ecrypt one

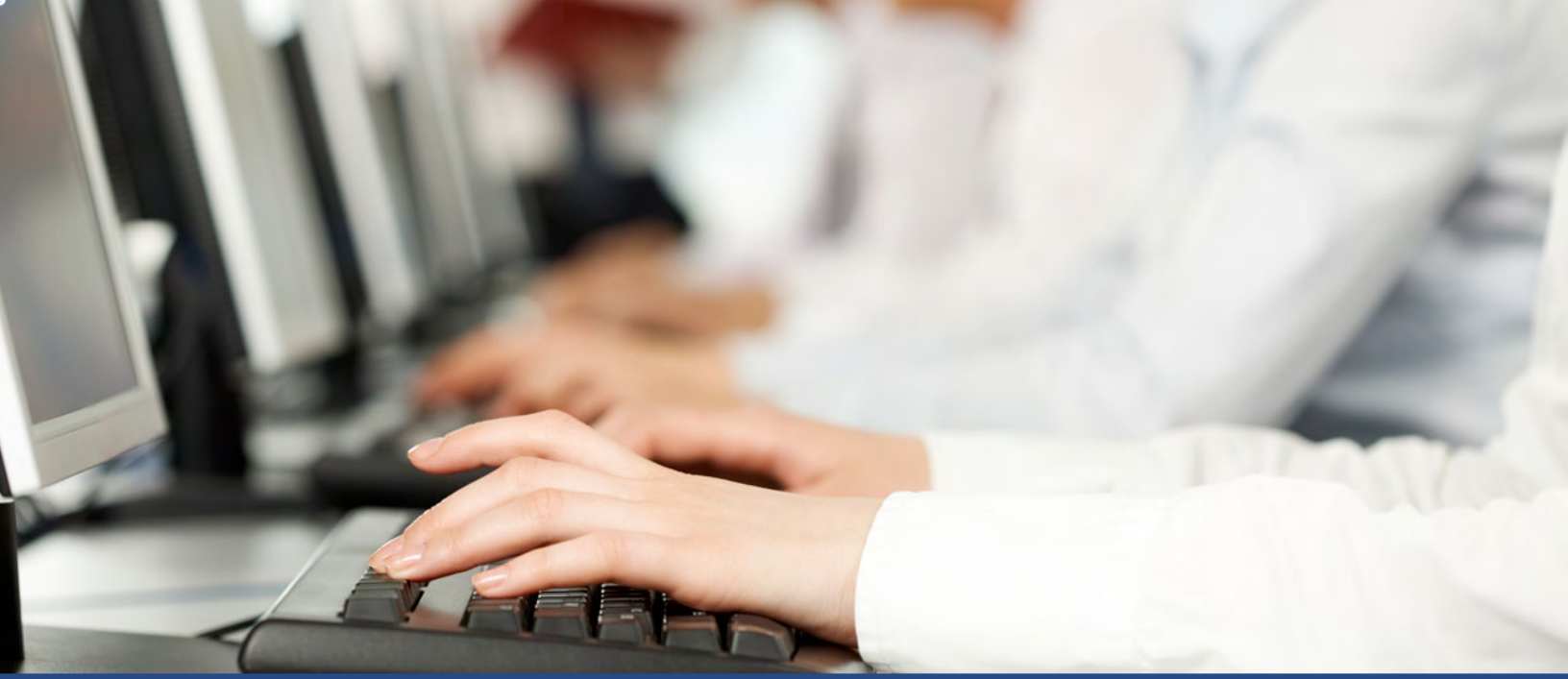
email security and data leak prevention for Government organizations and the Aerospace and Defense industry

bravatek

bravatek.com/ecrypt-one | sales@bravatek.com | 1.866.490.8590

Ecrypt One is designed to optimize internal and external security as well as to support the functional goals of each agency - independently and together

table of contents.



email is the centerpiece

of an organization's information system

Email is the centerpiece of an organization's information system. Almost every role in a modern government organization relies fully on their email system, with its messaging, calendaring and file sharing. For most organizations, their work revolves around the information flow of their email system. They have full trust, and reliance on the services provided by the email system.

The same email systems that let information flow so freely can also be detrimental and allow undesirable information to flow just as freely. Social engineering is the easiest way to get a virus behind the firewall – just send someone an enticing email with a viral payload. As a result, government agencies' 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 organizations. Some are effective while 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 "Newthink" on the approach to information flow, one that incorporates information security and privacy as core requirements. It needs to be a system that is simple and trustworthy.

the name is one. ecrypt one.

Ecrypt One is a security-first full service email system, designed to meet the risk tolerance levels of the most demanding and security-conscious government organizations.

Ecrypt One is designed to the highest national security and military specification standards.

