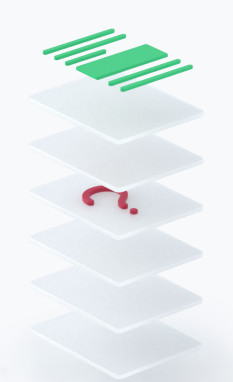


What is Content Disarm & Reconstruction (CDR)?

Everything You Need to Know



Content Disarm and Reconstruction, Content Disarm and Reconstruct, and CDR are all terms used for a technology that can eliminate all file-borne threats.

In this article, we provide an overview of what CDR is, how it's used, the history and evolution of the technology, its pros and cons, and how a new technology—Positive Selection technology—takes CDR to the next level in both security and user experience.

What is Content Disarm and Reconstruction?

Content Disarm and Reconstruction (CDR) is a security technology that—depending on the type of CDR involved—flattens malicious files, removes active content, or cleanses malicious code from files.

Also known as file sanitization, CDR has multiple forms. In general, CDR does not need to rely on detection to prevent threats. Instead of relying on databases of known signatures, the technology assumes all files are malicious and scrutinizes all files that are outside of the approved firewall.

Depending on the type of CDR, which is explained in detail below, content disarm and reconstruction can remove malware, strips any embedded code, and rebuilds the file in a way that disrupts any additional covert malicious code.

The end result of using CDR technology is:

- ✓ A flattened file delivered as a safe but unfunctional PDF (CDR Type 1)
- ✓ A file with active content, macros, and other malicious and safe content removed (CDR Type 2)
- ✓ A safe copy of the original file on a clean template, with all functionality intact (CDR Type 3,
- ✓ Positive Selection technology)

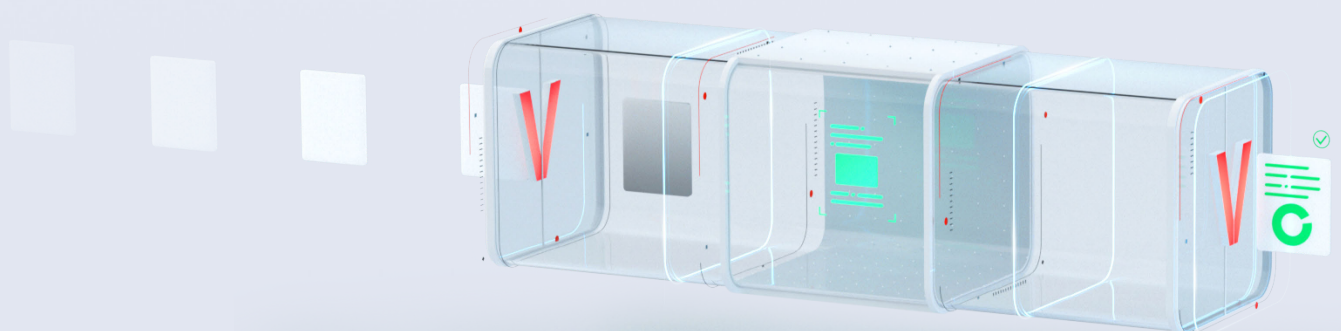
Who is Content Disarm and Reconstruction technology meant for?

CDR is most often used to prevent file-borne cyber security threats from breaching an organization's network. According to research, industries benefiting from CDR include banking, financial services and insurance, telecom and information technology (IT), manufacturing, construction, wholesale distribution, non-profit organizations, chemicals, food and beverage, retail, hospitality, government, public sector, health insurance and healthcare, among others.

Why is this technology needed?

File-borne threats are underestimated but highly risky. According to the Verizon Data Breach Investigation Report, the number 1 channel for enterprise malware delivery is Microsoft Office documents.

- ✓ **Traditional defenses are no longer effective.** Advanced threats are constantly evolving. Research indicates that an average of 10 million new malware threats are recorded per month. Many common cybersecurity technologies, such as anti-malware and anti-virus solution, can only detect known threats and cannot detect or protect corporate networks against undisclosed or zero-day attacks, meaning a vulnerability has been discovered but no patch for it has been developed. In fact, 80% of successful breaches are new or unknown zero-day attacks that are not recognized by traditional signature-based detection solutions.
- ✓ **Opportunities for cyber breaches abound.** Today's ever-increasing reliance on data brings with it elevated risks, threats, and vulnerabilities for organizations and communication networks, and many of these vulnerabilities are undetectable by traditional network security solutions. As the complexity of files increase, cybercriminals have more opportunities for exploits.
- ✓ **Sandboxes are not sufficiently effective.** Despite widespread use, sandboxes struggle to keep up with the increasingly advanced techniques deployed by malware creators. Simple Google searches will provide attackers with the information they need to ensure their malware can evade detection within the sandbox – only executing once inside the production environment – or bypass the sandbox altogether. In addition, large file uploads can cause bottlenecks in the sandbox, and maintenance requires extensive IT resources, time and money, as well as the need to continuously update complex security policies.



