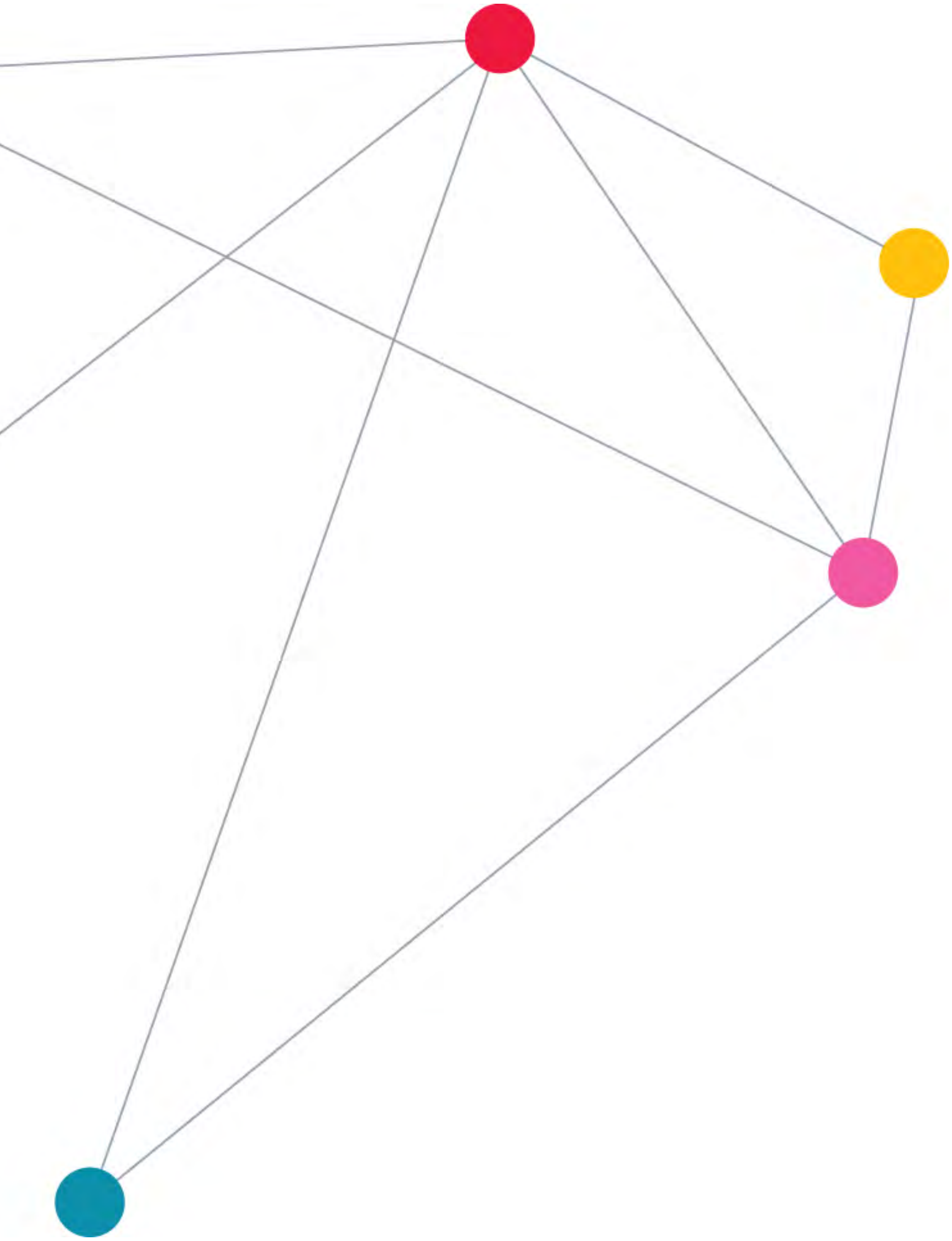
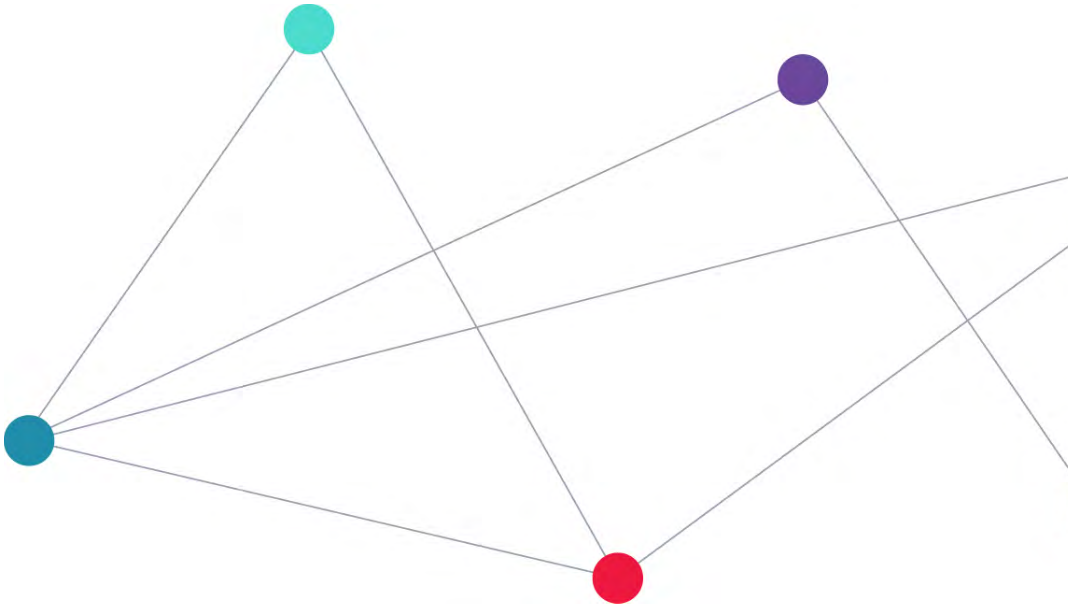
bravatek

