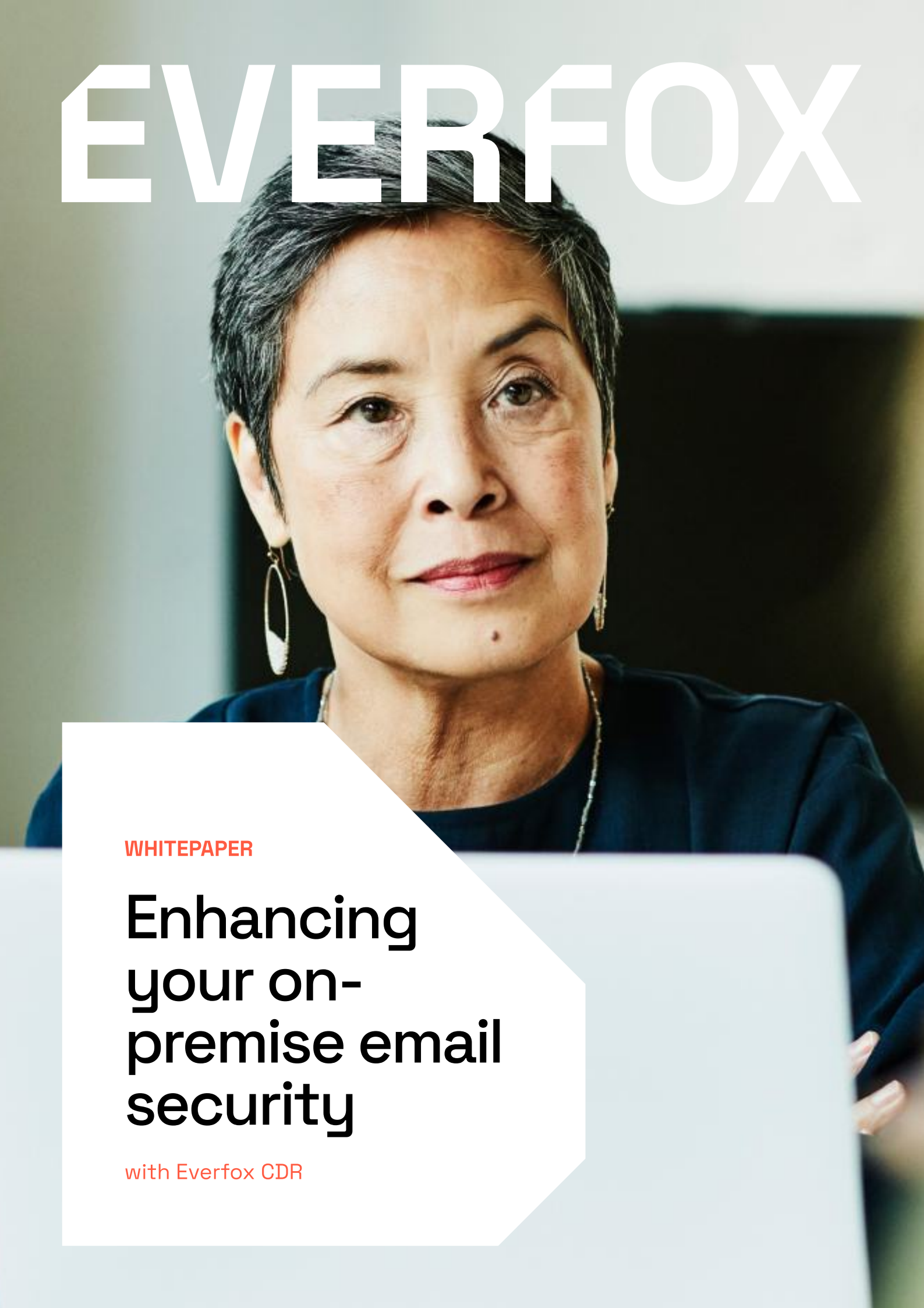
EVERFOX



WHITEPAPER

Enhancing your on-premise email security

with Everfox CDR

Organizations thrive when a cohesive security solution delivers the right tools for the job

Introduction

When it comes to protecting email services, the combination of Everfox Content Disarm & Reconstruction (CDR) and your Secure Email Gateway will provide unparalleled security.

