



IGI

Solve. Simplify. Secure.

CASE STUDY

Legal Industry

An established law firm based in Rochester, NY, with locations in several U.S. cities, is changing the way it protects its information with Nodeware vulnerability management and cybersecurity services from IGI. The firm has been in businesses for over 100 years, a tenure that was not earned by keeping the status quo, but by staying ahead of the curve with the latest security technology. From their perspective, taking extra measures to protect client information is not only an ethical duty, but a standard of care for the firm.

The Challenge

Data breaches are a significant and growing threat for law firms, even though it may not be as publicized as much as in other industries. Law firms are vulnerable to outside hacking incidents as well as data breaches within the law firm from BYOD policies, or lost and stolen devices. Law firms are also obligated to adequately protect client information by federal laws, such as HIPAA, FACTA and GLBA.

This firm represents a broad spectrum of clients, including many institutional clients, such as financial and educational organizations, where the protection of personally identifiable information (PII) is a significant concern. These clients require that the firm have robust cybersecurity protection and can report on the security of their data, including providing regular internal and external vulnerability scanning. This obligation to protect client confidentiality, as well as individual client data, makes cybersecurity a crucial component of business operations for law firms.

The Solution

The firm was overwhelmed by the complicated and expensive cybersecurity solutions available in the market. Drawn to Nodeware's simplicity and affordability, the firm deployed the Nodeware Vulnerability Management System in September 2016.

The firm is now utilizing eight Nodeware sensors, one for each of the firm's subnets, to scan its networks for devices and vulnerabilities. With Nodeware's true plug-and-play simplicity, the firm immediately gauged the health of each of their networks with Nodeware's internal scanning capabilities, and

leveraged the on-demand external scanning for themselves and their clients.

From the firm's perspective, Nodeware is the ideal solution for their vulnerability management needs due to several key attributes: the low price that caters to SMBs, the simplicity and ease of use of the solution and its UI, and the continuous monitoring with email alerts that enables to real-time security.

Due to the effectiveness of Nodeware and overall experience with IGI, the firm also leveraged IGI's cybersecurity services division in 2018 to perform penetration testing. By testing whether unauthorized access or malicious activity is possible, the firm was able to identify areas of weakness and fix them with the help of IGI's seasoned security team.

The Result

Nodeware filled a security gap for the firm by allowing them to easily manage their own network vulnerabilities and be responsive to client requests for vulnerability audits and reports. In the past, the firm made it a priority to run internal and external scanning annually, but now they're able to do so around the clock. This capability is important to clients and has positioned the firm as an industry leader in cybersecurity practices.

"The key benefit of Nodeware is the gap that it filled for us," said a Partner at the firm. "It's helped us be more responsive to clients' requests, as well as deliver something that clients are looking for. This shows our clients that we are making security a priority."

The firm's leadership and IT team has confidence in their security knowing that Nodeware is working to monitor each network, each device, and each vulnerability.