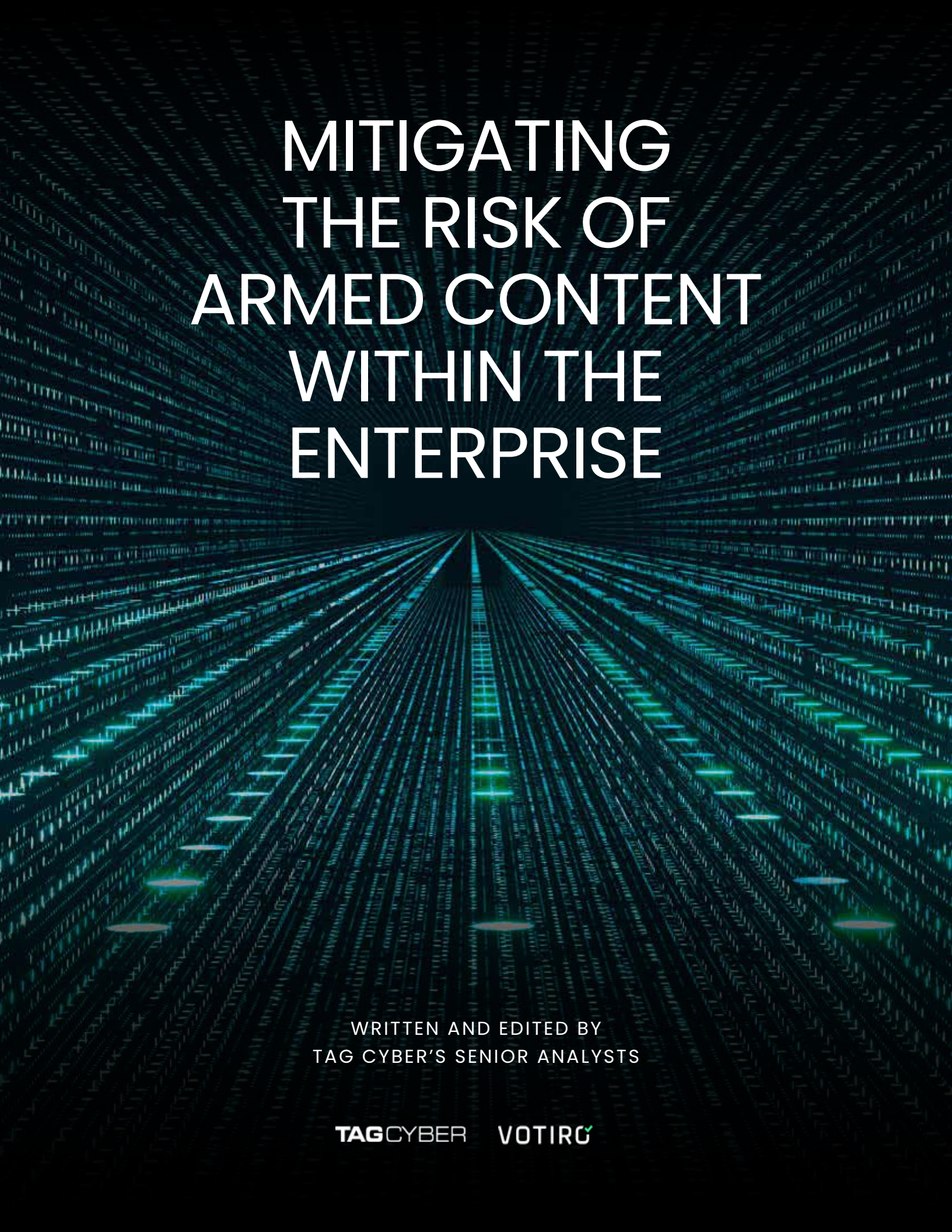


MITIGATING THE RISK OF ARMED CONTENT WITHIN THE ENTERPRISE

WRITTEN AND EDITED BY
TAG CYBER'S SENIOR ANALYSTS

TAGCYBER VOTIRO

INTRODUCTION

Dive into the world of Content Disarm and Reconstruction (CDR) with this comprehensive guide. Here, we'll unravel the fundamental concept of CDR and its pivotal role in safeguarding transmitted files. We'll uncover the lurking threats in today's browsers, shed light on the vulnerabilities of files such as SVG and XML, and touch upon the challenges in email file security and the limitations of contemporary email security platforms.

