VOTIRO

GUIDE

Integrating Votiro Into Your Existing Security Architecture

Introduction

Cybercriminals consistently innovate, attempting to bypass advanced security measures by embedding malicious code in seemingly harmless data. Their prey, regular businesses, are aware of these threats but struggle to counter the 450,000 new malware instances identified daily. They are caught at a crossroads, seeking to bolster their current defenses without discarding or replacing existing infrastructure—a daunting task considering the significant investments already made.

Many existing security technologies already excel at what they were explicitly designed for and need a way to cover where they are weak. The solution for savvy organizations is not to replace and exchange but to augment.

Votiro is unlike other security technologies. It is engineered to augment and enhance existing security measures. With a unique focus on prevention and augmentation, Votiro adds value to current security infrastructures, amplifying strengths while shoring up potential weaknesses. As a result, organizations are empowered to build upon their security investments, achieving a robust, comprehensive defense against known and hidden malware threats.

! **With Votiro, it’s about strategic augmentation rather than disruptive replacement.**

Cautious Changes in Security Investments

In the current cautious economic climate, decisions around security investments are far from arbitrary. Organizations deeply understand that replacing existing infrastructure comes with significant financial, operational, and temporal costs. Furthermore, replacing or removing security solutions can introduce an array of problems and disruptions. This situation often results in organizations feeling trapped in a must-upgrade scenario, creating insecurity and uncertainty.

The following sections aim to address these valid concerns and reassure organizations that an alternate, more effective approach exists. Instead of a complete replacement, organizations can enhance what they already have, thereby preserving their investments while boosting their security.

Investments Were Made

Organizations have already committed substantial resources to purchase and deploy various security measures. While these solutions may not always effectively identify hidden threats, they often address other critical security concerns or enable postlaunch threat remediation. Most organizations have invested significantly in these security measures spending an average of 9.9% of their IT budget on cybersecurity, marking a considerable stake in their overall expenditure. It’s crucial to note that prematurely discontinuing these solutions before they reach their end-of-life (EOL) can result in wasted cost, directly impacting the organization’s bottom line.

Therefore, finding ways to augment these existing measures, rather than replace them, can better protect this investment and offer more robust security solutions.

Replacement is Disruptive

Deploying a new security solution may introduce disruption, potentially leading to service outages, periods of vulnerability, or even simultaneous operation of old and new systems that can result in conflicts and system failures. Each of these can have severe implications on business continuity and data integrity. Beyond this, substantial resources were invested in setting up and configuring existing systems - efforts that could go to waste if the systems suddenly get replaced.

Furthermore, introducing a new security solution necessitates re-training users and getting their buy-in for the new system. This time-consuming process adds another layer of complexity and potential downtime to operations as users convert over.

Political Costs

The decision to remove or replace technology investments to meet specific security goals before their End of Life (EOL) can lead to considerable political costs within an organization. Board members and executives may start to question the acumen of the security leadership. They might wonder, were previous investments imprudent? Board members consider the inherent risk and uncertainty of what would happen if they purchase new technology to replace the old. Can they be sure that these new technologies will not be suboptimal choices as well? Such concerns can create an environment of doubt and hesitation around decision-making, affecting not just security but the organization's overall strategic direction.

Augmentation Rather Than Replacement

Votiro was designed with a unique principle in mind - to augment, not replace. It recognizes the value of the existing security solutions that organizations have in place and aims to enhance their effectiveness. Unlike many other solutions on the market, Votiro does not purport to be a catch-all security silver bullet, claiming to solve every aspect of cybersecurity. Instead, Votiro excels at one thing: preventing malware from hitching a ride into an organization on files.

This is achieved through Votiro's category-leading **Content Disarm & Reconstruction (CDR) technology.**

This concentrated focus allows Votiro to deliver an outstanding, unparalleled CDR solution. In doing so, Votiro can work in harmony with other security solutions already in place, allowing them to excel in their specialized areas. While these tools address their specific security domains, Votiro strengthens the overall security posture by shoring up areas where they may fall short. The result is a comprehensive and resilient security architecture built on the foundation of existing investments and boosted by the added power of Votiro's exceptional CDR capabilities.

> **Votiro excels at preventing malware from hitching a ride into organizations via files.**

What is CDR?

CDR, the primary focus of Votiro's offering, is a proactive cybersecurity technology that disarms potential threats hidden in files and then reconstructs the same files into safe versions. This process involves extracting known-safe elements from a file, which automatically eliminates harmful content, and recreating a perfectly usable file without said potential threats. The efficiency and precision of Votiro's CDR approach ensure that hidden malware threats, including zero-day exploits, are neutralized without affecting the file's functionality. This is done without relying on detection, allowing the elimination of zero-day and previously undiscovered threats.

