opentext™ | Cybersecurity

Effectively manage the 3 Cs of Cybersecurity – Communication, Correction and Compliance

October 5, 2023 |

Sam Kumarsamy
Director – Product Marketing

Lauren Urban
Product Marketing Manager

Agenda

- Intro to OpenText Cybersecurity
- 3 C's to Cybersecurity
  - Communication
  - Correction
  - Confirmation
- The 4th C: Coordination
- Q&A

Introduction to OpenText Cybersecurity

OpenText Cybersecurity

800,000
Global Customers

100+ million
Secured Endpoints

100 billion
API Calls Per Month

6+ Petabytes
Historical threat data

What We Do

- Threat intelligence
- Endpoint Detection and Response (EDR)
- Network Detection and Response (NDR)
- Application Security Testing
- Data Security
- Identity and Access Management
- Security Operations
- Digital Investigations and Forensics

Cybersecurity Software: Comprehensive Cybersecurity Coverage

Endpoint and Email Security

WEBROOT by opentext
EnCase by opentext
ZIX by opentext
Voltage by opentext

Identity and Access Management

NetIQ by opentext

Backup, Recovery, and Archive

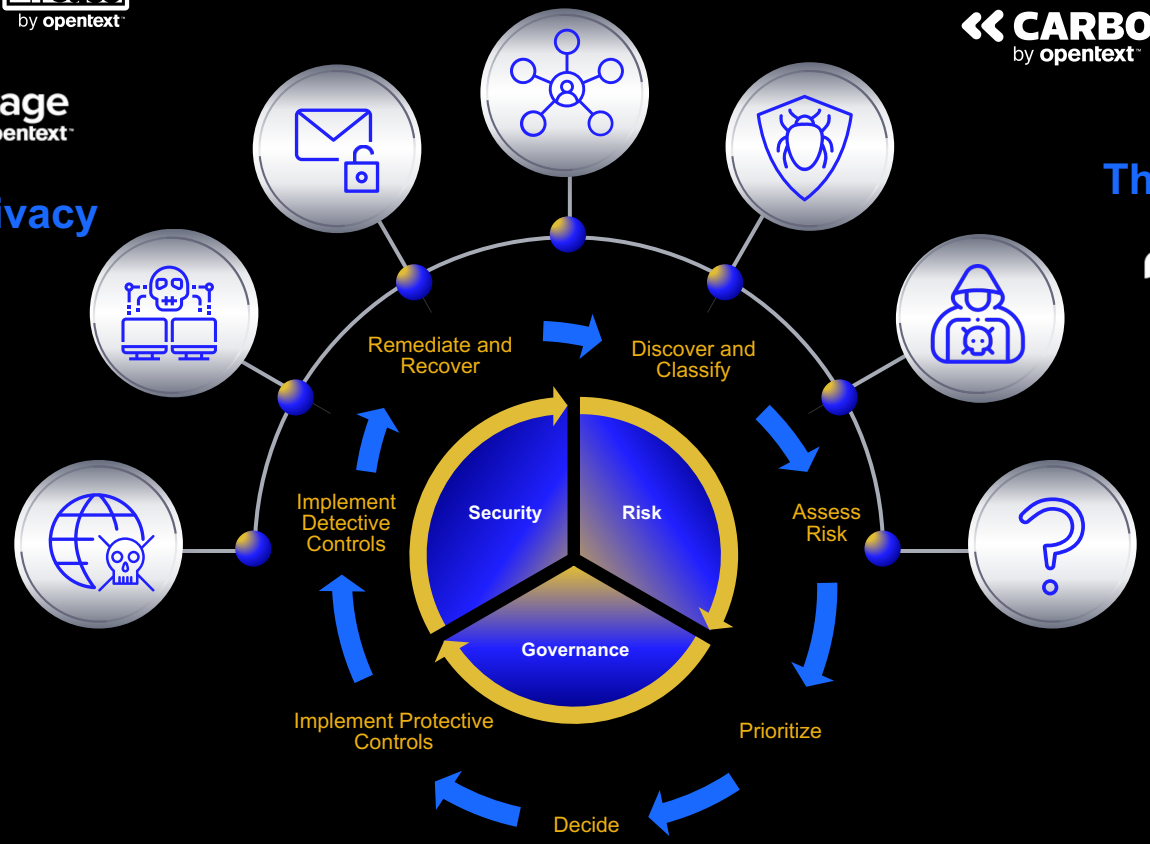
CARBONITE by opentext
ZIX by opentext
EnCase by opentext

