ecrypt ❍ne

data leak prevention and compliance
for the Healthcare and Medical Services industries

Ecrypt One is designed to provide healthcare organizations a HIPAA/HITECH compliant secure electronic communications system.

table of contents.

email is the centerpiece
of the enterprise information system

Almost every role in an organization relies fully on their email system, with its messaging, calendaring and file sharing. For most healthcare 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, your organization's sensitive information can flow outside with the same ease as well.

Numerous add-on and afterthought products 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 the Healthcare email systems 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.

HIPPA regulations are a moving target, making it difficult to maintain compliance. Conventional solutions provide a fragment of the required protection from data leaks and liability. We solve security and compliance problems holistically, ensuring the security of information, and HIPAA/HITECH compliance.

people make mistakes.
we're human.

Failure to follow policies and procedures are mistakes that come at a very high price. Especially in an industry so stringently regulated.
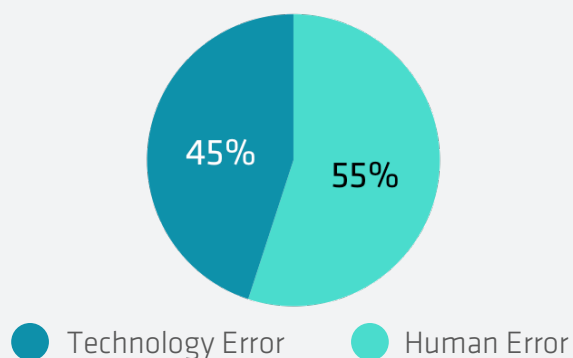
Data privacy and security regulations are changing frequently, placing the industry in a constant game of compliance catch-up. Positions to resolve the situation through conventional responsive approaches have proven expensive and ineffective. The penalty for not keeping up with the transforming landscape can be costly for an organization.

The industry needs to achieve a state of agility, embracing new tools to accelerate communications. Under conventional systems the move toward mobility can be a major threat to security. The search for balance between business needs and security, while managing compliance, is an ongoing business problem.

Ecrypt One is designed to protect the information system, despite its users.

"In the world of black market information, a medical record is considered more valuable than anything else."

Dr. Larry Ponemon
Chairman and Founder of the Ponemon Institute

FACTORS IN SECURITY BREACHES

45% Technology Error
55% Human Error

TOP HUMAN ERROR SOURCES

42% End user failure to follow policies and procedures

39% Lack of security expertise with website or application

Source: CompTIA's 11th Annual Information Security Trends Study (2013)

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 organizations.

Ecrypt One ensures that organizations not only meet today's HIPAA compliance obligations, but also exceed them to remain ahead of the regulatory curve for the future. This mitigates the risk of data breaches and subsequent litigation, while allowing organizations to be competitive.

