Forcepoint

Solution Brief

Forcepoint Zero Trust Content Disarm and Reconstruction for Web Gateways

Web browsing with total peace of mind

Challenges

- 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.
- Web downloads can contain threats that cause applications to malfunction and give attackers control over business systems.
- Web uploads can contain more information than an organisation wishes to divulge, damaging the business by revealing intellectual property.

Solution

- Forcepoint's unique Zero Trust CDR technology assumes all data is unsafe or hostile; it doesn't try to distinguish good from bad, making it the true Zero Trust solution.
- Zero Trust CDR can be integration with your existing web defense in a matter of moments.

Benefits

- Always delivers safe, threat-free content across the web boundary
- Defeat the unknown threat
- Transform your web security
- Enrich the browsing experience
- Seemless integration
- Stop malware
- Combat steganography
- Enjoy unparalleled protection

Organizations depend on the Web to share information, inform key business processes, and conduct transactions. Existing perimeter web defenses (web gateways and firewalls) are failing to cope with the onslaught of known, unknown, and zero-day threats concealed in business documents and images. Unchecked, this attack vector is an existential threat to business. The documents and images users download contain threats that can cause applications to malfunction and give attackers control over business systems. The documents and images they upload can contain more information than the organization wishes to divulge, damaging the business by revealing intellectual property. To date, no one has found a way to stem the flow of threats.

Defeat the Unknown Threat

Existing perimeter web defenses, gateways, and firewalls 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 Content Disarm and Reconstruction (CDR) for Web Gateways is the only way to defeat not only known but also zero-day and unknown threats in content as they cross the web 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 Web Security

Zero Trust CDR for Web Gateways works by extracting the business information from the documents and images in the web browsing stream. The data carrying the information is discarded along with any threat. Brand new documents and images 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 unique Zero Trust CDR technology assumes all data is unsafe or hostile; it doesn't try to distinguish good from bad.

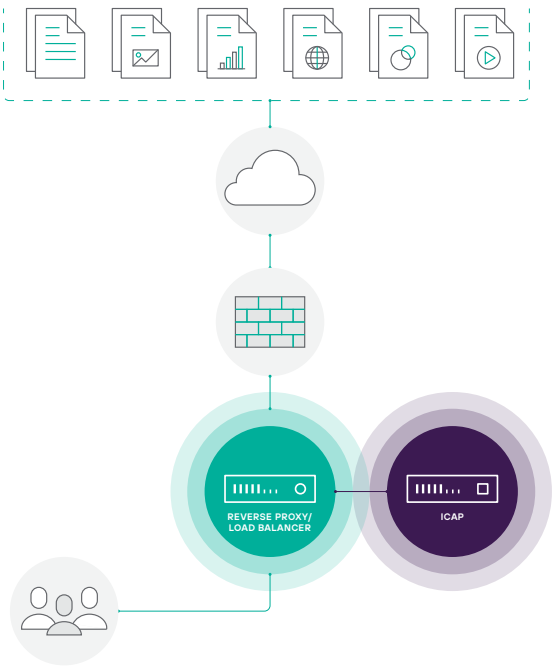
Enrich the Browsing Experience

As security teams battle to deal with cyber attackers who seem able to constantly stay one step ahead, it is the business user who suffers. Time spent dealing with false positive security alerts or waiting for documents to be checked and released inhibits business processes and limits productivity. And when things go wrong, remediation is costly and time-consuming.

Zero Trust CDR for Web Gateways enriches the user's experience of the web and social media because they get timely access to the business information they need to read, share, and transact, with absolutely no risk of compromise from the content they consume.

Ensure Digitally Pure Content

As web and social media usage continues to inform every aspect of business, it has never been more important to ensure that the content it carries is safe, pure, and threat-free. Any business that is able to establish a track record for guaranteeing its users, business partners, and customers access to clean, pure business content will differentiate themselves in what is fast becoming a lawless cyber landscape.



Zero Trust CDR for Web Gateways does exactly that, ensuring businesses can reap the benefits of Web and social media usage with confidence that the business content they handle is threat free.

Integrate Seamlessly with Existing Defenses

Zero Trust CDR for Web Gateways integrates seamlessly with existing perimeter web defenses, web gateways, and application firewalls using the industry standard ICAP protocol. Deployed as a "sidecar", the solution is configured so that the web gateway or firewall passes documents and images to a Forcepoint Gateway eXtension (GX) server over ICAP where they are transformed to remove any concealed threat and then passed back to the gateway for delivery onward to the user.

Integration with the existing perimeter web defense takes a matter of moments and pre-built integration files are available for a number of popular web gateways and firewalls to make the process even easier.

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 the Web is the perfect vector for infiltration.

Zero Trust CDR for Web Gateways ensures that business users can upload and download business documents and images over the web 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.

Stop Data Loss Concealed in Image Steganography

Steganography is the covert hiding of data within seemingly innocuous files. It's a way of encoding a secret message inside another message, called the carrier, with only the desired recipient able to read it. Now Stegware, the weaponization of steganography by cyber attackers, is on the rise. It is offered by default in malware-as-a-service kits on the Dark Web. It has been used in malvertising campaigns to extort money from thousands of users and bring reputable news sites to their knees. It has been used in conjunction with social media web sites to steal high value financial assets concealed in seemingly innocuous images. All of this is bad news for IT professionals using tools that identify unsafe data since steganography is impossible to detect.

Zero Trust CDR for Web Gateways ensures that every image viewed by a user browsing the Web or communicating via social media is completely free of any content concealed using Stegware. The transformation process destroys any hidden content rendering the image useless to the attacker. Zero Trust CDR for Web Gateways augments existing data loss prevention and governance initiative such as General Data Protection Regulation (GDPR) because it completely stops covert data loss via image steganography.

Disrupt Command and Control Channels (CnC)

The most sophisticated and pernicious cyber attacks typically involve establishing a Command and Control Channel (CnC) between the remote attacker and a workstation(s) inside the business network. Often these channels are established when a previously compromised workstation contacts a remote server, for example via an image on a social media site, or when previously unknown malware is brought in disguised as a valid business document.

Zero Trust CDR for Web Gateways ensures that attempts to establish a CnC are disrupted. The transformation process removes any threat that might be concealed in documents, Web ,and social media images. A forensic dashboard makes it possible to see "before and after" copies of documents and images, aiding in the identification of suspicious behaviour and helping bring users to account.

Build a Winning Solution

Along with our Forcepoint reseller partners, the Forcepoint solutions team provides a wide range of professional services that help you maximize your investment in Zero Trust CDR technology. We can help you to scope, plan, install, configure, and manage your Zero Trust CDR for Web Gateways solution.

Make sure that everything runs smoothly during and after deployment with Forcepoint Technical Support. Our highly skilled solutions team have a wealth of expertise and information at their disposal and can be relied upon to act as a natural extension to your in-house team.

Summary: Enjoy Unparalleled Protection

We're on the brink of a technological revolution. In the face of relentless and concerted cyber attacks, organizations are being forced to re-evaluate every aspect of how they acquire, share and transact digitally.

For more information check out Forcepoint Zero Trust CDR

forcepoint.com/contact