CASE STUDY · HEALTHCARE · LOS ANGELES, CA

From HIPAA Exposure to Zero-Trust Healthcare IT

0	103	100%	2 hrs
CRITICAL VULNERABILITIES	DAYS TO COMPLIANCE	PHI ENCRYPTION COMPLETION	RESPONSE SLA

CLIENT SNAPSHOT

CLIENT	PRACTICE AREA	STAFF	LOCATION	TIMELINE
Pacific Coast Specialty Group	**Multi-Specialty Clinics**	**210 Users · 9 Locations**	**Greater Los Angeles**	**103 Days**

THE CHALLENGE

A growing group practice running on a HIPAA time bomb

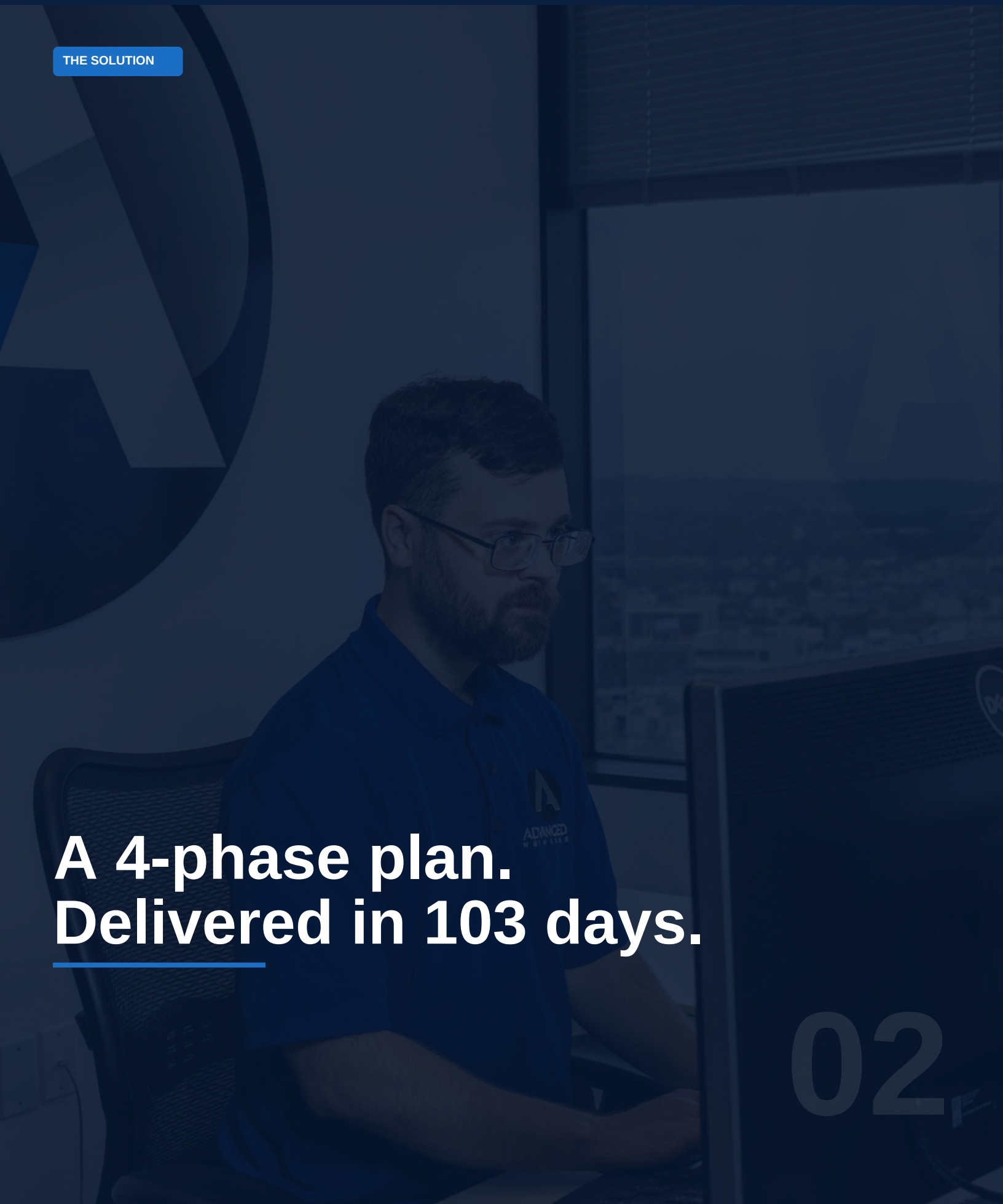
Pacific Coast Specialty Group had expanded rapidly — adding four new clinic locations through acquisition in less than three years. Each acquired practice brought its own legacy IT environment, and none had ever undergone a formal HIPAA Security Rule assessment. When the group's new COO commissioned an external risk analysis in mid-2024, the findings were severe.

