How a Top D.C. Law Firm Built a More Efficient and Effective Vulnerability Management Model with Kenna Security

The legal sector is increasingly becoming a high value target for cyberattacks, and many law firms are turning to Kenna to transform their vulnerability management to rapidly identify, prioritize and effectively remediate their most critical threats.

One of these customers is a prominent legal firm headquartered in Washington, D.C. that provides legal representation across a comprehensive range of practice areas. As with any law firm, sensitive client information is a core part of their business, and protecting that information is a top priority.

The Challenge - Quantifying Risk and Operationalizing Vulnerability Management

In supporting the cybersecurity needs of the firm’s global business network, Javan DeGraff, Cyber Security Lead, heads a small cybersecurity team that faced the dual challenges of implementing a quantitative risk-scoring methodology and enabling individual system administrators to more proactively handle risk management.

Prior to partnering with Kenna, the team operated around a centralized vulnerability management model. DeGraff commented, “We’re a small team, and we have to focus on a variety of things from vulnerability management to hunting, pretty much the whole gamut. We didn’t have enough time or people to manually manage thousands of vulnerabilities; it was critical that we found a way to make individual server admins better able to address vulnerabilities themselves.”

Our biggest challenge with vulnerability management was getting a quantitative risk-scoring methodology in place. We used to have to hand system administrators a printout from a vulnerability scanning tool, with a lot of technical details on how to mitigate a vulnerability, but it wasn’t necessarily clear or easy for them to put that report into action. Kenna makes that process simpler.”

Javan DeGraff
Cyber Security Program Lead
DeGraff and his team also faced difficulty when it came to accurately reporting on risk, largely because of the inefficient tools they were relying on in order to identify and remediate critical threats.

**The Solution: Kenna.VM**

By adopting Kenna.VM, DeGraff and his team have been able to empower individual system administrators to take responsibility for vulnerability management, rather than having them rely on top-down fixes from the core security team. This has had the effect of radically improving the efficiency and effectiveness with which the firm prioritizes and remediates cybersecurity threats.

"Kenna enabled us to decentralize our vulnerability management program so that individual server admins can take more personal responsibility for their machines. At a glance, admins can see the specific vulnerabilities that are pertinent to them, then click over to Kenna’s fixes tab that gives them a hyperlink to the patch they need. And all they have to do is click it and install it. It’s just that simple for them."

Kenna’s Cyber Risk Context Technology™ looks outside the organization to understand what attackers are doing in real-time to evaluate which of the masses of vulnerabilities are most likely to pose a threat. This enables organizations to create a personalized dashboard for each system administrator that not only displays the most critical vulnerabilities that pertain to the specific assets assigned to them, but also the steps needed to remediate them and the reduction of risk as a result of these efforts. As a result, they are able to identify threats far more quickly and respond to them in a more agile and effective way.

**Results: More Efficient and Effective Risk Management**

With Kenna, DeGraff and his team took a huge leap forward in their ability to measure, monitor, and reduce risk. The firm now benefits from a quantitative risk management model that paints a complete and holistic picture of their security posture at a glance, and how their remediations affect the company’s exposure to risks. Additionally, by decentralizing their vulnerability management process the firm’s IT Operations team enjoys a welcomed increase in individual accountability. “Our admins and executives can now visualize and track our general risk and security posture at a glance, in a way that is visual and intrinsically understandable. They don’t have to call me, they just look at their dashboard.”

This new model has enabled the firm to scale the effectiveness of their security team and optimize their resources to focus on patching critical vulnerabilities, rather than wasting time buried in pivot tables and spreadsheets. “Kenna has helped reduce our attack surface. We’ve been able to identify significant vulnerabilities much more easily, which enables our admins take action on those and harden their systems accordingly. We spend far less time on analysis, and more time on fixing.” Overall, the team has reduced the time it takes to deploy patches by a week and shrunk their backlog of vulnerabilities by 60%.