Data Protection and Privacy

Voltage by opentext

Threat Detection & Response

ArcSight by opentext
BrightCloud by opentext
BRICATA by opentext



Application and API Security

Fortify by opentext
debricked by opentext

Digital Forensics and Investigations

EnCase by opentext
ArcSight by opentext

Communication

Remote Work Concerns

Market Challenge:

Cyber threats increasing

Increased data leakage via email

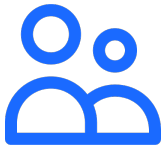
Lack of visibility is a top concern

Primary Use Case: Email Threat Protection

What is the issue?

Email-borne threats including phishing, ransomware, BECs, malware, and unsolicited spam are on the rise

Who does this affect?



Customers of all sizes in all industries

Why?

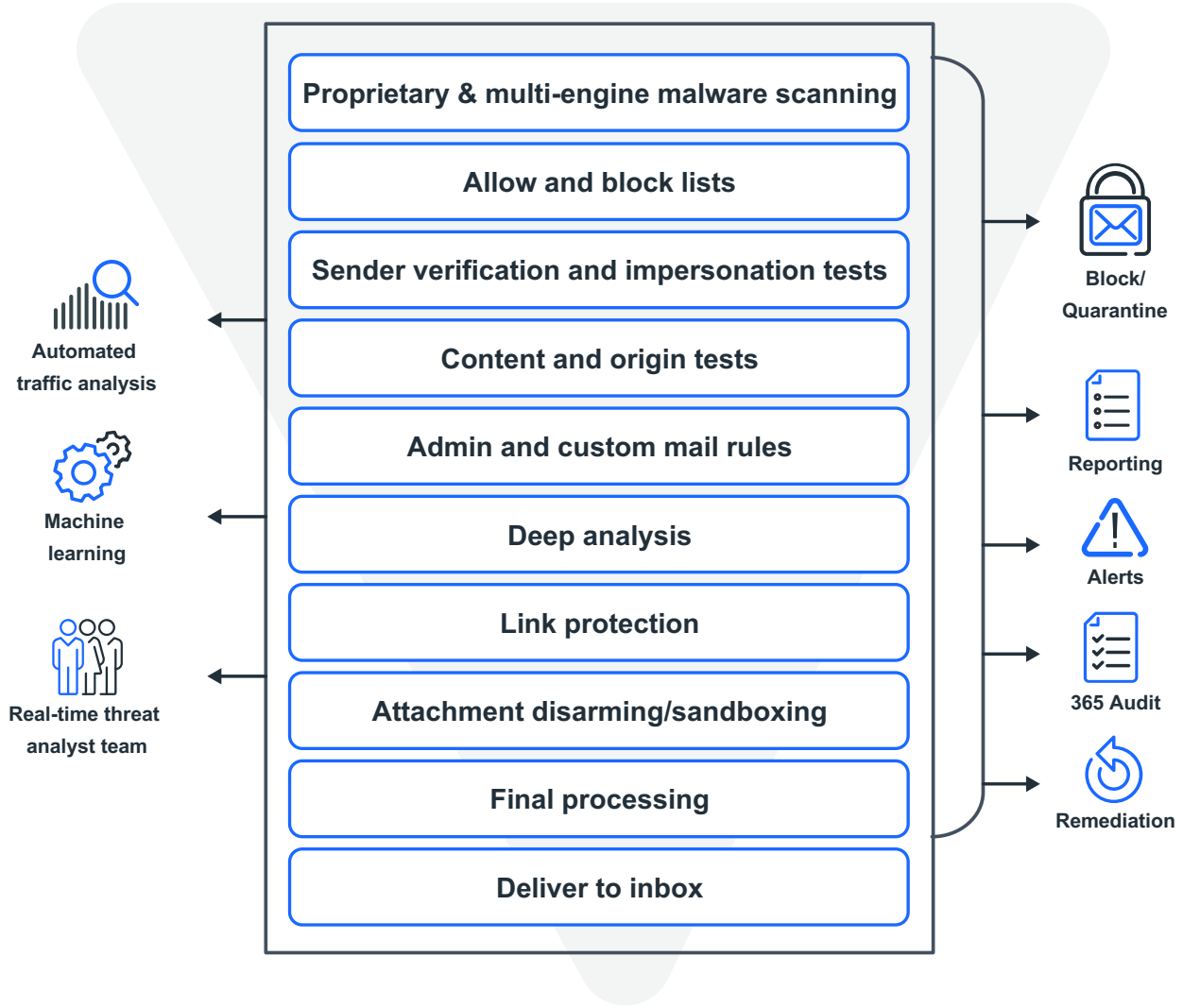
Combats pesky/relentless attackers; improving capture rates and empowering analysts

