Data Risk Management Bundle

Comprehensive cybersecurity solutions:
Protect, educate, and secure your business from every angle

It's time to level up with OpenText's Data Risk Management, which gives you:

- Enhanced security for business-critical communications through OpenText™ Core Email Encryption.
- 24/7/365 Live Threat Analyst Team constantly identifies new threats, updating the system and providing warnings with OpenText™ Core Advanced Email Threat Protection.
- Link rewriting to safe versions and performing time-of-click analysis on the destination address through OpenText Core Advanced Email Threat Protection.
- Fully remote endpoint management and control.
- High relevancy and frequency of OpenText™ Core 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™ Core DNS Protection (OpenText Cybersecurity Threat Report 2023).

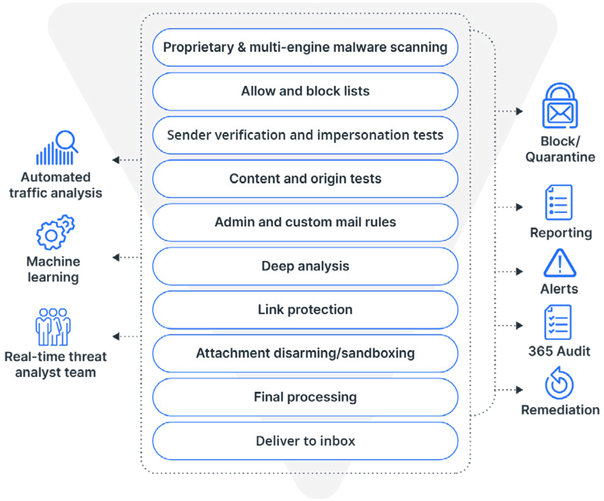
In today's threat landscape, companies must adopt a layered security approach to counter increasingly sophisticated cyberattacks. Social engineering and phishing attacks affect organizations of all sizes, with large enterprises facing over 5,000 attacks annually and mid-sized companies encountering about 2,600. Mitigating these risks requires multiple security technologies and extensive employee training, often involving various vendors, which can be complicated and frustrating. However, you can simplify this process and strengthen your defenses against evolving threats by using a unified solution from OpenText.

The OpenText Data Risk Management Bundle

Cybersecurity teams can combat and minimize the impact of social engineering and phishing attacks with the OpenText™ Data Risk Management Bundle. We take a holistic approach by layering your security and data protection with a comprehensive focus on processes (establishing robust policies and procedures), people (educating employees as the first line of defense), and technology (leveraging advanced product capabilities). Organizations of all sizes can seamlessly implement these cutting-edge solutions from a single vendor, supported by our knowledgeable and responsive team.

Advanced Email Threat Protection

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


Automated traffic analysis
Machine learning
Real-time threat analyst team
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
Block/ Quarantine
Reporting
Alerts
365 Audit
Remediation

Link Protection rewrites links and analyzes them at click time, redirecting users to safe sites or blocking malicious ones.

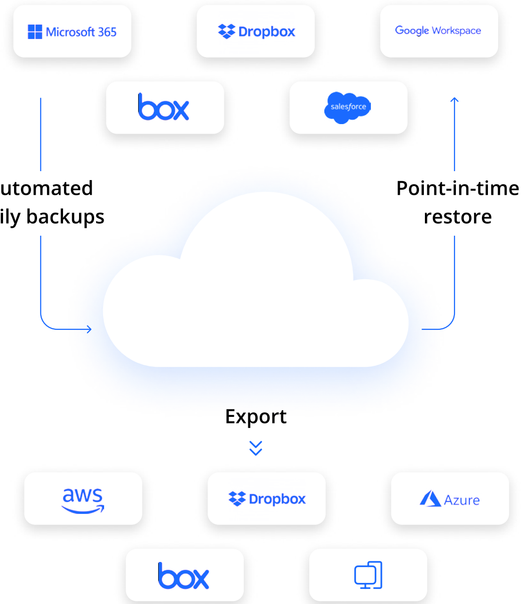
Attachment Quarantine performs forensic analysis in a secure cloud sandbox and can instantly deliver disarmed files by removing macros or converting to PDF.

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.

Cloud-to-Cloud Backup

OpenText™ Cloud-to-Cloud Backup offers comprehensive backup and recovery of SaaS application data, including Microsoft 365, Google Workspace, Salesforce, Box, and Dropbox. It boasts central management, granular restore, rapid recovery, and flexible retention options. The 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.



DNS Protection

OpenText™ Core DNS Protection is a DNS filtering solution that is easy to implement and manage, while greatly enhancing security and reducing 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.

Security Awareness Training

Reduce risky human behavior with continuous, relevant, and measurable education and testing from OpenText™ 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

Adopting a layered security approach is crucial for companies to navigate today's complex threat landscape. Our comprehensive Data Risk Management Bundle offers a unified strategy to combat cyber threats. By integrating robust policies, employee education, and advanced technologies, organizations can significantly enhance their defenses against social engineering, phishing, and other sophisticated attacks. With OpenText, businesses not only prevent and protect against threats but also ensure rapid detection, response, and recovery—achieving true cyber resilience in an ever-evolving digital world.