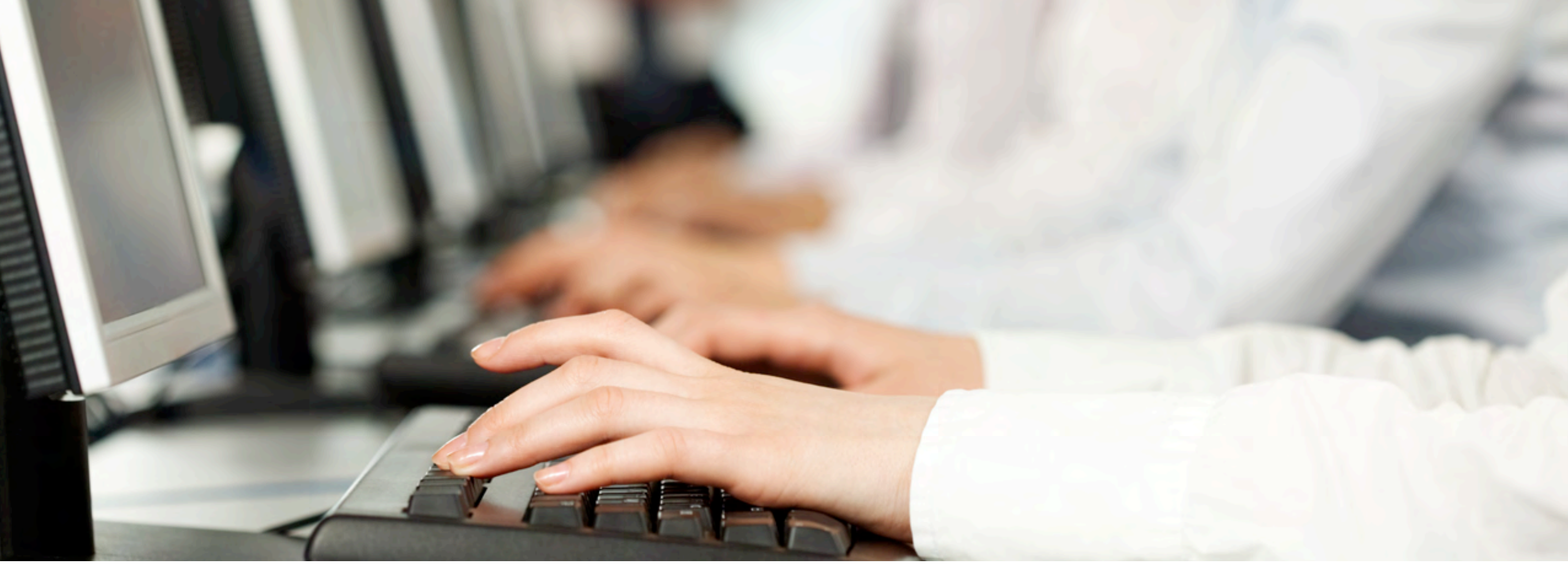


Enterprise Email: Simply Trustworthy?

A System Administrator’s POV

Contents.





Email is the centerpiece of the Enterprise information system.

Almost every role in a modern corporation relies fully on their email system, with its messaging, calendaring and file sharing. For most information workers, their work lives center around the information flow of their email system. They have full trust and reliance on the services provided by the email system – at their desk and on the road.

The email systems that let information flow so freely let undesirable information flow just as freely. Social engineering is the easiest way to get a virus into a corporation – just send someone an enticing email with a viral payload. Your company's sensitive information can flow outside with the same ease as well.

Numerous add-on and afterthought products exist that attempt to solve the issues that email brings to an organization. Some are effective and some are easily thwarted. The result is a hodgepodge of bolted together parts that leave the IT administrator hoping it might be good enough.