We'll also delve into automated document processing, emphasizing its significance and potential pitfalls, especially when intertwined with third-party interactions. To wrap things up, we'll offer a strategic roadmap for enterprises, showing them how to implement a CDR solution to achieve the best return on investment.

MITIGATING THE RISK OF ARMED CONTENT WITHIN THE ENTERPRISE

WRITTEN AND EDITED BY
TAG CYBER'S SENIOR ANALYSTS

This book focuses on the nature of Content Disarmament and Reconstruction (CDR), how it addresses the risks around transmitted content, and how enterprises can leverage CDR solutions as part of their business and technology modernization efforts.

CONTENT DISARM AND RECONSTRUCTION – WHAT IT IS AND WHY IT SHOULD BE IN YOUR TOOLBOX

JOHN J. MASSERINI,
SENIOR RESEARCH ANALYST, TAG CYBER

This chapter provides a bird's-eye view of **content disarm and reconstruction (CDR),** illustrating the contrasts between the *known-good* and *known-bad* methodologies. We'll delve into why enterprises should regard CDR as an essential augmentation to their security arsenal and highlight how enhancing security layers might mean transitioning from first-generation "sandbox" technologies, like FireEye, to second-generation counterparts like CDR. A critical takeaway from this section is the ineffectiveness of the dated "detection and response" model, positioning CDR as a forward-thinking approach that casts the CISO as a catalyst for business transformation.

As an increasing number of enterprises move toward modernizing their infrastructures and solidifying their new, post-pandemic business models, unexpected attack vectors have emerged. After decades of throwing network and endpoint-based controls at the problems, we have inadvertently opened brand new delivery mechanisms by which the ever-evolving threat actors are taking advantage.

If we look at a typical enterprise, the long-accepted practice of "defense in depth" is on full display. Firewalls/IPS/Endpoint for the network and Secure Email Gateways (SEGs)/Exchange Antivirus/Sandboxing for email are probably two of the most fundamental architecture models in use.

Modern CDR solutions address both necessities of the modern enterprise while substantially reducing the overall risk from document-born malware risks.

However, as more organizations digitize the entire consumer experience, more and more artifacts are now being delivered only digitally, forcing companies to develop means to ingest these documents as well.

This development is increasingly apparent in the financial industry, where applying for a loan with a significant financial institution involves uploading countless PDFs of checking statements, loan forms, investment accounts, and paystubs – all to a cloud-based portal driven by automated workflows which deliver the documents to the various loan processors within the organization. While the entire process focuses on making it easy for the consumer and the business, the attack vectors in this new world pose significant risks to the enterprise.

THE RISE OF CONTENT DISARMING

In our legacy environments, we almost exclusively used malware and antivirus scanners to dissect email attachments for malicious code. This strategy was effective when email stood as the sole method for sharing documents between companies and customers. Today, thanks to the rise of Microsoft Office 365, Google Workspace, and enterprise upload solutions like FileCloud, JScape, and Filestack, attackers can infiltrate enterprises with malicious documents more easily than before. This situation highlights the importance of CDR.

CDR solutions evaluate documents at the file-structure level, either in cloud-based file repositories, email platforms, or as part of the enterprise's file-sharing solution. CDR further disassembles documents into their various objects, evaluating them for malicious content and reconstructing them once the analysis is complete. These solutions approach file security in two ways: identifying known-bad malware and removing it; presuming the file is bad, and rebuilding it with known-good objects.

CDR solutions that use a known-bad methodology evaluate file objects for malware based on known malicious signatures or heuristics – a very similar approach to the antivirus scanning we're all accustomed to. Unfortunately, such solutions tend to fall into the same trap. With known bad signatures changing so rapidly, keeping them current is nearly impossible, even if leveraging the most up-to-date threat intel feeds.

Conversely, solutions using a known-good approach operate under the assumption that every document contains malware within its objects. After deconstructing these files, these solutions replace file objects with known-good versions, guaranteeing a final file version devoid of malicious content.

A NEW APPROACH TO AN OLD ISSUE

Conceptually, content disarming is an approach whose time has come. Most security teams will acknowledge that signature-based scanning, while still useful for older attacks, fails to identify today's constantly changing attack methods until it is too late. Since the sale of the first sandbox solution, attackers have been finding ways around detonating within them, leaving them virtually useless against today's assailants.

