Law Firm Engages Sophos to Protect Confidential Data and Provide Accelerated Incident Response and Remediation

With a rich heritage, a commitment to community, and an emphasis on long-lasting relationships, Jennings, Strouss & Salmon is a full-service law firm that has been providing clients with strategic legal guidance since 1942. Their home office is located in Phoenix, Arizona. They also have offices in Peoria, Tucson, and Washington D.C. Their growing client base includes organizations of all sizes.

CUSTOMER-AT-A-GLANCE

Jennings Strouss
LAW FIRM

Jennings, Strouss & Salmon (JSS)

Industry
Law

Sophos Solutions
Sophos MTR Advanced: 160 endpoints and 55 servers on their network
Sophos Firewall XG 310

"At the end of the day, we wouldn't be where we are without the Sophos relationship. This has allowed us to keep our strong ties to the community and continue to build the solid relationships we have with our clients."

Dave Nobile, Chief Information Officer, Jennings, Strouss & Salmon

Due to the confidential nature of the data that JSS deals with on a daily basis, security is a top priority for the law firm. Jennings, Strouss & Salmon always makes a conscious effort to deploy security solutions that best serve them, so they can best serve their community and clients. They chose to implement Sophos Managed Threat Response (MTR) Advanced service as a way to expand their security capabilities in an ever-evolving threat landscape and keep confidential information secure.

Building the Foundation

Chief Information Officer Dave Nobile and his team of seven are responsible for managing technology throughout the firm, across all four offices. They do about 80% of the IT work in-house and outsource the remaining 20% to a Managed Service Provider (MSP). In his role, Nobile evaluates, recommends, and deploys technology solutions for the whole organization and oversees technical support, operations and systems, and training.

The relatively small IT team at JSS is constantly working on projects and assisting users. Their most recent significant initiative was transitioning to the cloud. It was an immense effort that required some careful planning, as Nobile points out: "Examining the management, the cost, and time of moving to the cloud was important. We needed to fully comprehend the entire task and what was at stake."

As the IT team prepared to move to the cloud, they made sure they understood how the attorneys work, which was essential to ensuring that the cloud migration process was smooth and secure. The workflow of attorneys includes a broad variety of data types: emails, hardcopy letters, personal identifiable information (PII), and critical client and case information. With clients being the priority, the attorneys and the entire firm have a vested interest in ensuring the confidentiality of all types of information.

Nobile and his team exercised extreme vigilance during the migration: "Moving to the cloud meant transferring this information, and the central task was ensuring that everything from the process to the information itself was secure."

"Moving to the cloud meant transferring this information, and the central task was ensuring that everything from the process to the information itself was secure."

Dave Nobile, Chief Information Officer, Jennings, Strouss & Salmon

The Importance of Information and Valued Clients

In a business where trusted legal advice drives success and data and communications are highly confidential, the way clients perceive the firm's security is just as important as the firm's actual security controls.

As Nobile puts it, "It's very difficult to recover from the reputation damage caused if the firm gets breached. You want to protect the reputation and perception just as well as you protect the tangible data. We want our clients to feel confident knowing that, at our law firm, security is of the utmost importance."

Understanding the Threat Landscape

With years of security experience under his belt, Nobile is well aware that the threat landscape is constantly changing. Threats are becoming more sophisticated, with threat actors using more advanced ways to infiltrate networks and exfiltrate data. Something as seemingly harmless as an email from Pizza Hut could contain malware that could bring a firm to its knees.

"It's easy to get sucked into a spoofed email, even with extensive training," says Nobile. "For that reason, understanding the cybersecurity industry was key. Researching products and services and how they could serve the firm was essential."

How Sophos Can Augment a Team's Success

Nobile was already familiar with the Sophos platform from a previous role and was impressed with its value. The competitive product JSS was using at the time was not providing the peace of mind they were looking for. Instead, the product created a high volume of alerts, which meant more, not less, work for his team. Moreover, the vendor did not offer incident response.

It quickly became clear that it was time for a change. Nobile delivered a convincing message to the law firm's management team: "We needed a vendor that could take action. We didn't need a vendor to just give us 'pointers,' but true assistance—a responsive team with the right

knowledge and the ability to fix any potential issues." In other words, he wanted a comprehensive solution and service. "With Sophos MTR, we obtained just that," he affirms. Nobile immediately saw the positive benefits the Sophos platform gave his team, especially in terms of peace of mind. "Now our team can work on actual projects," he says, "and leave the incident response to the Sophos MTR team. Because of them, we are a success."

Taking Action a Step Further

Nobile confirms that it was easy to sell the value of Sophos to the law firm's management team. As he asserts, "You can spend X amount of dollars and have somebody who will say, 'Hey, somebody's in your network right now stealing stuff and destroying the network, here's how you fix it,' or, you can spend money to say, 'Somebody tried to get in, it's been stopped, and here's the report.'"

The MTR reports provide Nobile with tangible results to show the management team, which helps build a strong foundation for supporting the security team further and for achieving long-term success. After Sophos was deployed, Nobile disclosed to management what had changed and what was fixed. This honesty and transparency from the IT team to management, Nobile points out, was fundamental to management buy-in and boosted their confidence in the firm's security posture.

"The most secure law firm can be breached," he explains. "And once a firm's reputation is destroyed, that is even harder to recover from than data loss. We are responsible for our data and our clients. We must protect them and their information. A solid reputation will follow as a result."

"At the end of the day," Nobile concludes, "we wouldn't be where we are without the Sophos relationship. This has allowed us to keep our strong ties to the community and continue to build the solid relationships we have with our clients. It's the foundation our relationships are built upon that has allowed us to be the trusted advisor to our clients."

"We want our clients to feel confident knowing that, at our law firm, security is of the utmost importance."

Dave Nobile, Chief Information Officer, Jennings, Strouss & Salmon

www.sophos.com

SOPHOS

21-10-01 CCS-EN (NP)