How?

ETP Multi-layer filtering

- **Inbound and Outbound filtering**
- **Impersonation Protection**
- **Link Rewriting with Time-of-Click Analysis**
- **Attach Disarming/ Sandboxing**

Email Threat Protection – Filtering



Key Differentiators

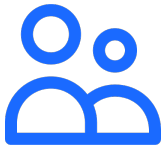
- Fast/Easy Implementation
- Simple to manage, support, and customize
- Includes key features in base offer other vendors charge more for
- Identity/Impersonation protection offers unlimited users/domains
- Link Protection performs time-of-click analysis, empowered by BCTI
- Attachment disarming avoids sandbox delays

Primary Use Case: Email Encryption

What is the issue?

Sensitive or private data exchanged “clear text” and open to prying eyes; opportunistic TLS vulnerable to “man-in-the-middle” attacks

Who does this affect?



Customers of all sizes in all industries, in particular those with regulatory requirements

Why?

Encrypted communications offer regulatory compliance, non-repudiation, and reduced cyber-insurance premiums

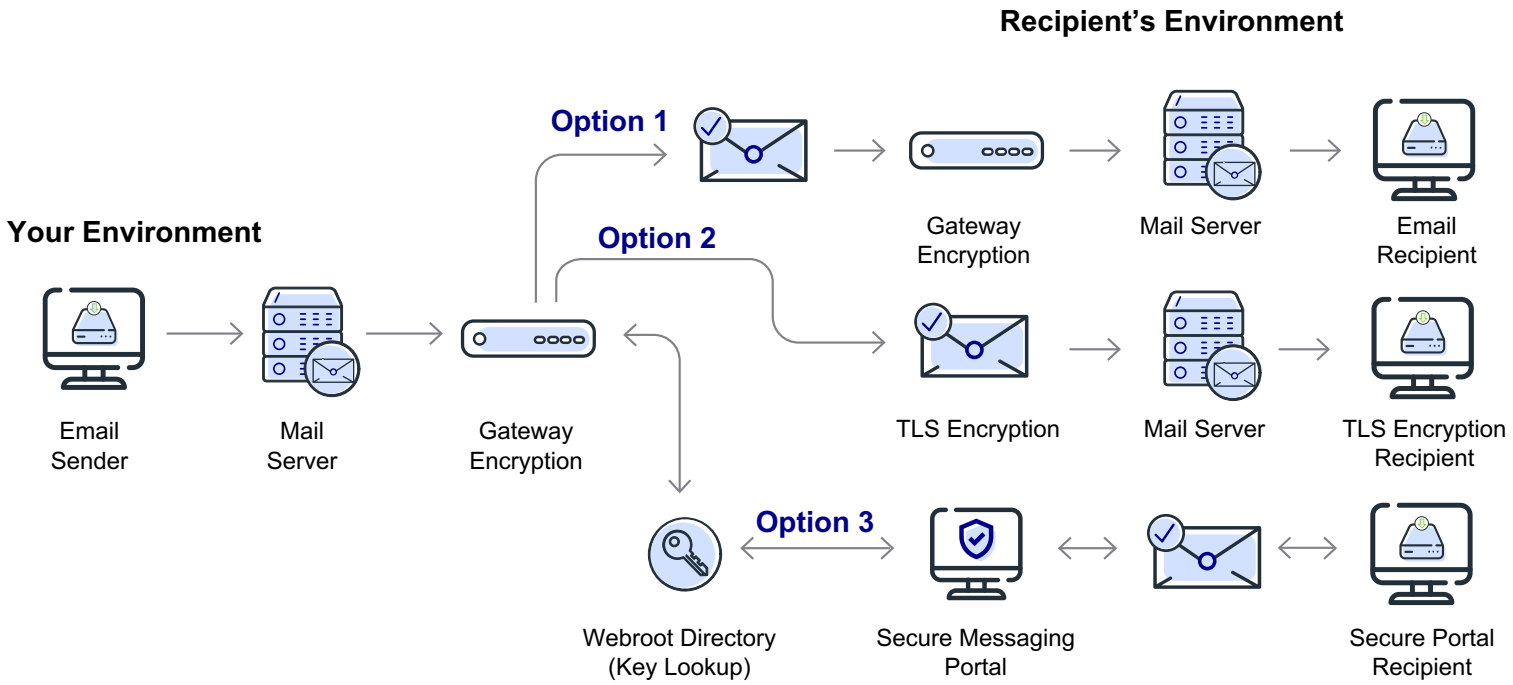
How?