The design of Enterprise email systems needs to be revisited. It needs a rethinking of the approach to information flow that incorporates information security and privacy as core requirements.

It needs to be a system that is simple and trustworthy.

Introduction.

Today's email systems are built on the standards defined with the creation of the Internet, when scientists were happy to be able to send each other a message at all. SMTP and X.400 were designed first with helping messages move between people within and outside organizations. Spam came along and then came anti-spam filters. Viruses and Trojans entered the fray quickly followed by anti-virus solutions.

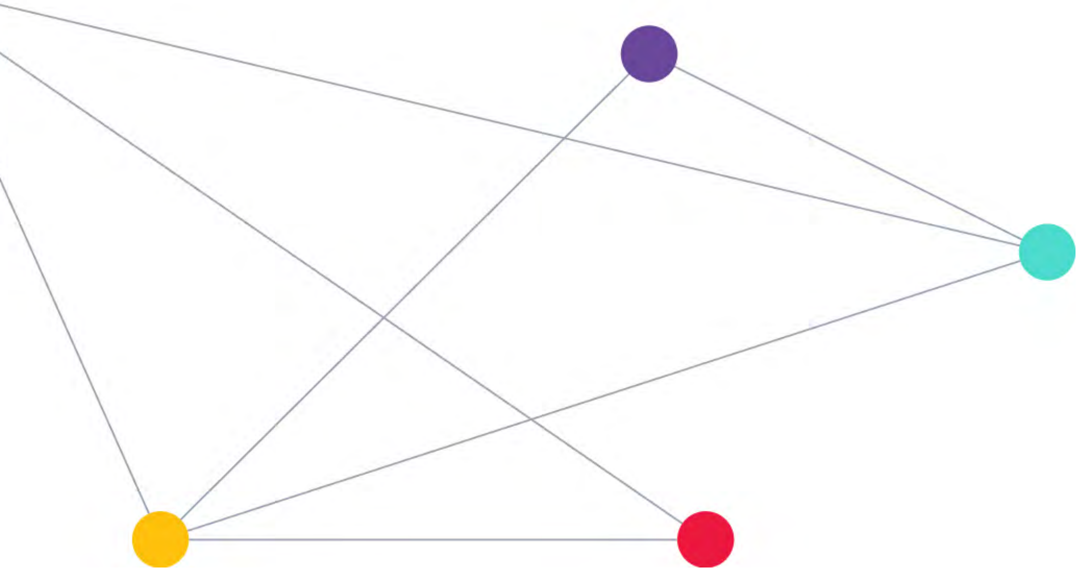
Information security and privacy became more important as organizations transmitted more and more sensitive information via email. Encryption solutions were made available, sometimes built-in and sometimes added on, with no clear standard. Adopting an encryption solution can help secure information flow within an organization where it can be held together by IT policy.

