CARBONITE + WEBROOT
opentext Security Solutions

DATA SHEET

Protect Your Email Data Automatically with Webroot Data Loss Prevention

Webroot's Data Loss Prevention (DLP) filters automate email encryption, work out-of-the-box and are highly customizable.

Current challenges

Exposing sensitive information is as easy as hitting "reply."

- Most companies must enforce an email data security policy to protect personally identifiable information only
- It's impractical for employees to always catch sensitive information
- Employees use approaches to data management that put your company at risk
- Training alone isn't sufficient
- Blanket security policies disrupt employee productivity
- Most enterprise DLP solutions tend to be cumbersome
- Remediation workflows are slow or undefined
- Greater security concerns due to increased remote workforce
- More endpoints and increased risk of exposing sensitive data
- Less budget to execute

Solution

- Automatically encrypt and deliver sensitive information over email
- Protection from day one—works out-of-the-box
- Industry-specific policies detect information in email subject, body and attachments
- Satisfies governance, risk and compliance (GRC) best practices
- Policy-builder to select the right combination of filters for your industry
- Free customization service to fine-tune filters
- Greater awareness—managers can review messages
- Implicit training—employees see why emails were flagged
- Identify employees in need of training

Benefits

Secure email data without sacrificing productivity.

- Get up and running quickly without the need to be an expert
- Gain visibility into sensitive information within your email network
- Access to filtering experts
- Simple DLP incident investigation and remediation
- Periodic updates based on your industry

DLP capabilities

Gold-standard email encryption with automatic enforcement with flexible policies.

- Automate custom notifications to explain actions to users
- Define your policy for reviewing or quarantining to and from unauthorized users
- Delegate outbound quarantine management to managers
- Manage quarantined messages with flexible searches and filtering
- Release or delete individual or multiple quarantined messages with one click
- Monitor quarantine activities and trends via reporting

DLP Email Filters

Webroot's filters are designed to be 99% accurate out-of-the-box. They were created with the help of regulatory experts and in partnership with our customers, who helped us fine-tune the filters using decades of real business email messages. The filters continue to evolve and are regularly updated.

Gain insight into sensitive information within email

Test filters before activating automation rules.
This helps you better understand what information is being managed, uncover individuals who need training or customize and tune new filters.

Improve security awareness by notifying employees when messages automatically encrypt.
If a user forgets to encrypt an email, the filter encrypts and then notifies them, highlighting the confidential words, phrases or attachments.

Understand context.
Did the employee reply to a message with sensitive information already in it, or did they attach the file?

Prove the system's effectiveness to auditors.
Easily provide examples or identify employees in need of additional training.

Empower Users with a Quarantine

Give employees the final say over whether or not to encrypt an email.

For organizations that don't wish to completely automate encryption, Webroot can simply hold a message for review by the sender (or a manager), highlight the content that triggered the policy and allow the sender to release the message with or without encryption along with a typed justification for audit purposes.

Stop messages sent by unauthorized users and hold for review by a manager.

For example, a bank teller sending financial data externally or an intern sending customer data to a personal account.

Stop inappropriate content.

Block any documents that contain an "internal only" header or any message containing profanity.

Communication through email isn't secure

Email is the most commonly used communication tool in business, particularly in the era of remote work. It enables organizations to conveniently collaborate and share valuable information with external customers and partners. But people are busy and it's easy to forget that email isn't secure.

Personally identifiable information within email messages and attachments can lead to data breaches, resulting in reputational risks and high costs. Many organizations turn to DLP solutions to protect email. However, most enterprise DLP solutions are difficult to implement. It is also challenging to detect various forms of unstructured data often creating false positives, slowing the flow of email and potentially driving employees to bypass corporate email by turning to alternative solutions and shadow IT.

Webroot's approach to email DLP is different

Webroot streamlines DLP deployment, reducing the timeline from months to hours, with minimal impact on your team. Our DLP filters have been fine-tuned for over 20 years. Webroot customers benefit from a unique policy selection tool that, within minutes, guides customers to deploy nuanced filters based on their industry and specific needs. With DLP policies built into Advanced Email Encryption, your organization can run efficiently while protecting and monitoring sensitive information sent by your employees.

Visibility into all violations

Understanding how your employees use email and what data is leaving your organization is foundational to meeting compliance requirements and addressing encryption needs. Advanced Email Encryption provides that visibility by detecting policy violations and capturing email content without impeding communication or hindering business workflow.

Webroot also helps promote awareness for your employees, letting them know when an email is encrypted due to sensitive content. The solution highlights sensitive information, helping them understand what caused the email to encrypt and where it was located.

Email messages captured through Advanced Email Encryption are easily accessible and managed. Policy violations are highlighted in the email text for quick reference. Violation summary information makes it easy to find the sensitive information located in attachments.

About Carbonite and Webroot

Carbonite and Webroot, OpenText companies, harness the cloud and artificial intelligence to provide comprehensive cyber resilience solutions for businesses, individuals, and managed service providers. Cyber resilience means being able to stay up and running, even in the face of cyberattacks and data loss. That's why we've combined forces to provide endpoint protection, network protection, security awareness training, and data backup and disaster recovery solutions, as well as threat intelligence services used by market leading technology providers worldwide. Leveraging the power of machine learning to protect millions of businesses and individuals, we secure the connected world. Carbonite and Webroot operate globally across North America, Europe, Australia, and Asia. Discover cyber resilience at carbonite.com and webroot.com.

CARBONITE + WEBROOT
opentext Security Solutions