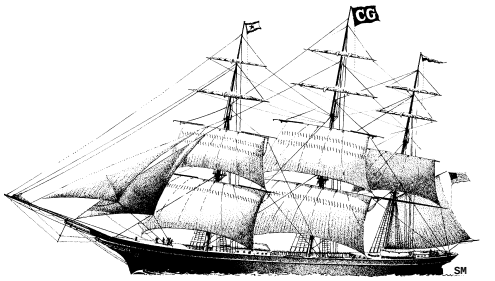
THE CLIPPER GROUP
# Navigator™



*Navigating Information Technology Horizons*℠

Published Since 1993 Report #TCG2005070 October 31, 2005

# Ruggedizing E-Mail — The Symantec/Veritas Solution

Analyst: Anne MacFarland

## Management Summary

The ideal of a trusted environment, under which much of today' IT processes were developed, is no longer a realistic design point. Actually, it has always been a comely but improbable concept, usually anchored to a place and to a point in time (often conveniently in the past). Gregarious partnering, usually undertaken to spread the risk and up-front costs of "global" operations, has led enterprises down a path of collaboration and geographic dispersion. Isolationism in such an environment becomes difficult and expensive to support. Enterprises see clear advantages to having multiple suppliers and multiple distribution channels keep operational costs under control, but they also produce an environment where trust should not be assumed. The edge to be fortified has become a pervasive fog.

**The response to pervasive fogs and other inclement situations is *ruggedization*, an attribute taken from telecommunications, transportation, military operations, and other industries and activities where the environment cannot be controlled.** In telecommunications, transmission elements must withstand the environment at the top of a telephone pole. In other industrial and military uses, equipment must function under water, or in high temperatures. It must withstand being dropped, hit with bullets, or installed at an angle to the pull of gravity. Like history's intrepid self-reliant explorers, who traveled in groups and carried all the supplies and weapons they might need, **ruggedization seeks to counter all the controllable risks that can be anticipated locally.**

These days, threats to IT environments abound from without and within. E-mail, the poster child for the new way of doing business both internally and externally, faces them all. Either we can try to wall off all the threats, which erode the usefulness of e-mail as a freewheeling communications medium, or we can beef up the email process, and its security, to meet the ongoing and quickly evolving challenges to its integrity. The former is counter-effective: the latter, a pervasive solution approach, is a better way, and one that can be modified as needed.

The baked-together combination of security enforcement and process control - that the combination of Symantec and Veritas can deliver - produces a rugged e-mail solution. Read on for more details.

## IN THIS ISSUE

## E-Mail Basic Requirements

There are three basic mandates for E-mail.

- ***Availability*** - E-mail must be available. The approach to spam and viruses must be deft enough so that the real mail gets through promptly but spam and viruses do not.
- ***Bulk Management*** - The volume of mail, and, increasingly, the content, must be managed. Frequently, all mail must be kept to document the operations of the enterprise, as a part of corporate documentation, governance, and regulatory compliance. Burgeoning mailboxes must be managed by quotas and offloading to an archive. In addition, the content of email must be in some ways searchable. This is needed for regulatory compliance and for the unavoidable threat of legal discovery orders, but it also needed, increasingly, for business coordination, collaboration, and expertise location.
- ***Integrity and Privacy*** - E-mail is both a form of documentation and a form of communication. As documentation, the integrity of the record must be protected from loss, corruption and tampering. As communication, the confidentiality of the contents, and sometimes, the privacy of the correspondents, must be assured.

The trick is to satisfy fully all three parameters at once. **Pervasive security must be an inherent part of the processes from end to end, in order that ease-of-use does not become ease-of-misuse.**

## Ruggedizing E-Mail Reception

Normal e-mail reception includes mailbox quotas, anti-virus and perhaps anti-spam point products. A dynamic, real-time component is key to a ruggedized solution. Lists of threats are useful for trending and after-the-fact forensics, but they do not fully address the dynamic nature of the problem.

The *Symantec Mail Security 8160* is an example of such a component. By using a strategy of constraining the bandwidth allocated to identified spam, the router hits the spam server where it hurts, inhibiting its performance while it quarantines the spam before it hits enterprise systems and becomes part of the incoming mail that must be saved. Over time, Symantec experience has shown that the enterprise protected by such a strategy becomes a less-attractive target and receives less spam, allowing fewer SMTP[1] gateways to be needed. Of course, the usefulness of this approach depends on the accuracy of spam identification. Symantec's expertise in this area came with *Brightmail* acquisition.