Simple API Integrations

Votiro takes the hassle out of integrating new security solutions. Unlike many security tools that require additional hardware or time-consuming deployment, Votiro's cloudbased solution can swiftly and seamlessly integrate into your existing infrastructure via API integrations. There's no need for time-intensive deployment or exhaustive installation processes requiring complex configurations. Simply update your existing configurations, and Votiro becomes an integral part of your IT stack, working diligently in the background to sanitize your data.

This streamlined process ensures that the addition of Votiro's security solution is not just effective but also efficient and economical.

Seamless Operations

One of the most remarkable aspects of Votiro's security solutions is their seamless operation. Uniquely designed to operate efficiently behind the scenes, Votiro's technology requires no intricate training or behavioral changes from end users.

This means that protection is not a task on a checklist that one can forget or skip but an automatic, continuous process that ensures all content is sanitized by default.

The value of Votiro's solution is realized instantaneously. With its smooth integration into your current system, the time to value (TTV) is immediate. Additionally, the lack of training time means your organization can focus on core tasks while benefiting from advanced security measures. In essence, Votiro enhances your security posture without disrupting the flow of your operations or imposing on your existing security ecosystem. It is a solution designed with the modern organization in mind, balancing robust security and operational efficiency.

Uniquely designed to operate efficiently behind the scenes, Votiro's technology requires no intricate training or behavioral changes from end users.

Building on Common Security Solutions

As we delve into the common security solutions that many organizations already have, we must appreciate the value these existing measures offer. These solutions, each with unique capabilities and advantages, form the bedrock of an organization's defense mechanism against cyber threats. However, no security measure is entirely foolproof; even the most sophisticated systems can have blind spots or vulnerabilities.

Here's where Votiro steps in. As a complementary layer to your security infrastructure, Votiro enhances and fortifies these measures, providing comprehensive coverage against known and hidden threats.

Antivirus

Antivirus (AV) software is critical to many organizations' security infrastructure. Known for its adeptness at detecting and mitigating known, cataloged threats, AV is fast, accurate, and exceptionally effective at safeguarding traditional endpoints. However, AV solutions have limitations. AVs frequently grapple with effectively detecting and mitigating zero-day exploits and other unprecedented threats. Their behavioral detection functions usually necessitate malicious content to begin damaging activities before any intervention occurs.

One of the challenges is the lag in AV updates. Even comprehensive platforms like VirusTotal, which gather data on all recognized viruses across multiple providers, have limitations. They cannot preemptively identify novel zero-day threats since they solely operate on previously identified data. This lag and limitation create a tangible window of opportunity for cyber attackers, leaving systems vulnerable.

Votiro understands these challenges and builds upon the existing strengths of your AV solution. As part of our approach, we Detect, Disarm, and Analyze content, either working in concert with your AV or by bringing our AV solution. Rather than waiting for the threat to manifest, Votiro preemptively sanitizes all content. This action effectively eliminates both known and unknown threats from entering your organization, thereby filling the gaps left by traditional AV software.

Votiro's approach enhances the overall strength of your security posture, ensuring that threats are nullified before they can cause harm.

! **As part of Votiro's approach, we Detect, Disarm, and Analyze content, either working in concert with your AV or by bringing our own AV solution.**

SIEM

Security Information and Event Management (SIEM) tools are integral to many cybersecurity programs, leveraging large data processing volumes to identify threats and generate alerts quickly. However, while SIEM solutions can detect early threats, they also tend to generate many false positives. This overalerting can burden security teams with additional investigative work. Further, in the realm of malware detection, a critical disadvantage of SIEM solutions is that they often only identify threats once the damage has already begun.

This is where Votiro steps in. Our approach targets and eliminates hidden threats at the outset, thereby reducing the amount of data your SIEM processes. This reduction not only improves the performance of your SIEM solution but also alleviates the strain on your security team by minimizing false positives. With Votiro, you get a more streamlined, efficient, and effective security operation, which allows for proactive rather than reactive threat management.

Endpoint Detection and Response

Endpoint Detection and Response (EDR) solutions, much like SIEM tools, take a detection-focused approach to security. They aim to rapidly identify perilous activities by software to facilitate immediate response and elimination. But similar to SIEM, EDR solutions also bear limitations regarding malware detection. The damage inflicted by the malware often has to be in motion before EDR solutions can detect and mitigate it, potentially leading to situations where a security breach has already occurred before it's noticed.

Votiro brings added value to the table. Our solution proactively removes hidden threats, thus addressing a visibility gap in many EDR systems. This enables EDR solutions to focus their resources on detecting other types of attacks and threats rather than being overwhelmed by commodity malware. In essence, Votiro creates an additional layer of defense, effectively removing threats before they need to be neutralized by your EDR solution. This collaboration not only fortifies your organization's security posture but also optimizes the operation of your EDR system by letting it concentrate on what it does best.