Unmatched in capability and speed, delivering pixel perfect, fully revisable files that are malware-free, in near real-time.

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.

Email is a simple way to share documents between organizations, using whichever platform or service is preferred. This means that email is still the main vector for bringing malware into an organization.

Emails can contain rich content with users often sending attachments, while also making use of HTML or Rich Text to create messages that include formatting, hyperlinks, colors and images as well as attachments. These combine to create risk to the organization that emails will bring in malware hidden inside the rich content.

Traditionally these risks are mitigated by Secure Email Gateways. A Secure Email Gateway provides multiple services to protect an organization, services such as spam blocking, detection and prevention of malware, and preventing data leaks.

With the current level of malware attack sophistication evolving year on year. Secure Email Gateways although effective against known malware are not enough on their own to defend against advanced malware threats.

Introduction

Todays advanced malware uses multiple methods to avoid detection.

Common techniques include:

Malware that can check the environment it is running in
If it detects a sandbox environment, it simply lies dormant only delivering its payload when it gets to the destination.

Polymorphic viruses which can create modified versions of themselves to avoid detection by signature-based defenses.
Each time they change, there is a period of time before the signatures in a defense are updated.

Polymorphic files which are valid as more than one file type.
For example, a file may be a valid image as well as a valid HTML script. Attackers use these to get past defenses knowing that a defense will pass a valid image file and not detect that it is a dangerous script as well.

Making use of rich features of complex file formats like Office to pull in templates from untrusted locations.
The document that gets past the defense may be safe, but the template it imports contains dangerous code which is executed once imported.

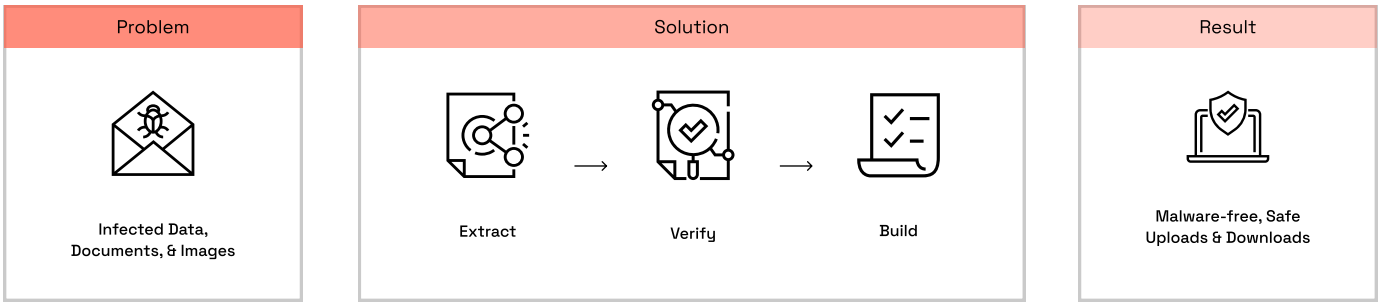
Using steganography to hide code or command and control data inside images.
While some types of steganography may be detectable, it is possible to hide data in images that cannot be found but can be extracted once delivered to the destination.

The Solution

Everfox Content Disarm & Reconstruction (CDR) alleviates these problems as it assumes nothing can be trusted.

Rather than attempting to detect malware or even attempt to remove constructs from files that are potentially malicious, our CDR simply extracts the valid business information from messages and their attachments. Once extracted, it verifies the information is well-structured, and then builds brand new, fully functional messages and attachments to carry the information to its destination.

