CUSTOMER CASE STUDY

MENLO SECURITY

A Global Asset Manager Disrupts Browser-Based Command and Control Risk

Purple team testing shows 100% attack disruption with Menlo deployed, compared to 17% disruption from existing defenses alone.

The Browser Was the Gap.

The firm evaluated several vendors but needed a solution that worked within their existing browser environment. Users had to keep working exactly as they always had.

Menlo deployed within the existing browser infrastructure. Most users wouldn't notice it was there. The few visible interactions, like prompts on file downloads, actually communicated protection rather than obstruction. Menlo also integrated with the firm's existing firewall infrastructure, preserving prior security controls and network decryption policies.

ORGANIZATION

Global asset management firm with thousands of users across international offices

CHALLENGE

Investment research demands permissive web access. That same openness is what attackers exploit.

SOLUTION

Menlo Threat Prevention

Phased global rollout through business test groups, 500 to 1,000 users per deployment

Deployed within existing browsers and firewall infrastructure, no endpoint agents, no browser replacement

> "It was the most like how we run things, and the least invasive," the security leader notes. "The few key touchpoints, like file downloads, actually make people feel good. They feel more protected."

Phased Rollout, Zero Business Impact.

Each rollout covers 500 to 1,000 users. Before any group goes live, the security team identifies champions representing different applications, workflows, and regulatory requirements. Those champions test the deployment, issues get resolved, and then the full group transitions.

The Menlo deployment serves a dual purpose: when users transition, the firm simultaneously shifts their network routing from permissive outbound to block-by-default for unknown traffic. Menlo handles the legitimate web traffic that makes that network lockdown viable for business operations.

> "We take a group, find champions representing different applications and critical processes, guide them through it, fix any issues, then roll out to everyone else," explains the security leader. "Zero business disruption."

The Results

Verified threat disruption: Purple team testing using a defined set of attack techniques showed 17% disruption from the existing defense-in-depth stack alone. With Menlo active, 100% of the same attacks were disrupted.

> "Defense in depth got us so far. Menlo got us the rest of the way."

Zero business impact: Just under 30% of the organization runs on Menlo today, with plans to reach 95-99% coverage by the end of 2026 at a pace of 500 to 700 users monthly. Completing the deployment is the firm's number one cybersecurity priority for the year.

Risk posture improvement: The firm tracks security using the MITRE ATT&CK framework, with metrics shared at the board level. When the rollout completes, the security team will document measurable improvement in command and control protection within the organization's risk appetite.

Every browser-based security incident observed since deployment began has involved users not yet protected by Menlo. In at least one confirmed case, Menlo would have disrupted the attack.

Business confidence: The firm's institutional clients conduct security due diligence reviews. Documented browser security controls change those conversations from defensive to confident.
"We can be much more forthright in client due diligence," says the security leader.

The solution also satisfies browser isolation requirements specific to Singapore's regulatory framework, the only jurisdiction to explicitly require browser isolation in its regulatory language.

What It Comes Down To

The firm didn't adopt Menlo because something went wrong. They adopted it because five years of adversarial testing showed them where their exposure was, and they were disciplined enough to close it before an attacker found it first. Completing the deployment is the number one cybersecurity priority for 2026.

> "It's been pretty easy to use from an admin point of view. Painless. It's a mature product, stable, feature-rich, and customizable enough. It works well with our existing controls. Least disruptive to us, least disruptive to the end user."