ARMIS | Rumberger|Kirk

Case Study

RUMBERGER | KIRK

Industry

Legal services

IT environment

250 employees across five locations in two states

Corporate Law Firm Gains Unprecedented Visibility into Assets and a Solid Handle on Potential Risk

Armis supports remediation efforts with rich, continually updated device information

As a regional litigation law firm with clients nationwide, Rumberger|Kirk knows how critical it is to maintain a coordinated and comprehensive approach to security. The firm's CIO has always believed in taking a preventative stance towards risk, which is what motivated his adoption of the Armis platform over three years ago. Not only does Armis provide extensive and deep visibility into known and unknown assets that connect to the corporate network, it also quickly identifies security gaps and vulnerabilities, which has helped evolve and enhance risk mitigation efforts.

A significant bonus is that by utilizing Armis, the law firm is able to confidently and favorably respond to questionnaires from existing and potential clients inquiring about the firm's cybersecurity protections and procedures. The impact on revenue from not being able to adequately address the security concerns raised in those questionnaires is no longer an issue for Rumberger|Kirk.

With proficiency in more than 20 practice areas—from corporate law and intellectual property to insurance and consumer defense—RumbergerlKirk provides expert litigation and legal counsel for clients in four locations in Florida (Orlando, Miami, Tampa, and Tallahassee) and in Birmingham, Alabama. The firm conducts early evaluation of cases, with the goal of settling cases for clients without incurring the cost of trial preparation whenever possible.

CIO Avi Solomon, who has been with the firm for nine years, works out of the Orlando headquarters office and is responsible for all things having to do with technical implementation, security, and IT. He holds numerous certfications, including the CISSP certification (security), and manages a team of six technology professionals. With close to 27 years of IT and security experience in the legal field, Solomon is especially attuned to the data protection and security needs of his firm.

“Law firms have become an attractive target for malicious activity, as they hold highly sensitive information on behalf of their clients—especially if they work with corporate entities with patents or M&As. Instead of going after one corporation, attackers can go after one law firm and gain access to data of hundreds of corporations,” he says.

He is always proactively looking for ways to step up the firm’s security posture, especially when it comes to defending its corporate network.

Priority one: protecting the corporate network

Solomon takes a multi-faceted approach to battling risk, taking into account factors such as people’s susceptibility to social engineering, attack tactics, and security gaps. But the biggest issue that keeps him up at night is safeguarding what he calls “the soft underbelly of the environment,” that is, the corporate network. He strives to keep a sharp eye out for attackers who leverage social engineering tactics to insinuate themselves into the corporate network.

Challenges

- Gaining visibility into unknown devices on the corporate network
- Having a single source of truth about connected assets
- Pinpointing and addressing vulnerabilities in a timely fashion
- Protecting employees and sensitive client data

How does he protect the law firm's environment? As he says, this requires having the right tools in place and "having visibility into the devices that are on the corporate network so we can evaluate where the high-risk points are and address those."

Armis as a visibility, risk mitigation, and accountability tool

Always taking a proactive stance to security, Solomon needed a tool that would help with vulnerability management so that he and his team could "get in front of a problem before there is a problem."

He was most impressed by the ability of Armis to solve his top concern: "The biggest fear I had was around devices appearing on the network that I didn't know about. That's what I consider the blind spot. Managing what you know is relatively easy; managing what you don't know is where the biggest risks lie."

Solomon initially considered a competing product, but in due time, he found the vendor difficult to work with during the sales process when contractual negotiations reached a stalemate. At a conference, he learned about the capabilities of Armis. To his delight, he later found out that Armis was also far more open to working with him on his fair and reasonable contractual requirements.

"I discovered how Armis fingerprints devices in order to discover what's out there and tell me what I've got on the network—that blew me away," he says.

Solomon did a proof of value (PoV) but did not feel the need to measure Armis against its competitors.

Since then, he has come to appreciate the many benefits that Armis provides: his firm has been an Armis customer for well over three years.

"At the end of the day, I have a solution that keeps everybody honest. When devices that meet certain criteria

Armis Results

- Exponential increase in visibility to network assets and devices
- Understanding and addressing risk with vulnerability management
- Fast and easy access to relevant, highly detailed data on devices when issues arise
- Protecting the privacy of employees by detecting unapproved cameras on the network
- Meeting the security requirements of the law firm's corporate clients

show up on my network, I get alerted by Armis. If I need to inventory how many devices I have and check to see if they are at an acceptable level of risk, I can do that. Armis is dynamic, so I never worry about stale data," he explains.

Exponential increase in visibility coupled with superior vulnerability management

Armis has improved visibility to a level Solomon could never have reached previously. "Armis has allowed me to have exponentially better visibility, control, management, and insight scaled by a factor that was unimaginable before. Prior to that, it felt like I had limited vision or wearing glasses with the wrong prescription," he points out.

For Solomon, one of the key advantages of Armis—and indeed the main reason he adopted the platform—is its asset vulnerability management capabilities. He finds it highly advantageous to have information about any given asset—including the asset owner, its location, what it is communicating with, and more—at his fingertips. When discussing the security posture of a particular device with his team, he can pull up the console and see a rich set of information on the device. It immediately points him in the right direction toward understanding the device, its communications, and remediating any potential risk. This helps Solomon gain a more complete understanding of the law firm's attack surface, how each asset may expose the organization to risk, and what actions to take.

