opentext™ | Cybersecurity

Four Surprising Ways OpenText Keeps Email Encryption Secure and Simple

Discover the measures you need to thrive in an evolving threat environment

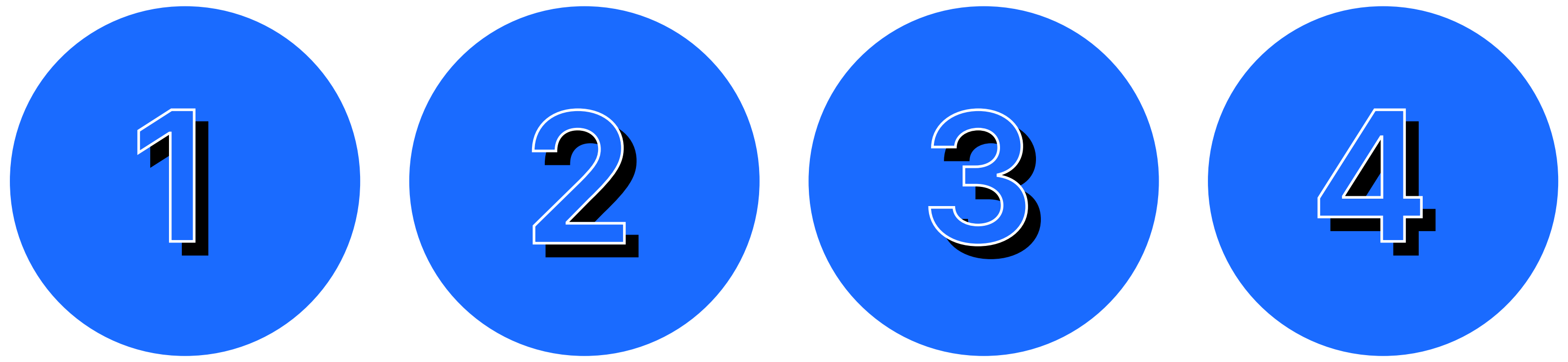
Introduction

▶▶ It’s no secret that traditional email encryption solutions have developed a complicated reputation. Many of them come with difficult and cumbersome instructions, time-consuming processes, and more than a few hoops for users to jump through.

There’s a big risk attached to these tools. When email encryption tools are difficult to use, people won’t use them. And when users don’t bother to use them, it opens businesses up to huge security risks.

However, skipping encryption simply isn’t an option in today’s cybersecurity landscape. The threat landscape has increased exponentially in the last few years, and isn’t showing signs of slowing down anytime soon.

All organizations—but especially those who deal with sensitive information—need an easier way to encrypt emails. And they might be surprised to learn that there is one: OpenText Cybersecurity’s Email Encryption.



This guide will shed light on **four ways** that OpenText Cybersecurity’s Email Encryption simplifies the email encryption process and provides users with an experience that’s simple, streamlined, and secure.

Contents

1 Transparent Delivery

▶▶ One of the biggest pain points email encryption software customers face is the recipient process, which has traditionally been complicated and cumbersome, filled with portals, secret passwords, and extra steps.

Nobody wants to make recipients go out of their way just to read an email—and now they don't have to.