A paradigm shifting secure email system, it assures the security, integrity and auditability of email and attachments, in transit and at rest.
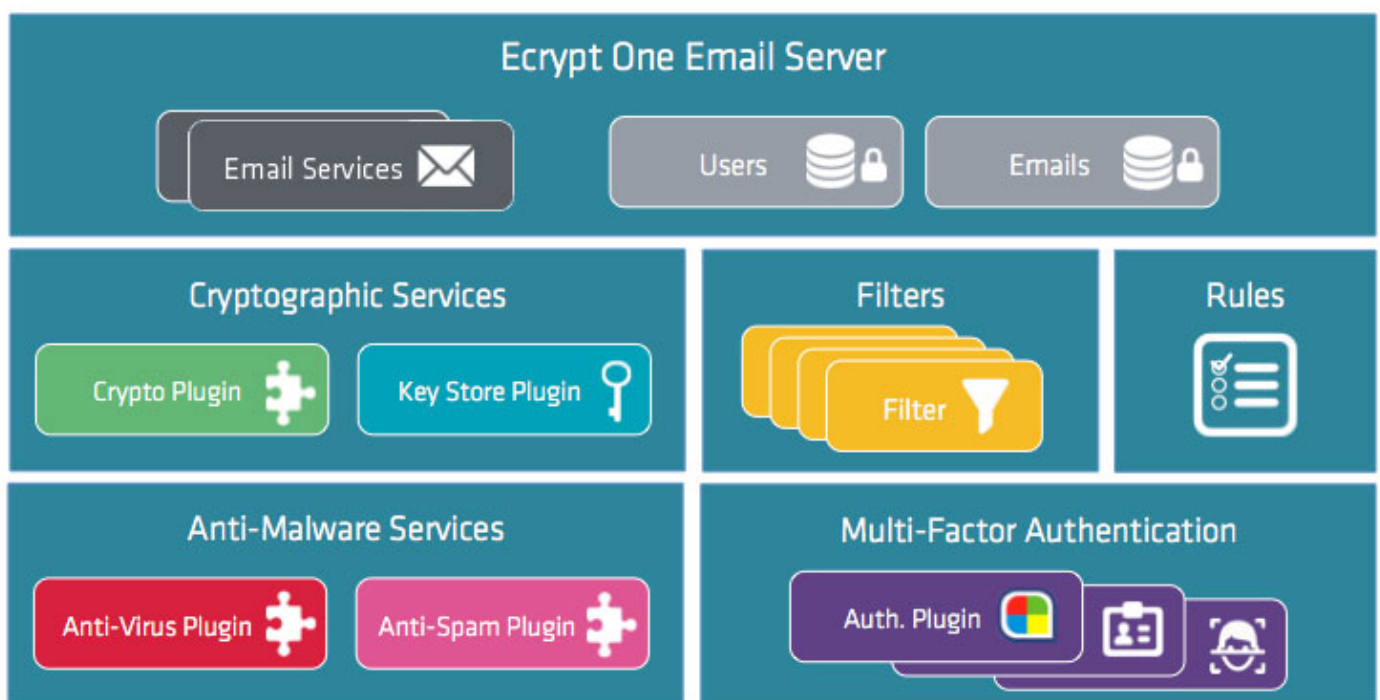
POWERED FOR 5P STAKEHOLDERS

Patients, Providers, Pharmaceuticals, Payers and Policy Makers

With Ecrypt One, securely exchanging personal health, medical, and financial information becomes attainable and realistic.

In our 5P stakeholder community's left pocket are hopes, dreams, and aspirations of a secure means to virtually review and respond to patient concerns, and in the right pocket are the tools to diagnose and treat each patient with utmost consideration for their privacy.

Each healthcare stakeholder is an island of excellence, but when collaboratively communicating and sharing images, scans, lab results, and vitals in a secure manner, Ecrypt One enables a hemisphere of hope for people around the globe.

5P stakeholder model.

With Ecrypt One, safe care can be delivered to patients anywhere, performed by multi-disciplinary and smart teams treating each patient not as an average, but as a unique, individual. All email communications with every patient in every clinic, home, and hospital is conducted with just as much care as is delivered to prevent suffering and improving the quality of life.

Ecrypt One means that faxes, paper, and post are no longer required to exchange patient and financial information, reducing diagnosis and therapy decision making from months and weeks to hours.

With more than 14% of the US population over age 65, the aging population creates additional demand for health care services, requiring greater use of digital technologies. Secure communications are vital and key to increasing access to care and emergency preparedness.

With Ecrypt One healthcare providers no longer need to be concerned with email account hacking, spam, or phishing and instead, focus all their energy on treating and safeguarding their patients. Providers collaborate on care across the continuum without privacy concerns, securely communicating with colleagues, researchers, clinicians, patients and their families via Ecrypt One.

Each communication in drug trials that advances through the Phases is better enabled when communicating experimental information securely using Ecrypt One.

Patients now have access to important existing medicines in a safe manner, thereby enabling pharma organizations to aim for the greatest health impact through, for example, secure email communications of patient experiences.

