Forcepoint

Solution Brief

Forcepoint Zero Trust Content Disarm and Reconstruction for Portal Protection

Upload the file—not the threat!

Challenges

- Stop zero-day attacks.
- Reduce latency
- Stop malware getting to the endpoints

Solution

- Move away from detection: stop trying to distinguish good data from bad. Zero Trust CDR assumes that all data is unsafe or hostile, meaning nothing travels end-to-end but safe content.

Benefits

- Portal protection ensures that uploaded content to your Internet-facing applications is always threat-free, without the need to detect the threat or isolate the business from the content they need. Zero-day exploits, ransomware, steganography exploits, fileless malware, and the threats inherent in polymorphic files are all removed.
- Easy integration with existing data centre Application Delivery Controllers, Load Balancers/ Reverse Proxies, and Web Application Firewalls.

Known, unknown, and zero-day threats concealed in business documents and images are routinely used to upload malware into organizations. Across a range of business process workflows, including recruitment sites, citizen portals, and financial services sites, organizations need to be certain that when they receive documents and images from the Internet they are not also uploading threats concealed in the content itself. Attempts to nullify these threats using conventional detection-based technologies and sandbox detonation introduce unnecessary latency into the business, frustrate users, and do not eliminate the risk posed by zero-day and unknown threats.

Defeat the Unknown Threat

Existing anti-malware technologies provide a first line of defense, detecting known threats by looking for the signatures of previously encountered exploits or unsafe behaviors. 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 Portal Protection is the only way to defeat not only known but also zero-day and unknown threats in business documents and images as they are uploaded to portals because it doesn't rely on detection or sandbox detonation. Instead it uses a unique process of transformation to ensure total protection.

Transform your Security

Zero Trust CDR for Portal Protection works by extracting the business information from documents and images as they arrive at the reverse proxy. The data carrying the information is discarded along with any threat. Brand new documents and images are then created and delivered to the target application. 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.

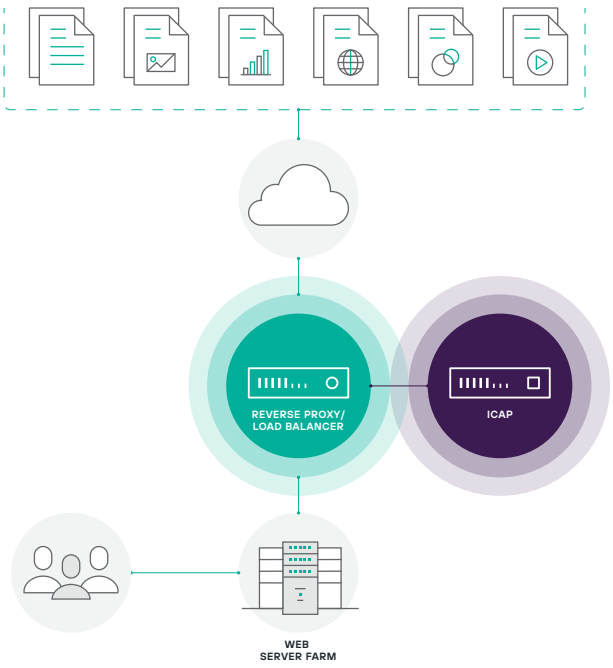
Accelerate Digital Transformation

We're in the age of the self-service portal. Prospects and customers alike are encouraged to upload documents in support of everything from personal loans and mortgages to motor insurance applications. The problem is that while these document formats are versatile and incredibly useful, they are also highly complex, easy to subvert, and are regularly used by cyber criminals to carry malicious payloads.

Using Zero Trust CDR for Portal Protection, organizations can accelerate their digital transformation projects, delivering Internet-facing applications and self-service portals, secure in the knowledge that uploaded documents cannot be used as a vector for uploading threats or compromises into the corporate network.

Ensure Digitally Pure Content

Any portal potentially increases the "attack surface" of the business. The Criminals know this and are intent on capitalising on any vulnerability. Now more than ever, it's vital to ensure that the content uploaded into the organization is safe, pure, and threat-free. Any business that is able to establish a track record for guaranteeing access to clean, pure business content will differentiate themselves in what is fast becoming a lawless cyber landscape.



Zero Trust CDR for Portal Protection ensures businesses can reap the benefits of their digital transformation projects, with confidence that the uploaded content they handle is threat-free.

Integrate Seamlessly with Existing Defenses

The Zero Trust CDR for Portal Protection solution comprises Forcepoint's Gateway eXtension (GX) product. GX is integrated with an existing reverse proxy, such as Load balancer or Web Application Firewall, using ICAP. Content is then passed to the GX by the reverse proxy which then performs content transformation to eliminate content-borne threats. GX is simple to integrate and requires minimal configuration.

Tested with leading reverse proxies, the GX can easily be integrated with third party security vendors including F5 BIG-IP, Citrix Netscaler, McAfee Web Gateway, and Symantec Blue Coat. 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.

Zero Trust CDR for Portal Protection ensures that business workflows (such as importing customer application forms, uploading of personal data, etc.), can continue with complete peace of mind because of the unique way the uploaded documents are transformed. Every document and image is subject to transformation and every one is threat-free.

Eliminate Threats Concealed in Images using 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 Portal Protection ensures that every image contained in an uploaded document is 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 Portal Protection not only protects the organization from inbound exploits concealed in images using steganography, it 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.

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 Portal Protection 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.

Defenses based on the detection of known threats are insufficient. Those based on isolation and sandbox detection inhibit the business and leave too much to chance. What's needed is protection.

Zero Trust CDR for Portal Protection provides unparalleled protection for the any business portal. It ensures that uploaded business documents and images are completely threat free.

For more information check out Forcepoint Zero Trust CDR

forcepoint.com/contact