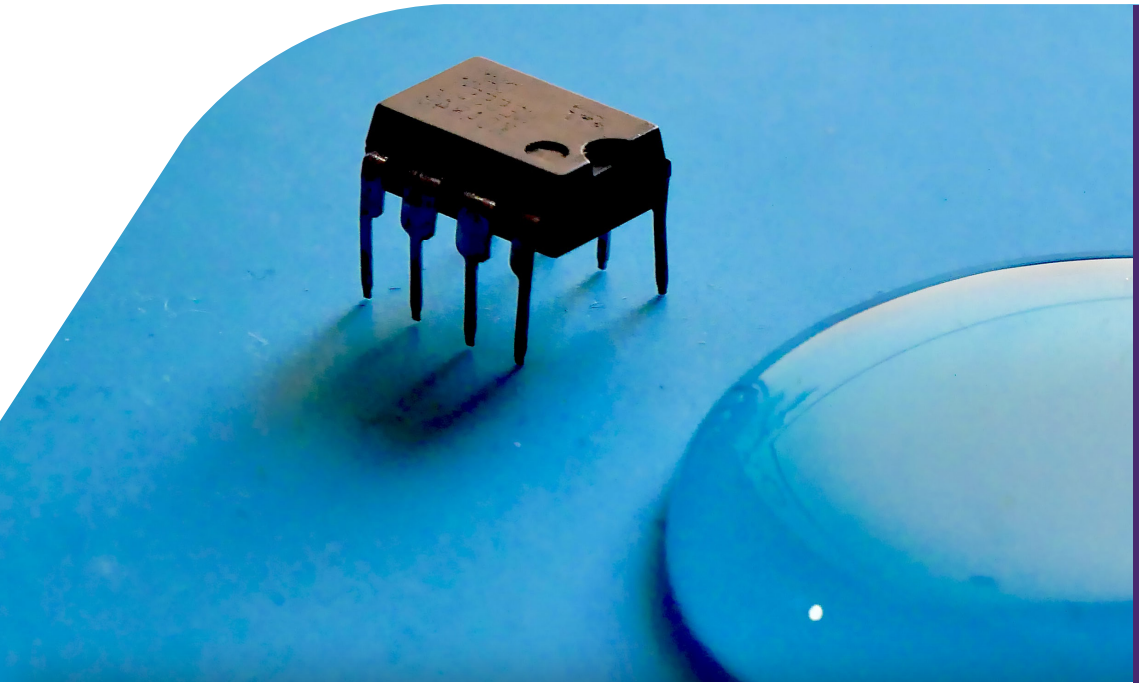

ALLEGRO MICROSYSTEMS

Customer profile

Global semiconductor leader in power and sensing solutions for motion control and energy-efficient systems

Industry

Technology

IT environment

More than 4,000 employees worldwide, with many managed and unmanaged BYOD assets across its global locations

GLOBAL SEMICONDUCTOR COMPANY UNCOVERS THOUSANDS OF NETWORKED DEVICES

Armis adds enhanced visibility for increased confidence and stronger protection

Allegro MicroSystems has been an established leader in the semiconductor industry across multiple sectors for over 30 years. Concerned about protecting vital corporate data in its growing cloud environment and about the lack of visibility into devices connecting to its IT and OT networks, Allegro MicroSystems decided to leverage Armis as a much-needed extra layer of defense for its entire corporate estate. Armis provides the IT team with insights into network activity that were previously not available with existing security tools.

CONNECT WITH US

Allegro MicroSystems has more than three decades of experience developing advanced semiconductor technology and application-specific algorithms for the automotive, industrial, and consumer sectors, helping customers make breakthrough advancements in areas like advanced mobility, green energy, and factory automation. Allegro MicroSystems leads the industry in the development of sensing solutions for motion control and energy-efficient systems, shipping more than one billion units to over 10,000 customers all over the world every year, including over 50 automotive OEMs.

Leading the company's team of IT and security experts are VP & CIO Phil Stathas, Director of Global Operations Manager, Gary Gomes, and Senior Manager for IT Security, Mike Vigneau. The IT team runs like a well-oiled machine, with 85 employees split evenly between the organization's U.S. and Asia presence. Most team members have had a long history with Allegro MicroSystems and are committed to continually upgrading and strengthening the security of the company's far-reaching, cutting-edge infrastructure.

The organization even has its own team of developers, who have created and support more than 300 internal applications. They are also heavily invested in integrations with and migrations to the latest cloud offerings.

Monitoring the Movement of IP in the Cloud

Security at Allegro MicroSystems has always been a top priority for the IT team, with one of the biggest concerns being the protection of high-value intellectual property (IP) related to semiconductor designs and proprietary algorithms.

"Our IP is our bread and butter, so our biggest fear is the potential for exfiltration of these resources, particularly across our cloud footprint," says Stathas. "Like most companies of our size, we have a heightened concern about security, especially in light of escalating ransomware attacks and data breaches. Since Allegro MicroSystems is a public company, we also need to be accountable to and report to the board about our security posture—how we are protecting our assets and precious data."

Who and What Is Connecting to the Network?

To bolster protection for sensitive data residing in the cloud, Stathas and his team recently implemented a cloud access security broker (CASB) solution to enforce security policies and enable safe use of cloud services. Even so, the team felt that this alone was insufficient. They were especially concerned about the 3,000 employees at the manufacturing plant in Manila, the Philippines.