The assessment uncovered unencrypted PHI stored on local workstations at six of the nine locations, two legacy EHR systems transmitting patient data over unencrypted HTTP connections, and a shared administrative login used by seventeen front-desk staff — a direct violation of the HIPAA Security Rule's access control requirements. The group carried no cyber liability insurance and had no documented breach response procedure. The COO engaged Advanced Networks to remediate the environment before the group's next Joint Commission review.

RISK PROFILE AT INTAKE

CRITICAL	Unencrypted PHI on local workstations across 6 clinic locations
CRITICAL	Legacy EHR systems transmitting patient data over unencrypted HTTP
HIGH	Shared administrative credentials in use across 17 front-desk staff
HIGH	No MFA on any clinical or administrative account (210 users)
MEDIUM	No documented HIPAA breach notification or incident response procedure
LOW	Outdated workforce security training (last completed: 2021)

THE SOLUTION



A 4-phase plan. Delivered in 103 days.

02

THE SOLUTION

A 4-phase HIPAA remediation plan built for a multi-site environment

Advanced Networks structured a 103-day engagement across four phases, sequenced to prioritize PHI exposure first and build a repeatable compliance foundation across all nine locations.

PHASE 01

Assessment & Risk Analysis

Days 1–18

Conducted a full HIPAA Security Rule gap assessment across all nine locations, inventoried every device handling PHI, and mapped all data flows including third-party integrations with billing and lab vendors. Delivered a prioritized risk register and an OCR-ready risk analysis report.

- ✓ Full network and endpoint inventory across 9 locations
- ✓ PHI data flow mapping including third-party integrations
- ✓ HIPAA Security Rule gap analysis report
- ✓ OCR-ready risk analysis documentation

PHASE 02

PHI Encryption & Access Remediation

Days 19–45

Deployed BitLocker encryption across all 214 workstations and laptops, decommissioned both legacy EHR environments, and migrated clinical data to a HIPAA-compliant cloud EHR with role-based access controls. Eliminated all shared credentials and enforced unique user accounts for all 210 staff.

- ✓ BitLocker encryption deployed across 214 devices
- ✓ Legacy EHR decommissioned; data migrated to compliant cloud platform
- ✓ Unique user accounts enforced; shared credentials eliminated
- ✓ Role-based access controls implemented per job function

PHASE 03

Network Segmentation & MFA Rollout

Days 46–78

Segmented clinical, administrative, and guest networks at all nine sites using VLANs and next-generation firewalls. Enforced MFA on all 210 accounts via Microsoft Entra ID and deployed MDM to manage BYOD devices used by traveling clinical staff.

- ✓ VLAN segmentation at all 9 clinic locations
- ✓ MFA enforced on all 210 clinical and administrative accounts
- ✓ MDM deployed for BYOD device management
- ✓ Next-gen firewall replacement at 4 legacy sites