This vital edge capability is available as software, appliance, or hosted service, whichever best fits customer capabilities. An equivalent product is also available for Web environments, managing HTTP and FTP traffic in a similar way, and for other network elements including caching servers and NAS.

## Ruggedizing Active E-Mail

To manage - properly - enterprise e-mail environments, an integrated wholeness is the key. Symantec mail security products for both Microsoft *Exchange* and Lotus *Domino* build on the basics of a heuristics-based anti-spam engine, custom filtering white lists, and other customizing options. They can include a premium anti-spam option (the Brightmail intellectual property), Symantec's research and support, and tight integration with the underlying E-Mail application. These products protect both incoming and outgoing E-Mail. Symantec's other security products, such as their *Symantec Client Security* and *WebRecon*, can enhance the security of the larger IT environment of which the e-mail application is a part.

Volume management from Veritas adds new dimensions of granularity to e-mail quota management. Clustering from Veritas adds high availability to e-mail[2]. Data recovery is provided both by Symantec's client agents and data services and by Veritas' volume management and replication. In the future, more integrated indexing will increase the business utility of e-mail – and the ability to target additional protection by content.

## Symantec *Enterprise Vault*

Transferring material to an archive is a

[1] Simple Network Transport Protocol.

[2] Remember, few explorers traveled alone, or with a single horse.

basic way to maintain control of a constantly growing volume of fixed data. Having a separate, policy-protected archive is a basic part of corporate governance and the basis of many forms of regulatory compliance. Because so much of business intellectual property, contractual agreements, and sources of legal liability reside in e-mail correspondence, its preservation is not something to be taken lightly by any organization that wishes to maintain a good reputation. Retention must be based on policy, not whim.

*Enterprise Vault* automatically indexes[3] all messages passing through *Microsoft Exchange* and stores them in their original form in a journal archive[4]. A stub is left in the mailbox, by which users have access to the e-mail housed in the enterprise vault. Enterprise Vault supports appending categorizing information, defining retention and business use, as well as the content-based attributes of indexing. The Vault can be segmented, for example, along departmental lines, to simplify the implementation of tiers of security. It can also import existing PST file data, either as a server-side *pull*[5] or as a client-side *push*, restoring searchability to these files.

Users can search all of their files through outlook or with Enterprise Vault's web-based search. The Enterprise Vault also has an option to provide broader, permissions-based search access to e-mail beyond one's own quota, and the ability to provide users with a local vault, on their PC drive, for offline access.

The Enterprise Vault is managed through the *Microsoft Management Console*[6]. It is media-agnostic. Further, it is integrated with *Symantec NetBackup*, and the EMC *Centera*, Network Appliance *NearStore*, and IBM *TotalStorage DR550* compliance arrays. A *Tiered Storage Option* automates the migration of files to different locations and/or media as they age. Single instancing of attachments and compression of data can also be done at this time. In addition, two enhancements further ruggedize the Enterprise Vault for the realities of today's business practices.

### *Discovery Accelerator*

Today, the risk of being served with a legal discovery order can never be fully avoided. Processes can and should be put in place to make the discovery process both easy and well controlled. *Discovery Accelerator* facilitates targeting, search, discovery, marking, and review of inbound and outbound e-mail. It includes the audit tracking and reporting to document due diligence. The Discovery Accelerator does not modify the original file, allowing the existing "last accessed" value to persist. Content can be copied to external files for deeper perusal. The search results also are retained, so that searches can be extended or modified.

### *Compliance Accelerator*

*Compliance Accelerator* allows organizations to sample and review relevant e-mail, and provides an audit trail of this activity to both achieve and prove compliance with regulations such as SEC 17a-4 and NASD 3010 and 3110. This proactive sampling does not involve manual processes[7] or administrative overhead. The review processes, once structured to the requirements[8] of the particular organizations, samples and then presents to a reviewer[9] only the emails that conflict with the regulations. Compliance Accelerator is available only for Exchange environments, at this time.

---

[3] Symantec uses Hummingbird's Enterprise 2005 content management platform for this.

[4] Enterprise Vault can also archive Microsoft and Network Appliance file systems, instant messaging and Microsoft *SharePoint* portal content, which are beyond the scope of the E-Mail solution but provides a useful extension into a broader fixed content solution.

[5] The latest version of Enterprise Vault has a" PST Sniffer" to seek out distributed PST files.

[6] In Lotus environments, there must be a Windows server to host Enterprise Vault management.

[7] Compliance Accelerator does support manual sampling for the times when it is required.