Stathas was familiar with Armis and a key competitor and did a side-by-side comparison. "The fact that Armis is agentless was a big selling point for me, along with its flexibility in policy generation, which is unique and different. My biggest source of trepidation was not having the resources to manage thousands of alerts, as was the case with the competing product. The availability of resources from Armis to help develop

Challenges

- Protecting and preventing exfiltration of patented intellectual property on premises and across the cloud infrastructure
- Detecting and preventing ransomware attacks and data breaches
- Lack of comprehensive visibility into devices connecting to the internal network, especially unsanctioned personal devices in manufacturing facilities that contain operational technology (OT) and industrial control systems (ICS).
- As a public company, required transparency in reporting its security posture

policies—and the fact that there was a team behind the walls of Armis to provide us with training, support, and consulting—pushed us in that direction."

Finding the Smoking Gun

Stathas points out that his team has already seen the benefits of Armis. "The challenge I put forth to the Armis people when they launched the proof-of-value (PoV) was this: 'show me the smoking gun,'" he explains. "What is the smoking gun? It's something we are not able to identify with any of the other tools we already had in place. And sure enough, Armis did just that."

The team then threw out an additional challenge to the PoV team. A big problem facing IT was rogue devices connecting to the wireless network in the Philippines. These users are primarily operators who bring in their personal mobile phones and tablets and hook up to the network to listen to their latest podcasts or speak to their relatives.

"No matter what we did to lock it down, people came up with creative workarounds," he points out. "If you can't find it, you can't stop it. We had no idea what was on those devices, so they represented a real risk. It's hard when you're thousands of miles away from Manila, so Armis is allowing us to exert some control over individuals who don't follow our security policies."

Getting a View into the OT Network

As a manufacturer, Allegro MicroSystems was also concerned about security issues arising from the convergence of its IT network with its OT network. While the organization had reliable asset tracking for the corporate network, it had little visibility to factory floor devices.

"Armis identified a number of networked programmable logic controllers (PLCs) and shined a light on their vulnerabilities, so this was a clear indicator that Armis could go beyond just the standard IT devices on the manufacturing floor," observes Vigneau. "For example, in our Manchester, New Hampshire location, we were able to detect personal devices crossing over from our guest network into the Allegro MicroSystems internal wireless network. Armis gave us a lot of visibility into the OT side that we never had before. With Armis, we can see both OT and IT devices from a single pane of glass."

A Steady Rollout to Global Locations

The PoV provided a head start on the deployment, first in the Philippines, where two Armis appliances are currently installed, followed by an appliance in Marlborough, Massachusetts and one in Manchester. Currently in "a learning phase" as he puts it, Vigneau and his team is in the process of installing eight additional Armis appliances to other locations worldwide, including South America, four of the company's larger European locations where IT staff is available, and several other U.S. sites.

From the moment the Armis appliances were plugged in at the outset of

Armis Results

- Provides an enhanced layer of security that offers visibility into IT and OT networks from a single pane of glass
- Discovers a significant number of personal and unmanaged devices connecting to networks, especially in overseas manufacturing plants
- Safeguards vital data across the cloud environment
- Enables policy setting and enforcement corporate-wide
- Offers both high-level and granular reporting on security posture for the board and equity partners
- Integrates into existing IT and security tools to enhance their capabilities.

the PoV, the team realized immediate time-to-value. “At first, prior to the PoV, I was skeptical about Armis and didn’t believe that it could offer us anything more than our existing tools could offer. But Armis proved me completely wrong. It was unique and differentiating—all the more reason to make the investment,” says Stathas.

Vigneau is now confident that Armis will help his team identify and block suspicious devices, and this will result in significant time savings and a decline in malicious activity on the network in the near future. As he asserts, Armis is an invaluable addition to the company’s security defense. With the information provided by Armis, his team finds it easier to do incident response.

“I see Armis as an aggregate of our solutions, providing a centralized dashboard that provides us with more comprehensive visibility. Another big plus is that it integrates with most of our existing tools” says Vigneau.

Armis Drills Down into the Details

Another way in which Armis has helped the IT team tighten up its processes is by detecting expired or about-to-expire software certificates. Vigneau and Gomes have always been diligent about ensuring that certificates are renewed in a timely fashion, but Armis uncovered some that had been overlooked.

“We found out through Armis that we had a certificate that had expired or was about to expire, and we didn’t know about it. It would have impacted our operations had we not dealt with it. This helped us realize that we were not doing as good a job babysitting certificates as Armis was doing,” remarked Gomes.

Armis Helps Maintain Peace of Mind

Creating security posture reports for the executive team is another clear benefit offered by Armis. Stathas reports to the audit committee on a quarterly basis, typically prior to the earnings call. Thanks to Armis, it’s easy for the audit committee—which consists of tech-savvy board members and members of the Allegro MicroSystems equity partner firm—to get a handle on the security mechanisms that have been implemented and the company’s overall risk profile.

According to Stathas, Armis has offered unparalleled value in terms of increased comfort and security: “Armis is helping me shorten my sleepless nights list, especially with regard to security of remote locations, visibility, and asset management.”

> “I see Armis as an aggregate of our solutions, providing a centralized dashboard that provides us with more comprehensive visibility.”
>
> **Mike Vigneau**
>
> Senior Manager for IT Security
> Allegro MicroSystems

About Armis

Armis is the leading unified asset visibility and security platform designed to address the new threat landscape that connected devices create. Fortune 1000 companies 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 Palo Alto, California.

armis.com

info@armis.com

20220204-1