PHASE 04

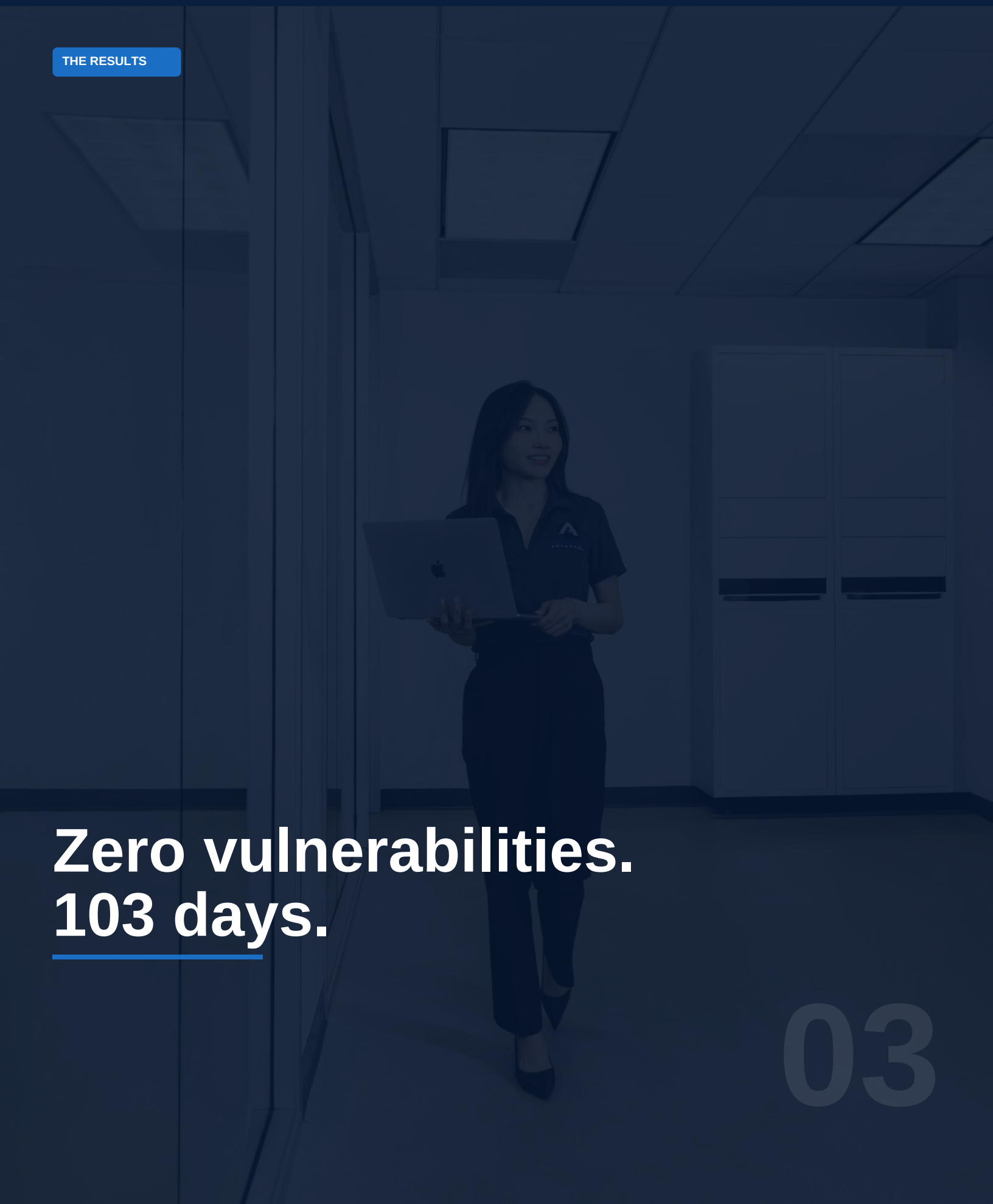
Training, Monitoring & Ongoing Compliance

Days 79–103

All 210 staff completed HIPAA-specific security awareness training. The group was enrolled in 24/7 SOC monitoring with a documented breach notification procedure reviewed by healthcare compliance counsel.

- ✓ 210-user HIPAA security awareness training (100% completion)
- ✓ 24/7 SOC monitoring with PHI-aware alerting
- ✓ Documented breach notification procedure (HIPAA §164.400)
- ✓ Quarterly HIPAA risk review calendar established

THE RESULTS



Zero vulnerabilities. 103 days.

03

THE RESULTS

Full HIPAA compliance. Zero unencrypted PHI. Across 9 locations.

0 Unencrypted PHI devices remaining (down from 6 sites)	**103** Days from assessment to documented compliance	**100%** Workforce security training completion
2 hrs Maximum incident response SLA	**$0** OCR fines or breach actions since remediation	**24/7** SOC monitoring across all 9 locations

> *"We had acquired four practices in three years and had no idea what we had inherited from an IT standpoint. Advanced Networks gave us a clear picture, fixed the most dangerous issues first, and left us with something we can actually show regulators. The peace of mind alone is worth every dollar."*
>
> **— COO, Pacific Coast Specialty Group**
> **9-Location Multi-Specialty Group · Greater Los Angeles**