Zero Trust CDR Business Use Cases

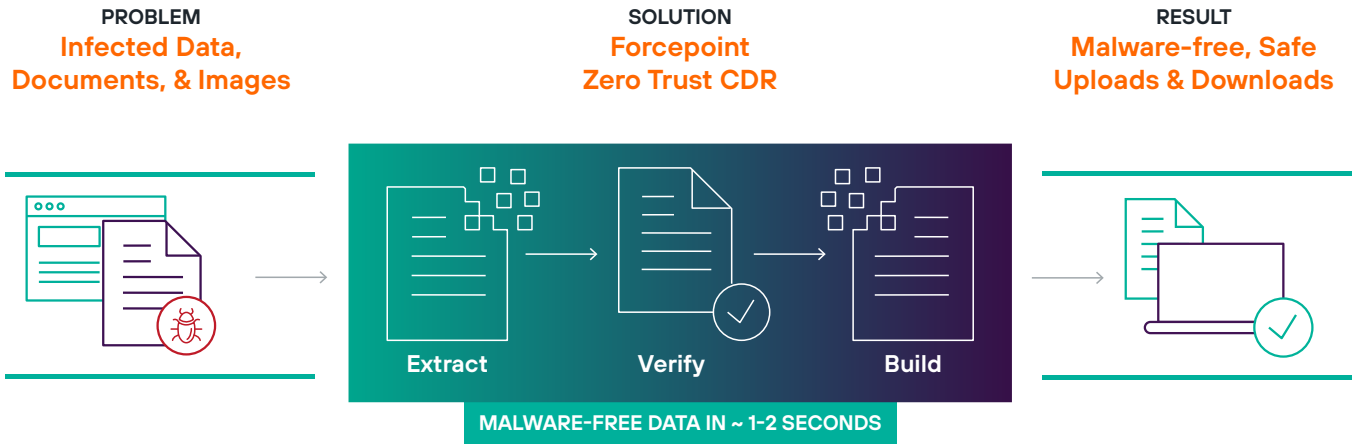
Forcepoint

Brochure

Introduction

The essential everyday business requirement of downloading data, documents and images — or receiving uploaded content — opens users up to significant risk from attackers intent on stealing the user's credentials and/or compromising the endpoint device to gain access to the corporate network.

Forcepoint Zero Trust Content Disarm & Reconstruction (CDR) eliminates file-based malware attacks by eliminating the risks associated with downloading and uploading web documents and images. Our unique, trusted, & proven technology transforms digital content in real-time and guarantees the only thing sent to the user is safe, malware-free data. Zero Trust CDR provides a seamless user experience and supports all common business documents and image file formats.



It's time to pivot from detection to prevention

Zero Trust CDR is designed around a high consequence, military-grade true Zero Trust approach. Where all content is assumed to be potentially malicious. Our unique technology ensures that none of the original data will ever reach the endpoint.

Forcepoint Zero Trust CDR operates at scale, delivers malware-free data, documents and images, requires no endpoint agent software, and does not impact the user experience. Trusted by many of the world's most targeted military, government, industries and commercial organisations to provide protection against even the most sophisticated cyber threats.

Table of Contents

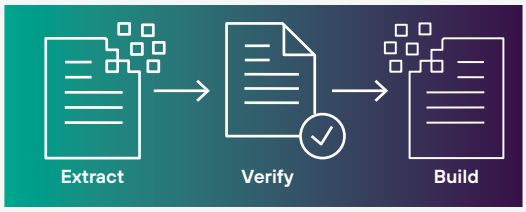
File Download

The everyday act of downloading business information from the internet provides attackers with an ideal threat channel into the corporate network.

1 The user downloads a document from a website. The document contains malware specifically designed to bypass Secure Web Gateways, Firewalls, AV, Sandboxes, etc.

2 The downloaded document is securely forwarded to Forcepoint Zero Trust CDR.

Forcepoint Zero Trust CDR



3 The data is decoded, and the valid business information is extracted. The original file is then discarded — along with any encoding context, unnecessary metadata, active code, or malware — or securely stored for forensic analysis. A completely new file is built using the extracted business information and is then formatted to match the original. All in approximately 1-2 seconds.

4 The brand-new, pixel-perfect, fully revisable, malware-free file is delivered to the user in an identical file format. Ensuring that none of the original data ever reaches the endpoint computer.