“Transparent” encryption with patented Best Method of Delivery

- **World’s largest S/MIME key community**
- **Regulatory or Custom Policy-based Encryption/DLP**
- **Multiple secure delivery options to fit needs**
- **Empower external collaboration via Secure Compose portal**

Email Encryption – Delivery Options

Best Method of Delivery (BMOD)



Secure delivery to any device, anywhere, anytime

Key Differentiators

Option 1

- Bi-directional secure delivery between Zix customers
- Message level encryption (SMIME)

Option 2

- Policy based TLS delivery

Option 3

- Secure Message Portal
- Delivery to any device, anywhere, anytime

Primary Use Case: Data Loss Prevention

What is the issue?

Inadvertent loss of sensitive, or private data

Who does this affect?

Regulatory bound customers (Healthcare, Finance, State/Local Government, etc)

Why?

Prevent regulatory violations due to sensitive data exfiltration

How?

Regulation-specific or customized DLP policies

- **Scans message subject, body, attachments**
- **Automatically blocks inappropriate communications**
- **Simple insight into policy violations and users**
- **Graphic reporting for compliance**

Correction

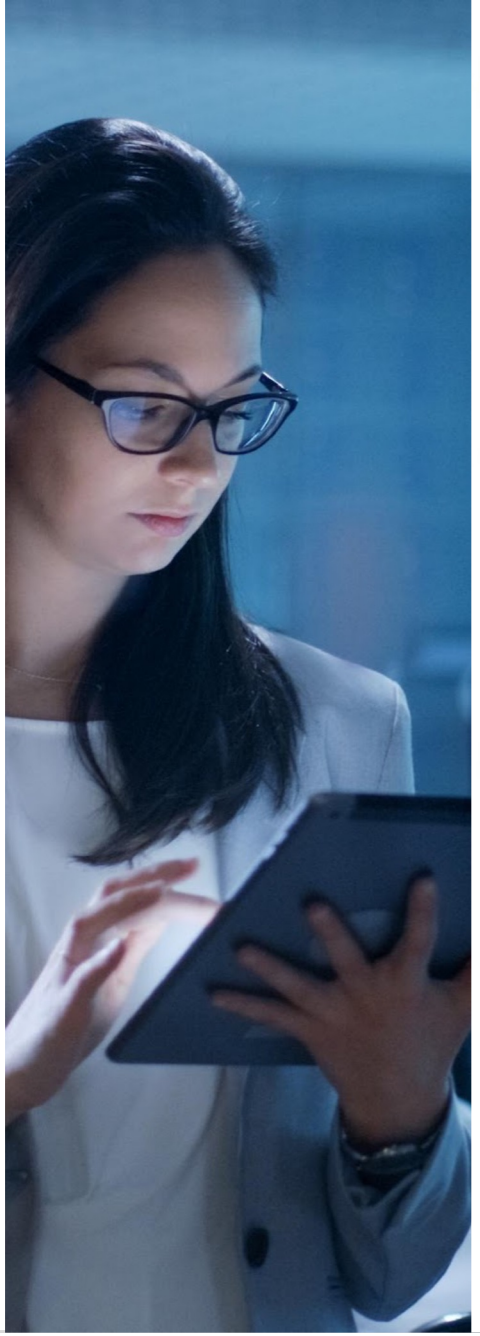
Why back up SaaS data?