- ✓ **Human error poses a risk.** 90% of data breaches are caused by human error. Despite organizational attempts to educate employees about the dangers of opening files from unknown or unreliable sources, clicking on suspicious links or downloading questionable files, 27% of employees in an organization fail phishing or social engineering attacks. This causes some organizations to restrict internet downloads or file attachments, despite the inconvenience and significant decrease in productivity.
- ✓ **Cost of breaches are increasing.** Consequences of a malware attack are significant. Many companies suffer data loss, disruption of service, downtime, damage to the enterprise or organization's reputation, and revenue loss. Accenturereports that the average cost of a malware attack on a company is \$2.6 million, with the attacks costing the business an average of 50 days in lost time.

What does Content Disarm and Reconstruction help protect against?

With the increase in file-sharing – both between co-workers working remotely and between customers, partners, and vendors – enterprises face elevated risks, threats, and vulnerabilities from file-borne malware, and many of these vulnerabilities are undetectable by traditional network security solutions.

By design, an exploit targets a vulnerability in an application and typically triggers an intruder's code. A vulnerability is a "hole" in an application—say, Adobe Reader—that can be exploited to launch an attack on a computer or network system. A common method used by attackers to exploit vulnerabilities is phishing or targeted spear-phishing: sending email messages that contain a malicious attachment and look harmless to the recipients. When a recipient opens the attachment, malware is deployed and the targeted attack begins.

To ensure a successful exploit, malware writers often carefully design and build multiple suspicious objects and embed them in a malicious complex file. For example, a Microsoft® Word file may contain an ActiveX® or OLE object to execute an attack, plus shellcode that is triggered by a malicious image or macro. (Shellcode is a small piece of code used as the payload in the exploitation of a software vulnerability).

As these attacks become more aggressive, novel approaches to security are needed to successfully protect enterprises. CDR technology protects organizational networks from cyber threats that originate from multiple channels, including files from many sources, including email, web browsers, file servers and FTP, the cloud and computer endpoint devices.

Content Disarm & Reconstruction Technology's Evolution over Time

CDR – as most technologies – has advanced over time, improving its capabilities and enhancing any drawbacks.

1 CDR Type 1: Converting files to PDF

This type of CDR technology utilizes file conversion or transformation in order to render the file safe. The technology converts all files into a PDF file format, which eliminates the possibility of a hacker activating malicious code when a user clicks on a link or opens a document. However, it also creates a flattened document, without any legitimate macros, tracked changes, image transparency, form fields, layers, etc., effectively transforming the file into an unusable document and negatively affecting the organization's productivity.

2 CDR Type 2: Stripping out active code and embedded objects

The next level of CDR technology aimed to improve on its earlier capabilities. It focuses on stripping out only certain types of content, such as embedded objects or potentially active content, in order to ensure the safety of each file. However, the file still loses functionality, such as links, essential macros, and business logic. It also overlooks a security risk by allowing fundamental, yet vulnerable, templates to remain within the document.

3 CDR Type 3 – Positive Selection technology: CDR evolved

The most advanced form of an evolved CDR, this technology focuses on template-based reconstruction that allows full preservation of features and full functionality. The technology rebuilds the document, copying only the known-good, positively selected content and ensuring only the safe template elements remain.

What is Positive Selection technology?

Positive Selection technology is the next evolution of the popular CDR technology. Positive Selection uses template-based reconstruction to re-create clean templates with only the known good content included.

Unlike detection-based file security solutions that scan for suspicious elements and block some malicious files, Positive Selection singles out only the safe elements of each file, ensuring every file that enters your organization is 100% safe.

How is Positive Selection technology different than CDR?

While most types of CDR rely on malware detection, signatures, and predictive analysis, only Positive Selection technology delivers fully functional content in milliseconds that is always effective against zero-day attacks with a 0% false positive rate.