An effective fortress safeguarding the exchange, storage, and audit integrity of email and attachments sent inter-agency, intra-agency and cross-border.

- *Built in always-on email transmission and store encryption removes reliance on end users to make security decisions like whether or not to encrypt an email.*
- *Reduces exposure to threat vectors like spam and phishing by employing a whitelist approach to control email traffic.*
- *Information rights management measures enable organizational control over message and file transmission and access permissions thereto.*
- *Role based access controls prevent arbitrary administrator access to email system resources, services and data.*
- *Private and public crypto algorithms are available. Key storage can be in dedicated hardware devices or software-defined devices with multiple levels of encryption.*

Ecrypt One is a paradigm shifting secure email system.

It assures the security, integrity and auditability of email and attachments, in transit and at rest.

Ecrypt One is modular, enabling capabilities to be added and removed as desired.

- *Deployment modularity enables granular risk tolerance variability based on use case and needs.*
- *Extensible architecture allows for customer-specific security and workflow extensions to be incorporated, supporting specialized needs.*
- *Designed to be scalable through support for load balancing and other deployment requirements.*
- *Pluggable authentication, cryptographic algorithms and key storage allow deployments to meet an organization's security needs.*
- *Solution design enables compartmentalization within a single system while supporting distributed auditing and reporting. Multiple risk-configured deployments can be integrated for departments with special security requirements.*
- *Can be deployed on site, off site, or a combination of both. Designed to leverage the cloud if desired.*

Ecrypt One enables information assurance and eases regulatory compliance. Federal security requirements like FIPS and IPv6 are built-in.

Ecrypt One is not disruptive to operations and provides a positive return on investment.

- Multiple protocols connect the system securely to already used and familiar email client software, regardless of operating system or device type.
- A single management console for email system and its built-in security allows administrators to be more efficient.
- Dependable and automated security and eliminated exposure to email borne threats improves the end user experience, reduces workplace stress, and increases productivity.
- Eliminating spam and phishing threat vectors by deployment configuration removes the necessity for common employee security decision-making.

Ecrypt One enables agencies to balance security and compliance with accessibility, collaboration and efficiency.

The solutions inherently secure nature allows it to be seamlessly integrated into existing workflows.

ecrypt one. key capabilities.

Secure Intra-agency and Inter-agency Collaboration

Enables agencies to communicate securely with each other without compromising internal security, group leadership and personnel divisions.

Provides agencies with absolute ability to control and limit access to the system, preventing the unauthorized access to, and distribution, of data.

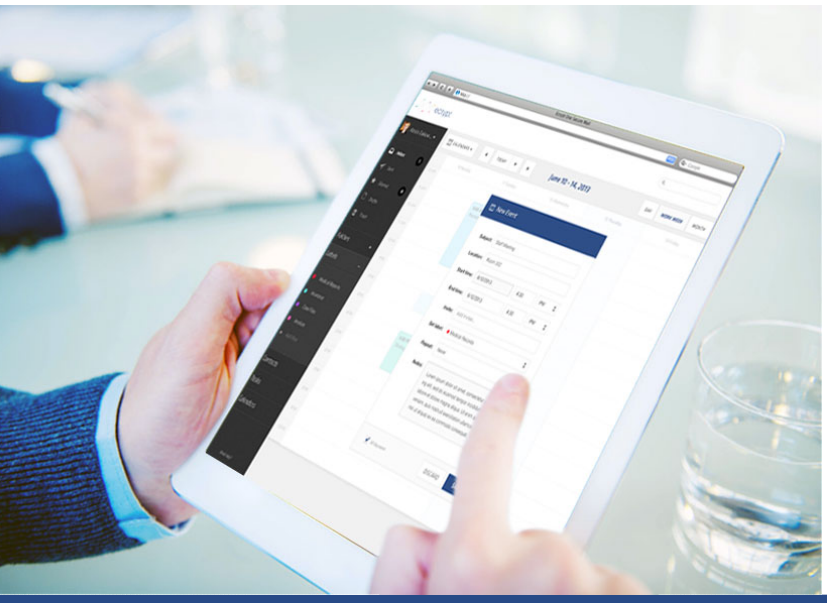
Secure Cross-border collaboration

The Visitor Access Point is a completely secure email interaction portal. It enables agencies to communicate securely with external parties, such as vendors, suppliers and foreign government agencies – and vice versa - without compromising internal security or structure.

The VAP is a spam and phishing free environment that allows access only to authorized parties, and built in anti-virus technology ensures infections don't enter the network.

Mobile and BYOD Security

Inherent security within the self-contained system enables agencies to secure all types of devices including desktop computers, laptops, tablets and smartphones. This supports operations in the field for mobile units and task forces.



