CASE STUDY

Financial Services Organization Gets a Reality Check On Its Assets

True, comprehensive asset management from a trusted vendor dedicated to resolving customer issues

Customer profile

Global financial services organization

Industry

Financial services

IT environment

Approximately 500 employees distributed across 15 offices worldwide, with a footprint in every continent

Introduction

In business for decades, this global financial services organization found it challenging to manage its growing inventory of digital assets, in part due to lack of visibility to its growing cloud infrastructure and to remote employees who travel frequently on the job. With disparate and often conflicting data from a dozen sources, the organization struggled to gain a better picture of its digital and physical environment. After implementing Armis, the financial services organization was able to get a clear, comprehensive view of its assets, along with insights into vulnerabilities. Best of all, Armis proved to be a trusted, collaborative partner dedicated to solving the organization's problems and addressing their security concerns.

Managing the security challenge of global operations

This rapidly growing global financial services organization is headquartered in the U.S and has approximately 15 offices worldwide. Many of the approximately 500 remote employees frequently travel all over the world for meetings with partners and other stakeholders. The organization also uses numerous cloud services and applications. In a highly regulated industry like financial services, maintaining strict security controls to protect privacy and valuable data are always top of mind.

The Director of Security Engineering works with the CISO on a daily basis to harden and continually improve security. He sees asset management as a critical and essential foundation for effective security. Every day, he reviews multiple data sources from various products that show how their assets are interacting. The problem is, the data revealed a great many discrepancies. There was no definitive, single source of truth about what was on the organization's network.

"Our biggest challenge was to understand what our reality is—what we have from an asset perspective. How can we consolidate and reconcile all these differences?" says the Director of Security Engineering.

Understanding the importance of asset inventory in any security framework.

According to the company's CISO, "Asset inventory is the first thing you need to do well in order to do security well." He adds, "If you are trying to protect a battlefield, a castle, or your home, you need to know where all the doors are, all the ways in, all the vulnerabilities, so that you can address these security gaps. And when you deploy your countermeasures, you need to know that they are operational and are working the way they are supposed to. Having visibility to this is critical in a complex and distributed organization like ours."

Following that line of thought, the organization made a strategic decision to build a secure "perimeter" around its devices and users while still maintaining its strong corporate network perimeter. But, as the CISO points out, simply focusing on network perimeter security is a "faulty model" because the perimeter has dissolved as a result of the cloud, work-from-home, and other technology trends. The security team needed to get relevant details on users and devices—where they are, what software they are using, where they browse—and then collect telemetry on all those pieces of information.

"We've had a long road of connecting data sources to our central logging platform. We started to feel comfortable that we had wrapped our arms around everything, but we could not prove it. That's when we started going down the asset inventory path," explains the CISO.

For a long time, the CISO believed that asset management was a security problem that would never be solved. The security team looked into a number of solutions for asset management and ultimately made a decision to choose Armis.

"Every methodology I looked at was painful. And I saw that none of the new tools worked the way they should. The pace at which new types of assets crop up makes it really hard to discover, categorize, and inventory them," he observes. "What I have seen thus far from Armis gives me hope. This is because Armis looks at assets more holistically. We're excited to be on the journey with Armis."

Challenges

- Getting a handle on asset management across the organization's entire footprint
- Making sense of data discrepancies to derive a true picture of the environment
- Collecting telemetry on remote users and their devices
- Understanding vulnerabilities and their implications for the organization's security posture
- Identifying a vendor ally with whom the organization could work closely to resolve issues

Partnership matters

Multiple factors were at play in the decision. In addition to favorable pricing and the solution's capabilities, the CISO's relationship with the Armis team was a crucial differentiator. In his prior role at another company, the CISO was Armis's first customer in the U.S. and that's when he cultivated a highly collaborative and close connection with the Armis team. As he says, "The relationship is as important as the product. And for us, that's really important. This is something we did not get from the competitors, who looked at us as a number, just another customer ID in a long list of customer IDs."

