VOTIRO

The Security Architect’s Guide to File Sanitization

Security architects defending financial organizations have a daunting task. They must ensure that all data is secure in the face of outside threats and simultaneously maintain compliance. For most organizations, this is already challenging, but the financial sector is a prime target for cybercriminals based on the vast quantity of instantly valuable data that they store and process daily. According to 2023 research by Verizon, the finance sector accounts for a significant percentage of data breaches, and as the report states, with threat actors gaining access without too much effort at all. IBM data breach research reveals that financial institutions commonly fall victim to attacks through email attachments, compromised websites, and other file-based attack vectors.

In this report, we will explore the challenges financial organizations have with stopping hidden threats and suggest methods to prevent these threats from leading to security incidents.

Hidden Threats Facing Financial Institutions

Financial institutions are highly susceptible to a plethora of hidden threats orchestrated by cybercriminals, positioning them as attractive targets for malicious activities. The sheer magnitude of hidden threats concealed within files is a matter of grave concern. Extensive studies have unveiled the astonishing volume of these threats, shedding light on the gravity of the issue at hand. These covert dangers can unleash chaos by pilfering sensitive data, subjecting it to ransom demands, or surreptitiously implanting backdoors, granting unauthorized access to cybercriminals who exploit vulnerabilities within the institution's systems. The repercussions of such attacks can be catastrophic, leading to substantial financial losses, with the average cost of a breach estimated to be a staggering $4.35 million. This does not even include the damage to the targeted financial institution's reputation that impacts customer growth and retention.

Data Loss

Sensitive data such as personally identifiable information (PII), financial account particulars, and invaluable internal secrets like trade information are at the heart of operations for financial institutions. This data is not collected on a whim but is a necessary portion of their operations, facilitating loan applications, opening accounts, and meeting numerous compliance mandates that reduce fraud and abuse. Unfortunately, storing this data comes with added risk as any exposure has severe consequences for their customers and, ultimately themselves.

According to Verizon research, cybercriminals are primarily motivated by financial gain. They recognize the value of this data and how quickly it can be exploited for fraudulent activities, identity theft, and direct financial theft, damaging customers and the organization itself. Whether the exposure comes from external cybercriminals or internal abuse, financial institutions face the risk of reputational damage and the legal liability associated with the loss and misuse of such data. Protecting and securing this information is paramount to safeguarding the institution's integrity and maintaining customer trust.

Compliance Challenges

Unlike most industry verticals, financial organizations are highly regulated, making compliance more challenging. They face a variety of legal and regulatory mandates that must be addressed, each of which comes with severe repercussions for any failure to comply. These compliance failures come from not taking appropriate steps in security and processes and can also come from accidental disclosures due to cyberattacks.

Some of these regulations include the Sarbanes-Oxley Act (SOX), which is a US federal law imposing obligations on public companies to maintain accurate financial records and implement internal controls to prevent fraud. Similar to this is the Gramm-Leach-Bliley Act (GLBA), which mandates financial institutions to safeguard the privacy and security of customers' personal information. Payment Card Industry Data Security Standard (PCI-DSS) regulations dictate protecting payment card data and user information, but unlike SOX and GLBA are put out by a private group rather than the government. Additionally, the General Data Protection Regulation (GDPR), applicable in the UK and EU, focuses on safeguarding personal information privacy and enhancing control over data sharing and usage.

Hitting the Bottom Line

The impact of a data breach on businesses goes far beyond the immediate aftermath. Research shows that companies experiencing a breach tend to underperform the market significantly for an extended period. According to a study by Comparitech, businesses that fall victim to a data breach can see their share price drop by an average of 15% and struggle to recover for up to three years after that. This decline reflects the erosion of investor confidence and the long-lasting consequences of compromised security. Moreover, the repercussions extend beyond the financial realm, as companies often suffer from a loss of customers. When customer data is compromised, trust is shattered, and individuals may seek alternative options, resulting in a decline in customer loyalty and potential revenue.