Whether it is email based, a browser upload/download, or a file transfer, malicious documents are finding their way deep into critical areas of the infrastructure. That's why today's enterprises need a modern approach to file security that supports the evolving cloud strategy of the infrastructure while invisibly ensuring that all files are safe to use.

Modern CDR solutions address both necessities of the modern enterprise while substantially reducing the overall risk from document-born malware risks. This includes the level of protection required for unstructured data when it comes to AI, collaboration tools, and digital transformation demands.

Layering on a CDR solution will provide substantial insight into where other platforms are failing – and may ultimately replace the older, outdated technology with one that can address today's threat vectors.

A MODERN APPROACH TO BROWSER PROTECTION

CHRISTOPHER R. WILDER,
RESEARCH DIRECTOR & SENIOR ANALYST, TAG CYBER

Browser security has advanced significantly over the past several years. From local virtualization to sandboxing to cloud-based virtual desktop infrastructure (VDI) solutions, securing the browser has had a well-deserved resurgence. More and more enterprises lack trust in endpoint devices due to BYOD efforts or other productivity-related security concerns. Even in remote access/VDI/zero-trust solutions, downloaded files from the internet can still be malicious, making third-party integration to CDR platform critical.

WHAT IS BROWSER SECURITY, AND WHAT ARE THE THREATS?

A modern approach to browser protection uses a combination of tactics to help protect users from various online threats. Browser protection includes using a secure web browser with built-in features and software to block malicious websites, files, and content to protect against phishing and malware attacks.

Unfortunately, sophisticated attackers bypass perimeter network security controls, such as web/email gateway scanners, by encrypting malicious payloads inside file archives, PDFs, HTML files, and other vectors.

Archive files like ZIP files can be encrypted, making it easier for cybercriminals to conceal malware within and bypass detection tools, especially when coupled with HTML smuggling attacks. Further, threat actors increasingly use script-based malware formats to run malicious code and rely heavily on built-in operating system utilities like file viewers and other utilities to evade endpoint defenses.

CDR is an evolving content security solution that protects against threats from various file types commonly used in online office documents and email attachments. CDR removes potentially malicious content, active code, and embedded objects from a file while preserving the original format and functionality.

Ultimately, this means more malicious emails will land in users' inboxes or web downloads, increasing the risk of cyberattacks. To counteract this, Enterprises should consider deploying CDR technologies.

CDR IS A PIVOTAL AND NECESSARY COMPONENT FOR BROWSER PROTECTION

CDR is an evolving content security solution that protects against threats from various file types commonly used in online office documents and email attachments. CDR removes potentially malicious content, active code, and embedded objects from a file while preserving the original format and functionality.

CDR allows the file to be safely downloaded, handled and shared without risking the endpoint system's or network's security and is often used in conjunction with other hygiene security measures, such as antivirus software and firewalls, to provide comprehensive protection against a wide range of threats.

For example, a recent aggressive bot campaign from the QakBot, Black Basta ransomware, and IceID threat groups used HTML files to direct users to a fake document viewer posing as Adobe and Google Drive. These fake viewers lured victims into downloading a harmful ZIP file; users then entered a password and activated the malicious payload.

A CDR solution unpacks, scans, and remediates the threat before it reaches the user. CDR assumes all files are potentially malicious and scrutinizes all expected files received from outside of the enterprise.

HOW VOTIRO PROVIDES ADVANCED CDR TO ADDRESS TODAY'S BROWSER SECURITY CHALLENGES

Most CDR solutions focus on detecting malware and signatures and incorporate predictive or behavioral analysis to mitigate malicious files and remediate security breaches. However, many of today's CDR solutions are not as effective as they could be when detecting web-based zero-day threats across a broad range of file types without generating false positives.

Votiro's Cloud solution focuses on delivering a comprehensive offering that protects many online and internal file formats, including complex file structures. Because Votiro secures all standard file types, including obscure and challenging files, they stand out where many next-generation antiviruses (NGAV), secure browsers, sandbox solutions, and other CDR providers fall short.

