Forcepoint

Solution Brief

Stop Malware with Zero Trust CDR for Mail: Microsoft 365

A complete SaaS offering that integrates seamlessly, enhances defenses and protects the inbox, all within minutes.

Challenge

› To protect the most common and relied upon way to share documents from delivery malware into an organisation, email.

Solution

› The majority of email protection services still rely on detection-based defenses that are simply outmatched by the ever-evolving threat landscape. Forcepoint Zero Trust CDR for Mail: M365 service pivots from detection, offering a complete SaaS solution that integrates directly with Microsoft 365 Mail to stop malware without needing to install and maintain any infrastructure.

Outcome

› Email protection that you can trust. Zero Trust CDR for Mail: M365 enables the safe use of email, ensuring that all, inbound, outbound and internal threats are stopped.

The Email Problem

Despite the large increase in usage of collaboration software such as Microsoft Teams and Zoom in the past few years, users still primarily rely on email for their day-to-day business communications.

Because email is the most used and relied upon way to share documents, it remains the preferred vector for delivering malware into an organization.

Protecting Microsoft 365 Emails, Users and Data

Zero Trust Content Disarm and Reconstruction (CDR) steers away from traditional detection defences, using a fundamentally different, trusted and proven, prevention technology. It transforms digital content in real-time and guarantees the only thing sent to the user is safe, malware-free data.

When using Microsoft Office 365, Zero Trust CDR: M365 cleans 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 gets delivered but safe content. **Attackers cannot get in and the business gets only what it needs.**

How Zero Trust CDR for Mail: M365 Works

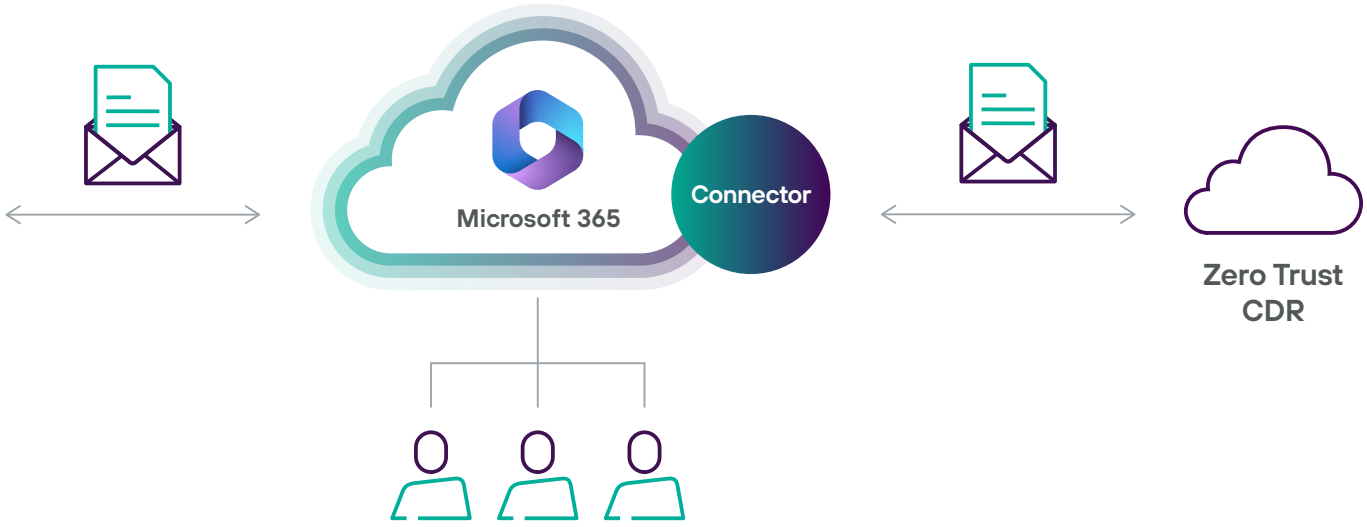
All email (internal or external) arriving via Microsoft 365 Mail destined for a subscribed mailbox is diverted to the Forcepoint Zero Trust CDR service using Microsoft standard interfaces. The M365 service will clean the complete email (headers, body and attachments) and send it back to Microsoft 365 for delivery to the mailbox, nearly instantaneously.

It provides uncompromising security, ensuring no unsafe attachments and no risky components of an attachment are received or delivered by:

→ Delivering clean, threat-free versions of all common business file types and more.

→ Removing potentially malicious elements in supported attachment types (e.g. removing macros from Office files)

→ Replacing non-allowed or supported attachment types (including password-protected attachments) with a notification indicating what has been removed.



Stop Malware Infiltration in Content

Office documents, Adobe PDFs, and images are 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 identify threats using conventional detection-based cyber security. Zero Trust CDR for Mail: M365 ensures that organizations can use email with complete peace of mind due to the unique transformation method.

Integrate with Microsoft 365 Seamlessly

Zero Trust CDR for Mail: M365 is a full Software-as-a-Service (SaaS) offering that integrates directly with Microsoft 365 Mail. It stops malware and 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 via 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. The Zero Trust CDR for Microsoft 365 Service will keep users safe and in nearly every case, users will not see any noticeable change in their Inbox messages.

Benefits

- → Defeats Advanced Malware: Zero Trust CDR for Mail: M365 stops advanced malware, zero-days and unknown attacks that can lead to ransomware and other devastating impacts.
- → Handling Hyperlinks: Zero Trust CDR for Mail: M365 can be configured to make potentially dangerous hyperlinks safe to interact with.
- → Internal Protection: Zero Trust CDR for Mail: M365 not only stops inbound malware but stops the internal spread of malware both externally and internally, blocking ransomware spread by email and helping clean up existing infections.
- → Simple Setup: Configuration of the Zero Trust CDR appliances is simple and takes only a matter | of minutes.
- → Non-Invasive: Zero Trust CDR for Mail: M365 works with existing boundary defenses and technologies.
- → Reliable: Zero Trust CDR for Mail: M365 is a cloud-native technology with 99.99% uptime on average.
- → Stops Data Theft: Zero Trust CDR for Mail: M365 prevents steganography.
- → True Zero Trust: Zero Trust CDR for Mail: M365 ensures that organizations can use email with complete peace of mind due to prevention-based technology. Every document and image arrives threat-free, pixel-perfect and in near real-time.

FAQ's

Privacy and Zero Trust CDR
The Forcepoint Zero Trust CDR service will have access to the messages being processed by Microsoft 365 for those subscribed mailboxes, aligned with how Microsoft 365 works. For peace of mind, the service run by Forcepoint is hosted in the Amazon Web Services (AWS) infrastructure providing the highest levels of security required for handling organizational data. In addition, if there are legal requirements for emails to remain in a specific country or region, the Forcepoint service can be run in that location, dependent on AWS regional services.

While the messages are being processed in the Forcepoint Service, all information is anonymized for logging. The message content, subject, sender and recipient information are not visible to any administrators of the Forcepoint service. The message identifier is logged and that can be used to track messages between Microsoft 365 and the Forcepoint Service in the event of any queries.

What if my organization already has security for 365?
It should be noted that existing security mechanisms including those in Secure Email Gateways and in the native Microsoft 365 Mail Service are based on detection methods (either anti-virus or sandboxing) and may not always prevent advanced malware from reaching user mailboxes.

The Forcepoint Zero Trust CDR for Mail: M365 service is designed to enhance existing security mechanisms. It can be used on top of existing Email Gateways in front of Microsoft 365 or if you already use some of the built in Microsoft security features such as Advanced Threat Protection available in the higher Microsoft 365 subscription tiers.

forcepoint.com/contact