Paths of Ingress

Financial organizations face numerous paths of ingress through which dangerous hidden threats can infiltrate their systems, bypassing traditional perimeters and security measures. They present potential vulnerabilities that threat actors can exploit to gain unauthorized access and inflict damage. From unsecured endpoints and employee devices to compromised third-party applications and services, each represents a potential entry point for hidden threats. Social engineering techniques, such as phishing emails or malicious links, can also deceive employees and lead to inadvertent breaches. Moreover, supply chain attacks targeting software vendors and suppliers can introduce hidden threats directly into the organization's infrastructure.

Primary Threat Vectors for Cyberattacks

Email

Email remains one of the most prevalent attack vectors for hidden threats, posing significant organizational risks, with the median organization receiving over 75% of its malware via email. Malicious actors often leverage email to deliver hidden threats, disguising them as seemingly harmless attachments such as documents or images. These attachments may appear innocuous to unsuspecting recipients, but they contain toxic code designed to exploit vulnerabilities and compromise systems. The widespread use of email makes it an attractive target for attackers, enabling them to target many potential victims with a single campaign. Studies have shown that email is one of the top two vectors for not just cybersecurity incidents but actual breaches.

Web Downloads

Web downloads present a significant risk regarding hidden threats, mainly as employees rely on gathering information from the internet as a vital aspect of their job responsibilities. Unfortunately, online resources are often unsafe, being infected with hidden threats. Malicious actors often target less secure websites and compromise them to upload infected content, strategically focusing on sites attracting users within specific industries. In the financial sector, this could include blogs with financial-specific topics, discussion boards frequented by individuals in the fintech vertical, or websites offering financial-specific data. These targeted attacks exploit the trust employees place in legitimate online sources, making it crucial for organizations to prioritize web security measures.

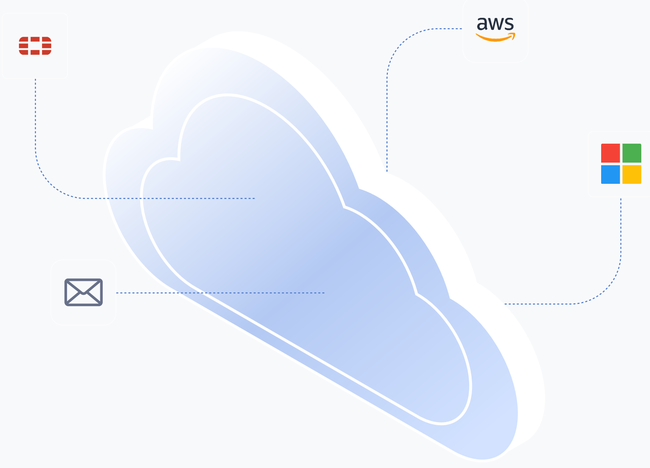
Files Uploaded to Data Lakes

Files uploaded to data lakes pose a significant risk in various industries, including the loan and insurance sectors, where collecting applicant data is a crucial part of the process. This collection includes large volumes of sensitive data such as identification, asset verification, and employment information. As these files all come from uncontrolled sources, there is a strong possibility that they harbor hidden threats.

Users often directly submit these files to web interfaces which amalgamate them back to servers or cloud storage, in many cases ultimately ending up in data lakes for processing. When users proceed to process these files, they unknowingly open themselves up to the harmful content within. Opening these files triggers the launch of hidden threats, exposing the organization to potential breaches, data loss, or other malicious activities. For individuals processing these sensitive files, the likelihood of sensitive data being exposed to cybercriminals is much higher, increasing the potential impact.

Content Collaboration

Content collaboration tools have become essential for teams to maintain connectivity and productivity, especially in remote or mobile work environments. However, these tools also introduce a potential risk regarding hidden threats. Users may unknowingly share harmful files, which can rapidly spread infections throughout the organization. This poses a significant challenge for security perimeters as content can propagate quickly and easily within the collaboration environment. The seamless and rapid nature of file sharing within these tools can make detecting and preventing the spread of hidden threats difficult.



slack Trello Dropbox monday.com OneDrive box

Stopping Hidden Threats With CDR

Content Disarm, and Reconstruction (CDR) is a powerful solution for stopping hidden threats before they breach secure perimeters. Unlike traditional detection-focused solutions, CDR takes a proactive approach by focusing on thoroughly sanitizing and rebuilding files from known safe components. This approach eliminates the risks associated with relying solely on detection, as it does not rely exclusively on recognizing known threats but neutralizes any potentially harmful content. One of the key advantages of CDR is its seamless protection, which requires no user intervention.

