

COMPUTER TECHNOLOGY REVIEW

STORAGE TECHNOLOGY & NETWORK SOLUTIONS

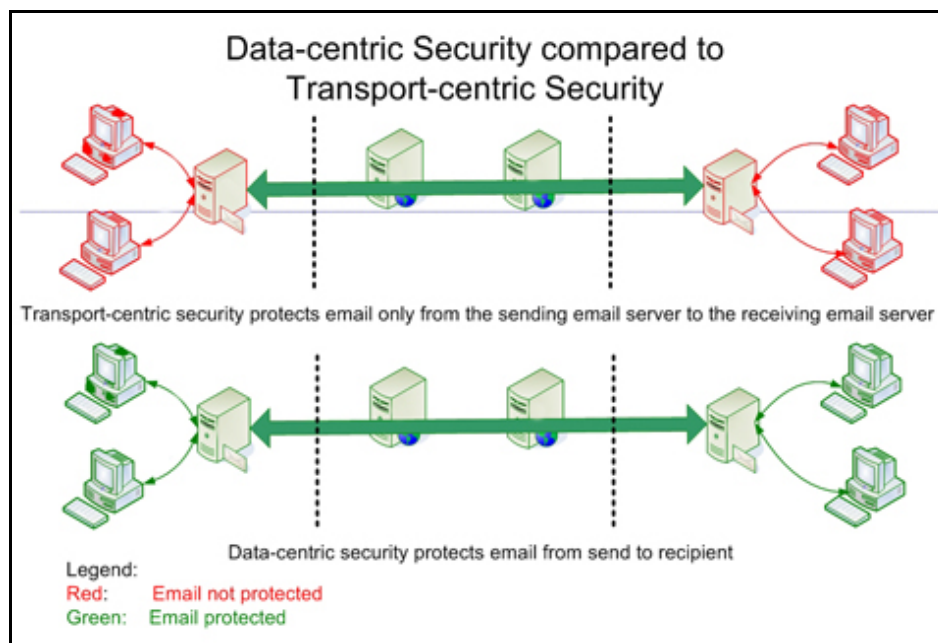
Data-centric E-mail Security: There are no boundaries!

By Jeff Cherrington and Jim Peterson

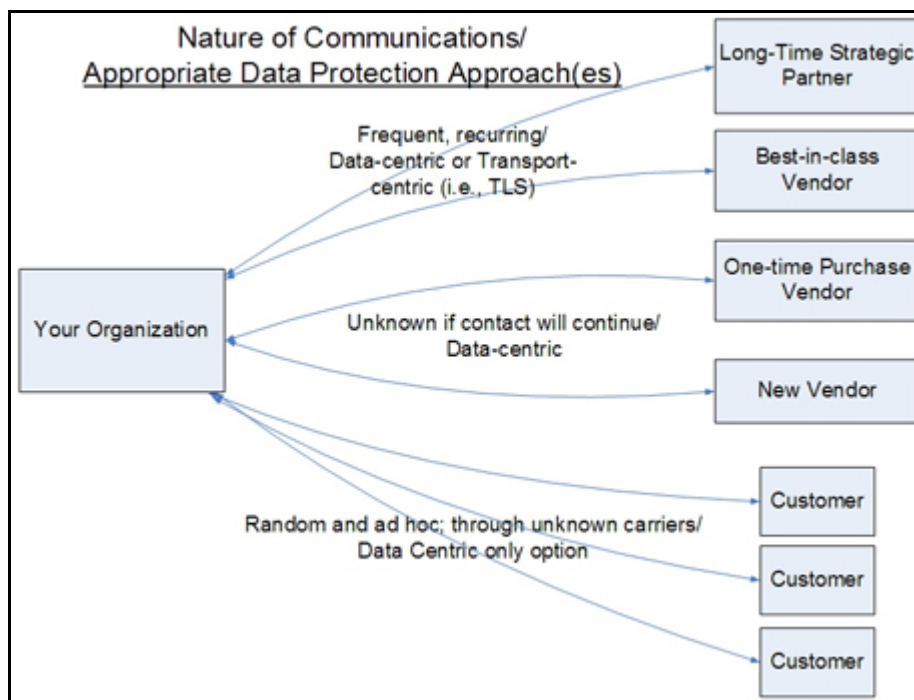
E-mail is one of the most successful advances of recent decades -- it permeates virtually every part of business and our personal lives. It marries instant gratification with the desire to connect, for both professional and personal needs. However, we are seeing the same trends with e-mail as with the rapid adoption of the automobile in the last century--safety and security have been afterthoughts.

The risk represented by e-mail lies in its fundamental structure. E-mails can contain highly sensitive information that we may expose inadvertently when writing an e-mail to an acquaintance or critical business communications intended to be read by only specific recipients. Such correspondence, as so many have described it, is like a postcard moving through the postal system--the contents are exposed to all who touch it as it flows from the sender to the recipient. Even though individuals may be extremely diligent about ensuring that their PCs are protected with antivirus, anti-malware, anti-spyware, and every other conceivable means to protect the data contained on that PC, once an e-mail is sent, none of those protections can apply to it.