Seamless Integration

Easily conforms and integrates into existing network enterprise equipment. The use of open standards where possible, ensures the highest levels of interoperability, availability and compatibility, with existing and future enterprise infrastructures.

Role Based Access Controls

Provides agencies with absolute ability to control and limit access to the system, preventing the unauthorized access to, and distribution, of data.

Compliance

Enables agencies to control, audit and verify the integrity of email and document transmissions. An extensive compliance toolset includes a dedicated compliance officer role, comprehensive easy-to-manage auditing and reporting capabilities.

Automated reporting of repeat external attacks and internal attempts to circumvent security policies. Ecrypt One demonstrates compliance with acts, standards and regulations, for example FISMA.

Productivity

Extremely transparent and seamless implementation and deployment, low latency, and excellent human factors interface for efficient workflow experiences.

Consolidates multiple technologies into a single system reducing pressure and strain on IT departments. Simplifying this process eases system administration and management.

Integrates seamlessly into existing workflows, supporting all popular email clients. Inherent security within the self-contained system enables agencies to secure email and attachments on all types of devices including desktop computers, laptops, tablets and smartphones.

ecrypt one. editions.

Email	Ecrypt One MI	Ecrypt One Gov.	Ecrypt One	Ecrypt One Light
Multiple server support with Encrypted Link	✓	✓	✓	
Multiple server support with Variable Crypto Encrypted Link	✓			
IMAP/SMTP protocols (pull)	✓	✓	✓	✓
ActiveSync protocol (push)	✓	✓	✓	✓
Contacts and Calendar synchronization	✓	✓	✓	✓
Web Mail and Visitor Access Portal				✓
Embeddable Web Mail and Visitor Access Portal	✓	✓	✓	
Standard Content Filtering	✓	✓	✓	✓
Custom Content Filtering	✓	✓	✓	
Rules Engine for Information Rights Management	✓	✓	✓	✓
Cryptographic Key Storage				
Windows Keystore	✓	✓	✓	✓
Ecrypt Encrypted Keystore	✓	✓	✓	✓
Hardware Encrypted Keystore compatibility	✓	✓	✓	
Custom Keystore plug-in support	✓			
Data Encryption				
AES data encryption	✓	✓	✓	✓
AES, Blowfish and Elliptic Curve encryption	✓	✓	✓	✓
Custom encryption plug-in support	✓			
Authentication				
Two-factor authentication via SMS	✓	✓	✓	✓
Two-factor authentication via email	✓	✓	✓	✓
Google Authenticator integration	✓	✓	✓	
Smartcard authentication integration	✓	✓	✓	
Biometric authentication support	✓	✓	✓	
Custom two-factor authentication support	✓	✓	✓	
Security				
Outlook Public Key integration (PGP)	✓			
Public Key security services	✓			
Standards and Compliance				
Basic auditing and reporting				✓
Enhanced, extensible auditing and reporting	✓	✓	✓	
FIPS compliance mode	✓	✓	✓	
Government Cloud hosting option	✓	✓		
Security standards compliance	✓	✓	✓	
Mobility				
iOS, Android, Windows Phone, and BlackBerry OS compatibility	✓	✓	✓	✓
Mobile Device Management system integration	✓	✓	✓	
MDM PKI security support	✓	✓	✓	

our service.

Our dedicated Government executive team will work alongside your management and technical teams to ensure the solution is fine tuned to meet your unique needs, and that installation is undisruptive to your operations.

Once you are up and running, our support staff will be available should you need any assistance with using or managing the system.

Discovery Phase

This includes assembling a comprehensive understanding of an enterprises current system infrastructure. We will explore both technology and operational needs to gain a 360° understanding of the business purpose for the security deployment.

We will work with you to define system requirements, outlining what will need to be added, removed or changed in the existing technical infrastructure.

Requirements Elaboration Phase

This is where the system is tailored to meet all your needs in a fully bespoke solution.

This includes tasks like applying your security policies to core system rules, and branding of user facing interfaces.

Implementation Phase

Our engineers will work with IT on installation, integration into your existing infrastructure, and system orientation.

Service specialists will work with other necessary departments on deployment, and orientation of relevant employees.

