



Ultimate Guide:

Questions to Ask Your CDR Vendors

Table of Contents

Introduction

Is it Zero Trust by Default?

How Does it Handle Compromised Vendors?

Does the CDR solution Integrate with Content Collaboration Tools and Platforms?

Content Preservation: Active Content, Macros, Javascript, etc

Does your CDR flatten files?

Can you lose macros in the CDR process?

Is there a risk of losing content in the CDR Process?

Does the formatting get lost in the CDR process?

Does It Support Numerous File Types?

How does it handle Locked Files?

Can it manage giant volumes of data?

How Fast Is It?

Can it handle massive imports?

Does your CDR seamlessly interoperate with cloud systems and data lakes?

Does it work with public portals?

How is the service after the sale?

How easy is the implementation?

Does the company have expertise in CDR?

Does your CDR work With Remote Browser Isolation (RBI)?

Can it improve security metrics?

Finding an Advanced CDR

Introduction

Choosing a solution provider for CDR (Content Disarm and Reconstruction) is not easy, with so many options on the market. Every vendor has a different selection of features and offerings, so it is easy to become overwhelmed. Selecting the right solution for your organization takes knowing the right questions to ask your vendor to ensure that their technology can meet your organizational needs.



We have compiled a comprehensive list of essential questions to pose to your CDR vendor and why this information is valuable to your company.

Questions

Is it Zero Trust by Default?

Attackers are constantly varying their techniques and technology to slip past existing defenses. This constant evolution is why there are over 450,000 new pieces of malware detected daily. Keeping abreast of this information to update signatures is impossible for even the most diligent detection-based solution, leaving them constantly vulnerable to unknown or zero-day threats.

How Does it Handle Compromised Vendors?

Business email compromises (BEC) and Vendor email compromises (VEC) happen, allowing attackers direct access to send emails from apparently legitimate email addresses. Many anti-phishing training programs teach users to look for abnormal domains in the email address and trust those from trusted vendors. When VEC occurs, the user receives a malicious email from an otherwise trusted domain, often leading to malware infections.

Blocking only when compromises happen leads to reactive, manual processes. Disarming and rebuilding by default eliminates the effort and reduces the load on staff while eliminating the risk of BEC and VEC.

Does the CDR solution Integrate with Content Collaboration Tools and Platforms?

Collaboration tools are essential for maximizing productivity and streamlining communication with a globally diverse workforce. With these tools comes the risk of sharing malicious files between peers across these channels. This amplifies the risk when third parties, such as vendors and contractors, are involved, using uncontrolled endpoints that may have less than stellar security practices.

Content collaboration platforms such as Box, O365, S3, and Slack remain uncontrollable for many CDR vendors. Alternatively, vendors that provide an Open API can integrate CDR support into a wide variety of software solutions, incorporating CDR protection every time users share files. This makes Votiro a true Zero Trust solution as it sanitizes every file, whether or not they are known to be malicious.



Content Preservation

Questions: Active Content, Macros, Javascript, etc

Preserving the content of files is something that not all CDR vendors perform at the same level to guarantee rebuilding without any loss. Determining if a product meets your needs and expectations requires knowing how accurately it recreates the data from its inputs. More advanced CDR solutions create a virtually identical version after disarming, vs. less advanced solutions may have to strip content or features to ensure a safe file.

Does your CDR flatten files?

Flattening files removes the multi-layer file formats of advanced graphics programs that manipulate an image on a fine-grained level. After CDR, some vendors take the layered structure and condense it to a JPEG, GIF, or TIFF, "flattening" the file and removing the ability to edit it later fully. Proper format-preserving CDR will not flatten a file but instead return it in the same original form presented.

Can you lose macros in the CDR process?

Many macros are essential components in many Word and Excel documents. They provide automated functions such as applying frequently utilized formatting to a document to preserve style. Attackers can also use macros to launch malicious actions against a user who opens a document that contains them.

Less robust CDR programs take an all-or-nothing approach to macros, stripping them out entirely from all documents. Vendors eliminate even the useful macros necessary for workers to do their jobs. More advanced CDR products can identify safe macros and re-include them in the rebuilt file, preserving the functionality users require while eliminating riskier macros.



Is there a risk of losing content in the CDR Process?

CDR solutions that are less complex strip away large portions of files when they detect something similar to their signatures. More advanced CDR solutions preserve all safe content ensuring that no crucial data is lost in the process.

Does the formatting get lost in the CDR process?