The key to the success and speed of Everfox CDR lies in the fact it does not rely on any detection whatsoever. It mitigates the threat of even the most advanced zero-day attacks, exploits and data loss.



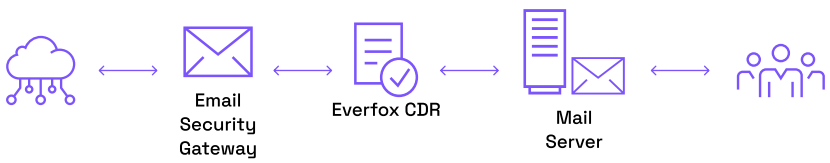
Enhancing Existing Defences

Everfox CDR can be used to extend the protection offered by your existing Secure Email Gateways by enhancing their capability to stop complex and unknown threats such as zero-days.

On-Premises or Hybrid

For organizations that host their own mailboxes, Everfox CDR can easily be placed between the Secure Email Gateway and the mailboxes.

The Secure Email Gateway is reconfigured to send some or all the emails to the CDR appliance, which will ensure all messages passing through are delivered malware free

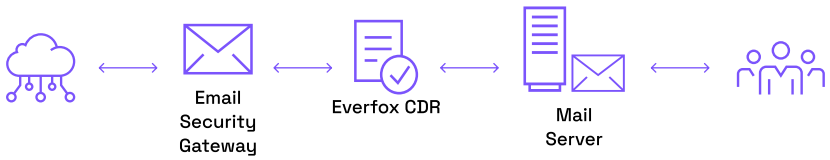


Everfox CDR

- → Stops advanced malware
- → Destroys steganography

Critical or Highly Sensitive Data

Additionally, in highly sensitive or critical environments, the Everfox CDR appliance can be split across multiple servers and includes a hardware logic based verification device which provides a full hardware protocol break, has logic-based verification of the data (i.e. no attackable software), and cannot be bypassed. This can enable some of the most sensitive and critical environments to safely receive email from the Internet.



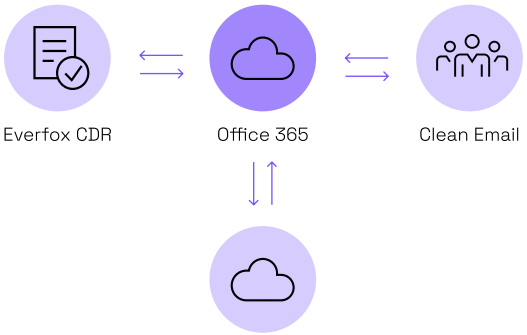
Everfox CDR

- → Stops advanced malware
- → Destroys steganography
- → Full hardware protocol break
- → Full logic based verification

Microsoft 365 Mailboxes

For users of Microsoft 365 Mail, Everfox CDR can enhance defenses without the need to install and maintain any infrastructure by using a Everfox CDR as a Service.

Administrators of the Microsoft 365 Mail account can arrange for some or all internal or external emails for an organization to be sent to the service without having to modify the existing external mail routing and defenses.



Everfox CDR

- → Stops advanced malware
- → Destroys steganography
- → SaaS = No Infrastructure

Solution Features

Simple Setup

Integrating Everfox CDR with your existing Secure Email Gateway is simple. Installation and configuration of the CDR appliances takes minutes and does not require constant updates to keep it running.

Defeats advanced malware

Everfox CDR stops advanced malware that can lead to ransomware and other devastating attacks. Since Everfox CDR does not rely on detection, features in malware to evade detection such as sandbox avoidance and polymorphic viruses have no effect. Polymorphic files are made safe as are any features that could import code into a file from untrusted external sources. Steganography is also disrupted by CDR to prevent images from bringing in malware (or leaking out sensitive information).

Handling Hyperlinks

While hyperlinks are important and a useful feature in emails and documents, they can be abused to send victims to unsafe websites or download unsafe content. Everfox CDR removes references to local resources (which could be dangerous). For hyperlinks to external resources in documents, Everfox CDR can be configured to make them safe, allowing administrators to determine which sort of hyperlinks or which external resources to allow.

