IoT Platform Leader Armis eliminates dependency on VPN technology, Adopts Axis Zero Trust solution

How a global security platform company defied convention, strengthened security and reduced VPN infrastructure costs by 90%

Founded in late 2015 and headquartered in Palo Alto, California, Armis is the leading agentless, enterprise-class security platform to address the new threat landscape of unmanaged and IoT devices. Armis discovers devices on and off the network, continuously analyzes endpoint behavior to identify risks and attacks and protects critical information and systems by identifying suspicious or malicious devices and quarantining them.

New CISO, New Priorities

In August 2019, Armis appointed Curtis Simpson as Chief Information Security Officer. His responsibilities include ensuring the Armis product continues to maintain its high standard and vigilant focus on platform and customer security and privacy.

As part of his initial risk management review, Simpson identified the opportunity to further mature and optimize remote access use cases. Though Armis' remote access capabilities were highly secure, multiple solutions were involved in delivering a less than optimal user experience. Similarly, though appropriate monitoring controls were implemented to identify insider and external threat events, the process to respond to such an event was not as real-time as desired.

Simpson also identified an opportunity to further improve insights into external SaaS application usage not only to validate and, as required, update least privilege role designs but also to detect potential misuse or malicious behavior. These insights are most effective when considered not just per session, but compared across recent and past behaviors and actions. This degree of visibility is critical for an optimized capability.

> “Axis Security is delivering a zero trust approach that offers a modern solution to a modern problem. Axis is a security tool, not just a network conduit. It is getting employees and third parties off the network, and we are able to understand the remote worker with great analytics, without time consuming manual processes that have to be built from scratch.”
>
> **Curtis Simpson, Armis (CISO)**

A Better Future with Zero Trust Network Access

Simpson and his team set out to find a Zero Trust Network Access solution that would be more than a conduit to connect. After discussions with several vendors in the ZTNA category, Axis Security emerged as ideally positioned to augment, extend and enhance Armis' existing VPN deployments with a new, modern approach to application access.

Why Axis Security?

Axis Security's vision for application access aligned with the vision of CISO Simpson. Axis sees a world where access to business applications is fully managed and secured based on modern cloud architecture, innovative technology and a zero-trust business-centric approach.

Like Armis' product solution, Axis Security is agentless. There is nothing to deploy on endpoints, no concerns over use of personal devices. There are no time-consuming network changes. Axis enables Armis to deliver secure, tightly managed private application access to virtually anyone, anywhere, on any browser-enabled device in minutes. This capability directly addresses the issues of the sales run around, and third-party access challenges.

How Axis met Armis' connectivity needs for employees, third parties:

1. A better user experience
Axis Security greatly improves usability and functionality for end users as a cloud-native solution. It delivers a familiar web-based interface that allows users to interact with managed applications from anywhere on any device.

2. Greater visibility
Axis Security eliminates blind spots into user activity, eliminates concern over the use of personal devices or home networks. The Axis Application Access Cloud provides complete visibility to the Armis team because it serves as a broker between all user access and the application. Axis can see it all and controls every request.

3. Reduced risk
Axis' Application Isolation Technology keeps users separate from the network and the application, greatly reducing the threat surface and the possibility of a hostile partner/user from gaining access to other network applications and systems. This is especially important when it comes to protecting Armis' Lab environment.

4. User analytics
Instead of making a binary authorization decision when the user first tries to access the application, Axis Adaptive Access Technology continuously assesses risk to restrict access as needed. Every user request is validated and authenticated based on the individual's policy settings. All users, internal and external, are treated with the same, Zero Trust vigilance.

Then came COVID-19

When COVID-19 hit and stay home orders swept the globe, from the California headquarters to the research and development teams in Israel, Armis was especially well prepared to quickly adapt from an infrastructure and access perspective with the Axis solution already in place.

The solution scaled from hundreds to thousands of users without the addition of hardware. Because users could leverage personal devices from home without downloading an agent, they gained immediate access to familiar applications safely (for them and IT) from home.

Safer Access, Lower Cost

The Axis Security Application Access Cloud has delivered on the promise of simple, secure and fully managed application access for Armis. As a result of its confidence in the technology, strategy and people at Axis Security, Armis is moving forward with the elimination of 90% of its VPN infrastructure and the many costs associated with a VPN, including the cost of hardware and third-party infrastructure maintenance and data center hosting costs. In addition, it circumvents the cost of managing, maintaining and monitoring a VPN infrastructure with five-nines availability, which is estimated to be in the hundreds of thousands of dollars per year.

> “
>
> Axis Security gave Armis the ability to face a challenge that might have brought other companies to their knees. Instead Axis delivered a rare opportunity to streamline business operations, reduce cost, improve productivity and deliver on digital transformation.”

Curtis Simpson, Armis (CISO)

1. Rapid ROI

The Axis Application Access Cloud solution is agentless, eliminating time-consuming network changes. There is nothing to deploy on endpoints and no concerns over use of personal devices. Axis can be operational in minutes.

2. Reduce Risk

With Axis Application Access Cloud end-users, never touch the corporate network or even the applications themselves. It first isolates and secures the application (both from users and the network) to diminish the attack surface and the risk of direct usage and horizontal attacks.

3. Continuous Monitoring

Those users that gain access have their every move monitored, disassembled, analyzed, recorded, authorized, reassembled, and controlled before their request is sent to the application. Using these techniques, Axis can even limit access to specific application functionality, and visually record user activity—critical forensic features not available from any other solution.

4. Cost Savings

As an application-level solution, Application Access Cloud removes the need for hard-to-manage VPNs or costly hardware appliances, releasing finances and already stretched IT team labor.