EVERFOX

DATASHEET

# Content Disarm & Reconstruction

**Malware evolves constantly. Your security should too.**

From email exchanges and web interactions to file uploads and web applications, technology generates the digital information that is the lifeblood of every organization. This information is shared and communicated with business partners, customers, supply chains, and local and remote workers. Information sharing on this scale has created a huge attack surface for cyber criminals to exploit using malware concealed in everyday files, documents, and images.

In response, the number of defensive technologies has increased to try and combat the problem. But these defenses are all based, to some degree, on the concept of detection. The problem with detection-based defenses is that they can only detect what they have "seen" before. There have been attempts to strengthen these defenses. Sandboxes can help, but attackers have learned how to spot them, and they still rely on detection to try and identify threats. In response, the cyber criminals are constantly looking to attack an organization with malware that the defense hasn't seen before and therefore regards as safe.

### Challenge

Organizations face a pressing challenge in ensuring the security of uploaded files within their applications and workflows. Traditional methods fall short, leaving vulnerabilities that malicious elements can exploit.

The need for a comprehensive solution to automatically extract, verify, and reconstruct files becomes paramount to mitigate potential threats and maintain data integrity.

### Solution

In addressing these challenges and risks, implementing a robust Content Disarm and Reconstruction solution becomes imperative. Such a solution not only navigates the complexities of diverse file types but also provides proactive defense against evolving cyber threats.

By safeguarding the integrity and security of a your digital assets, CDR serves as a cornerstone in fortifying the organization's overall cyber security posture.

### Benefits

- Defeats advanced threats
- Reduces strain on SOC team from day one
- Reduces latency by not subjecting incoming files to sandboxing or flattening
- Choice of Deployment: On-premise, cloud or application
- Highly versatile

# How Everfox CDR is different

Rather than trying to detect malware, Everfox CDR assumes nothing can be trusted. It works by extracting the valid business information from files (either discarding or storing the originals), verifying the extracted information is well-structured, and then building new, fully functional files to carry the information to its destination.

That's why Everfox CDR is a game-changer for mitigating against the threat of even the most advanced zero-day attacks and exploits. Pivoting from detection to prevention in this way is especially important with the recent evolution in hybrid workforces and their resultant usage of content and electronic information everywhere.

| | Signature Based AV | Sandboxing | Traditional CDR | Flattening | Everfox CDR |
|---|---|---|---|---|---|
| **No updates required** | 🔴 | 🔴 | 🟢 | 🟢 | 🟢 |
| **Defeats polymorphic malware** | 🔴 o | 🔴 oo | 🟢 | 🟢 | 🟢 |
| **No false positives** | 🔴 | 🔴 | 🟢 | 🟢 | 🟢 |
| **Stops unsafe data** | 🔴 | 🔴 ooo | 🔴 Δ | 🟢 | 🟢 |
| **Enhances user experience** | Depends on implementation | Slow | Depends on implementation 〉 | 🔴 | 🟢 |
| **Mechanism safe from attack** | 🔴 | 🔴 | 🔴 | 🔴 | 🟢 |

o Simply changing the malware in a small way can defeat signature-based detection
oo Changing the behavior of the malware can defeat sandboxes
ooo Malware that recognizes it is running in a sandbox can avoid detection
Δ Putting malware in unchecked locations in the file can avoid removal
〉 The reconstruction in some implementations leaves content looking significantly different to the original

## Outdated approaches

For over 25 years, the standard approach to combating these threats has been to use detection-based cyber defenses. The problem with detection however, is that it's easy to evade. Just change the signature of the exploit and the malware crosses the security boundary unimpeded. Detection alone is no longer sufficient to safeguard users from known and unknown threats, zero-day attacks & malware.

Everfox Content Disarm and Reconstruction stops file-based malware from entering the organization without using detection. Due to the unique way that CDR just extracts and delivers what is good in a file and doesn't try to detect what is bad, it protects users from even zero-day and totally unknown malware. This approach to preventing malware doesn't need constant updating with the signatures of the latest new and zero-day malware as they become available, so the defence is always up to date.

