ARMIS®

RS RUSSELL SAGE COLLEGE ALBANY & TROY

CASE STUDY

Upstate New York College Gains Deeper Visibility into all Connected Devices to Help Manage Insider Risk

Armis provides Russell Sage College with actionable insights to help tighten up security, stay compliant, and check the boxes for cybersecurity insurance.

Industry

Higher education

IT environment

Approximately 2,500 students and 450 employees and an environment consisting of managed, unmanaged, and IoT devices.

Introduction

Established more than a century ago as a women's institution of higher learning, Russell Sage College has evolved into a coed college that prides itself on its flexible academic programs and its supportive learning environment. Eager to improve device visibility and reduce security risk from inside the network, the IT department deployed Armis. The platform increased IT's device inventory 15-fold, enabling the team to find previously unseen assets, apply necessary updates, retire old equipment, and fine-tune policy. Armis has also helped the college meet stringent compliance and cybersecurity insurance requirements.

Founded in 1916 by feminist Margaret Olivia Slocum Sage and named after her late husband, Russell Sage College in Troy, New York catered exclusively to women, offering them a solid liberal arts education and career preparation in various professional fields. Today, it is a coed institution with undergraduate, graduate, and post-graduate programs in arts and sciences, education, health sciences, and business management. The college has over 2,500 students and 450 employees, including more than 100 full-time faculty members across its two campuses in upstate New York State (Troy and Albany). Russell Sage College prides itself on its supportive and high-engagement learning environment, with 10 to 1 student/faculty ratio and average class size of 15.

When homegrown is not good enough, Armis steps in to do the job

Assistant Director of IT and System Engineer John Harris, who is part of a team of six, has been with the college for 15 years and oversees all things technical—from security and compliance to the IT service desk and audiovisual resources. The managed IT estate consists of approximately 150 switches, 300 servers, 2,000 endpoints, and peripheral devices such as printers, scanners, cameras, and projectors. The number of unmanaged devices, which are primarily used by students and some employees, is about 15,000 (five devices per student). The college has well-defined acceptable usage policies that govern how students, faculty, staff, and guests use college-owned equipment and their own network-connected personal devices.

For years, Harris had been using a home-grown tool to manage the security posture of these assets, but he was getting increasingly frustrated chasing false positives—and he was not getting a complete picture of what was connecting to the network. “I had no clue what people were doing on the internet until someone triggered a firewall alert,” he said. “We needed a better solution, and that’s why we evaluated Armis.”

Harris connected with an Armis partner and decided to conduct a proof of value (PoV). Within only two to three days, Armis demonstrated its capabilities, identifying up to 30,000 devices on the college’s network.

Armis uncovers the unusual

There were a number of surprising devices discovered by Armis, including multiple internet of things (IoT) devices that the maintenance department had installed without informing Harris and, even a connected car. He also learned that many people were using outdated operating systems, such as Microsoft Windows 98, which clearly are a security risk. In addition, there were several inexpensive smart TVs used from instructional and entertainment purposes flooding the network and smart washing machines located in student dorms. All of these significantly slowed down network performance.

“Another big thing that Armis really helped us with is our printers. We didn’t realize that we were running so many different protocols for these peripherals—and these could potentially be exploited by malicious actors.

Challenges

- Getting visibility to insider risk.
- Discovering unmanaged and IoT devices.
- Meeting cybersecurity insurance and compliance requirements.

As a result, we set a policy to only allow the TCP/IP communication protocol for these devices. When we eliminated all the other protocols, we had a significant drop in network traffic," explained Harris.

Armis also discovered Hikvision cameras, which are made by Hangzhou Hikvision Digital Technology Co., Ltd., a Chinese governmentowned manufacturer and supplier of video surveillance equipment for civilian and military purposes. Armis helped Harris monitor outgoing communications and enabled him to isolate these devices to prevent potentially malicious activity from spreading across the college's network.

Corrupted settings, or vulnerabilities that can cause disruptions in internet connectivity and lead to DDoS, MiTM, or port-spoofing attacks. Based on this type of feedback from Armis, the team has been able to set automated security policies for various scenarios.

