Security Protection Plus Bundle

Comprehensive protection made simple

It's time to level up with the OpenText Security Protection Plus Bundle, which gives you:

- Enhanced security for business-critical communications through OpenText Email Encryption.
- The latest from our 24/7/365 Live Threat Analyst Team, who are constantly identifying new threats, updating the system, and providing warnings with OpenText Advanced Email Threat Protection.
- Link rewriting to safe versions and time-of-click analysis on the destination address through Advanced Email Threat Protection.
- Fully remote endpoint management and control.
- High relevancy and frequency of OpenText Security Awareness Training, with updates featuring useful, interactive, and effective content.
- A reduction in malware by an additional 27.1% vs AV alone with OpenText DNS Protection.[1]

Social engineering and phishing attacks significantly impact organizations of all sizes. Reducing these risks often requires multiple security technologies and extensive employee training, involving coordination with various vendors. Following this approach can be complex and resource intensive. Fortunately, there is another option.

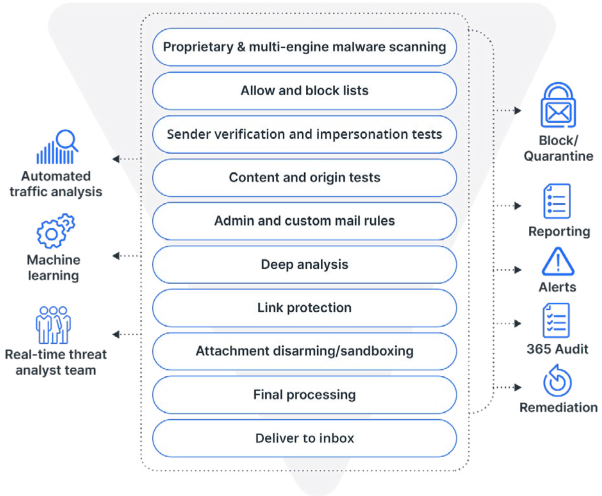
The OpenText Security Protection Plus Bundle

The OpenText™ Security Protection Plus Bundle combines email threat protection, DNS filtering, and comprehensive security awareness training into one cohesive package. This integration helps you strengthen your organization's defenses, streamline management, and ensure a more resilient cybersecurity posture. Designed to safeguard organizations of all sizes, the bundle's multi-layered defenses provide comprehensive protection across various threat vectors.

OpenText™ Core Advanced Email Threat Protection

OpenText™ Core Advanced Email Threat Protection (AETP) provides multi-layered filtering for inbound, outbound, and internal messages. AETP permits legitimate email while automatically blocking phishing, ransomware, impersonation, BEC, and spam-type messages.

- Link Protection rewrites links and analyzes them at click time, redirecting users to safe sites or blocking malicious ones.
- Attachment Quarantine performs forensic analysis in a secure cloud sandbox and can instantly deliver disarmed files by removing macros or converting to PDF.
- Message Retraction and Internal Mail Filtering (for Microsoft 365) retract malicious emails and safeguard internal communications, minimizing risk, speeding up remediation, and reducing lateral movement by threat actors.


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

[1] OpenText Cybersecurity Threat Report 2023

OpenText™ Core Advanced Email Encryption

OpenText™ Core Advanced Email Encryption (AEE) keeps sensitive data secure with simplified encryption. Using advanced content filters, it automatically scans and encrypts emails and attachments with sensitive information. AEE enhances threat defense and enables safe communication outside your network, automatically encrypting or quarantining messages based on your defined policies for any email environment.

- Data Loss Prevention Filters trigger policies to encrypt, route, block, or quarantine emails.
- Industry-specific policies detect information in email subject, body, and attachments, helping customers achieve governance, risk, and compliance (GRC) best practices.
- Policy-builder allows you to select the right combination of filters for your industry.

OpenText™ Core Endpoint Protection

OpenText™ Core Endpoint Protection delivers leading security with real-time threat intelligence, protecting against malware, ransomware, and phishing. It features automated endpoint detection, prevention, and remediation. Plus, cloud-based management enables proactive, predictive defense against complex attacks, without the need for constant updates.

- Multi-vector protection against malicious files, scripts, exploits, and URLs
- Remote policy definition and management
- Precision monitoring and roll-back capabilities for auto-restoring and infected files

OpenText™ Core DNS Protection

OpenText™ Core DNS Protection is a DNS filtering solution that is easy to implement and manage. It greatly enhances security and reduces exposure to malware and other threats. By leveraging machine learning through threat intelligence, you can accurately categorize and filter requested domains.

- Block alternate or unauthorized sources of DNS, prevent access to malicious domains or command-and-control (C&C) servers, and stop data exfiltration through DNS.
- Encrypt and log all DNS requests to prevent DNS hijacks and identify threats, vulnerabilities, and suspicious behaviors.

OpenText™ Core Security Awareness Training

Reduce risky human behavior with continuous, relevant, and measurable education and testing from OpenText™ Core Security Awareness Training (SAT). The full-featured phishing simulator provides an expanding template library based on real-world scenarios. Templates are categorized and regionalized for ease of use while schedule randomization enables staggered delivery.

One step to making your business cyber resilient

OpenText's Security Protection Plus Bundle is a comprehensive solution that helps prevent and protect against threats, ensuring compliance with evolving regulations. Our bundle minimizes the impact of adverse events by swiftly detecting and responding to potential breaches. With our advanced capabilities, your organization can confidently navigate the complex cybersecurity landscape, ensuring continuous protection and compliance.

opentext™