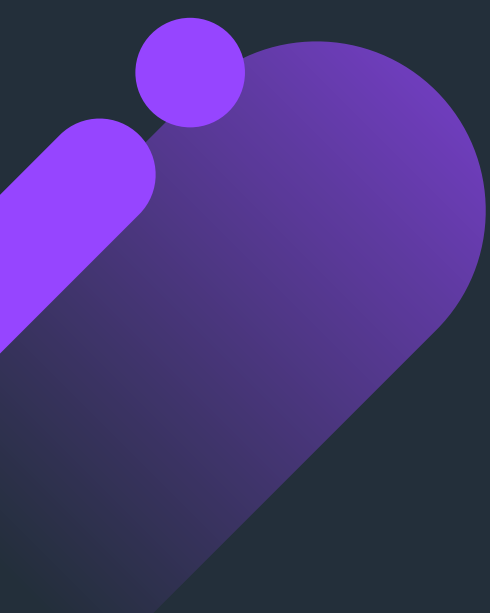**CARBONITE® + WEBROOT®**
OpenText Security Solutions

A Case for
Email Encryption

How financial institutions secure email communication and protect relationships

Easy, secure communication is a valuable asset in the financial services industry. Sensitive information is circulating on a day-to-day basis to customers, third-party organizations and strategic partners, and one communication tool emerges above the rest when exchanging sensitive personal information – email. With the convenience of clicking "send" and using email as a file-transfer method, financial organizations need to ensure the security of email for the privacy of its customers, the protection of its business relationships and brand and compliance with regulatory requirements.

Regulations and Regulators

The Gramm-Leach-Bliley Act (GLBA) protects consumers' personal financial information held by financial institutions. Its "Safeguards Rule" requires all financial institutions to design, implement and maintain safeguards to secure confidential data. Its guidelines also address standards for developing and implementing administrative, technical and physical processes to protect the security, confidentiality and integrity of customer information.

The Federal Financial Institutions Examination Council (FFIEC) released a handbook on information security practices. Regarding encryption, it stated that financial institutions should use encryption to mitigate the use of disclosure or alteration of sensitive information in storage and transit. Encryption should include:

✅	✅	✅	✅
Sufficient encryption strength to protect the information from disclosure until such time as disclosure poses no material risk	Effective key management practices	Robust reliability	Appropriate protection of the encrypted communication's endpoints

All members of the FFIEC, divisions of the U.S. Treasury, the Securities and Exchange Commission and more than 20 state financial regulators understand the risks of unsecure email. They've implemented email encryption, specifically using Webroot™ Advanced Email Encryption powered by Zix™ . As financial institutions assess risks and meet compliance standards, encrypted email should be a component of any strategy.

Outdated Technology Creates Risks

Business is no longer conducted behind a desk. Mobile devices have expanded the workplace and work hours, and more users spend time on email than any other mobile app. Outdated email encryption solutions haven't kept pace with increasing dependence on mobile devices, forcing users to overcome distorted screen layouts and numerous complex steps. The results are stifled productivity, user frustration and security workarounds. The inconvenience of outdated technology also creates an unnecessary burden on employees and recipients. Although compliance is critical, barriers to easy communication lead some employees and recipients to ignore policies and security practices simply to be efficient and move business forward. Even if employees and recipients are diligent, mistakes still happen if you rely on individuals to determine when encryption is needed. These risks can be avoided with innovative email encryption.

Of 1,000,000 Webroot encrypted messages sent every day, 75 percent are accessed without any extra steps

The leader in email encryption

Recognizing the evolving needs of your company, employees, customers and partners, Webroot™ Advanced Email Encryption powered by Zix™ provides innovative secure email that is just as easy to use as regular email. Raising industry standards, our top differentiators include:

Powerful filters and automatic scanning

Email encryption shouldn't disrupt employee workflow. It should work without your employees even knowing it, allowing them to focus on their responsibilities and attend to customer needs. With automatic scanning and the use of proven and up-to-date policy filters, emails with sensitive content are encrypted without user action. Removing the hassle and taking the decision out of your employees' hands eliminates human error and better protects your email.

Convenient delivery for recipients

If your employees don't have to take any extra steps to encrypt email, why shouldn't your customers and partners be able skip the hassle too? Webroot™ Advanced Email Encryption powered by Zix™ offers the industry's only automatic decryption of secured emails if recipients use the same platform. Of the 1,000,000 Webroot encrypted messages sent every day, 75 percent are accessed without any extra steps or passwords. For others who don't use the same platform, recipients can receive the message in less than two simple steps, removing hassle and confusion.

Smooth mobile experience

Convenient mobile delivery of encrypted messages is a critical component to keeping business moving and making your customers and business partners secure and happy. For senders and recipients using Webroot™ Advanced Email Encryption powered by Zix™, secure email on mobile devices is once again just as easy as regular email, because it is encrypted and decrypted automatically. For other recipients, optimized layouts designed for the user's screen combined with an easy registration and login experience ensure mobile access is as seamless as the desktop experience.

Taking the next step

With the right solution, email encryption can be an easy way to meet regulatory obligations and secure a top source of vulnerability for your organization. Email encryption also protects relationships and preserves loyalty with customers and strategic partners. After all, it takes years to build trust, yet only seconds to lose it with a data breach. By leveraging email encryption, financial institutions secure a basic communication tool and, ultimately, protect the value of its company and its assets.

To learn more about our solutions, visit our product page.

Sources

1. Privacy Act Issues Under Gramm-Leach-Bliley. http://www.fdic.gov/consumers/consumer/alerts/glba.html
2. FFIEC IT Examination Handbook Infobase. http://ithandbook.ffiec.gov/
3. Encryption Under the "FFIEC IT Examination Handbook Infobase." http://ithandbook.ffiec.gov/it-booklets/information-security/security-controls-implementation/encryption.aspx
4. "BYOD and Mobile Security Report" by Holger Schulze, Information Security Community, 2014. http://www.slideshare.net/ informationsecurity/byod-mobile-security-report

CARBONITE + **WEBROOT**
OpenText Security Solutions