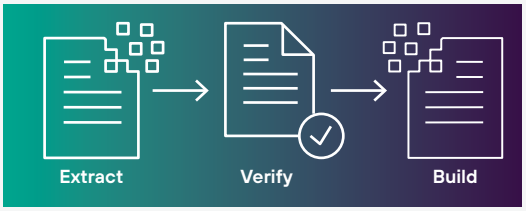
File Upload

The everyday act of uploading business information via the internet provides attackers with an ideal threat channel into the corporate network.

1 The attacker uploads a malicious document via the corporate web portal. The uploaded document contains malware specifically designed to bypass Secure Web Gateways, Firewalls, AV, Sandboxes, etc.

2 The uploaded downloaded document is securely forwarded to Forcepoint Zero Trust CDR.

Forcepoint Zero Trust CDR



3 The data is decoded, and the valid business information is extracted. The original file is then discarded — along with any encoding context, unnecessary metadata, active code, or malware — or securely stored for forensic analysis. A completely new file is built using the extracted business information and is then formatted to match the original. All in approximately 1-2 seconds.

4 The brand-new, pixel-perfect, fully revisable, malware-free file is then safe to store, or send via email.

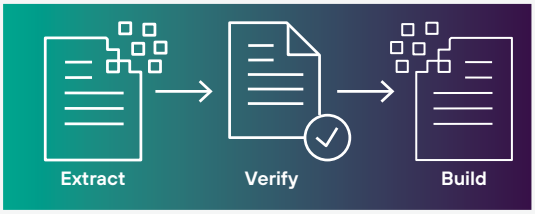
File Upload for Cloud Environments

Uploading business information via the internet from untrusted external sources, provides attackers with an ideal threat channel into the corporate network.

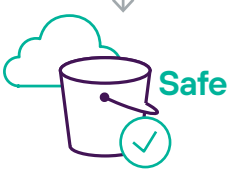
1 The attacker uploads a malicious document to the corporate web portal hosted on Amazon, Azure, or a corporate cloud environment. The document contains malware specifically designed to bypass all security checks - Web Application Firewalls, AV, Sandbox, etc.

2 At the portal it is stored in a 'dirty' container/bucket assigned as the destination for all untrusted content: documents and images uploaded from an external source.

Forcepoint Zero Trust CDR



3 The data is decoded, and the valid business information is extracted. The original file is then discarded — along with any encoding context, unnecessary metadata, active code, or malware — or securely stored for forensic analysis. A completely new file is built using the extracted business information and is then formatted to match the original. All in approximately 1-2 seconds.



4 The new file is then forwarded to a 'clean' container/bucket for retreival — completely malware-free, safe, pixel perfect, fully revisable and in the same file format type as the original.

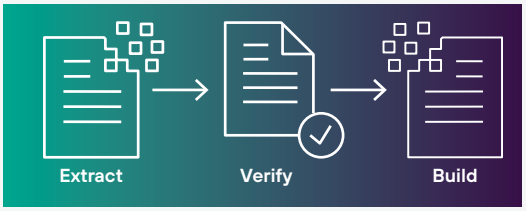
Applications & Workflows with Zero Trust CDR

Forcepoint Zero Trust CDR can run as a service to extract, verify, and build uploaded files automatically for applications and workflows.

1 The application or workflow requires a document or image to be uploaded which is intended to deliver a malware attack .

2 The document or image is presented to Zero Trust CDR using a cloud API.

Forcepoint Zero Trust CDR



3 The data is decoded, and the valid business information is extracted. The original file is then discarded — along with any encoding context, unnecessary metadata, active code, or malware — or securely stored for forensic analysis. A completely new file is built using the extracted business information and is then formatted to match the original. All in approximately 1-2 seconds.

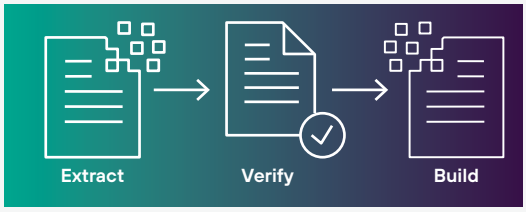
4 The brand-new, pixel-perfect, fully revisable, malware-free file is delivered to the application or workflow in an identical file format. Only safe data travels end-to-end through this process.

Sandbox Replacement

The act of downloading business information from sandboxes provides attackers with an ideal threat channel into the corporate network.

