EVERFOX

CDR for Mail: Microsoft 365

Datasheet

Challenge:

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.

Solution:

A threat-prevention SaaS solution that integrates directly with Microsoft 365 Mail that stops malware without needing to install and maintain any infrastructure.

Benefits:

- Seamless & quick integration
- Inbound, outbound & internal protection
- Fully SaaS, no on-premises infrastructure
- No false positives
- High level of protection
- Defense against the most sophisticated attacks

90% of 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

Everfox Content Disarm & Reconstruction (CDR) technology assumes all data is unsafe or hostile; it doesn't try to distinguish good from bad.

When using Microsoft Outlook, CDR for Mail 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 the reconstructed content.** Attackers cannot get in and the business gets what it needs.

Defeat the unknown threat

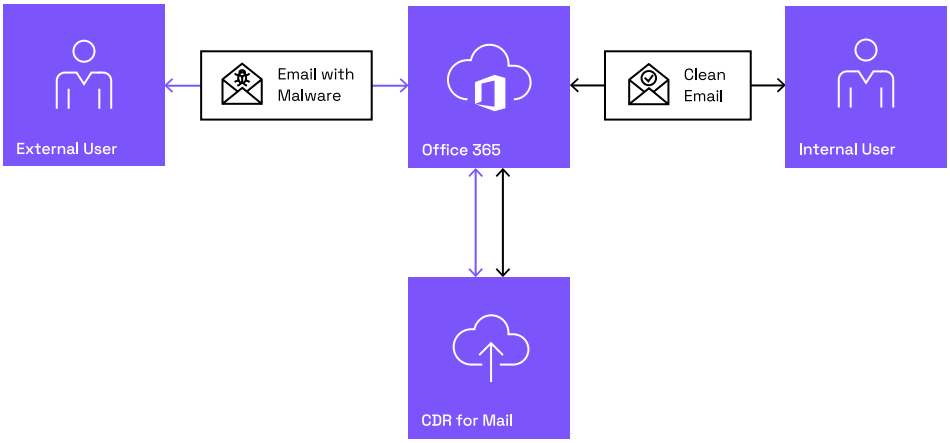
Existing perimeter email defenses and gateways (combining detection-based anti-virus, threat intelligence feeds, sandboxing, Flattening & SPAM filtering) including Exchange Online Protection (EOP) provide a first line of defense, detecting known threats by looking for the signatures of previously encountered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

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

Integration

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 traditional detection solutions or sandbox detonation.

Instead, it uses Everfox's unique process of CDR transformation to ensure complete protection.



Seamless integration with Microsoft 365

CDR for Mail is a full Software-as-a-Service (SaaS) offering that integrates directly with Microsoft 365 Mail. Enhancing your defenses without the need to install & maintain any infrastructure.

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

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

Everfox CDR for Mail for Microsoft 365 is a true zero trust implementation of CDR. The solution assumes that all content is bad, stopping malware, and enabling safer 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 file-less malware and file polymorphism **make it even more difficult to deal with threats using conventional detection-based cybersecurity**.

Using CDR for Mail gives organizations peace of mind when using email. Due to the way emails are transformed using our unique CDR technology. Using CDR helps ensure that safer and more secure documents are all that is transmitted to the end user.

Supported file types

- Doc / DocX
- XLS
- PPTX
- Adobe PDF
- Viseo
- GIF image format
- PNG image format
- JPEG image format
- BMP image format
- TIFF image format
- WebP
- JSON
- XML
- CSV
- ZIP
- TXT

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 and may not prevent advanced malware from reaching your mailboxes.

