Pro Security and Backup Bundle

Deploy multi-tiered protection to defeat social engineering and phishing attacks

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 Pro Security and Backup Bundle which provides:

- Protection from employees clicking on a link in an email or a text message leading to malicious content or opening up the door for cyberattacks
- Peace of mind and compliance for emailing confidential data or intellectual property to a threat actor impersonating a coworker or a business partner
- Prevention of users downloading and running a rogue app
- Prevention of going to a compromised website and entering credentials into a form
- Automated training management and compliance reporting at an individual, group, and company level

It's no surprise that social engineering and phishing attacks are top concerns 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 social engineering 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 often requires more than one, two, or even three security technologies, plus extensive employee training. Usually that means working with multiple security technology and training vendors to evaluate, install, and integrate multiple solutions. But it doesn't have to.

OpenText's Pro Security and Backup Bundle

The Pro Security and Backup Bundle from OpenText enables cybersecurity teams to deploy multi-tiered protection with solutions that work together against social engineering and phishing attacks. 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 backup solution helps organizations thwart ransomware attacks and maintain cyber resilience. Large and small organizations can deploy seven leading-edge solutions from a single vendor, backed by a knowledgeable, responsive support team.

The Pro Security and Backup Bundle from OpenText	
OpenText™ Core Advanced Email Encryption	Prevents employees from sending sensitive information outside the organization by email (data loss prevention).
OpenText™ Core Advanced Email Threat Protection	Prevents employees from clicking on links and opening attachments used in social engineering, phishing, and ransomware attacks.
OpenText™ Core Security Awareness Training	Provides organizations and employees with cloud-based training and simulated phishing attacks that enable them to recognize and report social engineering, phishing, and other email-borne attacks.
OpenText™ Core DNS Protection	Prevents remote employees and network users from accessing suspicious and inappropriate websites.
OpenText™ Core Endpoint Protection	Detects and blocks the execution of malware and malicious scripts used social engineering, phishing, and ransomware attacks.

[1] Verizon 2023 Data Breach Investigations Report (DIBR)

[2] IBM Security Cost of a Data Breach Report 2023

Learn More:

For more information about the solutions in the Pro Security and Backup Bundle, see:

OpenText™ Core Advanced Email Threat Protection ›

OpenText™ Core Endpoint Protection ›

OpenText™ Core DNS Protection ›

OpenText™ Core Advanced Email Encryption ›

OpenText™ Core Security Awareness Training ›

OpenText™ Core Cloud-to-Cloud Backup ›

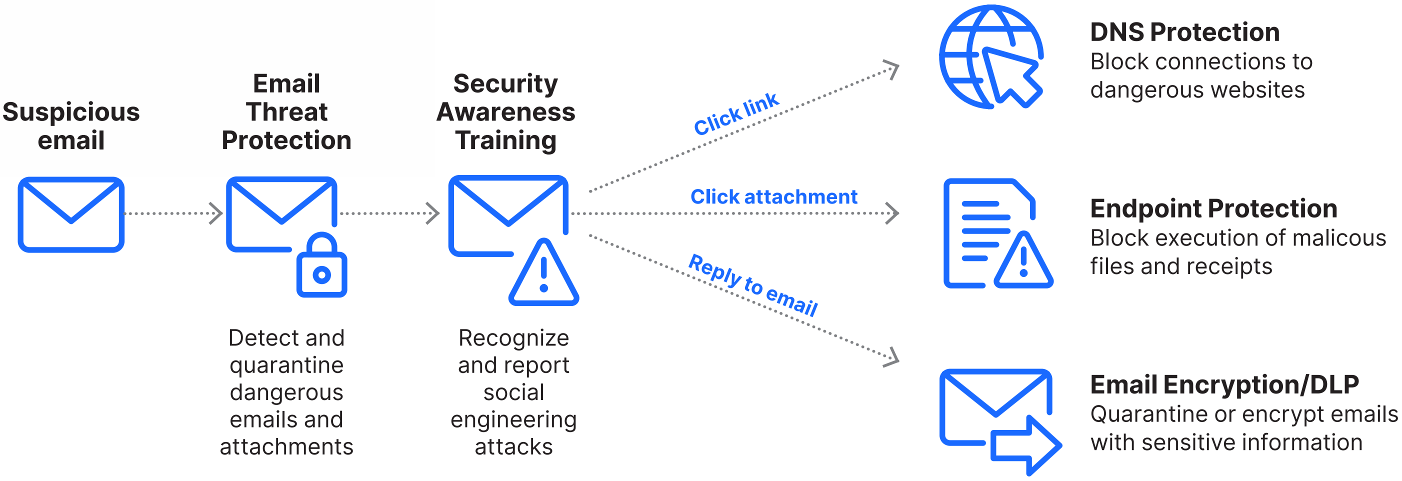
Solutions that work together to provide multi-tiered protection

No single technology or best practice can guarantee complete immunity from social engineering and phishing attacks. But OpenText's bundle provides a series of progressive defenses that work together to reduce risk to a minimum.

The diagram below illustrates how this can work with a suspicious email. Advanced Email Threat Protection has been found to detect as much as 99.9% of malicious emails. At the next stage, training programs using Security Awareness Training have succeeded in helping employees recognize social engineering attacks and reduce malware infections by 90%. But what about the small fraction of malicious emails that make it past these two defenses? OpenText is ready to deal with the unfortunate actions users might take such as clicking on a link to a dangerous website (DNS Protection), clicking on an attachment that contains a malware file or script (Endpoint Protection), or replying to an email with a message that includes sensitive information (Advanced Email Encryption).

Experience the benefits

See how a layered security strategy is necessary in today's threat landscape and how OpenText™ Secure Cloud simplifies the management of your cybersecurity.


Suspicious email
Email Threat Protection
Detect and quarantine dangerous emails and attachments
Security Awareness Training
Recognize and report social engineering attacks
Click link
Click attachment
Reply to email
DNS Protection
Block connections to dangerous websites
Endpoint Protection
Block execution of malicous files and receipts
Email Encryption/DLP
Quarantine or encrypt emails with sensitive information

Copyright © 2024 Open Text