Web Application Firewall

Web Application Firewalls (WAFs) are key tools organizations utilize to protect their web infrastructure from threats. WAFs scrutinize incoming traffic, effectively blocking requests that carry malicious payloads or attempts at exploiting vulnerabilities. WAFs are adept at preventing certain types of malware from infecting web applications and websites, providing a sturdy line of defense. **However**, WAFs can only detect and block known attack patterns, potentially falling short when encountering new or advanced malware that employs sophisticated techniques to evade detection.

Moreover, WAFs can be circumvented if they are not correctly configured or fall behind in updates, leaving your web applications susceptible to attacks. This is where Votiro steps in to supplement and strengthen your defenses. Our technology eliminates hidden threats, including 0-day and advanced malware that typically work to evade detection. Unlike WAFs, Votiro does not rely on detection mechanisms, providing a robust, additional layer of security that complements your existing WAF setup. By working hand in hand with your WAF, Votiro ensures your web infrastructure remains secure, even in the face of evolving and sophisticated threats.

Remote Browser Isolation

Remote Browser Isolation (RBI) is a cutting-edge web security solution designed to safeguard users by hosting their web browsing activities on a remote server rather than on their local devices. By doing this, RBI ensures that only a pixel-based representation of the web content is relayed to the user’s device, effectively separating any potentially malicious web content from the endpoint. As a result, hidden malicious scripts or codes are thwarted, unable to compromise the user’s device. RBI is a proactive response to the escalating threats from web browsing, particularly as businesses and their operations migrate more heavily to cloud-based platforms and services.

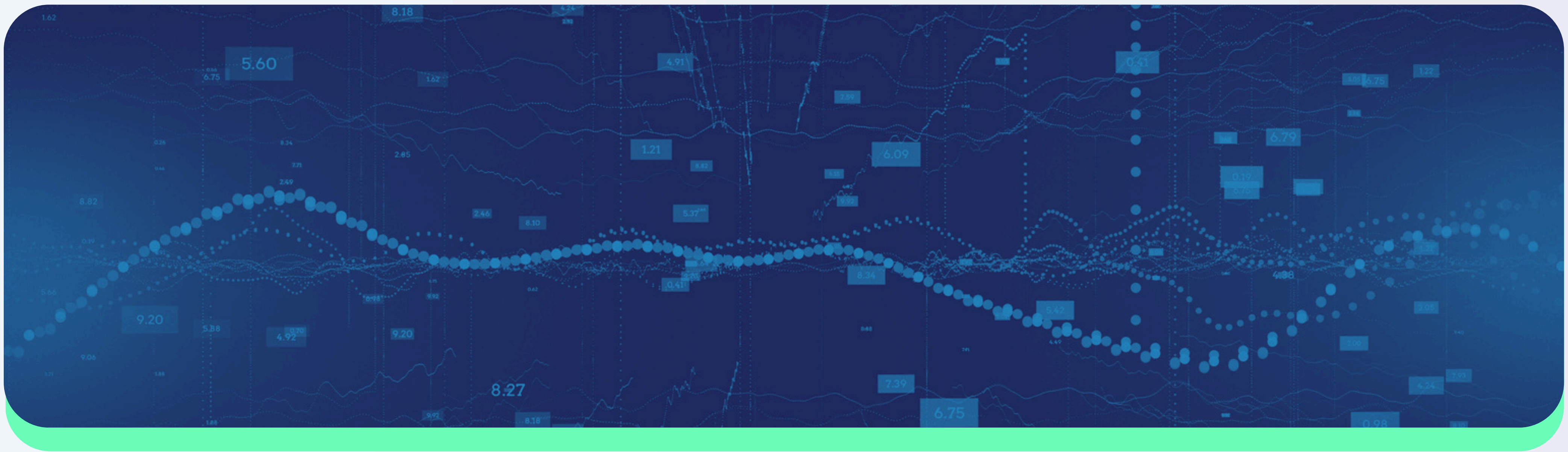
While RBI offers a robust protective layer against direct web-based threats, there are still vulnerabilities to address, especially when users download files from the web. This act of downloading can breach the virtual protective environment established by RBI, providing an entry point for malware to infect devices. Votiro seamlessly complements and enhances RBI’s capabilities to provide an added security layer beyond just isolating browser sessions. Votiro focuses on sanitizing files before they’re downloaded, ensuring that the associated cyber risks are neutralized even if users need to download content. By integrating technologies like RBI with Votiro, businesses can offer their users a truly secure and holistic web browsing experience.

