OpenText Core Advanced Email Threat Protection

Purpose-built to secure business email communications

Differentiators

- 99.9% catch rate with extremely low false-positives powered by artificial intelligence, automated traffic analysis, and machine learning
- 24/7/365 Live Threat Analyst Team constantly identifies new threats, updating the system and providing warnings
- Identity/Impersonation Protection included in base offer
- Rewrites links to safe versions and performs time-of-click analysis on the destination address
- Disarms and/or performs forensic analysis on attachments in secure, cloud-based sandbox environment

Key Benefits

- Enhanced security for business-critical communications
- Single management console for multiple email security products
- Enhanced security status in regulated industries
- Single vendor for all your cybersecurity needs

Challenge

Email is one of the most efficient and cost-effective means of communicating globally. Businesses depend on email even though it has become one of the most vulnerable aspects 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 email to steal privileged information.

According to our recent Webroot/BrightCloud Threat Intelligence Report, there was a 1,122% increase in phishing attacks year over year. In many cases, businesses 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: OpenText Core Advanced Email Threat Protection

OpenText™ Core Advanced Email Threat Protection provides multi-layered filtering for inbound, outbound, and now internal messages that permits legitimate email while automatically blocking malicious threats such as phishing, ransomware, impersonation, BEC, and spam-type messages.

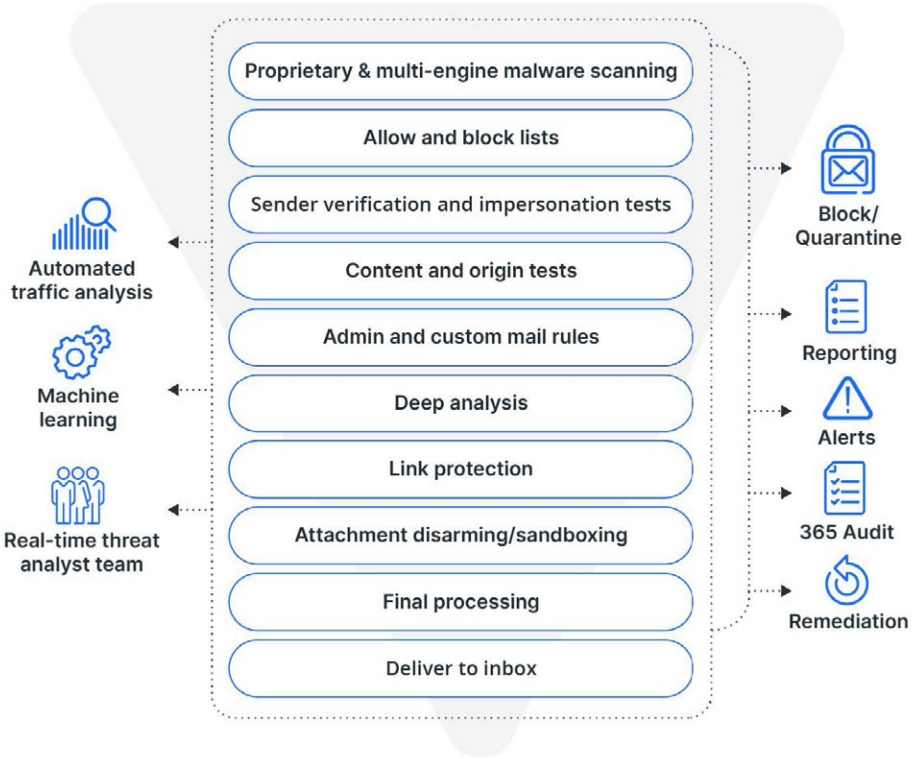
- **Link Protection** rewrites links and performs time-of-click analysis on the destination address. Based on testing, users are either automatically redirected to a safe site, provided a warning for suspicious sites or blocked from potentially malicious sites.
- **Attachment Quarantine** performs forensic 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.
- **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 provides a detailed audit trail.
- **Internal Mail Filtering (for Microsoft 365)** enhances protection from Business Email Compromise attacks by safeguarding internal (user-to-user) communications. This significantly reduces a threat actors' ability to leverage co-worker "trust" and move laterally within an organization.

Key Features

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

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 minimizes time spent managing the system and friction for users, keeping everyone productive.


Proprietary & multi-engine malware scanning
Allow and block lists
Sender verification and impersonation tests
Content and origin tests
Admin and custom mail rules
Deep analysis
Link protection
Attachment disarming/sandboxing
Final processing
Deliver to inbox
Automated traffic analysis
Machine learning
Real-time threat analyst team
Block/ Quarantine
Reporting
Alerts
365 Audit
Remediation

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. OpenText 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.

OpenText Core 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 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_010523