Built with deep expertise in the architecture of every file format – as well as close working relationships with file format companies like Adobe – [Positive Selection technology](#) understands and protects all file types—from .ppt, docs, pdfs and image files, all the way to more complex formats that no NGAV or Sandbox can possibly detect.

Features	CDR Type 1	CDR Type 2	CDR Evolved: Positive Selection
Usability & End User Experience	Flattens files into PDFs, rendering them static and useless	Removes active content, including safe, business-essential content	Retains full file usability, functionality, and fidelity
Password-Protected & Zipped Files	Does not sanitize ZIP or password-protected files	Does not sanitize ZIP or password-protected files	Sanitizes ZIP and password-protected files
Files Blocking	Blocks files with known threats	Blocks files with known threats	No files are blocked; all files are sanitized of both known and unknown threats
Templates	Original, potentially malicious template retained	Original, potentially malicious template retained	Template-based reconstruction places content on new, clean, safe template
Active Content	File is flattened	Removes all active content	Retains active content, just removes malicious elements
False Positives	High false positive rate	High false positive rate	0% false positive rate
Maintenance	Maintenance involved	Maintenance involved	No maintenance required; plug and play
Latency	Latency – seconds to minutes	Latency – seconds to minutes	Latency – milliseconds; employees receive safe files instantly

How does Positive Selection technology work?

Built with deep expertise in the architecture of every file format, Positive Selection understands and protects all file types—from .ppt, docs, pdfs and image files, all the way to more complex formats like Autodesk files. Positive Selection technology protects against even the most obscure, challenging file types that no NGAV or Sandbox can possibly detect.

1 Step 1: Identify the File Format

Every file must adhere to strict, vendor-based specifications that are unique to that particular file format. Positive Selection technology uses an intelligent fingerprinting technique that identifies a file's content type and format based on file structure and characteristics.

2 Step 2: Generate a New Version of the File

Positive Selection technology then generates a new, clean template of the file and imports over the positively verified content from the original file while leaving behind exploits and malicious objects. This regenerated, safe version of the file, based on known good templates from the file vendors, ensures that all the good content (including active content and embedded objects) is kept in its original format while preserving file functionality.

Macros, scripts, OLE objects, and all other elements are sanitized and regenerated into the new file as usable elements, neutralizing any exploitation attempts. This process ensures that both the user experience and file security remain intact. All files—suspicious or not—go through this process, which takes less than a second and is invisible from the user's point of view.

3 Phase 3: Use the New File

All malicious code and exploit threats are eliminated, positively selected elements transferred, and the new file preserves the integrity and functionality of the original file. The file is now safe to save, edit, use, and share.



Which vulnerabilities does Positive Selection protect against?

A software vulnerability opens the door to cybercriminals. A hacker who discovers a vulnerability can use it to gain entry to a system and then obtain unauthorized access to data. A vulnerability has a life cycle consisting of three stages: undisclosed, zero-day, and patched. Positive Selection technology protects organizations from file-borne cyber-attacks brought on by exploits at all three stages of the vulnerability life cycle.

1 Stage 1 Undisclosed

At this stage, a vulnerability in an application, system or hardware is unknown to the vendor or the security community but has been discovered by someone, possibly a researcher in a cyber warfare organization—or the hacker community. This type of vulnerability presents a high security threat to everyone and can go undetected for years.

Because the application's vendor does not know of the vulnerability, countermeasures cannot be developed to prevent or block its exploitation. Undisclosed vulnerabilities are frequently used by groups that gather cyber intelligence or trade information to receive large cash payouts.

2 Stage 2 Zero Day

At this point, the vulnerability has been disclosed to the vendor and the security community. A zero-day vulnerability is a software weakness that has just appeared for the first time, and no patch has been developed to overcome it. This type of vulnerability presents a high risk of exploitation; intrusion detection systems or traditional protection systems using signature-based detection might identify exploitation activity after gathering and extracting several samples, but an exploit that a hacker has manipulated will be able to avoid signature detection.

Zero-day vulnerabilities can go unaddressed for some time, because vendors may take 90 days or even more to respond to reported threats.

3 Stage 3 Patched

At this stage, although the vendor has already issued a patch for the vulnerability, it can be opportunistically exploited in non-patched environments of out-of-date applications. Large enterprises may be particularly susceptible to opportunistic attacks, because patch management is more cumbersome than in smaller organizations. The threat level at this stage is low, because the vendor has provided a patch.