> **Votiro proactively removes hidden threats, thus addressing a visibility gap in many EDR systems.**

Cloud Storage and Data Lake Security Stack

Cloud security stacks often come as an integral part of many cloud implementations. The shared security model's tools typically focus on network-based attacks such as DDoS, direct attacks, and account compromise. Many organizations resort to the cloud for storing vast amounts of data, which can originate from internal users or external parties. For instance, the cloud often houses crucial business documents such as purchase orders, invoices, contracts, and other official documents submitted by external parties.

However, any data uploaded to the cloud can harbor hidden threats, which may lay dormant and undetected for extended periods until accessed by an internal user. Once launched, the threat activates, and damage begins, making cloud storage particularly vulnerable to such hidden threats. Current cloud security measures offer little in preventing or mitigating such threats. This is where Votiro integrates with existing cloud storage and data lakes to sanitize current data stores and prevent incoming content from carrying embedded threats. Votiro thus provides a robust additional layer of security to your cloud infrastructure, enabling it to withstand and neutralize hidden threats effectively.



Working Together

Addressing the challenge of hidden cyber threats doesn’t have to be a complex or disruptive process that necessitates discarding tried-and-true technologies.
Votiro is committed to helping organizations bolster their defenses against such threats through seamless integration with their existing systems.

By enhancing and strengthening the existing security infrastructure, Votiro effectively empowers organizations to counteract threats without the need for drastic changes. Why start from scratch when you can build on what you already have?

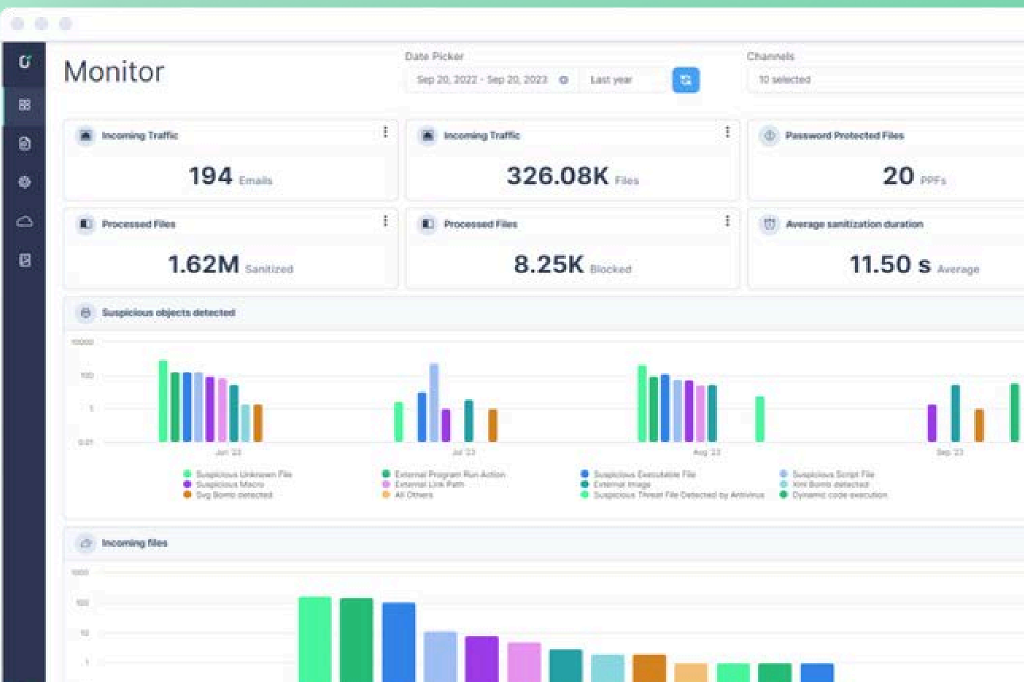
By adopting a proactive stance and integrating a zero-trust approach, Votiro provides a robust defense mechanism that addresses potential vulnerabilities before they can be exploited.

To learn more about Votiro’s Data Detection and Response capabilities, sign-up for a one-on-one demo of the platform, or try it free for 30 days and see for yourself how Votiro can proactively defend your data's security and privacy.

VOTIRO

Try Votiro Free for 30 Days

Take a free 30-day trial and see how Votiro stops threats and privacy risks before they ever reach your endpoints.



Monitor

Date Picker: Sep 20, 2022 - Sep 20, 2023 | Last year

Channels: 10 selected

Incoming Traffic: 194 Emails

Incoming Traffic: 326.08K Files

Password Protected Files: 20 PPFs

Processed Files: 1.62M Sanitized

Processed Files: 8.25K Blocked

Average sanitization duration: 11.50 s Average

votiro.com

sales@votiro.com