

CASE STUDY · MARCH 2026

# Securing and Segmenting Infrastructure for a Multi-State Law Firm

An anonymized project case study of how Massive IT deployed wired network authentication, VLAN segmentation, and Hyper-V and storage hardening for a legal practice serving financial institutions.



Conceptual illustration only; not the customer's production environment.

## Project snapshot

| Detail                | Summary                                                                              |
|-----------------------|--------------------------------------------------------------------------------------|
| Customer              | A multi-state creditor representation and collections law firm (customer anonymized) |
| Operating environment | Multiple offices handling sensitive legal and financial data                         |
| Services engaged      | Cloud, security, server infrastructure, network infrastructure, and vCIO advisory    |
| Core workstreams      | 802.1X wired access control, VLAN segmentation, and Hyper-V/SAN hardening            |
| Case study date       | March 2026                                                                           |

## Executive summary

A multi-state law firm representing financial institutions needed to strengthen the infrastructure supporting its legal operations. Sensitive account information, case management systems, document repositories, and staff workstations operated under multiple client-specific security and contractual requirements.

Massive IT assessed the environment and delivered three coordinated infrastructure workstreams: port-based device authentication, network segmentation, and virtualization and storage redesign. The engagement connected technical controls with documented configuration baselines and ongoing vCIO guidance to support compliance readiness and client security reviews.

*Customer location, financial details, and precise staffing figures are omitted to preserve anonymity. This account reflects the supplied project case study; it does not guarantee compliance, audit acceptance, or the elimination of security risk.*

## The challenge: boundaries that could be demonstrated

The assessment identified uncontrolled wired connection points, a relatively flat network, and configuration drift in the Hyper-V and storage environment. Workstations, servers, management interfaces, and inter-office traffic needed clearer boundaries and more deliberate access policies.

For a practice handling regulated financial information, these findings mattered beyond day-to-day administration. The firm needed infrastructure controls and documentation that could be explained during client reviews and maintained as requirements changed.

## Project 1: 802.1X wired network authentication

Massive IT reviewed switch infrastructure and device access across the firm's offices, mapping ports and identifying authentication gaps. Engineers designed and deployed a RADIUS-based 802.1X framework integrated with Active Directory.

- Configured managed switch authentication policies to evaluate supported devices before granting access.
- Established certificate-based or credential-based validation within the documented access design.
- Defined guest VLAN policies and controlled exceptions for legitimate temporary-device scenarios.
- Tested authentication flows, failure conditions, and exception handling, and documented the resulting configuration.

The delivered control strengthened enforcement at wired network entry points. Documented guest and exception paths remained part of the access design; the project should not be interpreted as proof that every possible unauthorized connection is prevented.

## Project 2: risk assessment and VLAN segmentation

The security assessment informed a segmentation architecture that separated workstation environments, server functions, administrative access, and inter-office traffic. Massive IT aligned routing and firewall policies with those boundaries.

- Separated production workstation networks by office and functional role.
- Segmented server workloads according to function and sensitivity.
- Isolated management and out-of-band administration behind controlled administrative pathways.
- Segregated inter-office traffic and applied encryption as described in the supplied project account.
- Realigned access control lists and firewall policies, and documented VLAN boundaries and routing rules.

These changes reduced unnecessary communication paths and supported a more demonstrable access model. Segmentation can constrain lateral movement, but it does not eliminate all lateral-movement or data-exposure risk, nor does it by itself establish isolation of every client dataset.

## Project 3: Hyper-V and SAN redesign

The firm's virtualization and storage platform supported production systems including case management and document repositories. Massive IT assessed host configurations, virtual switch layouts, guest network assignments, and storage access patterns.

- Redesigned virtual networking to align with the physical segmentation strategy.

- Separated production, management, and storage traffic through dedicated virtual switch configurations mapped to appropriate VLANs.
- Reconfigured storage-network zoning and access boundaries.
- Tuned virtual machine resource allocations, storage I/O policies, and host settings to address reported performance concerns.
- Established documented Hyper-V and SAN configuration baselines for change management and future review.

The supplied account reports platform hardening and performance improvements. It does not provide benchmark measurements or independent SLA verification, so this case study makes no quantified performance or service-level claim.

## Delivered controls and review evidence

| Workstream         | Delivered capability                                    | Review support                                      |
|--------------------|---------------------------------------------------------|-----------------------------------------------------|
| Wired access       | 802.1X device authentication with controlled exceptions | Authentication-flow and failure-mode documentation  |
| Network boundaries | VLAN segmentation and policy-controlled routing         | Network diagrams and documented boundary rules      |
| Virtualization     | Virtual network alignment and separated traffic roles   | Host and virtual-switch configuration baselines     |
| Storage            | Revised storage zoning and access design                | Documented storage configuration and change records |
| Governance         | Coordinated managed services and vCIO advisory          | Ongoing alignment with client-specific requirements |

## Project outcomes

The supplied case study describes deployment of port-level authentication, a segmented network architecture, and a hardened virtualization and storage platform. Together, the work strengthened the firm's infrastructure controls and the documentation available for client security and compliance reviews.

The business value was clearer control over device access and system communication, supported by maintainable baselines rather than ad hoc configuration. Ongoing cloud, security, infrastructure, and vCIO services provided a coordinated operating approach as the firm's needs evolved.

*Results are specific to this engagement. No independent audit result, guaranteed contractual compliance, protected revenue amount, or complete risk elimination is asserted.*

## **Why this project matters**

Compliance-sensitive infrastructure requires more than individual security products. This project connected authentication at the network edge, boundaries inside the network, and access separation in the server and storage platform, while making the resulting design understandable to administrators and reviewers.

## **Strengthen your infrastructure readiness**

Massive IT helps legal and other compliance-sensitive organizations assess infrastructure gaps, prioritize controls, and prepare evidence for security reviews. Schedule a consultation or call (813) 518-5454.