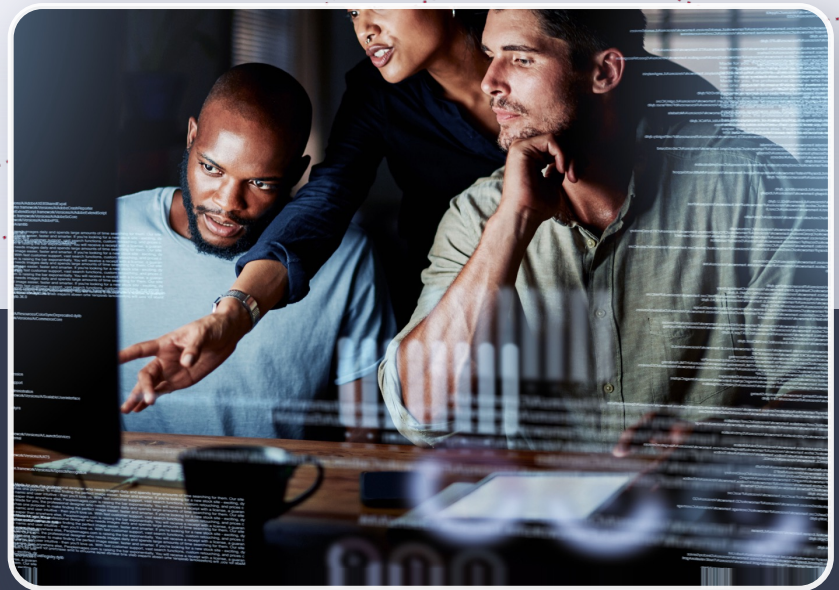
Like file flattening, format stripping can also occur on some CDR products. To limit risk, they strip out only the text and shove it into lower-functionality formats, such as converting a Word document to a PDF or a plaintext file. While this may preserve the text content, it removes the ability to edit later along with the format of the information.

More advanced CDR solutions can completely rebuild a file in the same type that it was, being intelligent enough to preserve all formatting so the file presents as intended. With this variety of CDR solutions, businesses will not lose any of the contexts that the format and layout convey.

Does It Support Numerous File Types?

Businesses do not only work in limited file formats such as word, pdf, or excel. They handle various formats, many of which may be proprietary or less common. How the CDR handles more obscure file types is essential to know. Less savvy CDR products may not have the flexibility to assess them properly and either block them by default or let them through because they do not understand what components are known safe.

When looking at CDR solutions, consider vendors who offer an extensive range of format support, especially those commonly used for your organization, are crucial for attaining a good fit.



How does it handle Locked Files?

Working with password-protected and encrypted files is a challenge for any CDR. Because the content is inaccessible by default to the CDR, they are challenging to assess appropriately. Less savvy CDR products will let them through without contention or block them by default as they cannot properly assess them. Both of these variations are not business-friendly. Either the file is let through with a potentially malicious payload, or the contents are blocked, preventing what might be business-critical data from being transmitted.

More advanced CDR solutions take a different path, where the file is held in a temporary storage requiring the recipient to provide a password or decryption key. Once the user provides the information, the CDR assesses it like any other file, then rebuilds it using only safe components for the user. With this process, the business gets the guarantee that no "bad" elements are passed into the organization while only temporarily obstructing transmission.

Can it manage giant volumes of data?


Businesses handle massive volumes of data daily, from email to file collaboration and cloud storage. Processing and assessing this information flow needs to happen quickly to not impede workers from doing their jobs. CDRs that introduce a delay in processing, especially during volume spikes when users are most busy, displease workers making it more challenging for them to complete their jobs.

Ask your CDR vendors for evidence that they can effectively handle large volumes of data. Look beyond the promises and request proof of performance. How are they at handling massive data volumes over time, not just in a single spike?

How Fast Is It?

Part of efficiently protecting your organization is doing it in a manner that does not diminish productivity. The speed of protection is a crucial component of the defense itself. CDR solutions that introduce delays in processing reduce the efficiency and effectiveness of employees as well as create general discontent about the protection.

Ask your CDR vendors for evidence that shows their sanitization speed doesn't leave users waiting on processing. Effective vendors should be able to show proof of sanitization in milliseconds rather than minutes or hours.

A decorative graphic consisting of several red dotted lines that flow from the left side of the page, across the bottom, and towards the right. The lines are of varying lengths and curves, creating a sense of movement and flow.

Can it handle massive imports?

Handling large volumes of data in one go can happen from a first-time review of files to a mergers and acquisitions scenario where you acquired a company but don't want to acquire its bad data. Anytime a large quantity of data has not been vetted for safety, there is a risk of lurking threats.

The first part is knowing whether your CDR can ingest and cleanse a large data store. The next component is understanding from the vendor what level of processing this will entail and the timelines associated with it. Even if a product can work with a large store of data, it is only valuable if it does so in a timely manner.

Does your CDR seamlessly interoperate with cloud systems and data lakes?