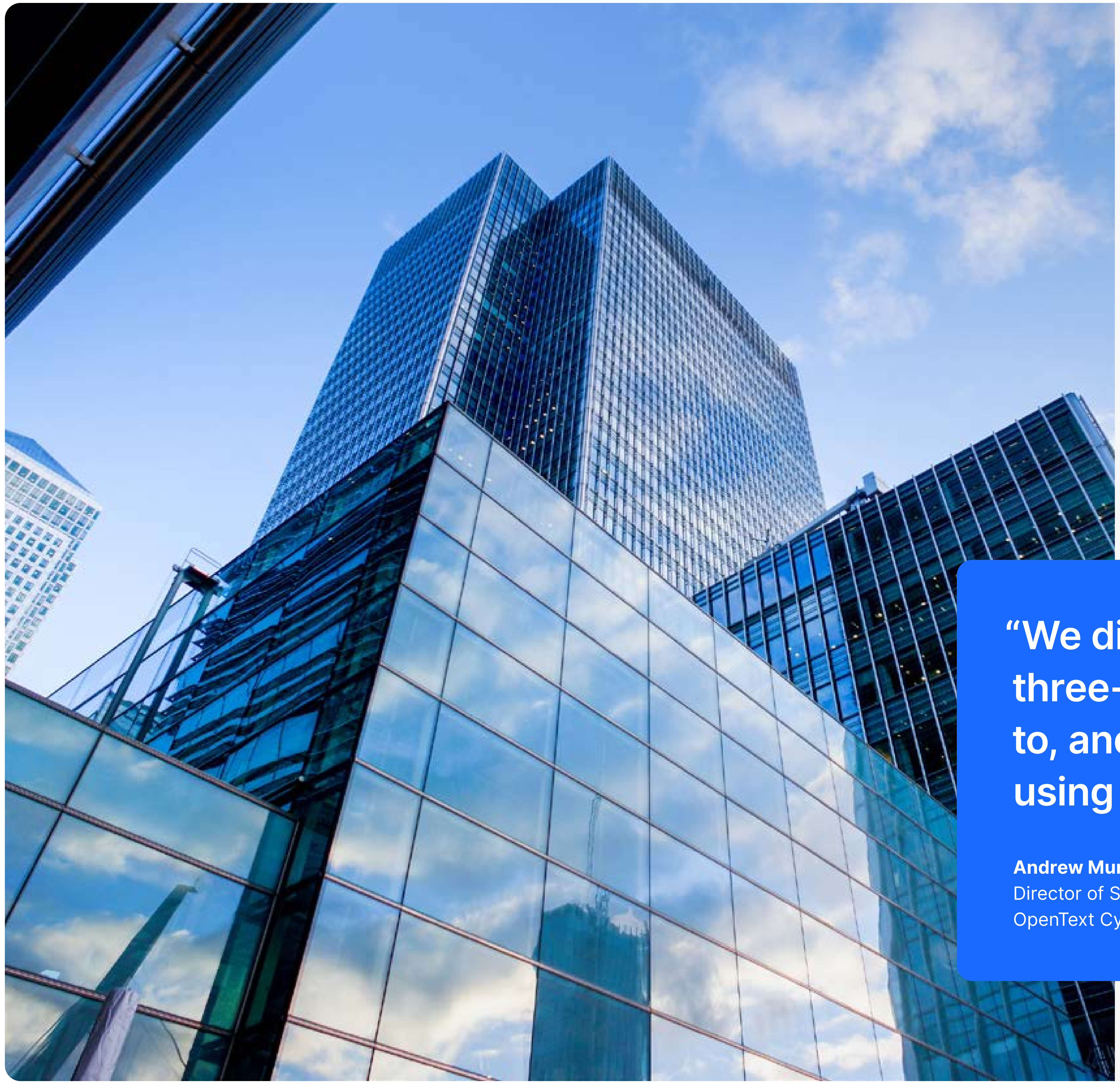
OpenText Cybersecurity's Email Encryption (powered by Zix) makes the email recipient process as easy as possible. If a message is going to other members of the OpenText email encryption world, the email is automatically encrypted, making it easy to receive.

How it works

Many organizations rely on encrypted communication to carry out their daily tasks. Let's use the example of a hospital communicating with a claims processor; there's a pretty good chance that the email content being sent between these two parties contains sensitive information.

OpenText Cybersecurity's Email Encryption makes this assumption when both the sender and the recipient are OpenText Cybersecurity clients. Regardless of the email content, OpenText Cybersecurity will encrypt the outgoing email from one customer, and send it to the recipient completely transparently. No portal, no passwords, no extra steps – just a blue bar at the top of the email confirming it was sent securely. From there, the recipient can reply to the email exactly as they would a regular email.

