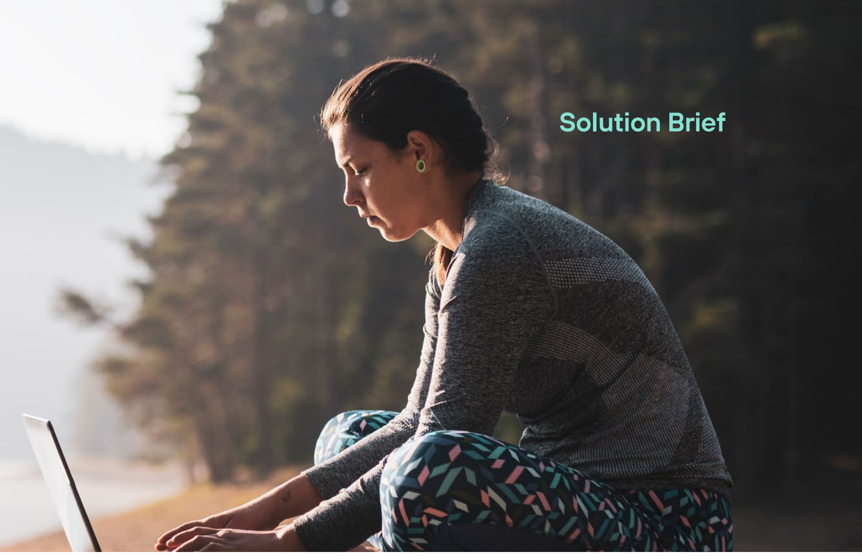
Forcepoint

Solution Brief

Forcepoint Zero Trust Content Disarm and Reconstruction for Mail

Threat-free email, pure and simple



Challenges

- Combatting phishing attacks - CISCO reported in 2021 that 90% of data breaches occured due to phishing.
- Zero-day exploits

Solution

- Boost your email security with Zero Trust Content Disarm and Reconstruction (CDR): The only way to defeat known, unknown and zero-day threats in content as it crosses the email boundary.

Benefits

- Delivers safe, threat-free email messages and attachments across the network boundary without the need to detect the threat or isolate users from the business content they need. Zero-day exploits, ransomware, steganography exploits, fileless malware, and the threats inherent in polymorphic files are all removed.
- Works with your existing Email Security Gateways, anti-spam filters, and perimeter anti-virus technology, dropping seamlessly into the boundary cyber defense and delivering a low risk, low cost route to total protection from content-borne threats.

Typically, corporate users have an email capability allowing them to exchange email messages from their workplace with both users inside their organization and users on the Internet. Emails can contain rich content with users often sending attachments while also making use of HTML or Rich Text to create messages to include formatting, hyperlinks, colors, and images, as well as attachments. This creates a risk to the organization that emails will bring in malware hidden inside the rich content.

Traditional Email Security Gateways rely on detection of the potential threat and are proving inadequate for the current level of attack sophistication.

Defeat the Unknown Threat

Existing perimeter email defenses and gateways (combining anti-virus, threat intelligence, sandboxing, and SPAM filtering) provide a first line of defense, detecting known threats by looking for the signatures of previously encountered exploits or unsafe behaviours. But time and again businesses are compromised by zero-day 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 only way to defeat not only known but also zero-day and unknown threats in content as they cross the email boundary, because it doesn’t rely on detection or sandbox detonation. Instead, it uses a unique process of transformation to ensure total protection.

Transform your Email Security

Zero Trust CDR for Mail works by extracting the business information from the email messages and attachments at the boundary. The data carrying the information is discarded along with any threat. Brand new messages and attachments are then created and delivered to the user. Nothing travels end-to-end but safe content. Attackers cannot get in and the business gets what it needs.