[8] These requirements can be set for ranges of senders and recipients, internal or external e-mail, particular words or phrases, and date ranges. Previously reviewed emails can be excluded from re-sampling. Sampling can be of email from a group or of a specific individual, and the percentage sampled can be set.

[9] Reviewers can invoke a pending status during the review, annotate reviewed messages, and can forward eh message in question if needed. All aspects of the review process are documented.

### *E-Mail Solution Extends Benefits Beyond Email*

If an enterprise handles its e-mail properly, many other IT utilities are enhanced. The discovery and documentation of compliance have already been mentioned. Enterprise data backup and recovery is simplified with most of e-mail's bulk segregated in the Enterprise Vault. Enterprise search can benefit by the more comprehensive e-mail searchability that Symantec's e-mail solution provides. In general, the Symantec E-Mail Solution changes e-mail from being part of the problem – a large part, often – and makes it part of the solution.

## Pricing and Roadmap

The combination of Symantec and Veritas offers a rich variety of delivery options – you can get this solution and others, in the future, as software, as a hosted service, or as an appliance. Many enterprises will want to take advantage of more than one paradigm, depending on how and where their operations are distributed.

Pricing is per user, regardless of how many servers the enterprise uses to implement the solution. This lets a business configure its e-mail topography locally, to serve its users best, without worrying about additional licensing fees. The pricing paradigm is also simple, and unclouded by technology definitions.

The scope of research and development across the now combined companies is broad, and the combination of storage and application management with security is an area full of promise for information-centric products and solutions.

As email becomes a component of a broader collaborative environment, the ruggedization of Symantec's E-Mail Solution can be extended to workflows. This applies most obviously to workflows subject to government regulations, but the benefits, in terms of satisfying both the enterprise need-to-know and its need for end-to-end security, may make this solution a paradigm for data solutions in other enterprise operations.

## Conclusion

Some idealists portray trusted environments as the epitome of the benefits of human civilization. For those with a more pragmatic view of how human civilization generally works, a ruggedized environment is the ideal that will work better over the long run. E-mail will continue to be of vital importance to enterprises. It houses a lot of intellectual property, and is the audit trail of partnerships and commerce. More collaborative business models will only make its proper management more important. Symantec has built a solution that is and will remain a key to keeping your business up and running.

### About The Clipper Group, Inc.

***The Clipper Group, Inc.,*** is an independent consulting firm specializing in acquisition decisions and strategic advice regarding complex, enterprise-class information technologies. Our team of industry professionals averages more than 25 years of real-world experience. A team of staff consultants augments our capabilities, with significant experience across a broad spectrum of applications and environments.

- ***The Clipper Group can be reached at 781-235-0085 and found on the web at www.clipper.com.***

### About the Author

***Anne MacFarland*** **is Director of Infrastructure Architectures and Solutions for The Clipper Group.** Ms. MacFarland specializes in strategic business solutions offered by enterprise systems, software, and storage vendors, in trends in enterprise systems and networks, and in explaining these trends and the underlying technologies in simple business terms. She joined The Clipper Group after a long career in library systems, business archives, consulting, research, and freelance writing. Ms. MacFarland earned a Bachelor of Arts degree from Cornell University, where she was a College Scholar, and a Masters of Library Science from Southern Connecticut State University.

- ***Reach Anne MacFarland via e-mail at Anne.MacFarland@clipper.com or at 781-235-0085 Ext. 128. (Please dial "128" when you hear the automated attendant.)***

### Regarding Trademarks and Service Marks

**The Clipper Group Navigator**, **The Clipper Group Explorer**, **The Clipper Group Observer**, **The Clipper Group** *Captain's Log*, **The Clipper Group Voyager**, and *"clipper.com"* are trademarks of The Clipper Group, Inc., and the clipper ship drawings, "*Navigating Information Technology Horizons*", and "*teraproductivity*" are service marks of The Clipper Group, Inc. The Clipper Group, Inc., reserves all rights regarding its trademarks and service marks. All other trademarks, etc., belong to their respective owners.

### Disclosure

Officers and/or employees of The Clipper Group may own as individuals, directly or indirectly, shares in one or more companies discussed in this bulletin. Company policy prohibits any officer or employee from holding more than one percent of the outstanding shares of any company covered by The Clipper Group. The Clipper Group, Inc., has no such equity holdings.

### Regarding the Information in this Issue

The Clipper Group believes the information included in this report to be accurate. Data has been received from a variety of sources, which we believe to be reliable, including manufacturers, distributors, or users of the products discussed herein. The Clipper Group, Inc., cannot be held responsible for any consequential damages resulting from the application of information or opinions contained in this report.