Case Study

San Antonio Area Foundation

The San Antonio Area Foundation is San Antonio's premier fundraising foundation and distributor of grants to other non-profit organizations. Kamin Associates, Inc., their Managed Service Provider, is a San Antonio based Information Technology company, specializing in computer systems management and networking solutions with a high degree of expertise with managing sensitive financial and data environments.

The Challenge

The Area Foundation's fundraising personnel are prominent people with high profiles. They seek funding from prominent, wealthy and high profile individuals, family funds, and institutions. The information they store both on premise and on the laptops and mobile devices is highly valuable and sensitive personally identifiable information (PII). The confidence and reputation of storing this information is critical to their existence and purpose.

A significant increase in people accessing sensitive information from remote locations, rather than the office due to COVID 19 required them to take extra diligence in knowing that data was safe and secure. Even before COVID, they had inconsistent enforcement of policy on IT-controlled internal assets and personal devices accessing the network. They did not have a clear picture of where all their user, computer, and application assets were, what computers had what data on it and where it was.

Kamin Associates was the outsourced Managed Services to augment the Area Foundation's IT department and facilitate their IT operations. As a finance business they are also required to maintain regulatory and proper IT hygiene to audit all systems they have once a month.

Most of their computers are being IT controlled while a growing number are end user personal computing devices. Due to COVID-19, the Area Foundation has needed to adjust from a full on-premise work environment to a hybrid remote work model, posing challenges in tracking computing equipment, data and user access. Being very conscious of the risks to their organization and the students, they endeavored manually to track the cell phones and computers the employees are using to access the network and what applications and data they access.

"From our devices, users, services and data, Sevco has given the Area Foundation a scalable view of our entire IT environment in real-time."

Gary Wise | Director of Technology | San Antonio Area Foundation

www.saafdn.org

Previous Approach

They had a hybrid of reliance on excel and some agent sources to manually aggregate, and constantly try to keep up with this information. The Area Foundation's internal IT Director manages computing resources, patch management, help desk, and software administration. His efforts to maintain some semblance of inventory were simply manual and sporadic.

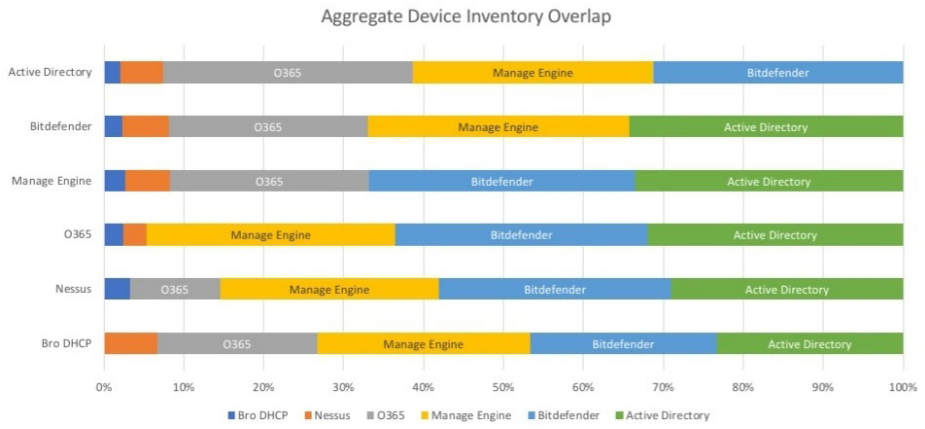
More specifically there were data management challenges coordinating the internal Area Foundation resource management practices with Kamin Associates information management applications they needed to ensure compliance and visibility. Additionally, to ensure compliance, the activity also required a project management process to gather all the information, investigate errors and omissions, compare across data sources, and report. This took three to five work days a month and usually disrupted business operations to obtain the data—all without being exact.

How Sevco Security Helped

Sevco Security Inc. conducted a 30 day application of the Sevco Asset Operations Platform at the San Antonio Area Foundation with the goal of identifying a **speedy** and **accurate** inventory of devices and users. Seven sources were leveraged to create an aggregate inventory.

All systems queried had a partial view of the device inventory, but no system had the complete view.

San Antonio Foundation identified approximately 30% **more** devices than they thought they had accessing their network. Also 57% were accessing the network from off-premise. Sevco's platform enabled visibility and control over the disparity of devices and users that were dynamically changing. Understanding of the context of the environment enabled them to see more vulnerabilities from devices that did not have controls on them, identify inappropriate configurations, unaccounted for application licenses and improper network rights. They also received insight to systems using deprecated operating systems, incomplete patches and people who had not changed their passwords in 180 days—a policy violation.



Benefits

- Audits are now automated
- Total time is less than 30 minutes a month to get the same information
- At any point in time, they can constantly monitor who has what with what on it
- Information is unified, consistent and shared between the Area Foundation and Kamin Associates MSP
- Overall better visibility to the IT environment
- Overall better understanding of risk
- Overall quicker time to investigate aberrations
- Overall better decision making

Sevco Security automates and captures the information that is manually attempted, but with greater accuracy and consistency and without all the effort.

Contact Us

sevcosecurity.com

@SevcoSec

1401 Lavaca Street
#857 Austin, TX 78701

About Sevco Security

Sevco exists to fix a decades-old problem: attackers know the networks they target better than the companies that own them. Sevco is a cloud-native asset intelligence platform that delivers converged asset inventory and generates real-time asset telemetry, then publishes both for use by other IT systems. Sevco makes sense of the data our customers already have, making their existing products and procedures more effective. Founded in 2020, Sevco is based in Austin, Texas. For more information, visit https://sevcosecurity.com or follow us on LinkedIn and Twitter @SevcoSec.