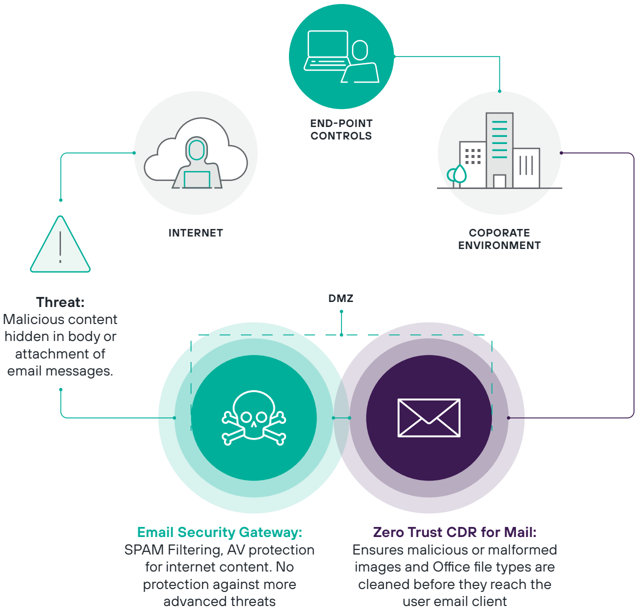
This process is called transformation. It cannot be beaten; the security team is satisfied because the threat is removed while business users are satisfied because they get the information they need.

Zero Trust CDR is the only way to ensure that threats are removed from content. Dispensing with the failed paradigms of threat detection and isolation, Forcepoint’s unique Zero Trust CDR technology assumes all data is unsafe or hostile; it doesn’t try to distinguish good from bad.

Extend your Existing Defense

Zero Trust CDR for Mail extends an existing Email Security Gateway and Email Server to remove the threats from email bodies and the commonly used file types that are attached to emails (images, Microsoft Office documents, and PDFs). Zero Trust CDR for Mail can be deployed on-premise and in cloud.

Zero Trust CDR for Mail complements existing email security controls by placing an extra component in the flow of inbound and outbound email traffic.


END-POINT CONTROLS
INTERNET
COPORATE ENVIRONMENT
Threat:
Malicious content hidden in body or attachment of email messages.
DMZ
Email Security Gateway:
SPAM Filtering, AV protection for internet content. No protection against more advanced threats
Zero Trust CDR for Mail:
Ensures malicious or malformed images and Office file types are cleaned before they reach the user email client

Integrate Seamlessly

Zero Trust CDR for Mail runs on a server on the corporate side of an existing Email Security Gateway. Inbound emails are routed from the Email Security Gateway to Zero Trust CDR for Mail where the messages are transformed to ensure they are threat-free before onward delivery to the corporate mail server.

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 manipulate 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 zero-day threat is inside an everyday business document. Techniques such as the use of fileless malware and file polymorphism make it even harder to deal with the threat using conventional detection-based cyber security and email is the perfect vector for infiltration.

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

Application Layer Proxy

Zero Trust CDR for Mail operates as a dual-homed application layer proxy for SMTP. It forms the secure boundary between the corporate network and the external systems, acting as a smart host for both the Mail Security Gateway for inbound messages and for the mail server for outbound messages. All content, including MIME and the message attachments, is transformed to ensure it is safe for delivery in the corporate network. Zero Trust CDR also provides transformation of user portal requests and responses for accessing held password-protected documents and transformation of password-protected attachments retrieved.

Zero Trust CDR for Mail transforms the content that it receives into an internal representation of the information. The original data is discarded and new “safe” data is created from the information. In this way, attacks carried in the content are removed, even if they are unknown, while allowing the information to reach the destination. This process is carried out for all content being transformed.

Password Protected Attachments

In some organizations, users password protect documents that are subsequently sent out over the Internet as attachments. These documents represent a potential threat as they cannot be transformed and rendered threat-free.

To balance the business need with the security risk, Zero Trust CDR for Mail can be configured to either non-deliver messages containing password protected attachments or to redact password protected attachments from messages. Alternatively, channels between specific users or groups of users can be configured to bypass the transformation process, where the ability to send password protected attachments is considered essential.

Signed and Encrypted Messages

Where there is a requirement to support messages that are signed and/or encrypted using S/MIME or PGP, this can be supported at a gateway level. The messages are first rendered threat-free using Zero Trust CDR and then passed to a separate Forcepoint guard server, for signature or encryption by the guard itself.

Macros and Executable Content

In some organizations, users exchange macro enabled Office documents using email. These documents represent a potential threat as macros are executable content that cannot be rendered safe by transformation.

To balance the business need with the security risk, Zero Trust CDR for Mail can be configured to either non-deliver messages containing Office macros or to redact attachments containing Office macros from messages. Alternatively, channels between specific users or groups of users can be configured to bypass the transformation process, where the ability to send Macro enabled Office documents is considered essential.

For more information check out
Forcepoint Zero Trust CDR

forcepoint.com/contact