Ecrypt works with large pharma to build a better, healthier world for everyone around the globe, ensuring only the information that patients choose to share are exchanged securely to achieve the best results.

Payers can deliver the highest quality of service processing claims, promoting wellness plans, and managing drug formularies while simply and smartly securing sensitive information whether it is embedded in an attachment or the body of an email.

Ecrypt One protects the exchange of information with third-party servicers, and creates a culture of secure communications across all payer divisions and staff members. Administrators, claimants, medical staff, pharmacists, and billing staff all provide real benefits, manage public health, measure quality, and prevent health care fraud with the Ecrypt One.

Healthcare agencies at all levels, federal, state, and local are required to protect the information they collect and maintain. Policy makers respect citizens' right to privacy, and aim to protect the information the community maintains, through laws, regulations and standards.

Ecrypt One is a response to the data security, privacy and auditability mandates created by policy makers. It also provides policy makers a method to securely disclose information to one another, and as the policy maker forms collaborations with healthcare stakeholders, public-private partnerships exchange sensitive data securely using Ecrypt One to enhance resilience against a range of transnational health security threats.

ecrypt one. key capabilities.

Compliance
Ecrypt One provides a comprehensive compliance toolset including full, easy-to-manage audit and reporting capabilities. HIPAA compliant, it exceeds current regulations keeping you ahead of the curve and frequent changes.

The system demonstrates compliance with acts, standards and regulations, including HIPAA, HITECH and PIPEDA.

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.

Secure Visitor Access Point
The visitor access point is a completely secure email interaction portal. It enables organizations to communicate securely with external parties, such as business associates and patients, without compromising security and privacy.

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.

Data Leak Prevention
Ecrypt One uses technological means to prevent leaks caused by human factors such as failure to follow policies, judgment errors and criminal intent.

Build in, always on encryption means information is always secure whether in transit, or at rest.

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 healthcare workers.

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.
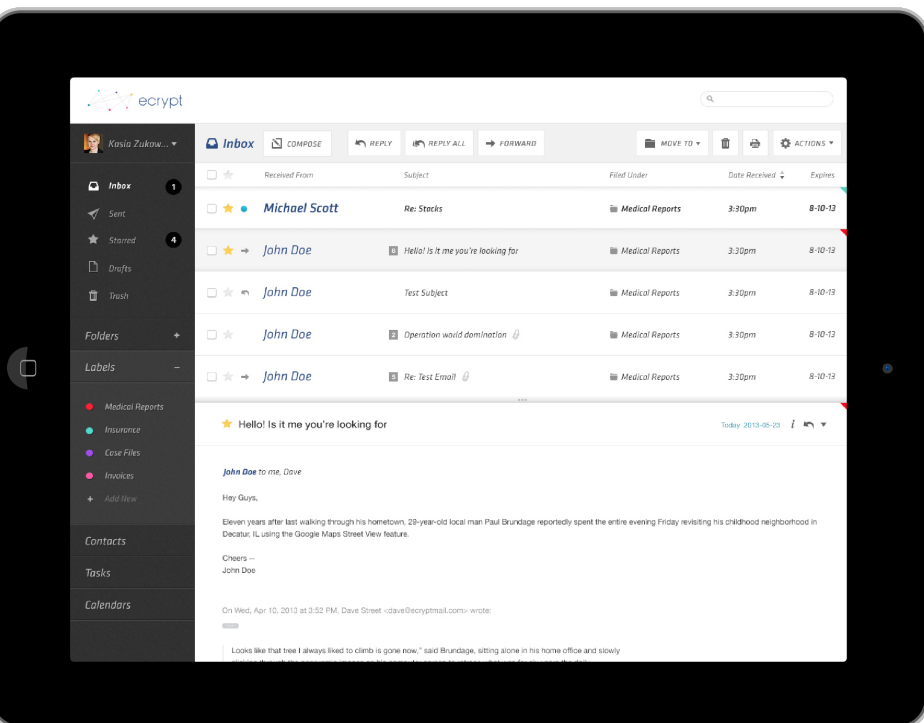
ecrypt one editions.