Unfortunately the decision to secure a message is often left in the hands of the user. With no standard for transmitting secure email to external parties, senders and recipients must agree to use the same technology and exchange security information. This is outside the typical user's intuition and so email flows outside the organization in the clear.

The decision to secure a message is often left in the hands of the user.

This same user also has to have security top-of-mind as they consider opening unsolicited messages from the outside. IT administrators are left with few good choices.

Modern privacy standards such as SOX and HIPPA in the USA, BDSG in Germany and others require that email be much more secure and controlled. Information security for Enterprises needs an audit trail yet users consider the ability to send messages to anyone a right and not a privilege. IT administrators need a new messaging system that addresses these modern requirements in the foundation of system's design.



Pandora's box.

There are multiple facets to the problems in today's email systems.

Information flows into, out from, and within organizations too easily. Information Security and Privacy standards require control of information flow yet it's very difficult to stop incoming email even with the best of today's offerings. Spam filtering and attachment blocking can be effective, but these solutions still attack the problem from the point of identifying a problem and then blocking it. This leaves motivated bad guys to work at ways around the filters. It's just a matter of time, effort and creativity.

Users need to make security decisions at every step. They are forced to think about the security of attachments, while attackers make more and more tailored and socially engineering Trojans and viruses. Users commonly approach email with either dis-trust or ignorance, requiring them to make judgement calls affecting the security of the entire organization while trying to do their job.

Maintaining information security within the organization is very difficult and almost impossible outside in most cases. Encryption is very difficult to understand and commonly only works within organizations. External email is almost always exchanged in the clear. When sending messages, users need to think about whether or not they can and should encrypt messages for the recipients of the message. They are forced to understand encryption systems at least to the degree that they know if a recipient will be able to read their message.

IT administrators are under increased scrutiny to provide compliance with the ever-evolving realm of security and privacy standards for all the regions of the world in which they operate. CIOs require that the organization have tighter control of information as it flows within and outside the organization.

Today's email systems attempt to do this with black-listing solutions. That's the best they can do. IT administrators are frustrated and accept that there is only so much they can do with the technology. They are left hoping that information can be secured with policy and that users will understand and honor policy and security.

It only takes one slip-up for an organization to be taken over.

There must be a better way.

Time for some Newthink.

Giving the IT administrator confidence that the system is always secure and protected necessitates an entirely new approach to email.

It is time to retire the messaging systems of the past, replacing it with one engineered from the ground up with a white-list mentality. One that leverages modern technology to provide security and accountability as core features, and is designed to enable the control and auditability of information for organizations operating in the modern world of compliance and oversight.

Securing user interaction by the nature of the design of such a system relieves users of the need to make daily security decisions. Setting policies to limiting email communications to an as-needed basis to limit exposure. The goal is to allow the IT administrator to trust the content in the system by ensuring that all sources of messages are known and approved.

The goal is to allow the IT administrator to trust the content in the system by ensuring that all sources of messages are known and approved.

Persistently encrypting messages at rest: data and metadata. Securing messages entering and moving within the system by default, without user interaction. Providing enforced secure access to the system by visitors and users of the organization.

A system that is locked down and private by design can begin to give IT administrators a peace of mind.

One system to rule them all.

Ecrypt One is a brand-new take on email, with all the expected features such as calendaring and contact management. The number one feature, however, is being fully locked down. This is meant to appeal to security and privacy conscious organizations such as government, health care and any enterprise that is bound by the various standards such as SOX and HIPPA, etc. At the same time, it was designed to be intuitive, so the end-user is not encumbered with security decisions such as encryption or attachment safety.

By default email only moves within the organization. That way there are no concerns with intellectual property loss or data theft. Nor are there concerns with incoming email from untrusted parties, phishing attacks, etc. Anti-spam or anti-virus services are not needed.

Users have a choice of an easy to use Web interface for email and time management, etc. They can also connect standard email client software to the Ecrypt system securely using multiple protocols.

