



A Law Firm's Success Against File-Borne Attacks with Menlo File Security

Menlo deployed within the existing browser infrastructure with zero disruption to user workflows.

THE CHALLENGES

A Legal Team Vulnerable to Threats

As one of Singapore's oldest and most established law firms, the organization advises clients on civil and criminal cases, business transactions, and complex legal matters requiring specialized expertise. This work demands that the firm remain connected to a wide network of clients, external counsel, and business partners across multiple jurisdictions.

However, that connectivity comes with risk. The firm's legal team receives emails and documents from external clients via non-organization domains. These emails often contain files critical to case investigations—contracts, evidence, discovery materials, and research documents. Additionally, case work requires the team to browse and download files from public sources, financial databases, and investigative resources without any sanitization layer.

ORGANIZATION

This Law Firm represents clients in civil and criminal cases, business transactions, and other situations where legal advice and other assistance is required.

CHALLENGE

Emails from external clients and downloads during case investigations exposed the firm to file-borne threats. Existing defenses only minimized risk to 95%.

SOLUTION

Menlo File Security

Menlo Security integrated seamlessly into the Law Firm's email and web browser. Zero trust. Zero disruption.

This open-access model, while necessary for legal work, left the firm vulnerable to file-borne attacks. Attackers could disguise malicious files as legitimate client correspondence or embed threats in seemingly routine business documents.

The Gap in Existing Defenses

To address this risk, the firm's security team deployed an Email Security Gateway and Secure Web Gateway platform. These tools provided important baseline protections using antivirus engines, threat intelligence (IOC matching), and sandboxing technology.

But testing revealed a critical limitation: these defenses only minimized file-borne risk by approximately 95%. Zero-day malware—threats never seen before, with no signature or behavioral signature in traditional threat databases—still posed a serious concern. For a law firm handling sensitive client data and high-stakes cases, that 5% gap represented unacceptable risk.

The firm needed a solution that could stop threats the existing tools missed—without forcing users to change how they work.

THE SOLUTION

Menlo File Security

The firm needed a solution that would integrate into its existing infrastructure without disrupting workflows.

Menlo File Security fit that requirement thanks to its advanced Content Disarm and Reconstruction (CDR) technology that works near-instantaneously in the background to deconstruct and reconstruct fully-functional and malware-less files.

Menlo's CDR does not require an endpoint, instead sitting between files and organization ecosystems. As a result, users don't experience downtime, and IT teams maintain visibility and control without an architectural overhaul.

How It Works

Menlo Security applies Zero Trust principles to every file that touches the firm's network. Rather than relying solely on signature matching or sandbox detonation, Menlo uses advanced file-analysis techniques to identify and neutralize threats—including zero-day malware that conventional tools miss.

When a user downloads a file from the web or opens an attachment from email, Menlo inspects it in real time. Suspicious files are isolated and remediated before reaching the user's device. Safe files pass through instantly. The result: seamless protection that doesn't interfere with productivity.

RESULTS

With Menlo Security Deployed, the Law Firm:

- Eliminated the 5% gap left by signature-based defenses with Zero Trust file protection.
- Prevented file-borne breaches that could cause financial loss, operational shutdown, or reputational damage.
- Reduced third-party risk from external files without requiring users to change workflows.
- Maintained compliance with client confidentiality standards with zero additional friction.
- Enabled legal teams to focus on clients and complex cases with confidence in their security.

About Menlo Security

Menlo Security is the pioneer of the Browser Security Platform (BSP), the industry's first infrastructure designed to govern a hybrid workforce of humans and autonomous AI agents. By centering the browser as the new enterprise operating system, Menlo provides a "Guardian Runtime" that resolves the unique risks created when AI agents operate at machine-speed without human skepticism. The Menlo platform enables the agentic enterprise to scale AI with confidence, providing universal connectivity to legacy data and unified zero-day threat prevention across every session. Trusted by over 1,000 global enterprises—including eight of the ten largest financial institutions and major government agencies—Menlo protects over 8 million users and millions of simultaneous AI agent sessions. Headquartered in Mountain View, California, and backed by investors including JPMorgan Chase, American Express Ventures, and Vista Equity Partners, Menlo is securing the browser for the agentic age. Learn more at www.menlosecurity.com.

Work without worry and move business forward with Menlo Security. © 2026 Menlo Security, All Rights Reserved



Learn more: <https://www.menlosecurity.com>

Contact us: ask@menlosecurity.com