TAG Cyber recommends considering Votiro for any enterprise transferring files and sensitive information among its customers, employees, business partners, and suppliers. Furthermore, their ability to protect users online is a bonus that provides a comprehensive solution to safeguard employees from the browser to the enterprise and beyond.

|Try Votiro Cloud free for 30 days|

ADDING FILE SECURITY TO YOUR EMAIL PLATFORM

JOHN J. MASSERINI,
SENIOR RESEARCH ANALYST, TAG CYBER

Since 2018, the user base of Microsoft Office 365 has steadily grown from 155 million to more than 345 million in 2022. Unlike Google's Workspace, which used a free email platform to promote growth, Microsoft's development arose through migrating large-scale enterprises from legacy on-premise Exchange environments to a cloud-based, O365 experience.

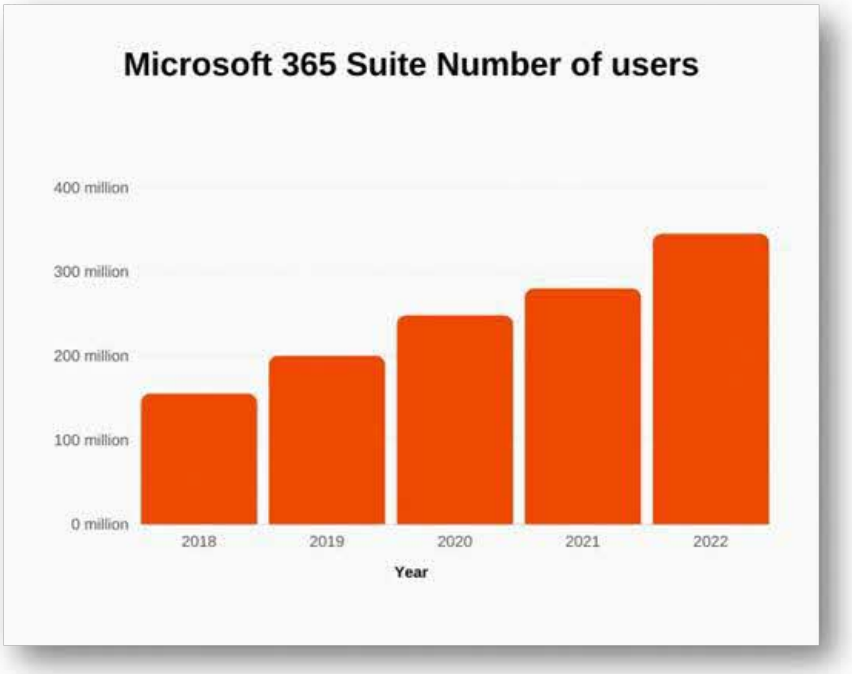


Figure 1: O365 User growth 2018-2022 - @SignHouse

As enterprises increasingly adopt SaaS-based collaboration tools, they must reevaluate their risk mitigation approaches and overall communication strategies. The adoption of modern collaboration platforms will continue and increase over the coming years, so security teams must have a plan to support this fundamental shift.

As these enterprises rationalized their new Software and a Service (SaaS) experiences, they quickly realized that many previously relied-on controls were no longer valid. Secure Email Gateways, antivirus scanning, and email sandboxing, the stalwarts of email security controls, were rendered useless in the new cloud model.

THE NEW COLLABORATION MODEL

As more organizations move towards SaaS-based collaboration platforms, the risk of introducing malware-laced files into the collaboration channel rapidly increases. No longer can security teams rely on inline devices, passive scans, or other legacy alternative solutions to protect enterprise communications.

One of the most challenging aspects of protecting an enterprise today is the amount of unstructured data shared amongst employees, business partners, third parties, and customers. As these SaaS collaboration tools become more ubiquitous, documents, spreadsheets, PDFs, and presentations all move in and out of the enterprise with barely a second glance. They consistently move across collaboration platforms and undergo reading and modification on various devices with unclear origins. Indeed, an enterprise remains unaware of a document's journey, changes, or contents.

For several decades, many enterprises have relied upon "sandboxing" techniques to capture and detonate potentially malicious file attachments within emails, networks, and web gateways. While these solutions were somewhat effective initially, attackers did not take long to figure out how to slip past them, either through timed detonation, virtual environment detection, encrypting and password-protecting files, or simply waiting for other events to trigger them. While many modern sandboxing solutions are in the market today, they generally all fall victim to a determined attacker trying to avoid them.