Integrations supercharge Armis

Harris and his team integrated Armis with key solutions in the college's technology stack, including Microsoft Defender for anti-malware protection, VMware to enable virtualization instances, Tenable for vulnerability scanning, Microsoft InTune for managing corporate and BYOD devices, Microsoft SCCM for configuration management, and Palo Alto Networks firewalls. As Harris describes it, all these integrations enable Armis do its job better.

"If something triggers the Armis-Palo Alto Networks firewall integration, the firewall blocks it and keeps it from going out—and that's really slick," he remarked. In this use case, Harris configured the automated authoritative quarantine capability in the Palo Alto Network firewall. Even if the alert is a false positive, it's easy for his team to clear it out. The Armis-Palo Alto Networks firewall integration eliminates the time and effort involved in going into the firewall, making changes, and reloading.

Armis Results

- Visibility to all devices—managed, unmanaged, and IoT—across both campuses.
- Faster remediation based on actionable information on device security posture and behaviour.
- Automated detection and response as a result of integrations.
- Adherence to compliance regulations.
- Improved security posture to meet cybersecurity insurance eligibility.
- Reduced burden on the IT team.

Armis simplifies internal visibility, asset management, and security

As Harris points out, his team has done an admirable job of keeping the college safe from outside threats. But keeping the college secure from potentially malicious insider threats—which are typically unintentional— has been a challenge, as students and faculty use personal devices that are not always updated with the latest operating systems and security protections.

Armis has noticeably simplified that task for Harris and his team, as it not only passively monitors devices on the network to detect malicious behavior, it also catalogues a wealth of information about them—from the IP address and OS to connection type and internet domains accessed. And that applies to IoT as well. Armis has helped the team identify and retire outdated IoT devices.

For asset management, Harris uses open-source Snipe-IT. Armis works seamlessly with this software and enables Harris to keep his inventory current. Harris pointed out that it's easy to run the scans with Armis and sort devices by category.

"All our college-owned computers are certain models, and Armis does a really great job of fingerprinting them. We can flow that asset data right into our management software and make sure the devices are properly updated with the latest OS and security patches," he observed. "If anyone asks me about a given device, I can find out in minutes exactly where the device is, what it has been doing, and what it is communicating with. Armis has made our lives so much easier and our campus so much more secure."

Overcoming cybersecurity insurance and compliance hurdles

Armis has also helped the college meet stringent cybersecurity insurance requirements. In the recent past, Harris and his team engaged a security assessment service to help them get a handle on their security posture and risk score. The college scored well on almost all parameters except for the fact that there were many older devices and old browsers in use—mainly by students.

"If anyone asks me about a given device, I can find out in minutes exactly where the device is, what it has been doing, and what it is communicating with. Armis has made our lives so much easier and our campus so much more secure."

John Harris
Assistant Director of IT and System Engineer
Russell Sage College

But the service didn't provide any information on the devices beyond that. Armis, on the other hand, expands the team's visibility, enables them to drill down into the details about devices and allows them to take corrective measures. For example, if Harris sees a device with an old browser, he can send the user a warning and ask them to update the browser.

Like any educational institution, Russell Sage is required to comply with Family Educational Rights and Privacy Act (FERPA), which protects the privacy of student education records. For every piece of student data that is compromised, colleges can get fined as much as $100,000. The college wellness center is also expected to comply with Health Insurance Portability and Accountability Act (HIPAA), which safeguards sensitive patient information. Because Armis aligns with the industry standard Center for Internet Security (CIS) Critical Security Controls, it helps the college adhere to these requirements. For example, if there is a Social Security Number that goes across the wire, Armis provides immediate visibility into that data and blocks the traffic.

Plans for the future: use Armis to its full potential

On the agenda for the future is learning to leverage more of Armis's capabilities and finding new cases for it.

"We've barely scratched the surface of what Armis can do, and we are looking forward to exploring its functionality more deeply and spending more time with it. We've pretty much picked all the low-hanging fruit, and now our goal is to keep getting better and better at using Armis," remarked Harris.

He also knows that, as he and his team deepen their understanding and utilization of the platform, help is always at hand. "I've been very impressed with the Armis support team. If I ever have a problem, it gets taken care of and they don't close the issue until we are happy with the resolution," said Harris.