"That's one of the most important pieces for me. I know about devices when they are on the network, and, with Armis's vulnerability management capability, I can feel comfortable if somebody plugs something in tomorrow, I will know about it, and I will know what level of risk it brings," he explains.

Discovering unknown and hidden devices

While Solomon had a good handle on PCs, printers, and other business devices on the corporate network, there were a whole host of assets that he wasn't aware of until he deployed Armis. These included everything from devices embedded in walls to switches built into conference tables. He now is able to tag all the devices he is aware of and can start digging deeper into any new ones that Armis discovers.

"While I am investigating these devices, Armis is learning about them and is reporting back the risk associated with each one," he says. "As I get to know about the device, I get an alert that it may be a risky device, so I am compelled to act, whether that means removing it, updating it, or patching it — whatever is necessary to mitigate that potential risk."

Keeping rogue devices and individuals in check

Solomon has seen his share of unusual devices. He once received an alert about a Raspberry Pi, a small, single-board computer, that was attempting to come online in the airspace of an access point at one of the law firm's locations. After investigating the matter, he discovered that a nearby neighbor in the multi-tenant complex where Rumberger|Kirk has their offices had a Raspberry Pi that was attempting a connection. Thanks to a strict policy rule disallowing Raspberry Pi computers, the device's attempts to connect were foiled.

He is also concerned about rogue individuals who may place cameras in inappropriate places, impinging on the corporate environment and on employees' right to privacy. "I'm very concerned about watching out for our people, and Armis is one way I can do that. I have a rule that, when anybody attempts to connect a camera to the corporate network, I immediately get an alert. This is one more way I

> "At the end of the day, I have a solution that keeps everybody honest. When devices that meet certain criteria show up on my network, I get alerted by Armis. If I need to inventory how many devices I have and check to see if they are at an acceptable level of risk, I can do that. Armis is dynamic, so I never worry about stale data."
>
> **Avi Solomon**
> CIO
>
> Rumberger|Kirk

can be a good citizen at my organization so that people can feel comfortable in the workplace," relates Solomon.

Integrations play a key role in risk management

Solomon and his team have integrated Armis with nearly a dozen solutions, including the firm's endpoint detection and response (EDR) system, cloud platform, Microsoft, and multi-factor authentication (MFA) tool.

Another important integration is with an agent-based inventory management system, which is tightly tied into Microsoft Active Directory and provides up-to-date, nearly microscopic details on Microsoft-oriented devices and assets. This rich store of information is fed into the Armis console, a single, central location where Solomon can see everything he needs to know about people, devices, and other assets—whether they are known or unknown, new or old. Additionally, he has vastly improved visibility into what is on the law firm's corporate network at any point in time and receives alerts if there are devices that are risky.

Down the line, Solomon intends to integrate Armis with firewalls to implement policy enforcement, which would work much like a network access control (NAC) solution in the environment. He envisions creating a policy in Armis and then leveraging that policy to determine enforcement action. Since Solomon and his team handle day-to-day oversight in-house, this type of integration would be especially useful for after-hours monitoring.

Armis is great for business

Solomon has uncovered an unforeseen and welcome use case for Armis. Often, the law firm is asked by a potential corporate client to answer a security questionnaire to assess its security maturity. Solomon had an "Aha!" moment when he received the first of many questionnaires and realized how many questions he answered with "Armis." At times, clients ask RumbergerlKirk how often the firm scans for vulnerabilities during the year. Solomon is able to confidently respond with "We do that with Armis 24 hours a day, 7 days a week. Our scanning is near real-time."

"Armis has allowed us to answer a good percentage of those questions to the clients' satisfaction. If you have potential clients coming to you requiring a certain level of security in your environment and don't have that, they won't give you the business. There's no question that we are more successful in securing opportunities, because we have the right tools in place," Solomon asserts.

Passing third-party penetration testing with flying colors

To test the robustness of the law firm's security, every year Solomon engages an independent third-party organization to conduct penetration testing. This year was the first time that Solomon requested a red team/blue team exercise, where the red team (the third party) simulates an attack and the blue team (RumbergerlKirk) attempts to defend against the attack. The third party first tried to penetrate the network from the outside using

social engineering tactics, but that was unsuccessful. The red team/blue team then went to an “assumed breach” scenario, where they attacked from the inside and tried to escalate the attack internally. Once again, the third party failed. Not only did the law firm’s security controls prevent them from loading a malicious command-and-control server, the third party’s lateral movement to search a risky domain name triggered an alert from Armis.

“This was the first year that they were completely unable to make progress,” says Solomon. In 2023, he plans to take the penetration to another level and hopes for a similar result.

Solomon finds it rewarding to communicate with the Armis team on a regular basis and offer his insights, experiences, and suggestions on how to further fine-tune the product and grow its capabilities. As a long-time user of Armis, Solomon observes that “It’s been amazing to see the growth in the product and to see how technically focused Armis is—that is so important to us.”

About Armis

Armis is the leading unified asset intelligence and security platform designed to address the new threat landscape that connected devices create. Our customers trust our real-time and continuous protection to see with full context all managed, unmanaged, and IoT devices, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS). Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in San Francisco, California.

1.888.452.4011 | armis.com