NOPALCYBER

CLM CASE STUDY

How One CLM and AI Provider Built Trust with Cybersecurity

Cutting Costs, Driving Revenue, Igniting Growth

The Challenge:

A Brilliant Solution….Encounters a Common Roadblock.

Contracts are the backbone of business, and Contract Lifecycle Management (CLM) platforms maximize their value. CLM systems serve as a central hub for AI-driven contract creation, editing, and management, leveraging large language models for efficiency. They streamline obligation tracking, risk assessment, compliance, and business exposure while managing the full contract lifecycle—from requesting and negotiating to execution, storage, and ongoing value delivery. However, one thing remains: the risk of cyber-attacks on contracts full of sensitive information.

One of the world's largest CLM enterprises experienced rapid growth in its SaaS platform and faced heightened cybersecurity scrutiny. As CEOs, General Counsel, CFOs, and procurement leaders grew increasingly aware of rising cyber threats and evolving compliance demands, they demanded absolute confidence in the platform's security. Protecting sensitive data with robust application security and strict security controls was non-negotiable.

Picking the Right Cybersecurity Partner

This CLM vendor wanted first to get an outside assessment of its external attack surface's security posture to find strengths it could highlight and weaknesses it could fix at both the application level and the foundational SaaS platform. Then, it wanted to make strategic product upgrades designed to lower cyber risk and ensure its reputation for data protection and privacy.

They needed a solution designed around its particular tech stack, threat exposure, compliance requirements, risk tolerance, and security needs. What multiple Managed Service Providers or various cyber tools/platforms had to offer was a one-size-fits-all product or service. Leadership understood this wasn't enough to secure a complicated multi-tenant platform or satisfy demanding legal and other customers basing buying decisions on security measures—prompting a continued search for the right partner.

Seeking a solution that seamlessly integrated cybersecurity with business strategy, they turned to NopalCyber. Unlike typical cybersecurity firms, NopalCyber brings a unique blend of expertise—rooted in the legal and CLM sectors, alongside deep experience in application, API, and AI security. This rare combination of skills made them the ideal partner. More importantly, NopalCyber offered a diverse range of specialists and services, enabling them to design and implement a cybersecurity solution that met immediate needs and continuously evolved to enhance security and maximize business value.

Picking NopalCyber to be its cybersecurity partner has proved to be one of the best decisions this CLM vendor has ever made.

Finding Solutions for Every Problem

Recruiting top global cybersecurity talent has been a challenge for our client—just as it is for many companies. At the same time, prospective clients began demanding deeper insights into security posture, holding it to the highest standards. To bridge this gap, NopalCyber was brought in to enhance security and transform it into a key differentiator and an advantage for the CLM platform.

To that end, NopalCyber became an essential resource for customers reviewing the CLM provider's cybersecurity posture. Our team now completes security questionnaires, deals with concerns and inquiries, and engages in client/prospect interviews, doing anything and everything necessary to help interested parties confirm that cybersecurity aligns with their exacting standards.

Behind the scenes, NopalCyber worked on multiple fronts to meet and maintain those high standards. An initial search for exposures yielded discoveries that resulted in quick and significant security upgrades in the platform.

With cybersecurity stabilized, NopalCyber set about raising the bar.

Offensive cybersecurity strategies, including Application Security Assessments, VAPT, Red Teaming, and External Attack Surface Discovery, identified vulnerabilities and mitigated future attack risks. Meanwhile, enhancements to SIEM, EDR, SOAR, UEBA, and Threat Intelligence fortified defenses, enabling proactive threat neutralization before they could compromise client data or trust.

Quick Wins and Constant Improvement

One of the first things NopalCyber did was quantify the strength of the security posture through our advanced Attack Surface Discovery process, which provides a detailed qualitative analysis and benchmark score: NopalCyber's proprietary Cyber Intelligence Quotient (CIQ). The CIQ score provides a single metric that considers the entire security ecosystem, from Red Teaming vulnerabilities, GRC, and real-time MXDR threats, and uses AI and machine learning to weight recency, priority, severity, and impact. Within 45 days of starting, that score had jumped by a very significant 30%.

NopalCyber reduced cyber risks and automated security operations to the degree that cybersecurity spending was optimized by 60%. Redeploying those investments saved more than the cost of NopalCyber's engagement.

Even more significant than the cost savings are the revenue gains they have seen in the year since partnering with NopalCyber with new wins, driven in large measure by customers' focus on cyber issues as a critical solution differentiator.

At a time when demand for CLM solutions and concern over data security are both surging in legal and other sectors, this company has perfectly positioned itself to lead this market.

NopalCyber has now established itself as a leader in helping SaaS companies strengthen and differentiate their offers at a strategic level—leveraging security as a service to help acquire and retain customers.

About NopalCyber

NopalCyber makes cybersecurity manageable, affordable and reliable. Managed extended detection and response (MXDR), attack surface management (ASM), breach and attack simulation (BAS), and advisory services fortify your cybersecurity position across both offense and defense. AI-driven intelligence in its Nopal360° platform, NopalGo application, and its proprietary Cyber Intelligence Quotient (CIQ) lets anyone quantify, track, and visualize their cybersecurity posture in real-time. NopalCyber's offensive and defensive services and external threat analysis are tailored to each client's need and budget, NopalCyber democratizes cybersecurity by making enterprise-grade security available to organizations of all sizes.