## Enhanced user experience

As organizations search for new and more effective solutions to the problem of concealed malware, they risk negatively impacting the user experience. Subjecting incoming files to multiple antivirus scanners or holding and sandboxing them for further scrutiny can add latency into business processes. Or attempting to render files safe by "flattening" them, leaving the user with documents that can't be easily shared, edited or updated. In many cases, the intentions are good, but the end result is that business processes become slower, resulting in increasingly frustrated users.

Everfox CDR enhances the user experience without compromising security. Because the process doesn't rely on detection, there's no waiting for the system to scan files trying to detect known threats. Additionally, there's no lengthy delays in crucial business processes as we don't use sandboxing. Meaning receiving alware free data from Everfox CDR solutions takes only a fraction of a second.

### Stop threats

Digital content is the vector of choice for cyber criminals to use for malware attacks and exploits. From web browsing and email to file uploads and social media, digital content is routinely embedded with known, zero-day, and even totally undetectable threats concealed in the files and images we use every hour of the working day.

### Free up your SOC team

Even with the very best detection-based defenses in place, many security operations center (SOC) teams still spend too much time and money preventing, detecting, analyzing, and responding to cybersecurity incidents caused by malware concealed in incoming files.

Everfox CDR frees up the SOC team from the day-to-day chores of handling quarantine queues, managing false positives, applying signature updates, and dealing with potential breach alerts. Every incoming file is subject to the CDR process – regardless of whether it does or doesn't contain malware - and every file is rendered threat-free.

### Highly versatile

Everfox CDR solutions work with your existing boundary defenses and technologies. Transforming a wide range of the most popular file formats including all Office files, images and PDFs (the formats most commonly used by attackers). Protecting a wide range of attack vectors including web, email and file uploads.

## How Everfox CDR works

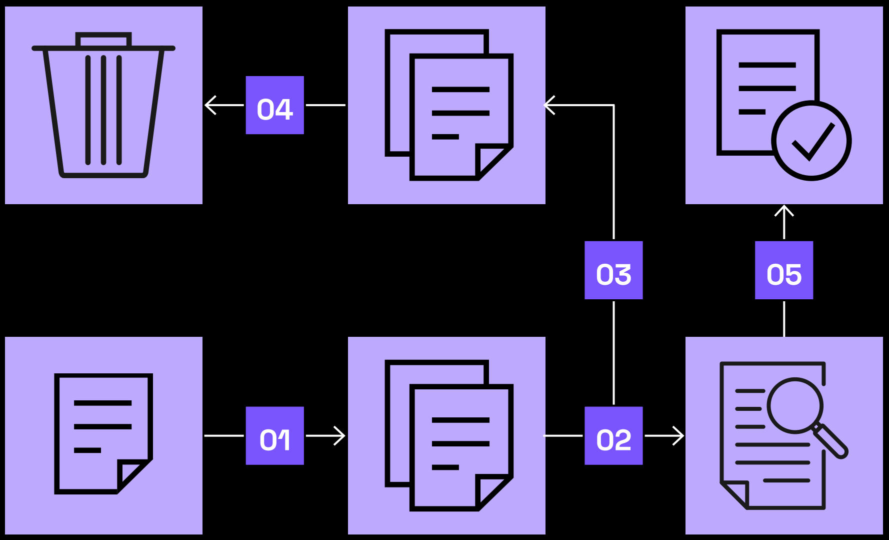
**01.** Rather than identifying known malware, CDR takes the data and extracts the useful information from it.

**02.** The extracted information is transformed into an intermediary format and verified.

**03.** This advanced threat protection process makes sure no threats or attacks can reach the next stage.

**04.** The original data is stored or discarded along with malware, known or unknown.

**05.** Brand new data is then built in a normalized way, containing the verified information. The new data replicates the original data, without the threat of embedded malware and is now safe.



**Learn More:** www.everfox.com