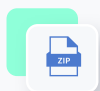
What file formats does Positive Selection support?

Positive Selection technology handles many types of files.



Password-Protected Files

Positive Selection technology can, in one seamless user experience, completely cleanse password-protected files. This is done without the need to bring IT in to open or unblock a password-protected file.



Zipped Files

Positive Selection technology supports containers, such as ZIP and other archive files, as well as the files within the containers. In the latter case, multiple compressed layers are recursively decompressed, analyzed for known elements, and recompressed, preserving the files' original functionality.



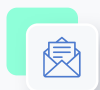
Documents

Positive Selection technology supports PDF, RTF, and text formats. Documents are broken down into individual elements for analysis. The trusted elements of the document are transferred to a known good template, resulting in the delivery of fully functional and completely threat-free document.



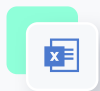
Archives

The technology supports all common archive formats: ZIP, RAR, 7Z, and CAB. As the container is unpacked, the Positive Selection process runs recursively to analyze individual elements in each file. After the content is successfully analyzed for known and trusted elements, the elements are transferred to known good templates, and the file is repacked for safe delivery.



Email Containers

Positive Selection technology supports several email containers, including EML, MSG, and PST. Votiro's Secure File Gateway for Email works with your Email Server to ensure incoming emails flow through Votiro's Positive Selection engine to have the trusted elements transferred to known good templates, ready to be passed safely to the recipients.



Microsoft Office Files

The advanced Positive Selection process unpacks a Microsoft Office file, recursively checking embedded objects such as images, documents, and OLE objects to the finest element. Trusted elements are transferred to known good templates, and safely delivered to the recipient or target location.



Images

The technology removes malicious content from all the common raster and vector image formats: JPEG, GIF, BMP, PNG, TIFF, EMF, and WMF.

How effective is Positive Selection technology?

The technology has been proven to achieve prevention levels of 100% for advanced file-based attacks. One vendor's technology has successfully processed over five billion documents—and did not allow a single breach.

What are the advantages of Positive Selection technology?

Compared to CDR types 1 and 2, and detection-based solutions, Positive Selection technology enables the following:

- ✓ Prevents cyber threats from multiple sources and vectors
- ✓ Protects against malware, including zero-day threats
- ✓ Promotes productivity; technology runs efficiently in background
- ✓ Eliminates need to rely on human compliance
- ✓ Allows greater access to content, with less restrictive Internet policies required

What are the benefits of Positive Selection technology?

You receive the same exact files, minus the risk.

Positive Selection guarantees you receive the exact same file, while getting rid of all potential risk. That way, your file remains 100% authentic and functional, yet 0% dangerous.

Positive Selection file sanitization does not impede the business workflow.

Unlike other slow, time-consuming solutions, Positive Selection eliminates weaponized files without disrupting your business for even a single moment.

Automate file security for your organization and reduce the manual workload.

Blocking and quarantining files doesn't just cost your business time—it also forces your security team to focus on the grunt work of unblocking files and taking them out of quarantine. With Positive Selection, you don't block or quarantine anything. Files smoothly and safely enter your organization the instant they're received.

Votiro's Positive Selection technology seamless integrates into your existing architecture.

- ✓ Easy implementation: less than 60 minutes
- ✓ Seamless integration with existing solutions
- ✓ Blazing fast: ultra-low latency
- ✓ Supports both cloud & on-prem
- ✓ Zero training required

Want To Learn More About Votiro's Secure File Gateway?

- Powered by Positive Selection Technology -

[Schedule A Demo](#)

About **Votiro**

Votiro introduces Secure File Gateway - the only solution that guarantees complete protection from weaponized files. Unlike detection-based file security solutions that scan for suspicious elements and block some malicious files, Votiro's revolutionary Positive Selection™ technology singles out only the safe elements of each file, ensuring every file that enters your organization is 100% safe.

Founded by leading file security experts, Votiro's new approach to file security works invisibly in the background, completely eliminating threats while ensuring zero interruption to business. Votiro is trusted by large enterprises globally, including top Fortune 500 companies, to completely eliminate file-based threats while ensuring business continuity.

Headquartered in the United States, with offices in Australia, Israel and Singapore, Votiro is trusted by over 400 companies and 2 million users worldwide to safely access files with complete peace of mind.

Contact Votiro

info@votiro.com
votiro.com

