EVERFOX

TECHNOLOGY BRIEF

Everfox CDR

Protecting Networks, Data and People. Without Relying on Detection.

Cyber threats hide in everyday files, bypassing traditional cybersecurity measures. Legacy detection-based solutions often fail to stop unknown or sophisticated threats, leaving organizations exposed.

Everfox Content Disarm & Reconstruction (CDR) takes a different approach. Removing potential risks by entirely transforming files into safe, functional versions in near real-time without impacting operations.

Try Everfox CDR Online Today

Cybersecurity Challenges

- → Malware, ransomware & zero-day threats, commonly hidden in everyday files.
- → Signature & behavior-based solutions can't stop unknown or sophisticated threats.
- → Traditional tools, scanning & sandboxing can delay file access and impact productivity.
- → Threat actors exploit vulnerabilities in trusted file types, compromising security.

The Everfox Approach

- → We don't scan for threats, we remove the risk by rebuilding new versions of files.
- → All original data is discarded, & a new clean file is made and delivered in its place.
- → No reliance on detection, helping to secure against zero-day and Advanced Persistent Threats (APTs).
- → Works in near real-time with little to no user impact or workflow disruption.

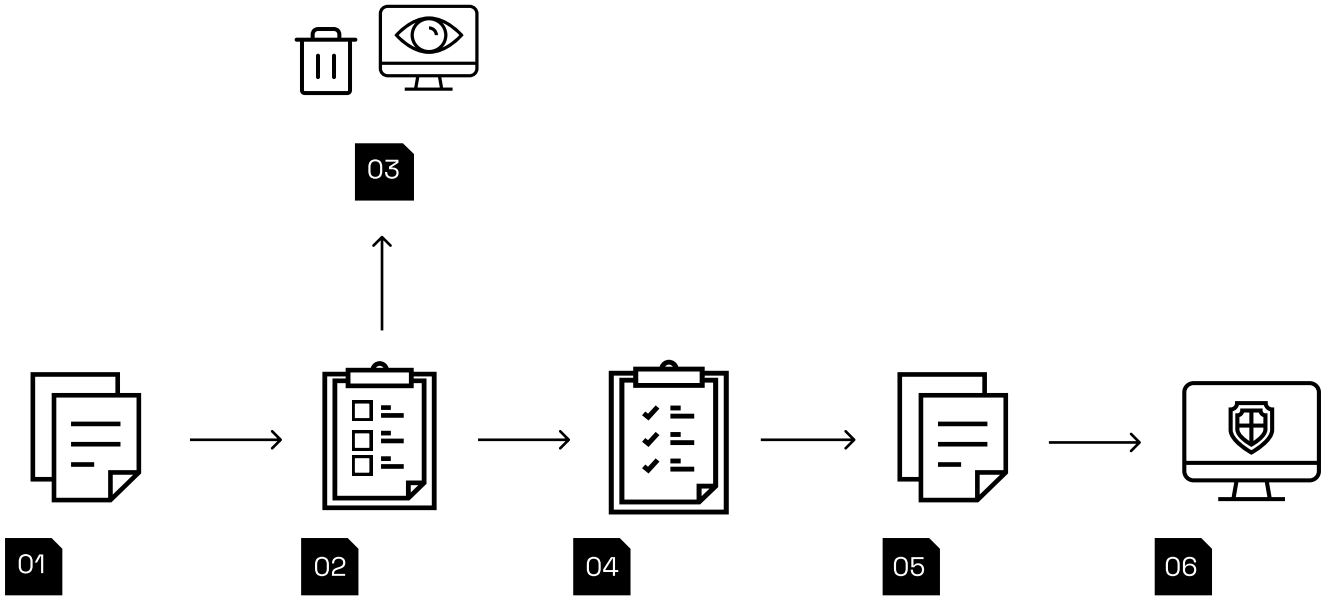
Key Benefits of Everfox CDR

- → Files and data with threats removed.
- → No delays from scanning or sandboxing.
- → Functional files that maintain original usability and edit-ability.
- → Forensic visibility with the ability to access original files for compliance or review.
- → Strengthened security posture without potential impacts to productivity.

How Everfox Content Disarm & Reconstruction (CDR) Works

Everfox CDR helps to remove malware threats while maintaining usability by delivering new safe files.

Simple. Secure. Safe



01

File Received
A document, image, email or other supported file type is received.

02

Analysis & Recipe Creation
Everfox CDR examines the file's legitimate content and creates a set of instructions (a recipe) for creating a new file with the same content but without including any of the original data.

03

Original File Discarded
The original file is either discarded or stored securely, complete with any malware, in your forensic suite for later analysis.

04

Recipe Verification
The generated recipe is verified to confirm it is complete, consistent and not carrying anything extra.

05

File Reconstruction
The recipe is followed to create a new, clean file, equivalent to the original content.

06

Secure Delivery
The newly built functional file is delivered to the user in near real-time.