For trusted external parties that need to send or receive information with the organization, a locked down Web-based email portal with limited functionality is available. Information sent to these external accounts has additional checks and auditing. Information sent in from external accounts has strict content and anti-virus checking of attached files. This eliminates the need to perform and coordinate email encryption between external parties, since the message content always traverses the Internet in a secure manner (i.e., using a secure browser session).

> *The Administrator remains in control of where information flows outside of the organization.*

All users, both internal and external, use multi-factor authentication to connect to the system. Hardware-based systems such as RSA cards and Smartcards are supported as well as software solutions such as Google Authenticator and other one-time password (OTP) implementations.

The administrator can enable standard outgoing email for those who need that capability. White lists for external recipients and domains allow the administrator to control the destinations for email sent to the outside on a per-group or per-user basis depending on the needs of the business. The Administrator remains in control of where information flows outside of the organization.

The administrator can also enable incoming email for users who need to interact with outside parties for roles such as customer support, sales inquiries, etc. White lists allow control of which addresses and domains are allowed to receive email from. Attachments are discarded by default but can be controlled by policy settings.

The SMTP service supports secure transport (STARTTLS) for additional security by other email systems that support it. Ecrypt strongly encourages and supports the use of VPN and IPSec for scenarios such as this, for added security when connecting to trusted partners.

For the highest inter-organization security possible, Ecrypt-to-Ecrypt allows for multiple organizations to transfer messages among themselves in a fully secure form. Information is always transmitted in a secure and full-fidelity fashion.

Data is encrypted while at rest. Hardware-based encryption devices and keystores are supported for maximum security by the use of DoD-approved security solutions.

Keystore devices store secrets such as encryption keys that are only accessed through code and not a standard file system, making them virtually impossible to access by an attacker. Encryption keys are rolled periodically as an additional defense-in-depth measure. All email system data is stored in a database server, which can be positioned security within the enterprise landscape.

Auditing of all transactions in the system is configured by default. For SOX compliance and other standards, groups such as Finance are defined that very strict information exchange policies enforced including the ability to not send to others in the organization. Standards compliance is aided by the generation of reporting data in standard file formats and schemas (HIPPA Schema, for example).

Bravatek servers run in FIPS-compliance security mode only – by design. Everything from the proper use of DoD-approved encryption systems to the enforcement of high security browser connections (at least TLS 1.0) ensure the system is always trusted and secure.

Business Benefits

The core benefit of Ecrypt One is its modern secure implementation and fresh approach to email.

By delivering a fully locked-down email solution, Bravatek allows for organizations to offer a fully trusted information system that is easy to use and standards compliant at the same time.

Other solutions' attempt security or ease of use, but in all cases entrust users with the security of the enterprise, whether they want that responsibility or not.

Ecrypt One eliminates the main security breach vectors coming to users today: socially engineered email with viral attachments.

Ecrypt One doesn't attempt to fill security holes – it eliminates them altogether.

In the end...

Ecrypt One’s fresh approach to Enterprise email and simplified security experience it second to none.

Administrators are always in control and are confident that not only can the system remain secure in the face of the ever evolving threat landscape but they can also trust that its inherent design goals will keep them in compliance as standards change.

Secure your information network simply and smartly with Bravatek.

info@bravatek.com ● ***1.866.204.6703***

About Bravatek.

Bravatek is an information security firm focused on developing smart and simple solutions for modern security and compliance challenges.

www.bravatek.com

bravatek

NO WARRANTY. Bravatek makes this document available AS-IS, and makes no warranty as to its accuracy or use. The information contained in this document may include inaccuracies or typographical errors, and may not reflect the most current developments, and Bravatek does not represent, warrant or guarantee that it is complete, accurate, or up-to-date, nor does Bravatek offer any certification or guarantee with respect to any opinions expressed herein or any references provided. Changing circumstances may change the accuracy of the content herein. Opinions presented in this document reflect judgment at the time of publication and are subject to change. Any use of the information contained in this document is at the risk of the user. Bravatek assumes no responsibility for errors, omissions, or damages resulting from the use of or reliance on the information herein. Bravatek reserves the right to make changes at any time without prior notice.