By sanitizing files at the entry point, CDR effectively neutralizes known and zero-day threats, offering robust protection against the ever-evolving threat landscape. Moreover, the rebuilding process in CDR ensures that safe and functional aspects of files, such as formatting, formulas, and even some macros, are preserved while eliminating any hidden risks. This provides that organizations can safely utilize files without compromising security or functionality.

Protecting Email Flow

CDR is critical in protecting email flow by blocking incoming emails and internal storage where users access their messages. By seamlessly integrating into the email flow, CDR ensures that threats are stopped as they enter the organization's network. Through its seamless sanitization process, CDR eliminates any hidden threats or malicious content from incoming emails, ensuring the data reaching users is clean and free from potential dangers. This proactive approach prevents the dissemination of hidden threats through email communication channels and safeguards sensitive information from being compromised.

Sanitizing Browser Input

Browsing the web puts users in touch with a vast volume of information and content which helps them stay ahead of trends and rapidly answer questions related to their job. However, there is a persistent risk of hidden threats lurking in any of the provided content. CDR sits between the end user and the vast internet, eliminating threats before they reach the browser.

By routing all web traffic through the CDR system, incoming information is automatically sanitized in real-time as it flows into the organization's network. This approach allows users to browse the web as they usually would, without the need for cumbersome isolation environments or virtual browsing solutions. They can go about their business, using the internet to facilitate their work, remaining protected while unaware of the seamless shield sanitizing their web traffic.

Defending Cloud-Stored Data

When defending cloud-stored data, CDR offers a multi-faceted approach to address the challenges data lakes and cloud storage face. Firstly, CDR acts as a protective layer between web ingestion and storage, actively sanitizing the content as it enters the organization's system. CDR ensures that only clean and safe data is stored in the cloud by intercepting and neutralizing potential threats in real-time.

Additionally, CDR can eliminate threats from existing data stores, providing a comprehensive defense against hidden dangers that may have already been present in the stored data. This is particularly crucial in scenarios where data lakes and cloud storage can accumulate vast amounts of information over time, whether through mergers and acquisitions or regular operations, ensuring that even old data does not pose a threat.

Seamless Collaboration Protection

Seamless collaboration protection is a crucial aspect of content security, and CDR is an API solution that seamlessly integrates into collaboration platforms. By sitting in between collaboration efforts, CDR ensures that file-sharing activities are continuously sanitized in real time as they occur. This means that users can freely share data and resources within the collaboration environment while having the assurance that any shared content is thoroughly cleansed of hidden threats.

CDR's role becomes even more valuable when collaborating with external partners, vendors, and other entities outside the organization's security perimeter. In such scenarios, where the organization has limited control over the security posture of external parties, CDR acts as a robust safeguard, neutralizing any potential threats present in the shared content. This allows for secure and efficient collaboration without compromising the organization's security posture or introducing unnecessary risks.

Seamless Data Protection

As a top target, financial organizations need top-tier defenses for file sanitization and CDR. Votiro, a leader in the CDR field, provides cutting-edge protection as CDR is its focus rather than another feature in a suite of tools. Votiro's advanced CDR generates high-quality reconstruction by rebuilding files with intact, safe functionality, ensuring that no necessary context or functionality gets lost in the rebuilding process.

Financial organizations don't have time to wait on complex configurations and installations, which is why Votiro is designed for rapid implementation. It uses an API-centric solution that seamlessly integrates into existing business workflows, enabling immediate protection against cyber threats. Implementation times are impressively short, with SaaS installations taking as little as 10 minutes and on-premises installations taking just 90 minutes.

Votiro Cloud

Votiro goes beyond CDR, integrating optional AV and RetroScan, which generates auditable tracking of threats eliminated by Votiro as they become discoverable by AV. With Votiro's well-established CDR solution, financial institutions can achieve a proven return on investment, meeting their stringent performance requirements while effectively safeguarding customers against hidden threats.

Want to Learn More About Votiro?

Contact us to see how we set the bar when it comes to addressing hidden threats in files.

Or, if you're ready to try it out for yourself, you can skip right to a free 30-day trial of Votiro Cloud.