Forcepoint

Solution Brief

Zero Trust CDR for Mail (Microsoft M365) Early Access Program Brief

Forcepoint is offering an Early Access program that provides unparalleled malware protection for users of Microsoft 365 Mail.

Challenge

- Email is one of the largest attack surfaces for most organizations
- Cybercriminals may embed dangerous malware into data

Solution

- Remove malicious or anomalous code from data before it hits an end users inbox
- Deliver clean usable files to your end users.

Outcome

- Keep privileged users productive
- Remove threats from data in your inbox and outbound email.

Forcepoint Zero Trust CDR for Mail (Microsoft 365 Mail) will enable subscribed users to access their emails safely, with the confidence that any malware sent to them via email has been removed prior to opening during this Early Access Program.

Zero Trust CDR uses a fundamentally different approach to all other forms of malware prevention by not attempting to detect the malware. Taking a zero-trust approach, Zero Trust CDR does not deliver the original data, but instead extracts the business information from the email and attachments and creates brand new data with the business information.

Users' inboxes will not be impacted, as each email appears as it would have previously - except that they can now be assured that the attachments are safe to open. Administrators will see a significant reduction in the number of false positives that detection-based tools have previously been reporting.

The Early Access Program opens on December 1, 2022, to organizations with a Microsoft 365 Mail instance located in the United States, United Kingdom, Europe and South Africa. It allows organizations to trial the capability for 20 end users at no cost for up to 30 days.

ZT CDR for Mail in action

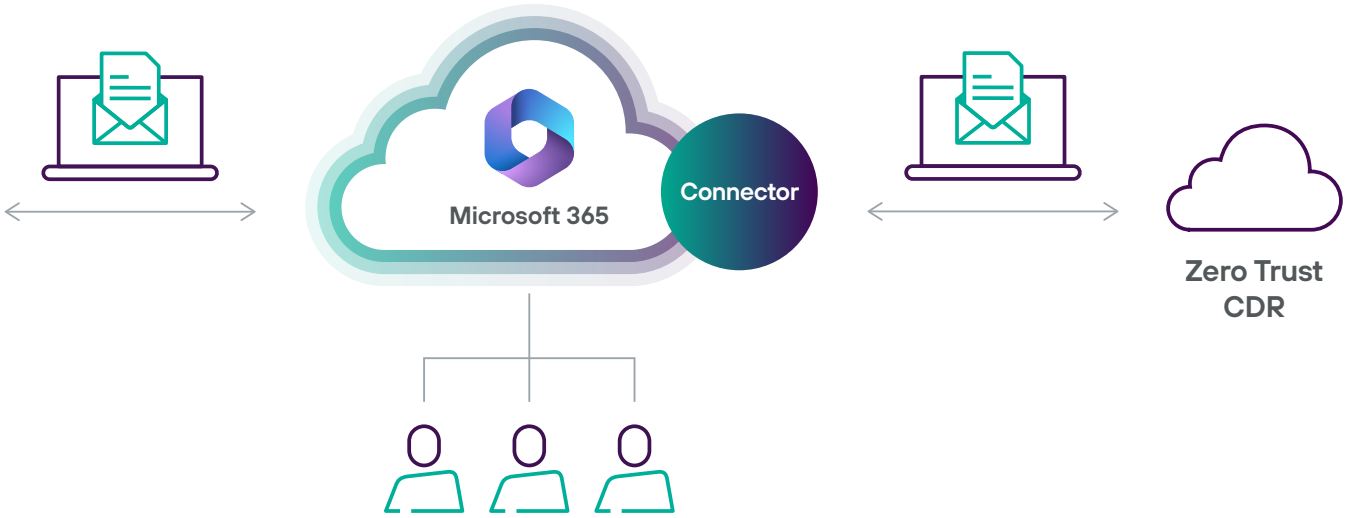

Figure 1: Email arrives, diverted via a Microsoft API to Forcepoint ZT CDR Service. ZT CDR cleans the email, then delivers the email to the M365 365 Mailbox.

How ZT CDR for mail works

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

The Zero Trust CDR service provides uncompromising security, ensuring no unsafe attachments and no risky components of an attachment are delivered to the user by:

- → Delivering clean, threat-free versions of the attachment types that are supported (e.g. PDF, Office files, images)
- → Removing potentially malicious elements in supported attachment types (e.g. removing macros from Office files)
- → Replacing all other attachment types (including password-protected attachments) with a notification indicating which attachments were removed.

Where an attachment is changed in a significant way, e.g. a macro is removed from a Word document, then a banner is added at the top of the email to indicate to the user what has been changed. Zero Trust CDR will always keep the user safe and in nearly every case, users will not see any noticeable change in their Inbox messages.

Joining the ZT CDR for mail early-access program

1. Complete the Sign-Up form on **this webpage**. Forcepoint Early Access Team will respond to your inquiry in less than 3 business days.
2. Meet with the Early Access team to scope your Zero Trust CDR needs with a short questionnaire.
3. Upon completion of the Forcepoint Pre-Release Solutions Evaluation paperwork, plan start date and schedule Zero Trust CDR Set up (takes approximately 1 hour or less to install).
4. Work with Early Access Team to check in during your 30-day trial period.

Program Requirements

- → Organizations will be able to subscribe 20 users for 30 days.
- → During that time, your organization would need to validate that the service is making emails safe for the subscribed users and provide feedback from the users and the administrators.
- → We will schedule an EA program review session for the end of the trial period.

Zero Trust CDR provides unparalleled levels of protection for Microsoft 365 mailboxes and will enhance your security posture against one of the most common attack vectors. The service uses the core Forcepoint Zero Trust CDR technology that is already in use protecting government and commercial organizations from the threat of malware today.

FAQs

Privacy and ZT 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.

Whilst 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?
The Forcepoint Zero Trust CDR service is designed to enhance existing security mechanisms. The Zero Trust CDR service can still be used if you already use a Secure Email Gateway 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.

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.

What if i want to stop the early access program?
If an organization wishes to stop using the service for a specific mailbox or for all users, the administrators can simply disable the rule(s) added during on-boarding. The rule(s) can be left in place so that the service can be re-enabled at any time.

Support during the early access program
For queries on specific emails, organizations will have a technical point of contact within the Early Access Program Team to ask questions raise issues.

For message tracking, Forcepoint will only have access to the unique message identifier and so for any requests related to tracking specific emails, it will be important that the organization can obtain the message identifier via Microsoft 365 message tracing.

The Forcepoint EA service will have the ability to save a copy of the original of every message to an S3 datastore nominated and owned by the organization participating in the EA program. Forcepoint will not have access to this datastore other than to write a copy of each inbound message into the store. The organization can then use this store to refer to any data pre-Zero Trust CDR, or to retrieve items they wish to submit to Forcepoint for analysis.

forcepoint.com/contact