OpenText Cybersecurity's Email Encryption makes the recipient process intuitive for non-OpenText clients, too. The recipient secure email portal is designed for non-technical people to be able to access, read, and reply to encrypted emails easily.



How OpenText Cybersecurity helped a bank throw out their 30-page process

Andrew Murphy, OpenText Cybersecurity's own Director of SMB Product Marketing, recalls a banking client that had a similar story of eliminating a cumbersome recipient process.

"Before becoming an OpenText Cybersecurity customer, they were using a competing solution for email encryption," he says. This solution proved to be so complicated that the customer had painstakingly created a 30-page document, complete with screenshots, showing how to read and reply to an encrypted email.

As Andrew recalls, once this customer switched to OpenText Cybersecurity, they completely eliminated the need for detailed documentation. "We did provide them with a three-page guide to refer to, and they didn't even end up using it. They didn't have to," he says. ■

> "We did provide them with a three-page guide to refer to, and they didn't even end up using it. They didn't have to."
>
> **Andrew Murphy**
> Director of SMB Product Marketing
> OpenText Cybersecurity

2 Automatic Email Encryption with State of the Art Filters

▶▶ Security tools are only effective when people use them. But IT departments only have so much influence over which actions their employees take when sending information over email. While many organizations have increased their employee training amid an increased threat landscape, there are also more opportunities than ever for sensitive information to be exposed accidentally.

Data protection isn't just an organizational issue; it's also a regulatory one. The Health Insurance Portability and Accountability Act (HIPAA) requires that all patient data is kept secure and private. With traditional email encryption solutions, this burden falls on employees every time. For healthcare organizations, this is an added layer of complication on top of an often hectic landscape for employees.

What's more, some employees don't even know when they've sent sensitive information (consider the example of someone sending a spreadsheet attachment that has a hidden column of Social Security numbers they failed to see). Thankfully, OpenText Cybersecurity offers automatic encryption, removing the burden from employees of having to remember to encrypt sensitive emails every time they send one.

How it works

OpenText Cybersecurity's Email Encryption provides out-of-the-box automatic policies for HIPAA, Social Security numbers, and financial information. When a policy is triggered—whether the sender has elected to encrypt the email or not—emails can be encrypted, blocked or quarantined.

The result is that any email containing sensitive information is automatically encrypted, saving both employees and the organization at large from the consequences of a security breach.

MEMORIAL HERMANN

Memorial Hermann relies on OpenText Cybersecurity to stay HIPAA-compliant

The staff at Memorial Hermann have an impressive reputation to uphold. The integrated health system is one of the largest not-for-profit health systems in Southeast Texas, and relies on the dedicated and tireless work of 5,500 physicians and over 26,000 employees.

Quality and patient safety are top priorities for Memorial Hermann, and each employee is held to high standards where these values are concerned. This means taking patient privacy very seriously, and putting the right solutions in place to ensure these values can't be easily compromised.

But policies like HIPAA put a potentially large burden on the end user. Without an automatic encryption solution, staff would need to be extremely vigilant about which emails should be encrypted.

In short, Memorial Hermann needed an email encryption solution that would allow them to protect patient privacy automatically while keeping communication flowing smoothly between physicians, nurses, staff, patients, and outside healthcare organizations.

They found that solution with OpenText Cybersecurity's Email Encryption. Since the product comes with out-of-the-box automatic policies for HIPAA, Social Security numbers and financial information, Memorial Hermann never had to put their staff through the undue stress of having to ensure the right controls were in place at the right time.

With these custom filters applied, everyone who's a part of Memorial Hermann can send emails worry-free. Any sensitive information that passes through the network's custom spam filters is automatically encrypted, which provides "A way for us to meet our HIPAA requirements and automatically prevent spillage for everyone in our organization," says the organization's Cyber Security Analyst. ■

Connecticut Orthopaedics

For Connecticut Orthopaedics, email encryption is an important part of a zero-trust frameworks

Mark Filiault had ambitious goals as the CIO of Connecticut Orthopaedics. At the tail end of the last decade, he describes himself as having been "hyper-focused on trying to evolve the organization to be more in line with a zero-trust framework."

