CASE STUDY · FINANCIAL SERVICES / PRIVATE EQUITY · CENTURY CITY, CA

From Regulatory Gap to SEC-Ready Infrastructure

0	74	100%	1 hr
CRITICAL VULNERABILITIES	DAYS TO COMPLIANCE	MFA ENFORCEMENT	RESPONSE SLA

CLIENT SNAPSHOT

CLIENT	FIRM TYPE	STAFF	LOCATION	TIMELINE
Westridge Capital Partners	**Private Equity · RIA**	**68 Users**	**Century City, CA**	**74 Days**

THE CHALLENGE

An SEC exam on the horizon and a cybersecurity program that existed only on paper

Westridge Capital Partners had operated as a registered investment adviser for over a decade, managing a mid-market private equity portfolio from its Century City office. When the SEC announced its expanded Cybersecurity Risk Management Rule enforcement posture in early 2024, Westridge's CCO initiated an internal review — and found a cybersecurity program that was largely undocumented and substantially non-compliant.

A third-party assessment commissioned by outside counsel identified 9 critical vulnerabilities across the firm's network perimeter and endpoints, no formal written information security policy, and no documented incident disclosure procedure as required under the new SEC rule. LP data and deal files were stored on an unencrypted shared drive accessible to all firm employees. Advanced Networks was engaged to remediate the environment and produce examination-ready compliance documentation within 90 days.

RISK PROFILE AT INTAKE

CRITICAL	9 unpatched critical vulnerabilities across perimeter and endpoints
CRITICAL	LP and deal files stored on unencrypted shared network drive
HIGH	No MFA on any employee account, including partners with fund system access
HIGH	No written information security policy or cybersecurity incident response plan
MEDIUM	No vendor/third-party risk management program documented
LOW	No employee cybersecurity training program in the past 18 months

THE SOLUTION

A 4-phase plan. Delivered in 74 days.

02

THE SOLUTION

A 4-phase SEC cybersecurity remediation plan — built to withstand examination

Advanced Networks structured a 74-day engagement mapped directly to the SEC Cybersecurity Risk Management Rule's disclosure, documentation, and controls requirements — producing artifacts designed to satisfy an SEC examination team.

PHASE 01

Assessment & Policy Gap Analysis

Days 1–12

Conducted a full technical vulnerability assessment and reviewed all existing cybersecurity documentation against SEC Rule 206(4)-9 requirements. Mapped all data flows involving LP information and produced a prioritized remediation roadmap with examination-ready gap analysis documentation.

- ✓ Full network and endpoint vulnerability assessment
- ✓ SEC Rule 206(4)-9 policy gap analysis and documentation review
- ✓ LP data flow mapping and classification
- ✓ Exam-ready risk register and remediation roadmap

PHASE 02

Critical Remediation & Data Protection

Days 13–38

Patched all 9 critical vulnerabilities, replaced aging firewall hardware, and migrated LP and deal files from the unencrypted shared drive to a SharePoint environment with sensitivity labels and access logging. Implemented least-privilege access controls segmented by role and deal team.

- ✓ All 9 critical vulnerabilities patched and verified
- ✓ Firewall hardware replaced and reconfigured
- ✓ LP and deal data migrated to encrypted SharePoint with access controls
- ✓ Role-based permissions enforced across all 68 users

PHASE 03

MFA, EDR & Secure Remote Access

Days 39–58

Enforced MFA across all 68 accounts via Microsoft Entra ID Conditional Access. Deployed enterprise EDR across all firm endpoints and replaced legacy VPN with a zero-trust network access solution. Implemented advanced email security with BEC and phishing detection.

- ✓ MFA enforced on all 68 accounts via Conditional Access policies
- ✓ EDR deployed across all firm endpoints and laptops
- ✓ Zero-trust network access replacing legacy VPN
- ✓ Advanced email security with BEC and phishing protection

