SAFEGUARDING CLIENT CONFIDENTIALITY
5 CYBERSECURITY ESSENTIALS FOR LAW FIRMS

Protect Client Data. Defend Firm Reputation. Stay Ahead of Threats.

Law firms are increasingly targeted by ransomware groups, data extortion gangs, and insider threats. From case files and financial records to privileged communications, your firm holds some of the most sensitive data in the business world.

Yet many legal environments still lack full visibility, real-time detection, or identity controls across their distributed networks and SaaS platforms.

Vijilan Security delivers 24/7, compliance-grade protection through a managed platform built on:
CrowdStrike Falcon for EDR/XDR, Identity Protection, and Exposure Management
Corelight, powered by Zeek, for east-west network visibility
Cribl Stream for smart log ingestion, filtering, masking, and pipelining

Cloud-native infrastructure hosted on **AWS**, with full support for **Azure**, **Google Cloud**, and hybrid environments

Here are the 5 cybersecurity essentials law firms must adopt to remain compliant, confidential, and resilient.

Continuous Monitoring Across DMS, CRMs, and Legal SaaS

Platforms like iManage, NetDocuments, Worldox, and Microsoft 365 house your most critical data—but often lack real-time visibility.

Vijilan deploys continuous SIEM and SOC monitoring across these platforms, detecting privilege abuse, credential misuse, and lateral movement.

Cribl Stream ensures secure, compliance-grade log collection and routing—filtering only what matters and masking sensitive metadata in real time.

Endpoint Protection for Attorneys, Staff, and Remote Devices

From courtrooms to home offices, firm endpoints are exposed to phishing, malware, and credential theft.

Falcon EDR/XDR, deployed and managed by Vijilan, delivers real-time endpoint protection with behavioral threat detection—stopping attacks before they escalate.

We support BYOD policies, encrypted remote devices, and integrated cloud-based case systems.

Identity Protection and Zero Trust Enforcement

Credential theft remains the leading cause of breaches in law firms.

Falcon Identity Protection monitors login behavior, detects anomalies, and enforces Zero Trust across systems like Microsoft 365, iManage, and firm CRMs.

We apply conditional access policies and automated privilege auditing across Azure AD and on-prem Active Directory environments.

Continuous Vulnerability Management for Legal Tech

Delayed patching in platforms like Zoom, case management systems, and billing software leads to risk.

Falcon Exposure Management provides scanless, real-time vulnerability prioritization. It highlights exploitable risks inside your document systems, extranets, and client portals.

Cribl routes vulnerability logs to your SIEM and archives them for annual reporting and client audits.

Compliance-Grade Logging, Retention, and Breach Readiness

ABA Model Rules, GDPR, HIPAA (for health cases), and client security questionnaires require audit-ready logging and breach reporting.

Cribl Stream, powered by Vijilan, enables scalable log management—collecting logs from Microsoft 365, legal billing, DMS, and email servers.

We support **CrowdStrike GovCloud** deployments and FedRAMP-aligned environments for regulated or government-facing clients.

Client Trust Begins with Cybersecurity

Your firm's reputation depends on protecting client confidentiality.

Vijilan Security gives MSPs the tools to defend law firms without complexity: Falcon, Cribl, Corelight, and a modern SOC infrastructure built on AWS.

vijilan
IT Security: Enabled

vijilan.com
info@vijilan.com
+1 (954) 334-9988