> "Secure communication became a vital part of how we could be more advanced and a better choice in the marketplace."
>
> **Mark Filiault**
> Chief Information Officer
> Connecticut Orthopaedics

This goalpost only continued to move as the cybersecurity landscape grew more complicated. For Mark, this meant having to double down and implement stronger layers of security to keep the organization safe from threats.

A key aspect of this push for layered security was implementing an email encryption solution. As Mark explains, "We needed an innovative and safe way to communicate with other physicians, insurance companies, patients, and more," while keeping sensitive information safe. This meant staying HIPAA-compliant by looking for a solution that would automatically detect—and encrypt—any information that HIPAA influenced.

Mark found the right solution in OpenText Cybersecurity's Email Encryption, and immediately noticed a tremendous change in the way staff were able to communicate. Having the right tool, he says, has allowed the organization to "embrace regulation, rather than running away from it." As he says, "Secure communication became a vital part of how we could be more advanced and a better choice in the marketplace." ■

3 Seamless Integration and Purpose-Built Add-Ons

▶▶ Encrypting potentially sensitive information is one way to protect your organization and end users from harm, but it's also just one piece of the cybersecurity puzzle. Every organization has a unique set of needs, and an unknown number of potential threats that could severely affect operations at any time.

That's why it's important to ensure your email encryption solution comes along with purpose-built add-ons and can also seamlessly integrate with other security solutions. OpenText Cybersecurity can be easily integrated, and is also part of a larger network of threat protection that keeps your organization safe.