Supporting different user needs

Everfox CDR is effective against all malware, but to achieve that it must stop any data that cannot be safely transformed from being delivered to the desktop including executables, unsupported file types and features like macros. In most organizations, there are a minority of users that must have access to that sort of potentially dangerous content. Organizations need to be able to take that risk, but not for everyone. With Everfox CDR appliances, multiple profiles can be configured to support different user needs and the Secure Email Gateway can direct to the correct profile based on the sender or recipient.

SIEM Integration

Everfox CDR appliances generate syslog and SNMP Traps which can be sent off-box to central SIEM servers, enabling full logging and traceability of emails entering and leaving the system

Existing defenses unchanged

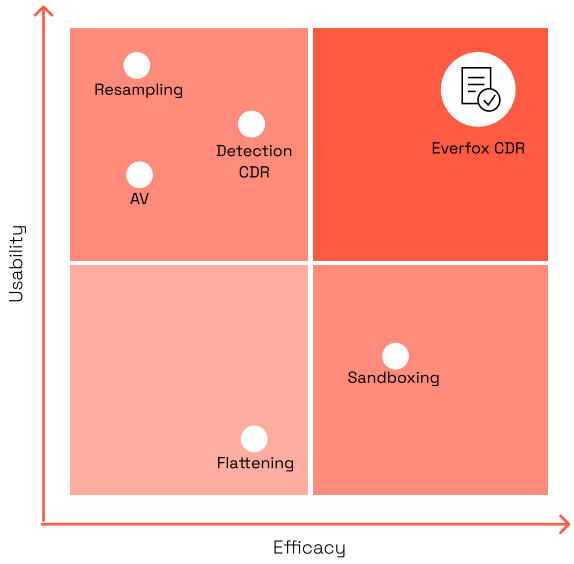
Any existing features and defenses provided by your existing Secure Email Gateway remains unchanged providing full protection against spam and preserving detection-based protection such as AV and sandboxing for any file types that are not suitable for Everfox CDR but which need to be allowed in.

Handling for Password Protected Content

Different policies on the Everfox CDR appliance can be set up to allow unmodified or block-encrypted content in emails. The Secure Email Gateway can then be used to identify this type of content and send to the appropriate policy on the Everfox CDR appliance based on the sender or recipient of the email.

Integration with Microsoft 365 Mail

A Everfox CDR service is available which integrates directly with Microsoft 365 Mail allowing your existing Secure Email Gateways that sit in front of Microsoft 365 to continue to function while adding the Everfox CDR capability to incoming and outgoing emails. An additional feature of this service is the ability to apply Everfox CDR to internal emails too, minimizing the spread of any malware laterally within an organization.



Summary

Existing email solutions provide great value to organizations by preventing data loss, stopping spam and detecting known malware threats. The detection- based malware prevention, however, cannot keep pace as malware has become more widespread and advanced.

Everfox CDR is a true zero trust implementation of CDR which assumes all content is bad, and only delivers content that has been through its three-stage sanitization process: extract-verify-build. This ensures all malware, is stopped, enabling the safe use of email.

For those with on-premises or hybrid deployments, Everfox CDR seamlessly integrates with your existing Email Security Gateway and can be deployed on-premises or as cloud appliances. For those already fully moved to Microsoft 365 Mail, Everfox CDR is delivered as a full Software-as-a-Service (SaaS) offering.

Everfox CDR can also be deployed to protect other key information flows including web browsing, Remote Browser Isolation, File Uploads, File Transfers, Web Services and embedded into applications .

About Everfox

Everfox, formerly Forcepoint Federal, has been a trailblazer in defense-grade cybersecurity for more than two decades. Leading the way in delivering innovative, high-assurance solutions. But we're just getting started.

Learn More

www.everfox.com