1 Web Gateway forwards the downloaded document to Forcepoint Zero Trust CDR.

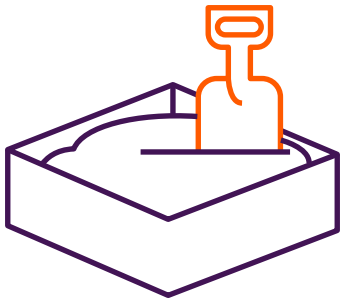
Forcepoint Zero Trust CDR



2 The data is decoded, and the valid business information is extracted. The original file is then discarded — along with any encoding context, unnecessary metadata, active code, or malware — or securely stored for forensic analysis. A completely new file is built using the extracted business information and is then formatted to match the original. All in approximately 1-2 seconds.

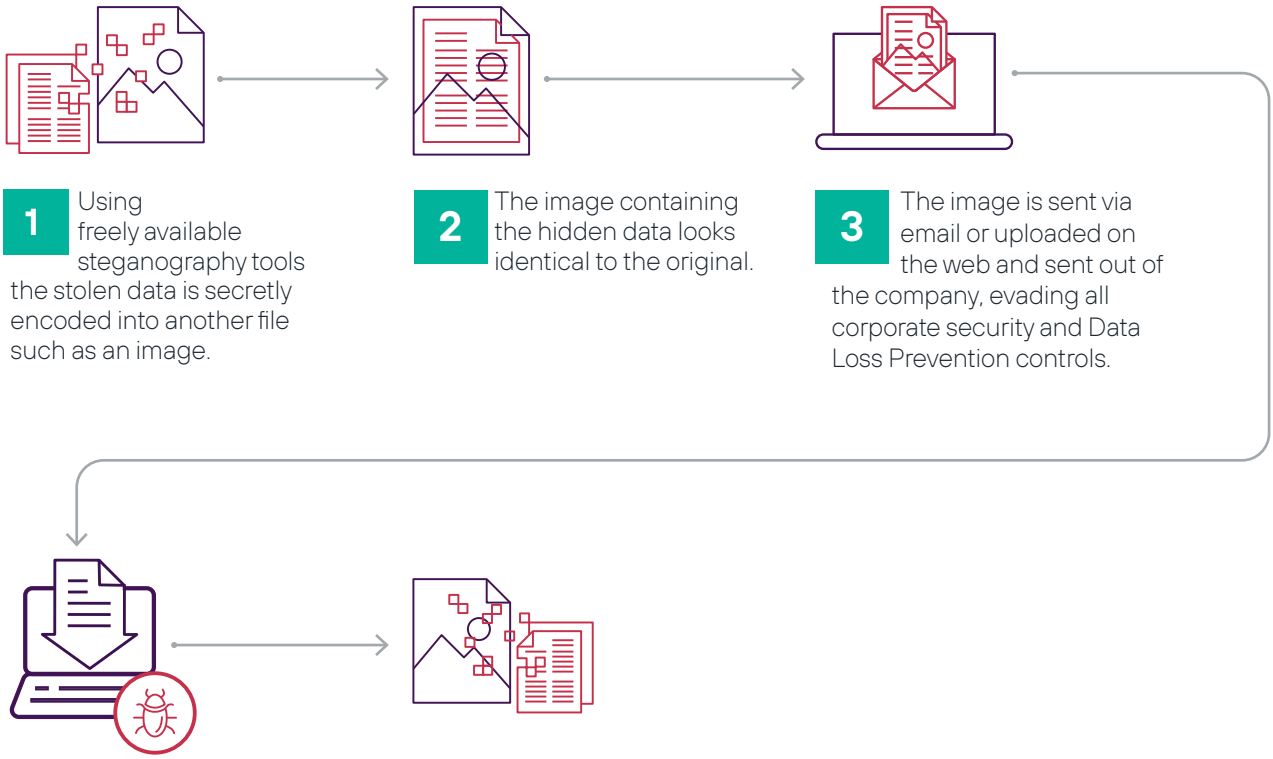
3 The brand-new, pixel-perfect, fully revisable, malware-free file can be downloaded and opened, and is in an identical file format.

Sandbox technologies quarantine downloaded content for security analysis to determine if malware is present. However, users can experience considerable delays whilst the document goes through the sandbox process. As well, malware is often designed to evade sandboxes— making them obsolete.



