

## Zero Trust CDR for Mail

# Microsoft 365

Stop Malware From Reaching Your Inboxes

## Key Benefits

- › Integrates in minutes
- › Stop malware (inbound & outbound)
- › Real-time protection against zero-day attacks
- › Fully SaaS – no on-premises infrastructure to manage
- › Delivers the highest guaranteed threat-free data – pixel perfect and fully revisable
- › Defend against the most sophisticated attacks
- › Works with existing boundary defenses and technologies
- › No false positives
- › Prevent steganography
- › Enhanced user experience
- › Reduce M365 costs
- › Cloud-native technology, with 99.99% uptime on average

Nine out of 10 data security breaches start with an email, resulting in organizational disruption, financial damage, and data loss. Get comprehensive protection for your most critical business investment – Microsoft Office 365.

## Transform your Email Security

Forcepoint Zero Trust CDR technology assumes all data is unsafe or hostile; it doesn't try to distinguish good from bad.

When using Microsoft Office 365 Outlook, Zero Trust Content Disarm and Reconstruction (CDR): M365 works on email messages and attachments when mail is being processed by Microsoft 365. The original data carrying the information is discarded along with any threat. Completely brand new messages and attachments are then created and delivered to the user.

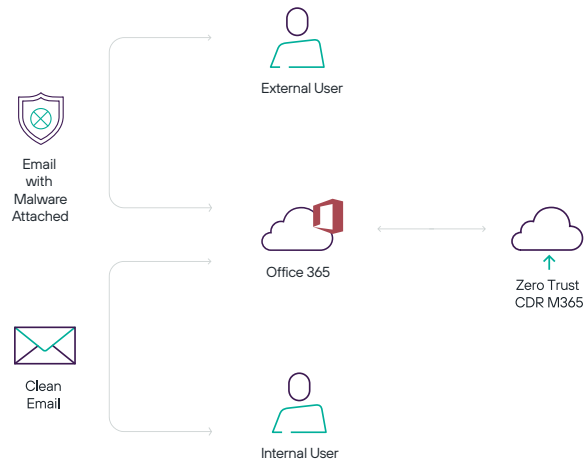
Nothing travels but safe content. Attackers cannot get in and the business gets what it needs. This process is called content disarm and reconstruction (CDR) transformation.

## Defeat the Unknown Threat

Existing perimeter email defenses and gateways (combining detection based signature based anti-virus, threat intelligence feeds, sandboxing, PDF Flattening and SPAM filtering) including Exchange Online Protection (EOP) provide a first line of defense, detecting known threats by looking for the signatures of previously encountered exploits or unsafe behaviours. These provide an important business function, with threats such as phishing attacks.

But time and again, businesses are compromised by advanced threats that penetrate the organization before detection-based defenses can catch up – or by completely unknown threats that succeed without ever being properly identified.

Zero Trust CDR for Mail is the best way to defeat not only known but also zero-day, advanced and unknown threats in emails as they are processed by Microsoft 365, because it doesn't rely on detection or sandbox detonation. Instead, it uses Forcepoint's unique process of transformation to ensure total protection.



## Integrate with Microsoft 365 Seamlessly

Zero Trust CDR for Mail is a full Software-as-a-Service (SaaS) offering that integrates directly with Microsoft 365 Mail, enhances defenses without the need to install and maintain any infrastructure.

Administrators of the Microsoft 365 Mail account can configure external and internal emails to be sent to the Zero Trust CDR for Mail Service without having to modify any of their existing mail routing and defenses.

As well as protecting against inbound mail, Zero Trust CDR for Mail is also applied to outbound and internal emails, stopping the spread of potential malware within your organization and to your customers.

Zero Trust CDR for Mail for Microsoft 365 is a true zero trust implementation of CDR. It assumes that all content is bad, ensuring that all malware, is stopped, enabling the safe use of email.

## Stop Malware Infiltration in Content

Office documents, Adobe Portable Document Files (PDFs), and images are now the most common carriers of malware.

The complexity of these file formats and the applications that handle them make them a natural target for attackers. Whatever the malware—from ransomware and banking trojans to remote access kits and keyloggers—cyber criminals know that the best place to conceal their latest advanced, or zero-day threat is inside an everyday business document. Techniques such as fileless malware and file polymorphism make it even more difficult to deal with threats using conventional detection-based cyber security.

Zero Trust CDR for Mail ensures that organizations can use email with complete peace of mind due to the unique way messages are transformed. Every document and image is subject to transformation and arrives threat-free.

## Supported File Types

- Microsoft Word
- Microsoft Excel
- Microsoft PowerPoint
- Adobe PDF
- Visio
- GIF image format
- PNG image format
- JPEG image format
- BMP image format
- TIFF image format
- WebP
- JSON
- XML
- CSV
- ZIP
- TXT

[Request Your Customized Demo](#)