SaaS providers are NOT responsible for backing up customer data

SaaS platforms like Microsoft 365, Google Workspace, Salesforce, Box and Dropbox offer flexibility, scalability and collaboration. Even though these platforms are secure, your data isn't protected to the same extent as their infrastructure.

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

ESG, The Evolution of Data Protection and Cloud Strategies, May 2021.



Microsoft

"We recommend that you are regularly backup your content and data that you store on the services or store using third-party apps and services."

salesforce

"Effective July 31, 2020, Data Recovery as a paid feature will be deprecated and no longer available as a service."

Google

"You have a limited time from when the data was permanently deleted to restore files and messages. After that, the data is gone forever."

Dropbox

"Deleted files are marked for deletion in our system and are purged from our storage servers. They can no longer be recovered."

The solution: Carbonite™ Cloud-to-Cloud Backup

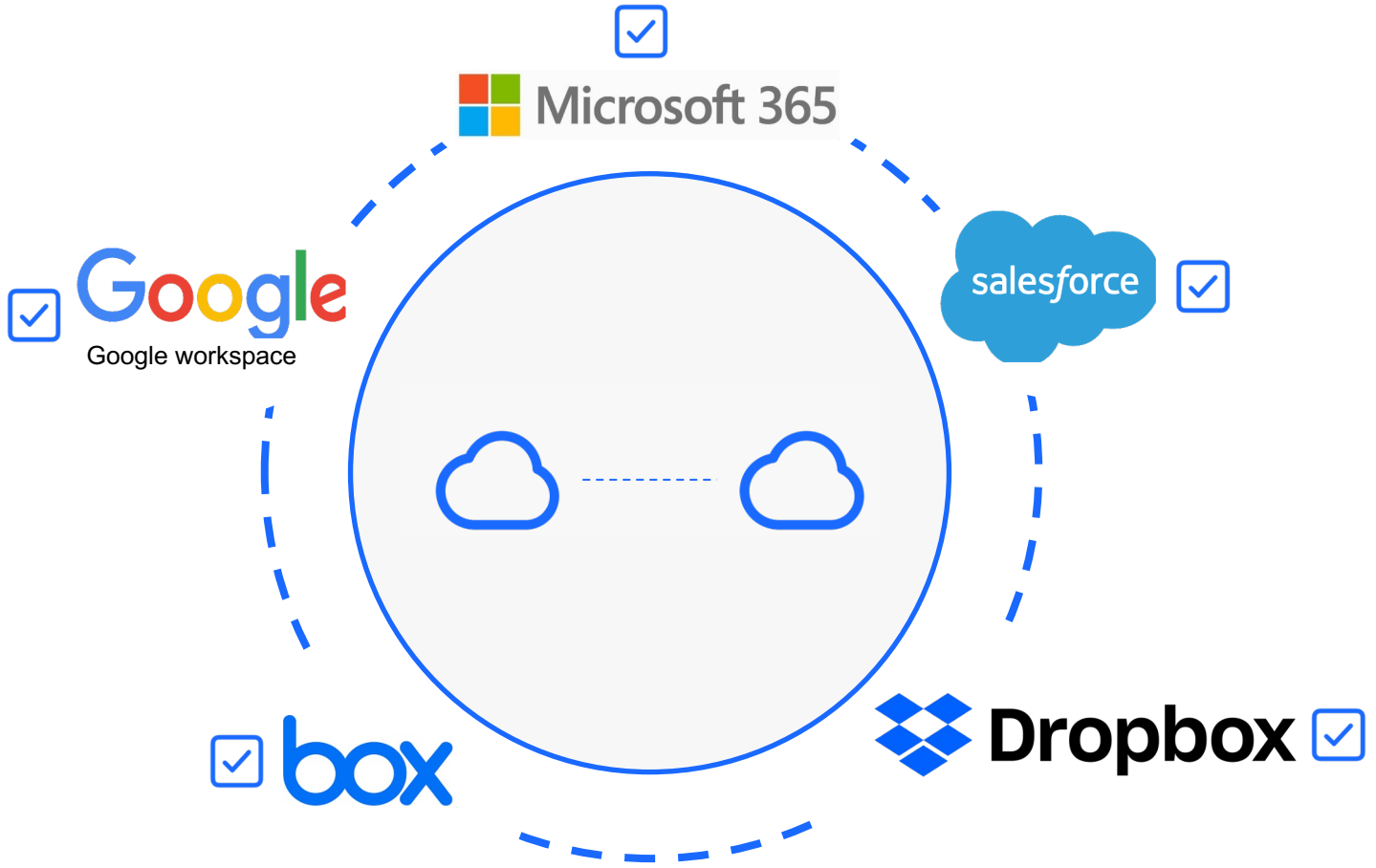
Automated daily back ups

with unlimited retention and full point-in-time recovery

The Ease of Carbonite™ Cloud-to-Cloud Backup

Simple set-up and management

- Single-pane management
- Intuitive User Interface (UI)
- Set-up in 5 minutes, 6 basic steps
- Manage multiple SaaS applications: Microsoft 365, Google Workspace, Salesforce, Box and Dropbox
- Flexible recovery: point-in-time, keyword, hierarchical, cross-user, cross-org



Carbonite™ Cloud-to-Cloud Backup features

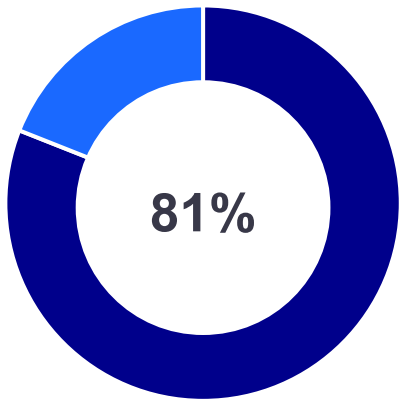
- **Protect** against data loss, data breach and ransomware
- **Automate** backups of Microsoft 365, Google Workspace, Salesforce, Box and Dropbox.
- **Fast**, flexible and granular restoration of items, mailboxes or sites.
- **Easily** recover data with point-in-time recovery.
- **Browse** daily snapshots and run searches.
- **Feel** more secure with full redundancy.