Inside Data Theft without Zero Trust CDR

Reasons why an employee can opt to become involved with malicious insider activity include financial gain and espionage. How do they exfiltrate the stolen data without being detected?



1 Using freely available steganography tools the stolen data is secretly encoded into another file such as an image.

2 The image containing the hidden data looks identical to the original.

3 The image is sent via email or uploaded on the web and sent out of the company, evading all corporate security and Data Loss Prevention controls.

4 The email is recieved, and the image is downloaded.

5 The image file is then decoded to reveal the hidden data. The target data has been successfully stolen and exfiltrated by the malicious insider.

90% Organizations that feel vulnerable to Insider Attacks.
— CA Technologies

62% Business users who have access to company data they shouldn't.
— Ponemon Institute

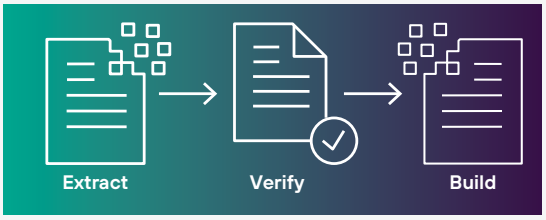
60% Cyber Attacks that are an inside job.
— IBM

Inside Data Theft with Forcepoint Zero Trust CDR

Zero Trust CDR effectively protects against the covert exfiltration of stolen corporate data by eliminating the ability of the malicious insider to obfuscate the data by using steganography.

1 Web Gateway forwards the downloaded document to Forcepoint Zero Trust CDR.

Forcepoint Zero Trust CDR



2 The data is decoded, and the valid business information is extracted. The original file is then discarded — along with any encoding context, unnecessary metadata, active code, or malware — or securely stored for forensic analysis. A completely new file is built using the extracted business information and is then formatted to match the original. All in approximately 1-2 seconds.

3 The brand-new, pixel-perfect, fully revisable, malware-free file can be downloaded and opened, and is in an identical file format.

Phishing Protection without Zero Trust CDR

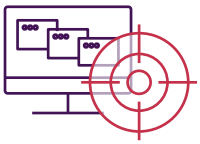
A hacker targets a company using social networks or other internet data. How do they use this to exfiltrate data without being detected?

1 The hacker finds employees with access to company data/systems. Following the social trail, the attacker identifies other people the employee may know.

2 A fake but recognizable email address is created to impersonate a colleague or boss. A personalized email is sent to the employee from the fake address with a link or attachment.

3 The email passes through the spam filter, AV scanning, sandbox, etc. and arrives at the employee's inbox. The email is opened because they 'know' the sender.

4 A link is clicked, or attachment opened, causing a malicious document to be downloaded which infects computer/network.



5 The hacker uses the compromised computer to infiltrate the corporate network to locate and covertly exfiltrate the target information.

95% 95% of all attacks on enterprise networks are the result of successful phishing
— SANS Institute

92% 92% of malware is delivered via email.
— Verizon

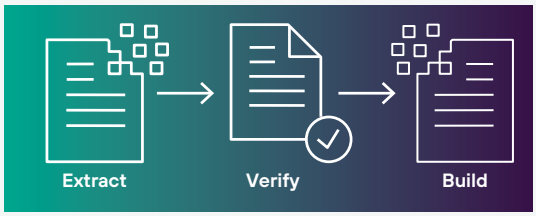
70% 70% of targeted attacks use spear-phishing emails.
— Symantec

Phishing Protection with Forcepoint Zero Trust CDR

Forcepoint Zero Trust CDR assumes all data is malicious, providing effective protection against Phishing attacks by removing threats from email attachments and web downloads.

1 Web and/or email gateway Gateway forwards the downloaded document to Forcepoint Zero Trust CDR.

Forcepoint Zero Trust CDR



2 The data is decoded, and the valid business information is extracted. The original file is then discarded — along with any encoding context, unnecessary metadata, active code, or malware — or securely stored for forensic analysis. A completely new file is built using the extracted business information and is then formatted to match the original. All in approximately 1-2 seconds.

3 The brand-new, pixel-perfect, fully revisable, malware-free file is delivered to the user in an identical file format. Ensuring that none of the original data ever reaches the endpoint computer.

Learn More

Visit forcepoint.com/product/zero-trust-cdr

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.