opentext™ | Cybersecurity

DATASHEET

Webroot™ Advanced Email Threat Protection

Purpose-built to secure business emails and communications

Challenge

Email is one of the most efficient and cost-effective means of communicating globally. Businesses depend on email communication even though it has become the most vulnerable aspect of their business. Threat actors target email because of its ubiquitous usage and its unique vulnerabilities. Ever-increasing phishing attacks, viruses and spam only represent a small fraction of existing email-borne security threats that can lead to monetary loss or reputational damage. With increases in social engineering, ransomware attacks, Business Email Compromise (BEC), impersonation and targeted attacks, cybercriminals exploit known vulnerabilities in the biggest email providers to steal privileged information. According to the 2022 BrightCloud Threat Intelligence Report, there was a 1122% increase in phishing attacks in Q1 2022 compared to Q1 2021. In many cases, businessess do not catch the breach, do not know how to assess the impact or do not have tools for remediation. Since many businesses are subject to regulatory requirements, email threat protection is essential to staying compliant.

Solution: Advanced Email Threat Protection (AETP)

Webroot™ Advanced Email Threat Protection provides multilayered filtering for both inbound and outbound emails that permits legitimate email while automatically blocking malicious threats such as phishing, ransomware, impersonation, BEC and spam-type messages.

- **Attachment Quarantine** performs forensic analysis on attachments in a secure, cloud-based sandbox environment. It can also instantly deliver a disarmed version of files by removing macros or converting files to PDF.
- **Link Protection** rewrites links to safe versions and performs time-of-click analysis 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 incident response with the ability to retract malicious emails already delivered to users' inboxes. This minimizes risk by taking malicious email out of users' hands and quickens remediation. The system also keeps a detailed audit trail.
- **24/7/365 Live Threat Analyst Team** constantly identifies new threats, updating the system and providing warnings.

Differentiators

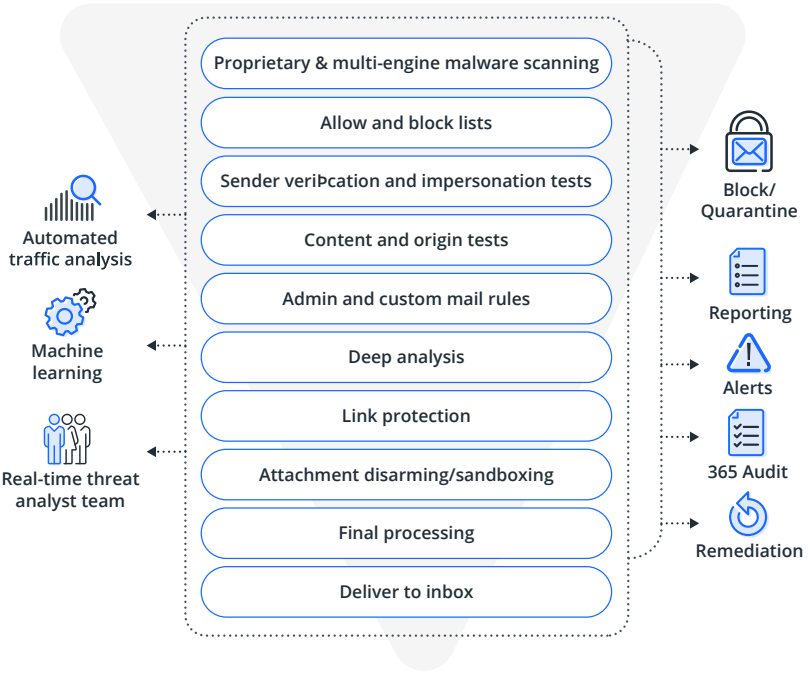
- Rewrites links to safe versions and performs time-of-click analysis on the destination address
- Disarms and performs forensic analysis on attachments in secure, cloud-based sandbox environment
- 99.9% catch rate with real-time threat analysts, automated traffic analysis and machine learning

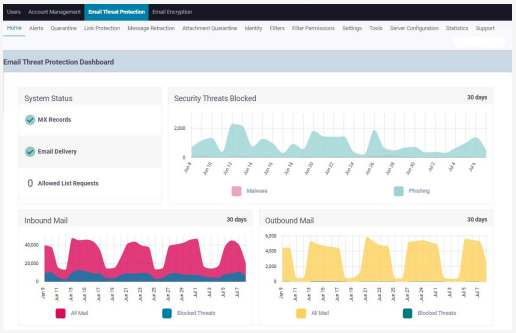
Key Benefits

- Enhanced security for business critical communications
- Enhanced security status in regulated industries
- Single management console for multiple email security products
- Deal with a single vendor for cybersecurity soluitions

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.





Key Features

- Easy to use portal
- Dashboards for intuitive management
- Customizable filtering
- Comprehensive logging and reporting
- Mobile access

Purpose-built to enhance your resilience against cyberattacks

OpenText Cybersecurity helps your business achieve cyber resilience by bringing together best-in-class solutions and enabling you to continue your business operations even when under attack. Together, Carbonite and Webroot can help prevent and protect you from breaches in the first place, minimize impact by quickly detecting and responding to a breach, then recovering the data quickly to reduce the impact and help you adapt and comply with changing regulatory requirements.

Webroot™ Advanced Email Threat Protection is an integral part of our cyber resilience solutions and improves your security posture by providing the first line of defense via multilayered security against email-borne threats such as phishing, ransomware, impersonation and BEC.

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk. DS_041023