- **Store** more with unlimited storage and retention.

Carbonite™ Cloud-to-Cloud Backup

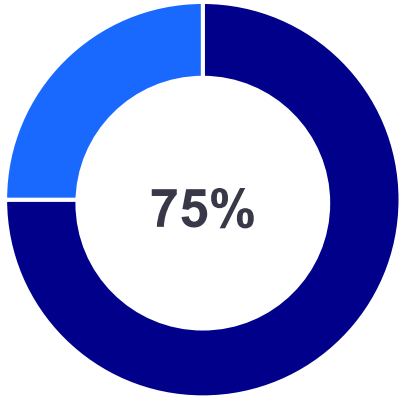
Protect data from the cloud, in the cloud

Confirmation

Maintaining compliance: A growing challenge



of organizations currently support six communication and collaboration applications



of organizations **completed over 50 eDiscovery requests** in the last year[2]

$4 Million

lost on average due to a single non-compliance event[3]

1. Enterprise Strategy Group Research Report, Unified Communication and Collaboration Integrations for Modern Business Workflows, February 2023.
2. ESG : https://www.proofpoint.com/us/resources/e-books/ediscovery-market-trends-and-challenges
3. Globalscape; The True Cost of Compliance with Data Protection Regulations

Modern archiving challenges

Sharing data securely

Sharing eDiscovery with outside council may expose your data; setting up an SFTP site or mailing an external drive could get in the hands of unintended parties

Single-source archiving

Most solutions only archive email – and more companies are realizing that they need to archive more sources for compliance and litigation purposes

Expensive and complex

Many archiving solutions are complex to set up and use

Running internal investigations can be challenging and requires the help of IT

What is Carbonite™ Information Archiving?

A modern archiving solution to help business comply with changing regulations

- Archive 50+ data sources, including emails, Teams, SMS and any other business communication tool you use
- Proactively schedule reviews and flag potential issues
- Simplify the eDiscovery process, with an easy-to-search solution
- Meet and exceed compliance needs (e.g., GoBD, GDPR, HIPAA, SEC, FINRA and more)
- Securely share specific information with legal counsel without the need to export

Carbonite™ Information Archiving

Archive all your business communication and make eDiscovery easier for your team.

