to user and distribution list routing and acceptance information from all of the directories and data sources in the enterprise, and populates that information into the Directory Master.

Integrated Tools for Easy Management

Sendmail Directory includes the Sendmail LDAP Console and tools to load, back-up and restore a directory, without requiring the administrator to be an LDAP directory expert. Scripts and documentation are also available to assist in monitoring the health and operations of the directory. In addition, Directory provides a full suite of command line tools for use when the GUI is not convenient, such as when processing large batches of changes.

Manage Multiple Domains, Delegate Responsibilities

The Directory administrative GUI provides granular, delegated administrative options. Delegation is on a per-domain and per-function

basis. Example: Administrators can grant some people email list management roles, but those same people cannot edit user accounts.

SENDMAIL DIRECTORY: STANDARDS-BASED INTELLIGENCE TO SECURE THE ENTERPRISE EMAIL INFRASTRUCTURE.

Sendmail Directory is a proven and secure method of using directory information to increase security across the entire email infrastructure. All Sendmail products are designed to integrate with and leverage directory server data to unify administration, user access, and key routing components to take maximum control over the messaging environment.

Sendmail's benefits are clear:

- Volume of accepted messages reduced by a minimum of 50%
- Defense against directory harvesting attacks
- Enhanced network and mailstore efficiency
- Optimized routing and delivery accuracy
- Improved corporate and regulatory compliance
- Powerful policy management
- Delegated and centralized administration

EMAIL INFRASTRUCTURE AND DIRECTORY ANALYSIS

As a trusted advisor with over 1,000 enterprise messaging implementations, Sendmail knows the challenges facing large organizations today, and provides products and services that enable 360-degree management and security of business communications.

To enable this Sendmail has designed an "Email Architecture Review" service. The "Email Architecture Review" analyzes the configuration of the messaging infrastructure, documents findings, and provides Sendmail "Best Practice" recommendations for the future. All of the principle systems in the messaging environment will be reviewed.

For more Information, or to schedule an Architecture Review, please contact Sendmail directly at 1-87-SENDMAIL (877-363-6245), or send an email to: archreview@sendmail.com

About Sendmail

Sendmail is the leading global provider of trusted messaging. With 25 years of leadership delivering innovative messaging technology, Sendmail ensures the protection and trust of employee and customer communications. Sendmail technology, driven by the industry's most powerful and flexible policy engine, provides protection where 80% of security and compliance violations occur - within inbound and outbound messaging. Large enterprises in 33 countries, and the majority of the Fortune 1000 trust Sendmail to shield users from unwanted messages, defend the messaging infrastructure, stop data and privacy leaks and effectively manage messaging to maintain brand and shareholder value and support regulatory compliance. Sendmail is headquartered in Emeryville, CA with offices and distributors in Europe, Asia and North America.

Sendmail, Inc.

6425 Christie Avenue,
Emeryville, CA 94608
Tel: +1 888 594 3150
Fax: +1 510 594 5429
www.sendmail.com