Data Defense Bundle

Deploy multi-tiered cyber-resilient solutions to defeat and minimize the impact of social engineering and phishing attacks

It's time to level up with the OpenText Data Defense Bundle, which helps you achieve:

- Productivity 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.
- Peace of mind with a 24/7/365 Live Threat Analyst Team that constantly identifies new threats, updating the system and providing warnings with Advanced Email Threat Protection.
- A reduction in malware by an additional 27.1% vs AV alone with DNS Protection (OpenText Cybersecurity Threat Report 2023).
- High relevancy and frequency of Security Awareness Training with updates featuring useful, interactive, and effective content.
- Time and money savings by consolidating 50+ business communication sources into one archiving search.
- Intuitive searches archiving data across email, social media, and collaboration tools like LinkedIn, Twitter, and Microsoft Teams.

Social engineering and phishing attacks are major concerns for IT teams, affecting organizations of all sizes. Large enterprises with over 2,000 employees face over 5,000 attacks annually, while those with 500–2,000 employees encounter about 2,600 attacks (twice as many per mailbox). Mitigating these risks typically requires multiple security technologies and extensive employee training, often involving various vendors. Fortunately, there is a simpler option.

The OpenText™ Data Defense Bundle

Combat social engineering and phishing attacks with the OpenText™ Data Defense Bundle. Organizations of all sizes can easily implement these advanced solutions from a single vendor, supported by a knowledgeable and responsive team.

Cloud to Cloud Backup

OpenText™ Core Cloud-to-Cloud Backup offers comprehensive backup and recovery of SaaS application data, including Microsoft 365, Google Workspace, Salesforce, Box and Dropbox. Tap into capabilities like 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.

Advanced Email Threat Protection

OpenText™ Core Advanced Email Threat Protection multi-layered filtering for inbound, outbound, and internal messages permits legitimate email while automatically blocking malicious threats, such as 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 (for Microsoft 365) retracts malicious emails, 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.

DNS Protection

OpenText™ Core DNS Protection is a DNS filtering solution is designed to be easy to implement and manage while greatly reducing exposure to malware and other threats. This is achieved by leveraging machine learning through BrightCloud Threat Intelligence to accurately categorize and filter requested domains.

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

Advanced Email Encryption

OpenText™ Core Advanced Email Encryption ensures data is secure with simplified email 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. It automatically encrypts or quarantines messages based on your defined policies for any email environment, extending security beyond native capabilities.

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

Security Awareness Training

OpenText™ Core Security Awareness Training provides the continuous, relevant, and measurable education and testing your business needs to help minimize risky user behavior and achieve cyber resilience. The full-featured phishing simulator provides an ever-expanding template library based on real-world scenarios. Templates are categorized and regionalized for ease of use, while schedule randomization staggers delivery to maximize campaign impact.

OpenText Core Business Communication Archive

OpenText™ Core Business Communication Archive is an easy-to-use unified information archiving and eDiscovery solution that stores an unlimited number of files and communications from over 50 different sources including email, social media, and collaboration tools. This simplifies the eDiscovery process by simultaneously searching all communications—saving time and money.

- Unlimited cloud-based storage and eDiscovery for over 50 different sources of communication.
- SimplyShare technology that enables you to share datasets with third parties—without external hard drives or SFTP.
- Flexible search capabilities, such as proactive glossary scanning, data classification, message flagging, attachment OCR scanning, and content indexing.

One step to making your business cyber resilient

OpenText's Data Defense Bundle can help you prevent and protect threats from happening in the first place and comply with changing regulations. Minimize the impact of adverse events by quickly detecting and responding and then seamlessly recovering data.

opentext™