When the CISO evaluated asset management vendors, they presented the vendors with a list of what he and his team wished to accomplish, the things each solution does well, and what his team needed but was not included in the product.

"When we talked to competitors, they had no real answers or assurance that they would supply us with what we really needed," observes the CISO. He found that, more often than not, other partnerships he tried to establish with vendors did not work to everyone's mutual benefit. Most vendors, he asserts, are just interested in making a sale and there is little real interaction or commitment beyond just a vendor-customer relationship.

With Armis, it was a completely different story. When the CISO approached Armis with his ideas, Armis team members were eager to roll up their sleeves and work with his team to solve their problems and address their concerns.

"Armis saw this as an opportunity to make the product better and leverage our knowledge and expertise. And we saw it as a way to work with a partner who would join us on this journey," remarks the CISO. "Armis saw the value in the ideas that we brought to the table and reflected that in the way they worked with us and in the pricing. It was a really good fit. Now, 12 months later, I feel that we made the right decision."

Armis Results

- Bringing together and reconciling data from multiple sources on a single, centralized platform for greater accuracy
- A good asset inventory solution offering visibility into assets across users, devices, and networks
- Providing foundational data that can enable behavior analytics in the future
- Alerting when new devices connect to the network and protections are not installed, not running optimally, or improperly configured
- Close, collaborative relationship with a caring vendor, resulting in faster problem-solving and additional product enhancements

Integrations contribute to a wholistic view of assets

An important advantage that Armis brings to the table is its ability to easily integrate with other solutions. Data flows into Armis from approximately 12 sources: from traditional sources, such as Microsoft Active Directory and the Microsoft Azure cloud platform, and on the network side, from switches and firewalls. Armis can easily detect agentless devices as well. The aggregation of large amounts of data in one place is a huge boon for the team.

“No other vendor is able to bridge the gap between the network-level data sources and asset-level data sources”, says the Director of Security Engineering. “Armis does a really great job of marrying those two.”

The financial services organization now has a high-level view of assets that closely coincides with a matrix they use that maps NIST security operations categories to assets. The matrix names five asset types: devices, networks, users, data, and applications. The CISO notes that most asset inventory solutions focus primarily on devices and rarely on the other categories: “We were interested in getting visibility into all five asset classes because that’s what asset inventory means. With Armis, we get a wholistic view of assets in most categories. We can see the data and discover it in one place.”

> *“Armis is much more than an agentless asset management tool—it’s a mind map that shows us how our assets are connected and how they are behaving—and I really like that. Armis has a lot more power than other competitors we’ve come across.”*
>
> **The Director of Security Engineering**
> **Financial Sector**

The strength and potential of Armis analytics

Another benefit provided by Armis is network-level analytics. The Director of Security Engineering is impressed with how Armis displays information based on service level, traffic level, and device connection level. And it goes even further, showing how devices are connecting to the networking at the switch level.

In the future, the Director of Security Engineering foresees using Armis for device-level analytics. He also plans to leverage machine learning technology in combination with Armis data to derive connection-level behavior analytics.

"That type of data is not something we can easily get from other vendors. While this project may happen in the future, we're confident that we can make this happen. Armis provides an accurate and rich data set that's already aggregated, so I know we can do a whole lot more than what we're doing right now—and I'm excited about that," he declares.

Additionally, as more employees come back to work on site, the team will take advantage of another Armis feature, namely alerting on new devices that join the network, never-before-seen applications on a given machine, and status on security protections that may not be running correctly or are not even installed on the device. As the CISO puts it, "It's not enough to know I have something. I need to know that it's in good working order and whether it needs to be updated. Armis does a great job with that, and we plan to make use of that in the near future."

With Armis in place, the Director of Security Engineering believes that Armis provides the organization with a strong foundation on which his team can build a more resilient security strategy and infrastructure going forward.

"Armis is much more than an agentless asset management tool—it's a mind map that shows us how our assets are connected and how they are behaving—and I really like that. Armis has a lot more power than other competitors we've come across," he concludes.