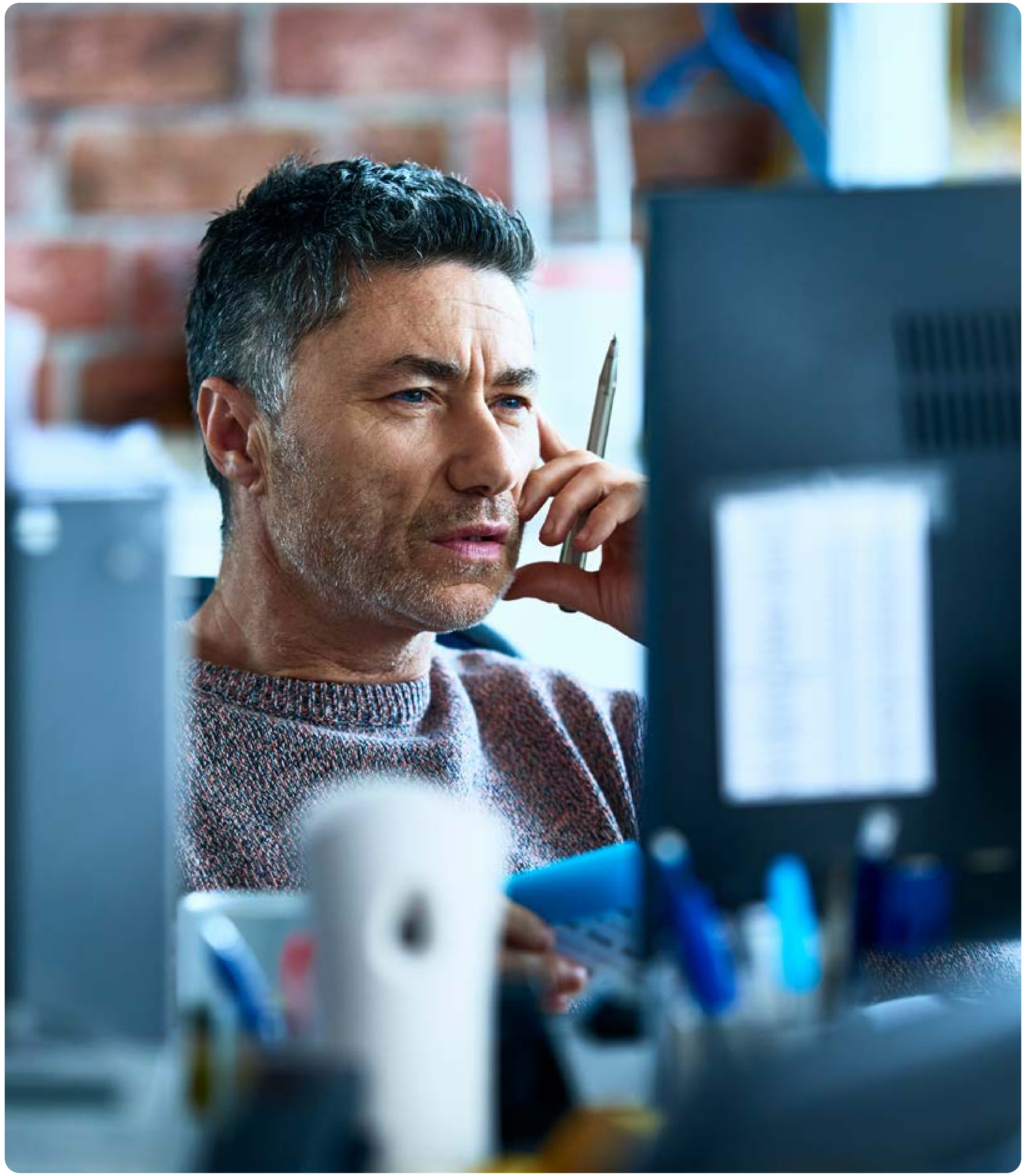
How it works

OpenText Cybersecurity brings together a number of features that can be brought in to improve and enhance the overall user experience. Let's take a look at each:

Enable Single Sign-On with SAML 2.0

Some organizations have strict authentication requirements, and others want a seamless experience between their current company website and their branded portal. For both of these users, Single Sign-On (SSO) is available as an additional service at no extra cost.

SSO allows a user to login to their custom-branded OpenText Cybersecurity portal with existing credentials they already use for the customer's website or other applications. Without having to login again, users click a link to be taken directly to their secure inbox. This feature is implemented in using SAML 2.0, which authorizes user access to web services across organizations.



Protect inbound and outbound emails with OpenText Threat Protection

Even with encryption offering substantial protection, there are still an ever-growing number of phishing attacks that can make their way through and compromise business. OpenText Advanced Email Threat Protection provides multilayered filtering for both inbound and outbound emails that lets the right emails through while blocking malicious threats such as phishing, ransomware, impersonation, business email compromise (BEC) and spam.

OpenText Email Threat Protection is built to offer best-in-class protection:

Attachment Quarantine performs forensic analysis on attachments in a secure, cloud-based sandbox environment. It can also instantly deliver a disarmed version of files by removing macros or converting files to PDF.

Link Protection rewrites links to safe versions and performs time-of-click analysis on the destination address. Based on testing, users are either automatically redirected to a safe site, provided a warning for suspicious sites, or blocked from potentially malicious sites.

Message Retraction (for Microsoft 365) enhances incident response with the ability to retract malicious emails already delivered to users' inboxes. This minimizes risk by taking malicious email out of users' hands and quickens remediation. The system also keeps a detailed audit trail.

24/7/365 Live Threat Analyst Team constantly identifies new threats, updating the system and providing warnings.

OpenText Cybersecurity is an Essential Part of a Powerhouse Portfolio

Ultimately, customers need to effectively reduce risk, preserve trust and minimize disruption. From prevention, detection and response to recovery, investigation and compliance, and robust end user training, OpenText Cybersecurity helps customers build cyber resilience via a holistic security portfolio of smarter and simple solutions delivered through our unified end-to-end platform.

Want to learn more about how OpenText Cybersecurity can help make email surprisingly secure and simple?

Request a demo here

About OpenText

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio.

Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience, and simplified security to help manage business risk.

Visit OpenText.com

opentext™ | Cybersecurity