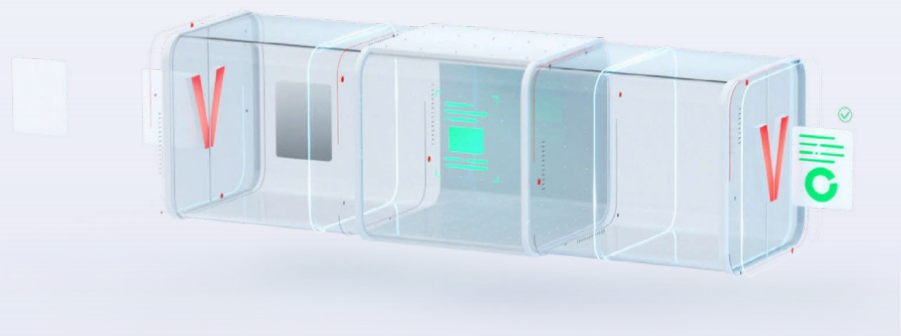
Not every CDR has the capability to integrate with more complex environments such as the cloud. Even for those that can, doing so in a manner that does not require a massive effort from engineers to install and configure is not common.

With the growth in cloud computing, most organizations need a seamless integration that does not require manual efforts for processing and workflows. Easy interoperability that leverages automation eases the burden on staff, allowing them to focus on more important tasks while still gaining all of the protective capabilities of the CDR.

Does it work with public portals?

Allowing customers to upload data to your portals is necessary for many organizations, such as insurance, loan processing, supply chain, or purchasing. This capability reduces the load on staff, allowing customers to self-service delivering documents in a secure manner. Unfortunately, allowing external parties to upload anything to your organization creates a risk of lurking threats in the files.

A CDR that integrates directly into the portal for processing customer-provided data before anyone internal has a chance to interact with it eliminates this risk.



Service & Deployment Questions

How is the service after the sale?

When a vendor sells a product, there should be a total commitment throughout its lifecycle to help the customer support and maintain it. Knowing what the vendor provides before buying helps to set expectations and determine if what they provide can meet your organization's needs.

Nobody wants to do business with a massive vendor and be nothing more than another customer number to them. Generally, they want concierge-level personalized service that can help them quickly, especially if it is for support. Knowing if there is an outage in the middle of the night and support is called, whether it is going to a 3rd party overseas or landing directly with a company support person, is vital before committing to a purchase.

How easy is the implementation?

It is crucial to know how complex the onboarding process is. Some CDR solutions require dedicated hardware and specialized configurations before they can start service. More advanced ones can be installed with automated processes such as a VM image or docker image on virtualized hardware which dramatically simplifies and speeds up the time to go live. Other ones use a SaaS implementation where everything is ready; you need to point it to what to protect. Depending on the implementation type, products on the market vary from months and weeks to a matter of minutes before they are operational.

This information helps identify how much effort is involved in setting it up and the timelines from the purchase to having the CDR protect your assets.

Does the company have expertise in CDR?

When selecting a CDR product, it is crucial to evaluate the company producing it. If the company offers myriad security or other products in addition to its CDR offerings, it might be a jack of all trades yet master of none. Alternatively, if CDR is their core business, they are more likely to have in-depth expertise and focus on providing a top-tier solution. A focused CDR provider is the best choice for organizations that wish to have a CDR with the best performance and latest features throughout its lifecycle.



Does your CDR work With Remote Browser Isolation (RBI)?

Using Remote Browser Isolation (RBI) allows users to navigate the web safely with a buffer between their system and online threats by creating an isolated environment. This buffer dissolves when users need to download and save files locally, leaving an exposure when no CDR is present to compensate.

Having a CDR solution integrated with an RBI partner allows users to get all of the benefits of the RBI for generalized web browsing while adding on the protection of a CDR for the times when puncturing the airgap is necessary.

Can it improve security metrics?

Security operation centers (SOCs) performance is judged on metrics such as time to detect a threat. A good CDR solution helps improve these metrics by removing the threats early in the MITRE ATT&CK framework or the Lockheed Kill Chain. Both models seek to identify and stop threats in the earliest stages of exposure to reduce potential impact. Eliminating them at initial access rather than after infection occurs dramatically reduces the time to detect, improving operational performance metrics.

Finding an Advanced CDR

[Votiro](#) leads the pack for advanced CDR functionality. Unlike other CDR vendors, Votiro's focus is CDR, it is our specialty, and we strive to ensure our solution is the most reliable out there. With Votiro, your data is quickly and efficiently processed, delivering sanitized files that match the original format without losing file features along the way. Our CDR solution is built to scale, with existing individual customers handling over 70 million files per month without delays impacting user productivity.

[Contact us today](#) to learn more about how Votiro can help you protect your enterprise from malicious data.

About Votiro

Votiro is an award-winning zero trust content security company serving hundreds of commercial and government organizations, worldwide. Votiro Cloud offers an open, API-centric Content Disarm and Reconstruction (CDR) solution to deliver safe content to your modern digital business processes, content-rich applications, data lakes and eliminate file-borne threats targeting remote workers, supply chain collaborations and B2C digital interactions.

Headquartered in the United States, with offices in Australia, Israel, and Singapore, Votiro is trusted by millions of users worldwide to receive content with complete peace of mind. Votiro Cloud is SOC 2 Type II compliant solution and certified by the international standard of Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408). Learn more at votiro.com or connect with us on [Facebook](#), [Twitter](#), and [LinkedIn](#).