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.

We 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.

Customization Phase
This is where the system is tailored to meet all your enterprise 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.
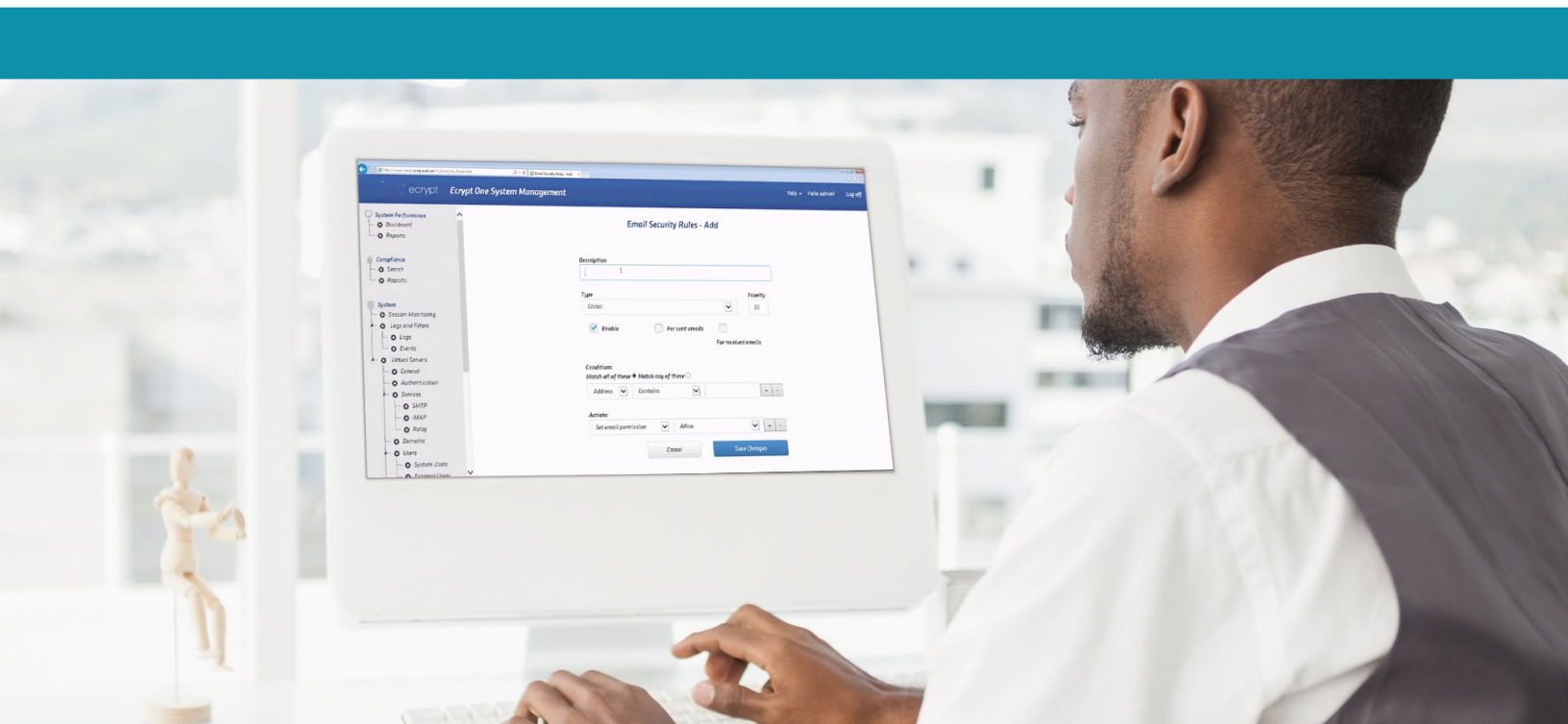
what's next?

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

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