FORTRA®

CASE STUDY (DIGITAL DEFENSE)

Leading Law Firm Leverages Managed Service to Bolster Security

Law Firms are a target for Cyber Criminals

Imagine the paralegal who unknowingly clicks on a malicious link embedded with spyware; the junior lawyer who accidentally leaves his laptop in a taxi cab only to have it fall into the wrong hands; the managing partner who stores files on a cloud-based service, unaware of a possible entry point for a devastating breach.

Those in the legal industry have been applauded for being early adopters, eager to embrace technology to improve efficiency. However, with innovation comes the need for improved security. Without it, the legal industry is at risk. Law firms are often the primary target for cyber criminals looking to gain access to intellectual property, trade secrets and other business capital.

Law firms, large and small, are finding current and future clients are growing more concerned with their firm's ability to keep confidential information safe.

> ***"There is no silver bullet when it comes to security and new vulnerabilities are being discovered every day. DD is a key player in our risk mitigation strategy and they help us to identify and eliminate internal and external vulnerabilities quickly and throughout the year."***

AT-A-GLANCE

KEESAL & YOUNG LOGAN

Keesal, Young & Logan is committed to security
Keesal, Young & Logan, a full-service business law firm, opened its first office in Long Beach, California in 1970. The firm's goal is to help business clients grow and prosper in the face of rapidly changing laws and challenges by competitors.

To protect clients and the firm's reputation, security initiatives are of the utmost importance to Keesal, Young & Logan. The information security team led by Justin Hectus, Director of Information, is committed to not only comply with information security regulations such as HIPAA, HITECH and recent ABAB standards, but also to go beyond compliance to better protect sensitive data from access by unauthorized resources. With a finite number of IT personnel available to apply towards information security-related activities, they understood the value of outsourcing security solutions to a team they could trust.

Many prospective security savvy clients are demanding assurances that any firm/client relationship will include a secure, digital foundation. Earlier this year, The New York Times detailed the growing concern in the industry, as well as the steps taken by the FBI in partnership with top law firms to get out ahead of the issue. Despite these efforts, the FBI officials and security experts say that law firms remain a "weak link."

Legal Industry Security Challenges

P**rotect attorney-client privileged information from access by unauthorized resources** - Cyber-attacks are inevitable in all industries including law firms. The compromise of digital assets can have a devastating impact on a law firm's reputation.

Comply with information security regulations such as HIPAA - Preventing unauthorized access to confidential data such as personally identifiable information (PII) is essential in today's digital world

Law firms with access to protected health information likely will find themselves classified as "business associates" under new HIPAA rules and therefore subject to new privacy, security, and breach-notification requirements governing their handling of such information.

Recognizing the risk of not complying exceeds the risk tolerance of the organization, law firms are seeking solutions

> ***"Our Personal Security Analyst was deliberate with his processes and methodologies but remained FLfl exible and accommodating to our changing needs and requirements. The overall customer service and expert insight has helped us improve security while exceeding our expectations."***

that enable them to demonstrate their due diligence in complying with all necessary requirements.

Overwhelmed and understaffed - With a finite number of IT personnel available to apply towards information security-related activities, many growing firms are challenged with implementing, maintaining and managing traditional vulnerability scanning tools.

Many Scanning Tools Bring Obstacles

Vulnerability scanning has been relied upon for years to mitigate risks. However, many scanning tools in the marketplace today lack ease of use and protection required for organizations to defend against potential security breaches.

Cumbersome Reporting - Organizations rely on detailed reporting, as well as executive level analysis. Often, scanning tools in the market today make report generation time consuming.

False Sense of Security - When security is approached as an occasional project, scanning tools are often not engaged frequently enough to accurately evaluate potential risks.

An Idle Investment with Poor ROI - A scanning tool that is challenging to implement and manage may sit idle and collect dust. The result is not only a poor investment but also an open door for devastating security breaches.

> ***"We were committed to vulnerability scanning and securing our netwrok, and we invested time in evaluating in-house scanning tools and managed solutions. DD's scanning technology identified vulnerabilities in our network that were not seen by other scanning methods. DD's managed solution not only identified weaknesses but also helped us prioritize them so that we could more effectively manage risks."***

Solution: VLM-Pro

Vulnerability Lifecycle Management-Professional

DD's solution, Vulnerability Lifecycle Management – Professional (VLM-Pro), is used to conduct host discovery and vulnerability scans on external (internet facing) and internal IP-based systems and networks. DD employs a variety of scanning techniques built on a patent pending proprietary scanner to survey the security posture of the target IP-based systems and networks. These scans proactively test for known vulnerabilities and the existence of mainstream industry practice security configurations.

DD assigns each VLM-Pro client a Personal Security Analyst (PSA) who serves as the client's primary point of contact for more involved technical questions. The PSA provides the client clear, consistent security consulting advice on their Vulnerability Lifecycle Management program. The consistent quality of this advice is achieved by providing the PSA access to a common technology platform kept up-to-date by dedicated teams of security analysts and vulnerability researchers.

Security Made Manageable

The managed vulnerability scanning solution, VLM-Pro, is helping Keesal, Young & Logan reduce the likelihood of a cyber-attack, which would have a negative impact on the firm's reputation.

- **Reduced Scan Times** - DD's Scanning Engine reduced scan times by almost 80%. This allows DD to respond quickly to any enterprisewide issue the Firm may encounter.
- **Fewer False Positives** - DD's ability to reconcile and correlate recurring security assessments produces more accurate assessment data and requires less time and fewer resources to validate false positives.
- **Realizing a savings of approximately 40%1 over three years** - With no hardware or software to purchase and maintain, and significantly fewer IT resources that need to be trained and dedicated to the ongoing execution of the vulnerability management program, the VLM-Pro solution is saving the Firm over 40% in 3 years when compared to traditional premise-based tool deployments. Not only is a cloud-based offering more cost effective, but it is a much better solution for organizations focused on reducing the carbon footprint of their data center.
- **Winning more Customers with a Commitment to Security** - Today's legal clientele are security savvy and want to be reassured that the firm they choose is diligent in protecting sensitive information. With VLM-Pro, firms are able to provide clients security assurance and the peace of mind needed to put their trust in the organization.
- **Security GPA®** - Security GPA is a metric developed by DD that provides clients with a more granular and easily relatable measurement of improvements made to the security of their network over time. Security GPA takes into account the perceived criticality of individual systems and system types. The Firm's Security GPA has steadily increased since the inception of the VLM-Pro service. Such an increase translates into reduced likelihood of a network security breach occurring and better protection of digital assets (e.g. attorney-client privileged information and personally identifiable information).

DD Has A Less Than 1% False Positive Rate

For more information contact sales@ddifrontline.com

At the time of this case study, Fortra VM and its corresponding security solutions were referred to under the Frontline brand.

FORTRA®

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.