Share data quickly and securely

Speed up eDiscovery while securely sharing specified datasets with legal council.

Multi-source solution

Archive over 50 data sources to meet and exceed compliance and corporate governance needs.

Flexible search

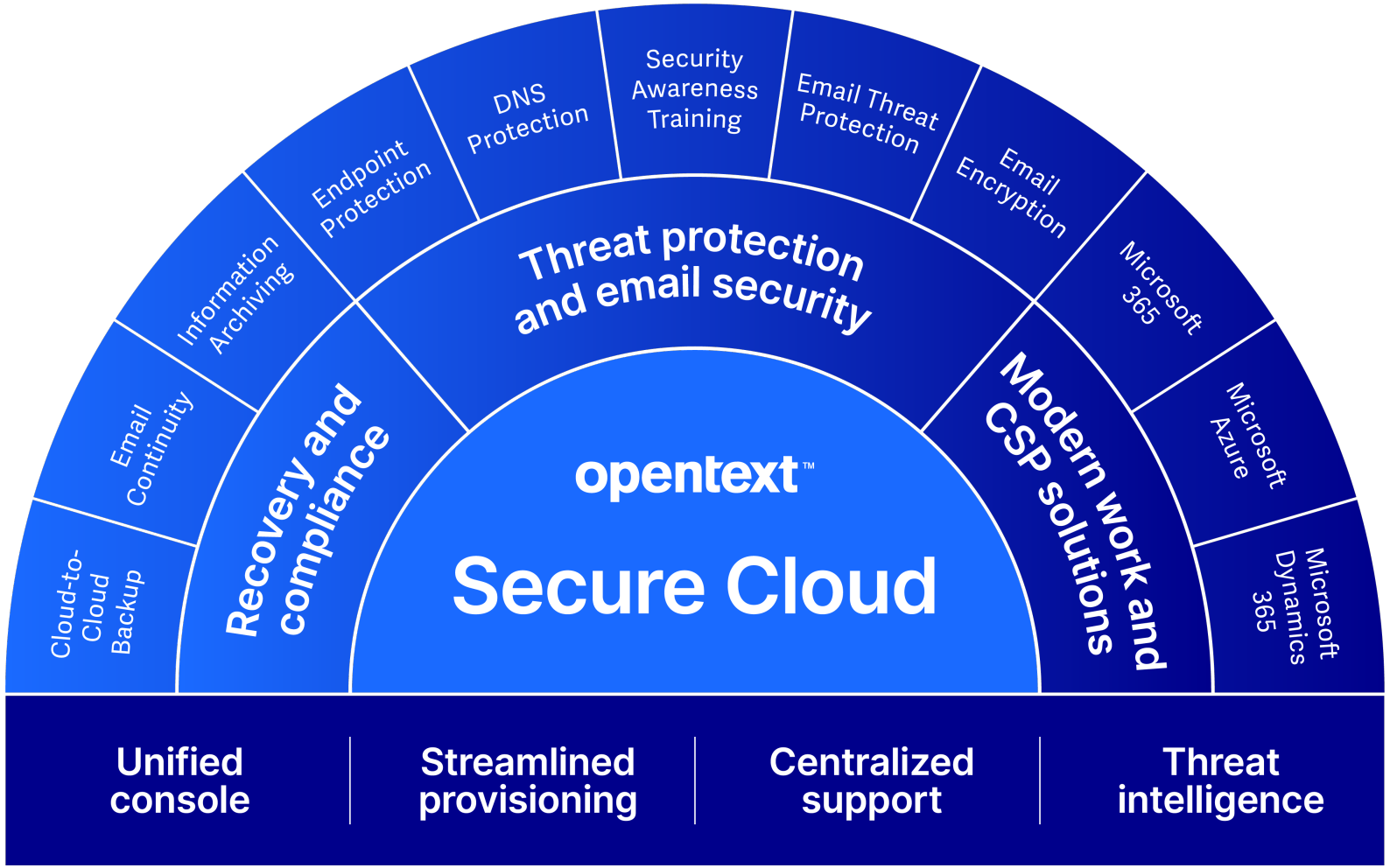
Easily search archived communications without technical expertise.