THE CALL FOR CDR

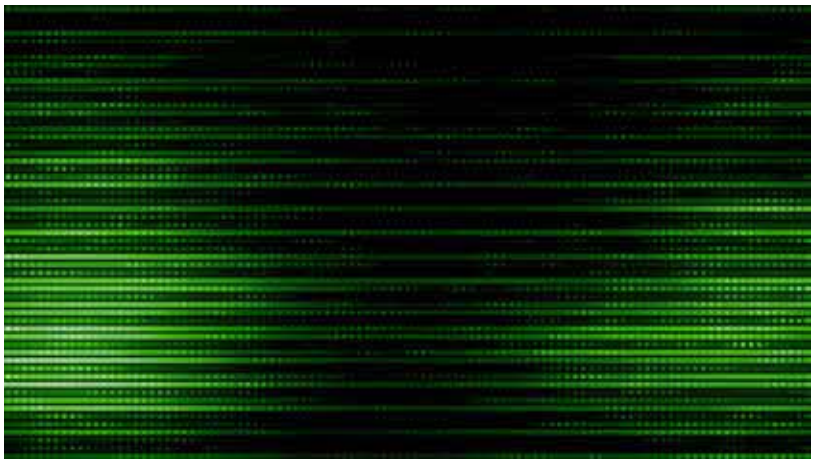
Today's enterprises need a far more effective solution that covers all of the organization's communication channels, not just email. This is where a modern CDR solution shines. Where Secure Email Gateways, Exchange antivirus scanners, and sandboxes all focused on email, modern enterprises leverage everything from Office 365 and Google Workplace to Slack, Zendesk, Salesforce, and Box – along with dozens of other collaboration platforms, all capable of transferring unstructured data files in and out of your company.

Unlike the old method, where you search for and remove malicious objects within files, CDR solutions take the known suitable components from a file and rebuild it using those trustworthy parts based on a standard, trusted template. This approach ensures full document functionality without any embedded malicious objects that might detonate unexpectedly, and works seamlessly with all modern, API-enabled collaboration channels –

irrespective of the file transfer method. Companies now conduct much of their business over platforms like Slack, MS Teams, or Google Chat. Overlooking this channel in your data security program can substantially affect your content security strategy.

Additionally, a CDR solution can also empower your internal business process by enabling customer self-service by facilitating customer uploads of financial documents, healthcare records, or any other kind of document needed – all while knowing the documents will be completely safe and sanitized by the time the employees review them or the automated workflow ingests them. Gone are the days of subversive malware bringing your automation workflows to a grinding halt.

As enterprises increasingly adopt SaaS-based collaboration tools, they must reevaluate their risk mitigation approaches and overall communication strategies. The adoption of modern collaboration platforms will continue and increase over the coming years, so security teams must have a plan to support this fundamental shift. Integrating SaaS solutions with a cloud-based CDR platform is paramount to ensuring that it is possible to share documents and unstructured data in a way that securely aligns with modern business processes.



DESIGNED TO BE BREACHED– AUTOMATED DOCUMENT CONSUMPTION

DAVID NEUMAN, SENIOR ANALYST, TAG CYBER

The use of automated document consumption and data extraction processes presents the opportunity for greater business efficiency, lower cost of process ownership, positive customer experience, and, wait for it…risk of cyber exploitation and material business impact. Automated document consumption is the process of importing or extracting valuable information from varied manual formats. Companies spend an extraordinary amount of time on manual form processes that are costly, inaccurate, and time-consuming. Imagine the environment where a business integrated workflows and efficiently consumed or extracted data from documents. There are many industries on this journey. The Value of Automated Document Consumption

THE VALUE OF AUTOMATED DOCUMENT CONSUMPTION

In the healthcare sector, numerous forms come with free-form text, lengthy paragraphs, checkboxes, and tables. Among the most sensitive in this field are prescriptions. It is vital to guarantee the precision of protected data, especially when it holds crucial details about medications or medical treatments. This accuracy becomes even more critical to patient safety when data moves between different entities – not to mention the many scripts that travel digitally between entities.

Imagine the potential patient's experience during an appointment when a doctor asks the patient to fill out a paper form, knowing that data already exists in their medical record. If they need to see a specialist, they need the information in other electronic documents, a data lake of images, or

Automated document processing can transform the patient experience, enhance the quality of care, and drastically reduce costs. This transformation becomes apparent with the increasing embrace of cloud data and digital content management services

medical systems. The experience of similar data in different forms updated by different entities is not only a miserable experience but potentially dangerous to patient safety and well-being.