The same applies to the protections that an organization may have on their network and its logical perimeter--no matter the degree of investment in intrusion detection systems, intrusion prevention systems, firewalls, and all of the other necessary perimeter protections, none apply to an e-mail once it passes from the organization's e-mail servers to the broader Internet for delivery. While transport level security (TLS) offers an excellent strategy for known point-to-point connections (from one business to a specific partner, for example), the constantly changing population of external recipients means it cannot mitigate all risks. Any protections that are not directly attached to e-mail messages are ineffective as the messages transit from origin to destination.



This certain fact, then, implicitly and unavoidably narrows the focus of e-mail protection to protection that can be attached directly to the data itself. While perimeter-oriented protections remain both appropriate and necessary to protect the infrastructure that supports the sending or receiving of e-mail, any protection that is in any way boundary-based or limited can never completely protect the risk of anyone sending e-mails. It is obvious that only a 'data-centric' approach to security will protect an e-mail sender's risk.



The term data-centric is self-defining in this context of data protection. It pinpoints the focus to the data itself and not to the application that originates the data, the network that carries the data, the servers that store the data, or anything outside of the data as a discrete unit. E-mail security that qualifies as data-centric, then, must attach the protection of an underlying security scheme directly to an e-mail that needs to be protected. Moreover, that protection must remain in place even if the data is moved from one point to another point (as with sending an e-mail), the data is copied one or more times (as with PC backups or e-mail archives), and even if as the e-mail moves from one operating system to another. Anything less will always leave the originator of the data at risk.

Fortunately e-mail protection schemes that apply a data-centric philosophy are available from a number of sources and in a variety of architectures, all applying encryption to e-mails, in one manner or another. Options include:

- Open source (such as the GPG and OpenPGP variants, the several S/MIME libraries, or encrypted ZIP archives)
- Closed and semi-closed e-mail security systems that require the sender and the receiver to use the same proprietary e-mail clients and limits the operating systems supported
- Hub & spoke webmail systems that depend on a server hosted by the sponsoring organization

Choosing the option that is best will always depend on the specifics of a given organization's needs, but for the greatest majority of circumstances, the following guidelines prove useful:

- **Data-centric** – as this article illustrates, the best e-mail protection results when the protection is attached directly and inextricably to e-mails sent.
- **Works off-line** – since many recipients work with their e-mail in off line environments (on an airplane, at the beach, at a customer site, etc.), select an e-mail protection scheme that does not require an active connection with an internal or external server across the network.
- **Standards-based** – applying e-mail security serves two overlapping needs (for business communications, at least): 1) actually protect the data and 2) satisfy auditors, customers, stakeholders and stockholders that data has been protected. Both are best addressed by adopting products that support appropriate recognized standards for encryption (AES), key bit-length (minimum of 128), hashing algorithms (SHA-2) and key format (i.e., X.509 v3), so no explanation or education of those third parties is required

- **Platform independent** – while Windows remains the dominant end-user operating system, e-mail is integrated into many processes that involve other platforms, including Mac, UNIX, Linux, and even the mainframe. Select a solution that supports data-centric protection for all the major operating systems, so scope is restricted as little as possible.
- **Efficient** – encryption's data protection benefits impact resources in two ways – it is computational intense, impacting processor capacity, and creates output that is not compressible (by its nature, encryption randomizes data and removes the patterns that make data compression possible). Best choices, then, are those products that apply industrial-strength compression before encrypting.
- **Transparent to users** – look for those e-mail security products that operate within the users' existing work habits and do not require them to use alternate or substitute e-mail clients. Best are those that apply e-mail security immediately within the native application without intruding on the user experience at all.
- **E-mail-client 'agnostic'** – no one even attempts to learn what e-mail client an e-mail recipient is using. While Microsoft Outlook, Outlook Express, and Windows Mail are all popular, Lotus Notes, Novell GroupWise, and browser-based e-mail clients are also popular. An e-mail protection scheme must support all without constraint.
- **Flexible:** – It will be the rare individual who needs to encrypt every single e-mail sent – the copy of Grandma's ginger bread recipe sent to a relative may not require the same degree of care as, for example, the financial analysis of a company merger. Choose a product that both allow flexibility and control, so that the degree of latitude offered to the user reflects the data security policies appropriate.
- **COTS** – select common off the shelf (COTS) products that include standard user interface metaphors, integrate with the existing desktop productivity applications, and include full documentation. Open source-based projects developed in-house are an alternative, but come with hidden costs in terms of user education, on-going maintenance & enhancement and, most important for this issue, high support costs for external e-mail recipients. A product that include context sensitive help for all users and, particularly, live phone, e-mail, and chat room support for external recipients provide the best benefit. If versions of the product are available at no charge and that allow recipients to read incoming e-mails, all the better!

These nine parameters provide buyers an excellent filter for narrowing their review of possible e-mail data protection solutions.



Jeff Cherrington is vice president of Product Management for PKWARE



Jim Peterson is chief scientist for PKWARE

PKWARE®

www.PKWARE.com

USA
Headquarters
648 N. Plankinton Ave.
Suite 220
Milwaukee, WI 53203 USA
ph: 414.289.9788

EMEA
PKWARE U.K. Limited
Crown House
72 Hammersmith Road
London W14 8TH
United Kingdom
ph: +44 (0) 207 470 2420

Asia-Pacific
PKWARE Japan K.K.
Cerulean Tower 15F
26-1 Sakuragaoka-cho,
Shibuya-ku
Tokyo 150-8512 Japan
ph: +81 3 5456 5599