MENLO SECURITY + VOTIRO

Solution Brief

Menlo Secure Enterprise Browsing with Votiro Advanced Content Disarm & Reconstruction

A seamless, proactive security framework that isolates browser-based threats and ensures all files are free of zero-day malware.

Today, secure enterprise browsers serve as an essential business technology that enable employees and third-party vendors to communicate, collaborate, and access cloud applications without compromising workspace security. As organizations look to further bridge the gap between productivity and security, they've begun adopting the use of Artificial Intelligence, particularly Generative AI, in hopes to facilitate critical services.

However, just as AI is being integrated into workspace applications, threat actors are leveraging its speed and repeatability to create more sophisticated attacks, including zero-days that can compromise endpoints, steal data, and spread unknowingly throughout enterprise systems.

This evolving threat landscape has led organizations to look for multi-layer data security solutions that can protect browser sessions from phishing attempts, drive-by downloads, and file-based exploits that traditional tools like AV, EDR, and DLP often miss.

Together, **Menlo Secure Enterprise Browser** and **Votiro CDR** enable enterprises to facilitate seamless, safe browser sessions. Both technologies work in tandem to provide a **complete workspace security solution** that is proactive, not reactive, allowing internal teams and third-party vendors the freedom to upload, download, and share files without hindering productivity or compromising security.

The Menlo Secure Enterprise Browser solution is a frontline defense that prevents malicious scripts and exploits from reaching user devices. Using a combination of click-time analysis, adaptive client rendering, and dynamic policy enforcement, Menlo is able to deliver an isolated, virtualized browser session that still allows for safe content to be rendered to the end-user.

Advanced Content Disarm & Reconstruction (CDR) from Votiro is a proactive file security solution that uses zero trust principles to sanitize files in real-time without the need for time-intensive sandboxing and quarantining processes. Votiro bypasses the reliance on known malware signatures while preserving file fidelity, preventing zero-day malware without blocking productivity.

Solution Brief

Secure Enterprise Browser with Advanced CDR

Two Technologies

Secure Enterprise Browser

- **Creates a virtualized browser session**, preventing malicious scripts from executing on local devices and infecting entire enterprise networks.
- **Blocks drive-by downloads and phishing attempts** by streaming only safe-rendered content to the end-user(s).
- **Reduces web-based threats** by isolating web activity from endpoints and keeping enterprises in control of the browsing experience for teams and third-parties.

Advanced CDR

- **Sanitizes downloaded files** by removing embedded threats, malicious macros, and hidden exploits without the need to block or quarantine.
- **Doesn't rely on detection**, ensures all files are clean without the need for known threat signatures, and delivers full file functionality to avoid work stoppage.
- **Available as an open API with native connectors** for suites like O365—and deployable as an SMTP relay—to protect multiple enterprise channels.

One Complete Solution

- Web-based **threats are isolated** before execution
- Specific, per-user privileges can be set to control the **uploading, downloading, and sharing** files or data
- CDR ensures that there's **no need for IT teams to block, quarantine, or sandbox files**, which can still miss malware
- All attack vectors—**web, email, cloud**—are covered under one security framework
- False positives and alerts are reduced, **freeing up resources and reducing stress**
- **Files remain functional and accessible** while being threat-free
- Sanitization **happens in real-time**, behind the scenes
- **In-depth analytics accompany all CDR actions** for easy threat retrospection and future attack preparation

Workspace Security Starts with a Demo

MENLO SECURITY + VOTIRO

Book a Demo Contact an Expert