Deep Secure Content Threat Removal for Mail

Threat-free email, pure and simple

Typically, corporate users have an email capability allowing them to exchange email messages from their workplace with both users inside their organisation and users on the Internet. Emails can contain rich content with users often sending attachments whilst also making use of HTML or Rich Text to create messages to include formatting, hyperlinks, colours and images as well as attachments. This creates a risk to the organisation 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.

Key Advantages

Content Threat Removal for Mail

- Always 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 defence and delivering a low risk, low cost route to total protection from content-borne threats.

Defeat the Unknown Threat

Existing perimeter email defences, gateways (combining anti-virus, threat intelligence, sandboxing and SPAM filtering) provide a first line of defence, 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 organisation before detection-based defences can catch-up or by completely unknown threats that succeed without ever being properly identified.

Content Threat Removal for Email is the only way to defeat not only known but also zero day and unknown threats in content as it crosses 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

Content Threat Removal 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.

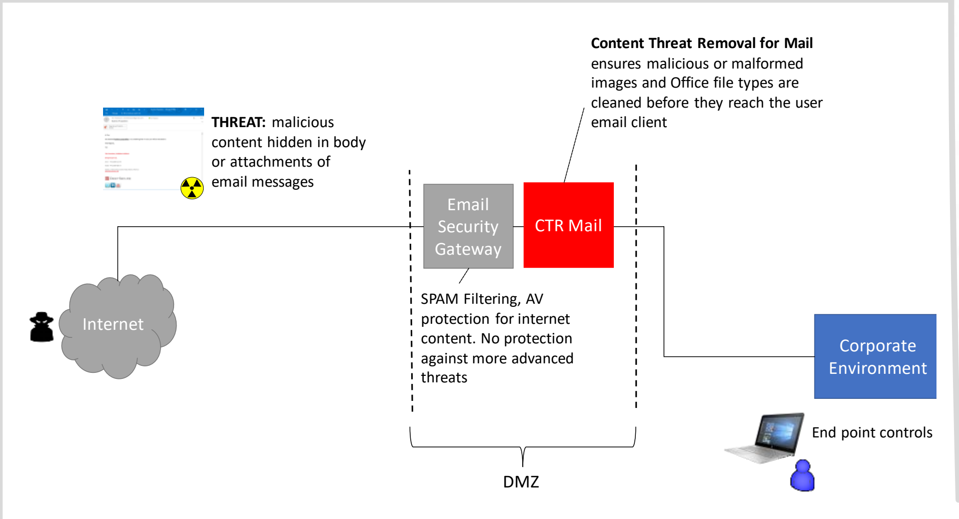
This process is called transformation. It cannot be beaten; the security team is satisfied because the threat is removed while business users are satisfied because they get the information they need.

Content Threat Removal is the only way to ensure that threats are removed from content. Dispensing with the failed paradigms of threat detection and isolation, Deep Secure's unique Content Threat Removal technology assumes all data is unsafe or hostile; it doesn't try to distinguish good from bad.

Extend your Existing Defence

Content Threat Removal 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). The Content Threat Removal for Mail can be used for both on-premise and cloud based email systems.

Content Threat Removal for Mail Gateway solution complements existing email security controls by placing an extra component in the flow of inbound and outbound email traffic.



Content Threat Removal for Mail ensures malicious or malformed images and Office file types are cleaned before they reach the user email client
THREAT: malicious content hidden in body or attachments of email messages
Email Security Gateway
CTR Mail
Internet
SPAM Filtering, AV protection for internet content. No protection against more advanced threats
Corporate Environment
End point controls
DMZ

Overall Mail Solution Architecture

Deep Secure Content Threat Removal for Mail

Integrate seamlessly

Content Threat Removal for Mail (comprising the information eXchange or iX Appliance) runs on a server on the corporate side of an existing Email Security Gateway. Inbound emails are routed from the Email Security Gateway to the CTR for Mail platform where the messages are completely transformed to ensure that the message bodies and attachments are clean before delivering them on to the corporate mail server to be accessed from within the corporate environment.

Users who also require access to the corporate mail system from their mobile devices present an additional risk to the corporate network. A complementary solution, Deep Secure Content Threat Removal for Mobile Mail, enables mobile access without risk to the corporate mail system. This is described in the Deep Secure Content Threat Removal for Mobile Mail Solution Brief.

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.

Content Threat Removal for Mail ensures that business users can use email with complete peace of mind because of the unique way they are transformed. Every document and image is subject to transformation and every one is threat free.

Application Layer Proxy

Content Threat Removal 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 are transformed to ensure it is safe for delivery in the corporate network. It also provides transformation of user portal requests and responses for accessing held password protected documents and transformation of password protected attachments retrieved from the quarantine area.

Content Threat Removal 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, whilst allowing the information to reach the destination. This process is carried out for all content being transferred.

Password Protected Attachments

Increasingly users are password protecting documents that are sent out over the Internet as email attachments. These encrypted documents cannot immediately be transformed by the iX appliance as it requires access to the content to be able to extract the business information. For PDF attachments, a list of possible passwords can be configured to try to decrypt the content to allow transformation. For all other types, the organisation can decide to remove the attachment or allow it in untransformed. Future versions of Content Threat Removal for Mail will enable the recipient to supply a password to get access to transformed versions of the document.

Signed and Encrypted Messages

Messages that are encrypted using S/MIME or PGP cannot be transformed without access to the decryption key. Future versions of Content Threat Removal for Mail will support validation of signatures and decryption of the content prior to transformation. Transformed messages will then be delivered either unsigned or signed by the iX appliance and either unencrypted or re-encrypted to the user.

Macros and Executable Content

By default, Content Threat Removal for Mail will not carry through any executable content in messages or message attachments. This includes embedded binaries, scripts and macros.

Organisations often need to use documents that contain macros and share these externally. Not bringing in these macros can cause a loss of functionality. In order to support organisational macros, the administrator can configure specific Content Threat Removal for Mail channels to allow macros in while transforming the rest of the document.

Using this feature in conjunction with a Secure Mail Gateway can enable certain users or domains to receive documents containing macros.

Future versions of Content Threat Removal for Mail will provide a macro whitelisting capability.

Learn More

For more information on how the Content Threat Removal for Mail solution uses Deep Secure’s information eXchange (iX) product, visit **www.deep-secure.com/products**.