Automated document processing can transform the patient experience, enhance the quality of care, and drastically reduce costs. This transformation becomes apparent with the increasing embrace of cloud data and digital content management services, enabling organizations to capture, distribute, and utilize data and collaborate efficiently with third-party business partners.

Other industries, such as chemical and utilities, have been keeping records for decades, containing valuable information about business operations, maintenance records, and safety standards. The documents have a mix of text and images, making producing a document pipeline challenging. In insurance, fields such as estimates for repairs, property addresses, case identity numbers from sections of a document, or classification documents on claims between parties are areas of opportunity to improve processes.

WHAT ARE THE RISKS OF AUTOMATED DOCUMENT CONSUMPTION?

All these examples make the opportunities for automated document consumption very enticing, but as with other technologies and digital transformations, it is not without its risks – nothing is without risk. Most security problems are data problems, making this area ripe for cyberattack and exploitation. Some of the dangers are traditional such as data corruption through uploading malware or compromising access to sensitive data. This can also lead to ransomware attacks on large data repositories.

Unbeknownst to customers, many service platforms that provide data sharing, collaboration, and orchestration are not scanning for these kinds of threats natively – and many threats are undetectable via scanning. It is the customer's responsibility to protect their data in shared security models that are long overdue to be updated. This risk becomes even more complex when dealing with third- and fourth-party relationships.

These technologies and process transformations also present challenges for developers. Those who rely on vast data lakes in the cloud where the file uploads to the developer space need cleaning before ingestion into the data lake.

So, who shoulders this responsibility, what frameworks ensure the security and integrity of data, and who steps up when anomalies or breaches arise in multi-organizational or multi-national scenarios?

It is not sufficient to land a solution for automated consumption, especially for sensitive information, that doesn't clarify the protection capabilities in process and technology. Today's environment presents all these challenges. Sometimes, one solution can generate unforeseen problems.

As document consumption becomes automated at scale, it has the potential to change the stateful condition of information. For example, an application process for a position of high trust in an organization may require information on a person's credit, criminal background, current and previous addresses, financial investments, friends, family, acquaintances, etc. Together, the stateful condition of this application is highly sensitive. All this information requires verification and spawns other processes (i.e., breaking up the data into smaller pieces, possibly other forms given to third parties).

Let's say a third party or service takes on the task of address validation. While this information might be less sensitive, if someone finds a discrepancy and fills out another form with potentially harmful details, the information's status becomes highly sensitive again. This potential shift arises from the increased efficiency in document consumption and might introduce previously unknown risks.

SOLUTION CONSIDERATIONS IN PLANNING THE USE OF AUTOMATED DOCUMENT CONSUMPTION

Does the CDR Solution Integrate with Content Collaboration Tools and Platforms?
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 various software solutions, incorporating CDR protection every time users share files.

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 lead 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.

How Does CDR Handle Password-Protected 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. The file is temporarily stored with an advanced CDR solution, 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. This process passes no harmful elements into the organization while only temporarily obstructing transmission.

Does Your CDR Work with Remote Browser Isolation (RBI)?
By creating an isolated environment, RBI allows users to navigate the web safely with a buffer between their system and online threats. Having a CDR solution integrated with an RBI partner will enable users to get all the benefits of the RBI for generalized web browsing while adding on the protection of a CDR.

Can it Provide Security Metrics?
A good CDR solution helps provide security metrics by removing the threats early in the MITRE ATT&CK framework. This framework seeks to identify and stop threats in the earliest stages of exposure to reduce potential impact. Eliminating them at initial access rather than after infection dramatically reduces detection time, improving operational performance metrics. Additionally, integrating this data into security operations helps provide leading intelligence indicators on attack vectors against an organization.

What Analytics Does the Platform Provide?
Given the volume of data orchestrated by a CDR platform, analytics should be able to identify trends in the throughput of files, sizes, and types. For example, huge files being transferred instead of using cloud storage. In addition, analytics can surface insights on threats found within files that the platform blocks. Highlighting suspicious files from a specific source or through a particular application can be an essential indicator for cyber defenders or threat hunters.

Solutions within various platforms and against diverse threats aren't just an option—they're necessary. The dynamic relationship between CDR and collaboration tools, compromised vendors, password-protected files, Remote Browser Isolation, and security metrics illuminates a proactive and adaptive security path. It emphasizes not just defense but a transformation in the way we approach cybersecurity, moving from reactive measures to anticipatory strategies.