Coordination

Bringing it all together with Secure Cloud

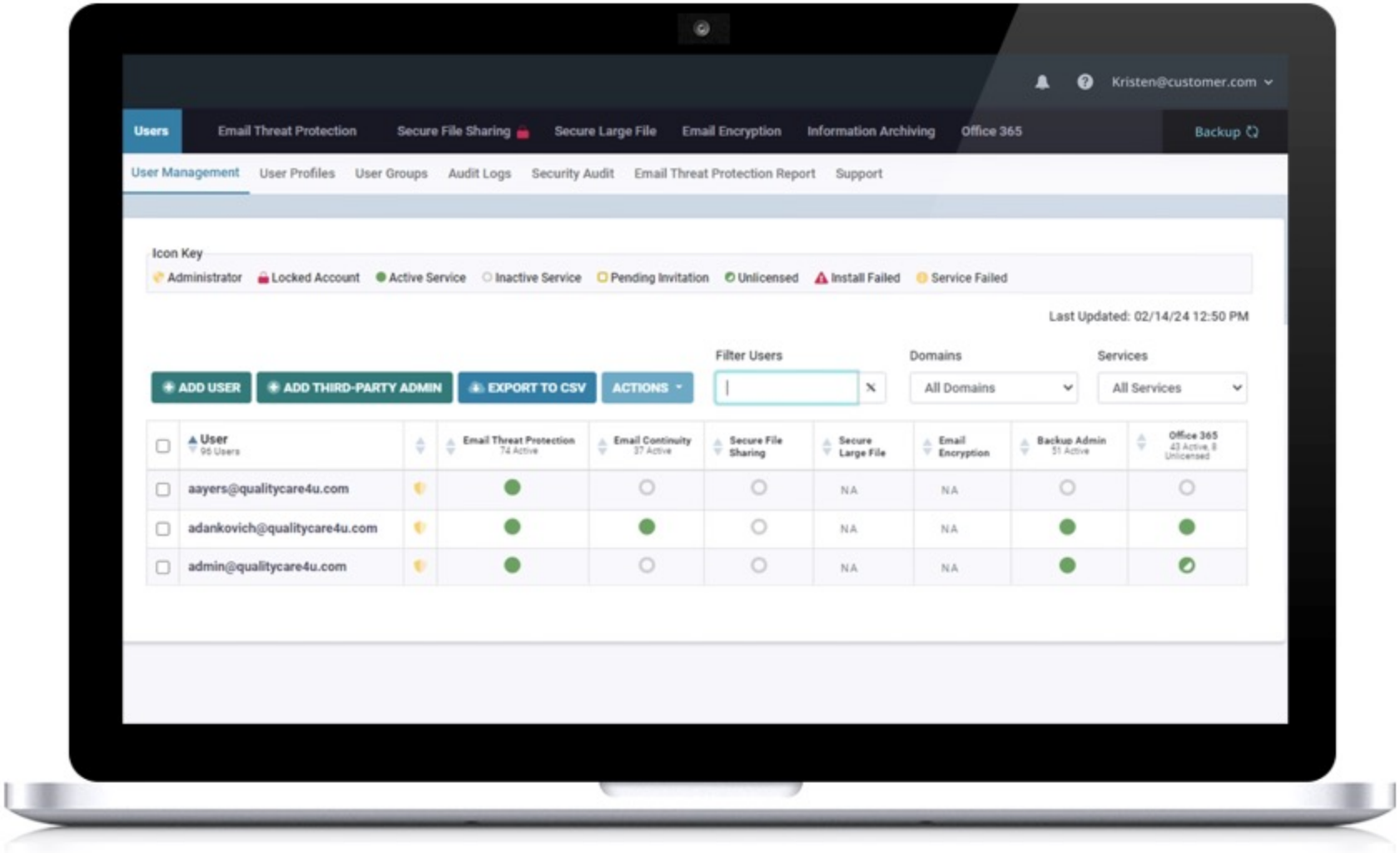
Secure Cloud

A unified platform to streamline cybersecurity



Secure Cloud

A unified platform to streamline cybersecurity



OpenText Cybersecurity is dedicated to protecting your data

MAKING SURE IT'S THERE WHERE AND WHEN YOU NEED IT.

Question and Answer

Thank you

twitter.com/opentext

linkedin.com/company/opentext

opentext.com

opentext™ | Cybersecurity