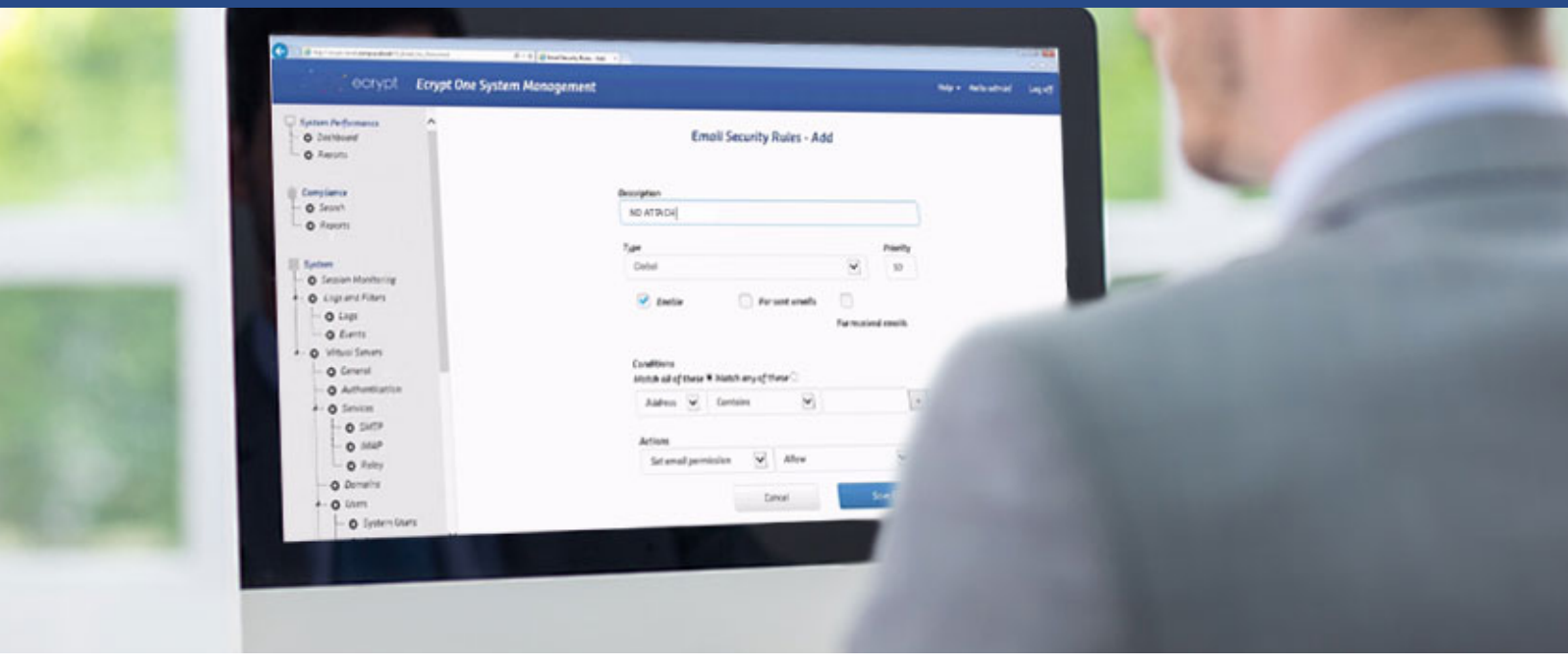
Post-Sale

Included in our service are unlimited access to help desk assistance, and product updates.

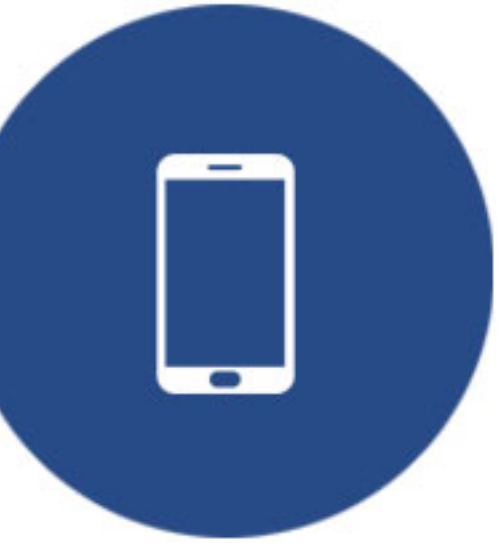
Added Benefit Options

We also offer complimentary technologies - through trusted partnerships - to optimize your system for things like data integrity assurance and user authentication.

We can, of course, also integrate with your existing solutions already in place.



what's next?



Let's talk about your security and innovation initiatives, and how our solution might fit in.

1.866.490.8590

sales@bravatek.com

Visit our website for more information about Ecrypt One, and the other great products in our portfolio.

bravatek.com/ecrypt-one

Share and socialize - check out our other informative content:

twitter.com/bravatek

facebook.com/bravatek

linkedin.com/company/bravatek-solutions-inc-

vimeo.com/bravatek

smart simple security

About Bravatek

Bravatek Solutions is a high technology security solutions portfolio provider that assists corporate entities, governments and individuals protect their organizations against both physical and cyber-attacks through its offering of the most technically-advanced, cost-effective and reliable software, tools and systems.

bravatek.com
info@bravatek.com
1.866.490.8590