Email Risk Management Bundle

Comprehensive protection of email communications and your business-critical SaaS data

74%[1] of all breaches include a human element, and the average cost of a breach exceeds $4.5 million[2].

It's time to level up with OpenText's Email Risk Management Bundle, which provides:

- Efficiency with fast recovery for reduced downtime costs and seamless business continuity with Cloud-to-Cloud Backup.
- Secure SaaS application data with unlimited backup and recovery from any point in time.
- Compliance with GDPR, HIPAA, FINRA, CCPA with secure and encrypted backup.
- 24/7/365 Live Threat Analyst Team constantly identifies new threats, updating the system and providing warnings with Advanced Email Threat Protection.
- Enhanced security for business-critical communications.
- Single vendor for all your cybersecurity needs.

1 Verizon 2023 Data Breach Investigations Report (DIBR)

2 IBM Security Cost of a Data Breach Report 2023

It's no surprise that email threats are a top concern for IT groups today as organizations of all sizes are affected. Enterprises with more than 2,000 employees are targeted by more than 5,000 email attacks every year, and those with 500-2,000 employees are targeted by about 2,600 (twice as many per mailbox).

Mitigating these risks and recovering data quickly often requires working with multiple security vendors to evaluate, install, and integrate multiple solutions. But it doesn't have to.

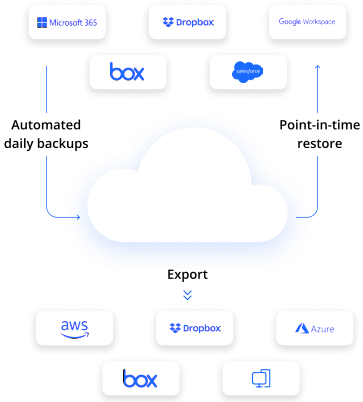
The OpenText Email Risk Management Bundle

The Email Risk Management Bundle from OpenText enables cybersecurity teams to deploy multitiered protection against advanced threats. The elements of the bundle work together to prevent employees and other system users from clicking links, opening attachments, downloading malicious software, leaking confidential information, and otherwise falling victim to threat actors. In addition, the Cloud-to-Cloud Backup solution helps organizations quickly recover data and maintain cyber resilience. Large and small organizations can deploy these solutions from a single vendor, backed by a knowledgeable, responsive support team.

"Only 13% of IT professionals understood that they are solely responsible for backing up the data for SaaS applications."

OpenText Core Cloud-to-Cloud Backup

OpenText™ Core Cloud-to-Cloud Backup offers comprehensive backup and recovery of SaaS application data— Microsoft 365, Google Workspace, Salesforce, Box, and Dropbox—and boasts central management, granular restore, rapid recovery and flexible retention options. This purpose-built backup solution ensures IT administrators can recover as much or as little SaaS application data as necessary.



- Automate backups of Microsoft 365, Google Workspace, Salesforce, Box, and Dropbox
- Flexibly search and recover items, mailboxes or sites at any granular level
- Easily recover data with point-in-time recovery
- Browse daily snapshots and run searches

Learn more:

For more information about the solutions in the Email Risk Management Bundle, visit:

www.carbonite.com/business/products/cloud-to-cloud-backup

www.webroot.com/us/en/business/products/advanced-email-threat-protection

OpenText Core Advanced Email Threat Protection

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

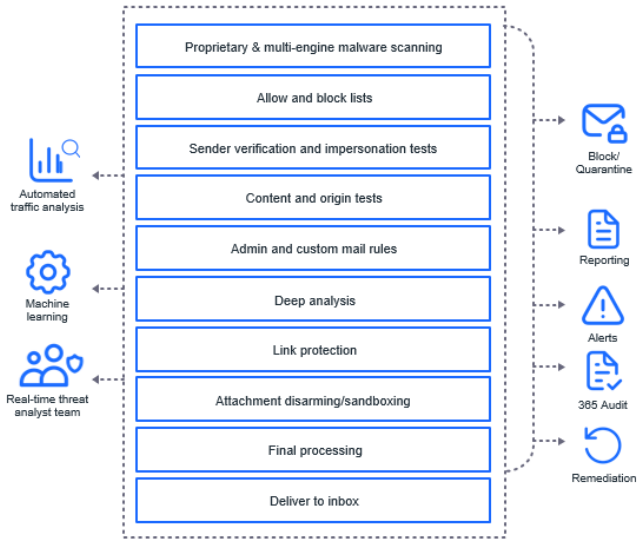
- Link Protection rewrites links and performs time-of-click analysis, automatically redirecting users to safe sites, warning them of suspicious sites, or blocking access to potentially malicious sites.
- Attachment Quarantine performs forensic analysis in a secure cloud sandbox and can instantly deliver disarmed files by removing macros or converting to PDF.
- Message Retraction (for Microsoft 365) enhances incident response by retracting malicious emails from users' inboxes, minimizing risk and speeding up remediation.
- Internal Mail Filtering (for Microsoft 365) protects against Business Email Compromise by safeguarding internal communications, reducing the risk of lateral movement by threat actors.

The diagram below illustrates how this can work with a suspicious email. Webroot Advanced Email Threat Protection has been found to detect as much as 99.9 percent of malicious emails.

One step to making your business cyber resilient

No single technology or best practice can guarantee complete immunity from social engineering and phishing attacks. But OpenText's Email Risk Management Bundle brings together best-in-class solutions that provide a series of progressive defenses that work together to reduce risk to a minimum and help your business remain cyber resilient.

OpenText Cybersecurity can help you prevent threats happening in the first place and help you comply with changing regulations. We also minimize the impact of adverse events by quickly detecting and responding and then seamlessly recovering data. Cloud-to-Cloud Backup and Advanced Email Threat Protection are two pieces of the cyber resilient puzzle that help prevent email-borne threats and provide a comprehensive recovery solution for your SaaS applications if data loss does occur.



opentext™