Email Protection Fundamentals

Explore the key features of our base bundle

Webroot™ Advanced Email Encryption powered by Zix™

Protect your email communications

Email is the most vulnerable aspect of your business. It's quite easy for employees to send sensitive information through email. With remote work, the need for your customers and business partners to easily send you sensitive emails and files has never been greater.

Key features

- Data Loss Prevention (DLP) quarantine enables the monitoring, prevention and reporting on sensitive data being sent outside the organization by unauthorized users
- Single management console for multiple email security products
- Multiple methods of delivery based on organizational needs (sender and recipient)
- Potentially lower costs for cyber insurance

How it works

Advanced email encryption removes the hassle of encrypting email and gives teams the peace of mind that sensitive data sent via email is secure. Using advanced content filters, emails and attachments are scanned automatically and any message containing sensitive information is encrypted for delivery. It automatically encrypts or quarantines based on policies you define for any email environment to secure your mailbox far beyond its native capabilities.

Webroot™ Advanced Email Threat Protection

Purpose-built to help protect your business

Advanced Email Threat Protection provides multi-layered filtering that permits legitimate email while blocking malicious threats such as phishing, impersonation, malware, ransomware and spam-type messages—all automatically.

Key features

- Attachment quarantine performs forensic analysis on attachments in a secure, cloud-based sandbox environment. It can also deliver a disarmed version of files by removing macros or converting files to PDF.
- Link protection rewrites all links to safe versions and performs time-of-click analysis (TOCA) on the destination address. Based on testing, users are either automatically redirected to a safe site, provided a warning for suspicious sites, or blocked from potentially malicious sites
- Message retraction (for Microsoft 365) enhances your incident response with the ability to retract malicious emails already delivered to users' inboxes for 30 days. This minimizes risk by taking malicious email out of users' hands and quickens remediation. The system keeps a detailed audit trail.
- 24/7/365 live threat analyst team is constantly identifying new threats, updating the system, and providing warnings.

How it works

The multi-layer filtering engine delivers an extraordinary level of accuracy that reduces both false negatives (bad emails getting in) and false positives (good emails kept out). This reduces the time you spend managing the system and reduces friction for users.

Webroot® Security Awareness Training

Easily maximize your ability to secure your business and employees

As cybersecurity threats continue to evolve, security awareness training helps businesses decrease help desk costs, protect their reputation and secure their overall cybersecurity investment.

Webroot makes it easy to implement an ongoing training program that significantly reduces the risk of security breaches through phishing simulations based on real-world attacks and training that covers relevant security and compliance topics.

Key features

- Multiple media formats allow you to extend your reach with infographics, posters, videos and more
- 4 learning categories with automated campaign creation and management: security, business, compliance and IT skills
- 120+ courses available all at one inclusive rate
- 200+ phishing template adapted from real-world attacks

How it works

Webroot Security Awareness Training offers efficient delivery of relevant knowledge-based information on various topics, including information security, social engineering, malware and compliance. By participating in security awareness training, employees learn to avoid phishing and other types of social engineering cyberattacks, spot potential malware behaviors, report possible security threats, follow company IT policies and best practices.

In addition to Email Protection Fundamentals, get enhanced endpoint and DNS protection, as well as cloud-to-cloud backup with our **Security Protection Plus** and **Pro Security and Backup** bundles.

Security Protection Plus	Pro Security and Backup
Webroot™ Advanced Email Encryption powered by Zix™: Remove the hassle of encrypting email and protect sensitive business data.	**Webroot™ Advanced Email Encryption powered by Zix™:** Remove the hassle of encrypting email and protect sensitive business data.
Webroot™ Advanced Email Threat Protection: Multi-layered filtering that permits legitimate email while blocking malicious threats.	**Webroot™ Advanced Email Threat Protection:** Multi-layered filtering that permits legitimate email while blocking malicious threats.
Webroot® Security Awareness Training: Easy to implement, ongoing training program that reduces the risk of security breaches through phishing simulations and microlearning.	**Webroot® Security Awareness Training:** Easy to implement, ongoing training program that reduces the risk of security breaches through phishing simulations and microlearning.
+	+
Add-on	Add-on
Webroot® DNS Protection: Secure your DNS connection against cyberattacks, get total visibility into web usage, and enforce acceptable web usage policies to reduce security risk.	**Webroot® DNS Protection:** Secure your DNS connection against cyberattacks, get total visibility into web usage, and enforce acceptable web usage policies to reduce security risk.
Webroot® Business Endpoint Protection: Offers highly intuitive management console to deliver automated cloud-based endpoint detection, prevention and remediation.	**Webroot® Business Endpoint Protection:** Offers highly intuitive management console to deliver automated cloud-based endpoint detection, prevention and remediation.
	+
	Add-on
	Carbonite™ Cloud-to-Cloud Backup: Comprehensive, automatic backup and recovery for Microsoft 365, SharePoint, Google Workspace, Salesforce, Box and Dropbox.

CARBONITE® + WEBROOT®

Carbonite and Webroot, OpenText Security Solutions, 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 email security, 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.