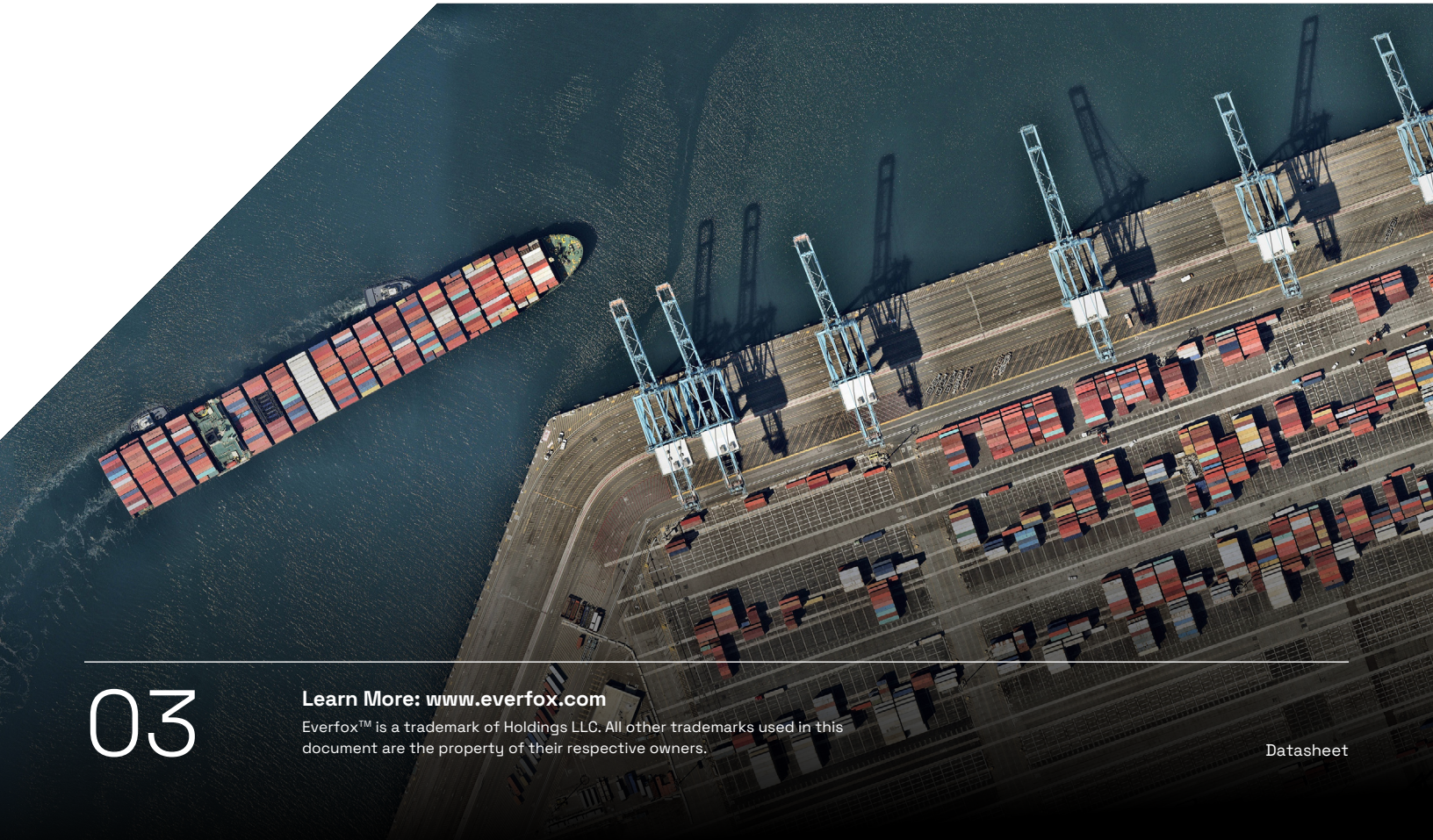
Everfox CDR for Mail: M365 service is designed to seamlessly enhance existing security mechanisms. Offering unmatched protection for organization that require the highest levels of protection.

Privacy and CDR for Mail

Everfox CDR SaaS will have access to the emails being processed by Microsoft 365, for subscribed mailboxes only, aligned with how Microsoft 365 works.

For peace of mind, the service run by Everfox 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 Everfox service can be run in that location, dependent on AWS regional services.

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



Learn More: www.everfox.com