Email Encryption – Easier Than You Think

When it comes to keeping sensitive data safe, email encryption is a necessity. But it doesn't have to be a necessary evil.

Transparent Delivery Simplifies the Recipient Process
The recipient process has historically been one of the biggest pain points for email encryption software customers. It's often complicated and cumbersome, filled with portals, secret passwords, and extra steps. It shouldn't be that difficult just to read an email, and now it doesn't have to be.

Email Encryption drastically simplifies the email recipient process. When both the sender and the recipient are clients of the same email security system, the software will encrypt the outgoing email from one customer, and send it to the recipient completely transparently—regardless of the email content. No portal, no passwords, no extra steps – just a blue bar at the top of the email confirming it was sent securely. From there, the recipient can reply to the email exactly as they would a regular email.

Even without transparent delivery, Email Encryption makes the recipient process intuitive for clients with different systems. The recipient secure email portal is designed for non-technical people to be able to access, read, and reply to encrypted emails easily.

State of the Art Filters Enable Automatic Encryption
Security tools only work when people use them, and even with the best IT policies in place, it's difficult to stop employees from sending sensitive information without encryption. While many organizations have increased their employee training amid an increased threat landscape, training only goes so far.

Exposing sensitive information isn't just an organizational problem, it's also a regulatory one. The Health Insurance Portability and Accountability Act (HIPAA) requires that all patient data is kept secure and private. With traditional email encryption solutions, this burden falls on employees every time. For healthcare organizations, this is an added layer of complication on top of an often hectic landscape for employees.

Thankfully, Email Encryption offers automatic encryption, removing the burden from employees of having to remember to encrypt sensitive emails every time they send one. Webroot Email Encryption provides out-of-the-box automatic policies for HIPAA, Social Security numbers, and financial information. When a policy is triggered—whether the sender has elected to encrypt the email or not—emails can be encrypted, blocked or quarantined.

The result? Any email containing sensitive information is automatically encrypted, saving both employees and the organization at large from the threat of a security breach.

Purpose-Built Add-Ons Make Integration Seamless
Email encryption is just one piece of the cybersecurity puzzle. Every organization has a unique set of security needs, and a threat could severely affect operations at any time.

That's why it's important to ensure your email encryption solution comes along with purpose-built add-ons and can also seamlessly integrate with other security solutions. Webroot Email Encryption can be easily integrated and is also part of a larger network of threat protection that keeps your organization safe.

OpenText Cybersecurity brings together a number of product families (Webroot, Carbonite and Zix) that can be brought in to improve and enhance the overall user experience, like:

Single Sign-On with SAML 2.0: Allows a user to login to their Secure Message Portal with their own credentials they've already created through the customer's website. Without having to login again, users click a link to be taken directly to their secure inbox. This feature is implemented in using SAML 2.0, which authorizes user access to web services across organizations.

Email Threat Protection: Email Encryption provides multilayered filtering for both inbound and outbound emails that lets the right emails through while blocking malicious threats such as phishing, ransomware, impersonation, business email compromise (BEC) and spam. It also offers attachment quarantine, link protections, message retraction, and a round-the-clock live threat analyst team.

Ready to Learn More?
Seeing how simple email encryption can be is surprising, we know. And we've only just scratched the surface. If you want to learn more about how Computer Dimensions can help make email surprisingly secure and simple, call us today at (520) 743-7554.