By considering these aspects, businesses are fortifying their current security measures and investing in a resilient future, turning potential vulnerabilities into opportunities for enhanced protection and intelligence. This shift reflects a maturing and forward-thinking cyber defense culture, pivotal in the age of relentless digital innovation and threats.

AN ENTERPRISE ACTION PLAN FOR CDR

DAVID NEUMAN, SENIOR ANALYST, TAG CYBER

Information is the lifeblood of 21st-century businesses. They depend on safely and securely collecting, collaborating, sharing, and using information as part of every business or operational process. The vastness of unstructured data that businesses use also makes them susceptible to risks from cyber threat actors seeking to steal, exploit, or destroy that information.

In this chapter, we'll outline how organizations can develop an enterprise action plan on how to leverage CDR technology to analyze and protect that information so it can continue to drive business success.

ADOPTION OF MODERN COLLABORATION PLATFORMS

The adoption of modern collaboration platforms has grown exponentially over the last five years. With the rise of remote work and the need for remote collaboration, the demand for these platforms has increased dramatically. Here are some key growth trends:

- **M365:** According to Microsoft's FY2022 Q3 report, Microsoft 365 has grown to 345 million paid seats in 2022 - up from 258 million seats in 2020.
- **Google Workspace:** According to Google, more than 3 billion monthly active users now use the G Suite platform in 2022, which includes Google Docs, Sheets, and Slides. This represents a significant increase from the 1.5 billion active users reported in 2018.
- **Slack:** As of 2023, Business of Apps reports over 18 million daily active users in 156,000 organizations.
- **Dropbox:** According to Dropbox's 2022 Q4 earning report, paying users ended at $17.77 million compared to $16.79 million for the same in 2021.

The adoption of modern collaboration platforms has grown exponentially over the last five years. With the rise of remote work and the need for remote collaboration, the demand for these platforms has increased dramatically.

Overall, various factors drive the growth of online collaboration platforms, including the rise of remote work, increased focus on productivity and efficiency, and the need for more effective ways to collaborate and communicate across geographically dispersed teams. Online collaboration is also accelerating the increase in attack methods by cyber threat actors seeking to exploit this rapid adoption.

HOW DOES CDR MITIGATE THREATS IN DIGITAL COLLABORATION?

Traditionally, organizations relied on malware and antivirus scanners to pull apart email attachments and determine if malicious code is buried within them to protect enterprises from falling victim to the delivery of cyber weapons. Organizations have recently relied on Endpoint Detection and Response (EDR) to detect malicious files once they land on their endpoint systems. This approach worked well for businesses primarily using email to share documents with companies or customers. However, with the rapid adoption of collaboration platforms and other means of cloud-based file ingestion, the ability of an attacker to infiltrate an enterprise with malicious documents is as easy as ever – and this is where CDR can add significant value.

CDR solutions evaluate documents at the file-structure level, either in cloud-based file repositories, email platforms, or as part of the enterprise's file-sharing solution. CDR solutions disassemble documents into their various objects and evaluate the objects individually for malicious content and known-good content, reconstructing them once the analysis is complete.

The most advanced CDR solutions approach file security by presuming all incoming files are bad and rebuilding them with known-good objects. Solutions that leverage a *known-good* approach presume every document has potential embedded malware within its objects. In this case, following deconstruction, known-good file objects are transferred onto a clean file template, ensuring that the final version of the file is free from any malicious content.

AN ENTERPRISE APPROACH TO IMPLEMENTING CDR

As with any technology implementation, an enterprise action plan must ensure the realization of all the benefits and demonstrate a value return throughout the enterprise. This kind of plan starts with understanding the need for CDR technology. Businesses should ask: **How important is information collection, collaboration, and sharing (even with external parties)?**

Following insights from this question, **ask if your organization is protecting information used across all its collaboration platforms and channels, internally and externally.** While these are the necessary questions, there are deeper considerations of an enterprise action plan.

How does integration with cloud systems and data lakes work? Not every CDR can integrate with more complex environments like 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 rare.

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 the protective capabilities of the CDR.

Integrating CDR with Content Collaboration Tools and Platforms: Content collaboration platforms such as Box, O365, Microsoft Teams, and Slack remain uncontrollable for many traditional security controls. Alternatively, security vendors that provide an Open API can integrate CDR support into various software solutions, incorporating CDR protection every time users share files. This approach creates a true Zero Trust solution as it sanitizes every file, whether or not they are known to be malicious.