PHASE 04

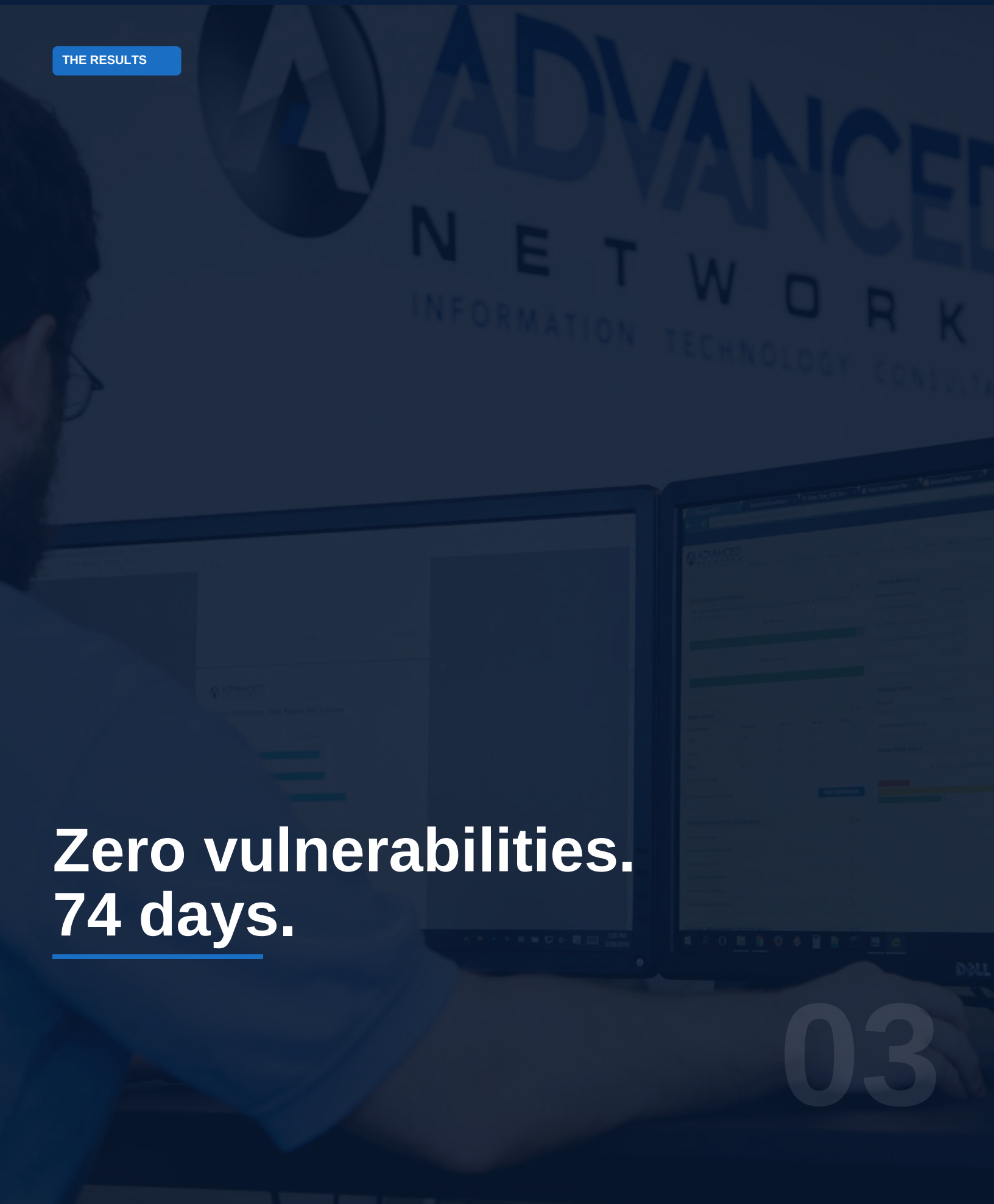
Documentation, Training & Monitoring

Days 59–74

Produced a complete written information security policy, incident response and disclosure plan, and third-party vendor risk management framework — all reviewed by outside compliance counsel for SEC examination readiness. All 68 staff completed annual cybersecurity training.

- ✓ SEC-examination-ready WISP and IRP documentation
- ✓ Third-party vendor risk management framework
- ✓ 68-user annual cybersecurity training (100% completion)
- ✓ 24/7 SOC monitoring and quarterly review schedule

THE RESULTS



Zero vulnerabilities. 74 days.

03

THE RESULTS

SEC examination-ready. Zero critical vulnerabilities. In 74 days.

0 Critical vulnerabilities remaining (down from 9)	**74** Days from assessment to exam-ready compliance	**100%** MFA enforcement across all accounts
1 hr Maximum incident response SLA	**$0** Regulatory fines or SEC actions since remediation	**24/7** SOC monitoring across all endpoints

> *"Our CCO described the engagement as the first time she felt genuinely confident walking into an exam cycle. Advanced Networks didn't just patch vulnerabilities — they gave us the documentation, the policies, and the monitoring program to prove we take cybersecurity seriously. That's exactly what regulators want to see."*
>
> **— Managing Partner, Westridge Capital Partners**
> **Private Equity RIA · Century City, Los Angeles**