File types supported: 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 familiar. Knowing how the CDR solution handles more obscure file types is essential. Less savvy CDR products may not be able to assess them properly and either block them by default or let them through because they do not understand what components are known safe. A CDR solution must offer extensive format support, especially those commonly used for your organization.

Ensure content and format don't get lost in the CDR Process: CDR solutions that are less complex strip away large portions of files when they detect potentially harmful signatures. More advanced CDR solutions preserve all safe content, ensuring no crucial data disappears. 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 retain all of the contexts that the format and layout convey.

Volumes of data required for your business: Businesses handle massive volumes of data daily, from email to file collaboration and cloud storage – processing and assessing this information flow must happen quickly to ensure workers can do 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. CDR solutions must effectively handle large volumes of data.

CONSIDER A COST-BENEFIT ANALYSIS

The cost-benefit analysis of using a CDR solution will depend on various factors, such as the size and complexity of the organization, the number of users who will be utilizing the solution, the cost of security practitioners, and the potential loss of productivity. However, we do know about some costs. According to Statista's Cybersecurity Outlook, the global cost of cybercrime will likely surge in the next five years, rising from $8.44 trillion in 2022 to $23.84 trillion by 2027. And according to the 2023 IBM Cost of a Breach report, the average cost of a breach is $4.45 million.

BENEFITS OF A CDR SOLUTION

A CDR solution offers multiple advantages. Firstly, it significantly reduces the risk of malware infections by being specially designed to extract potentially malicious content from files, which minimizes the chances of experiencing data breaches or other security incidents. Secondly, it boosts productivity. Users can work more seamlessly as the solution eliminates the need for manual file analysis, wipes out malware alerts in files, and sanitizes files by removing possible threats automatically. Lastly, it aids in enhancing compliance. Organizations can more easily adhere to data privacy or cybersecurity standards with the assistance of a CDR solution.

COST OFFSET OPPORTUNITIES

When evaluating the cost dynamics of implementing a CDR solution, several opportunities arise to offset expenses. Consider the licensing fees for products within your enterprise that might not fully meet all data collaboration needs – these fees may counterbalance the investment in a CDR enterprise solution. Additionally, a CDR solution can provide enhanced features and functionality for organizations looking to modernize or replace their secure email gateway.

Furthermore, the costs associated with developing, delivering, administering, and maintaining products and platforms that don't offer universal integration across the enterprise can be higher than those of a well-integrated CDR solution.

TAG Cyber recognizes the intricacies in this vital domain for business success. Votiro stands out as a proactive partner, adeptly addressing current security challenges while catering to enterprises' burgeoning digital needs.

ABOUT TAG INFOSPHERE

Founded in 2016 by Dr. Edward Amoroso, former executive at AT&T Bell Labs, TAG Infosphere is a trusted research and advisory firm, providing unbiased insights and recommendations to commercial vendors, government agencies, and business groups. The focus at TAG Infosphere is on three areas of considerable importance to our world: Climate Science (TAG Climate), Artificial Intelligence (TAG AI), and Cybersecurity (TAG Cyber). TAG Infosphere bucks the trend of pay-for-play research by offering in-depth analysis, expert consulting, and personalized content based on thousands of engagements with clients, all from a practitioner's perspective.

ABOUT VOTIRO

Votiro is a Zero Trust Content Security company trusted by industry leaders around the world to deliver billions of safe files between commercial and government organizations, their employees, and the customers that rely on them. The Votiro Cloud solution is an open-API that detects, disarms, and analyzes content at the speed of business – delivering teams with fully-functional files, reduced risk, lower costs, and increased productivity. Votiro Cloud proactively eliminates file-borne threats targeting email environments, collaboration platforms, data lakes, supply chains, web downloads, B2C digital interactions, and more.

Votiro is headquartered in Austin, TX, with offices in Australia, Israel, and Singapore. Votiro Cloud is SOC 2 Type II compliant and certified by the international standard of Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408). Learn more at **www.votiro.com.**

IMPORTANT INFORMATION ABOUT THIS DOCUMENT

Contributors: John J. Masserni, David Neuman, Christopher R. Wilder

Publisher: TAG Cyber, a division of TAG Infosphere Inc., 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman at lgoodman@tag-cyber.com to discuss this report. You will receive a prompt response.