Case Study

Elisity Microsegmentation Platform Leverages Armis Centrix™ Integration and Data Sharing to Enrich Asset Intelligence

The Challenge

- Enriching native data with more granular asset data
- Mapping Elisity data to Armis Centrix™ - specific attributes already in use by customers
- Building policy around standardized, customer-recognized attributes
- Avoiding redefinition of existing asset groups and policies

The Solution

- Integrated Elisity with the Armis Centrix™ API to enable bidirectional data sharing between platforms
- Mapped native Elisity labels to known Armis Centrix™ labels
- Enabled reporting within Armis Centrix™ on Elisity policy enforcement

The Results

- Increased customer satisfaction through highly valuable integration
- Allowed customers to use Armis Centrix™ data directly to enforce policy
- Ensured existing Armis Centrix™ segments map cleanly to Elisity policy
- Supported English-language policy creation within Elisity
- Increased the value of both the Elisity and Armis platforms
- Eliminated the need for post-release rework

Industry: Software

Location: San Jose, CA

Size: 125

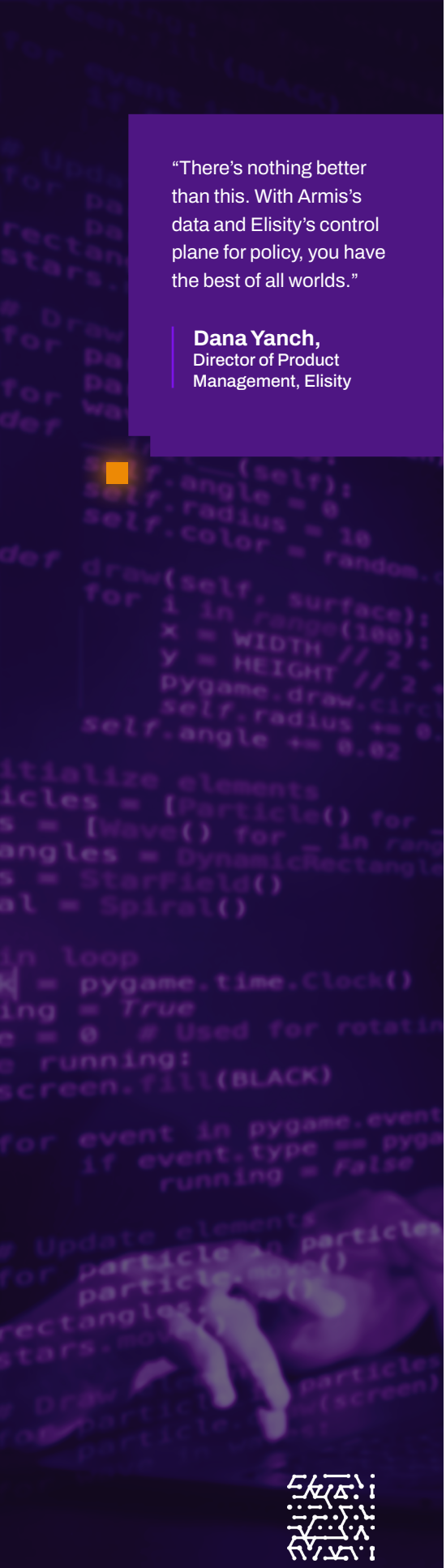
Armis Developer Portal

Background

Based in San Jose, Elisity is a customizable microsegmentation platform for network security that leverages identity to build segments for its customers' OT, IT, and IoMT networks at scale, helping them to achieve Zero Trust security. Founded in 2018 by industry veterans from leading Silicon Valley security and networking companies, Elisity was created to redefine enterprise security by separating protection and access from rigid, underlying network constructs.

Director of Product Management Dana Yanch works on a core component of the Elisity platform known as Elisity IdentityGraph™, which enables customers to leverage identity signals from across the enterprise environment. Elisity IdentityGraph™ aggregates these signals into a single system; builds policy to segment critical assets, users, and workloads; and then distributes and enforces that policy across the environment through Elisity's control plane. Part of Yanch's role includes keeping Elisity up to date with API sets, migrating to newer generations of APIs, and helping engineering teams implement these changes efficiently.

© Copyright Armis 2026



> "There's nothing better than this. With Armis's data and Elisity's control plane for policy, you have the best of all worlds."
>
> **Dana Yanch,**
> Director of Product Management, Elisity

The Challenge

A core function of Elisity IdentityGraph™ is reconciling identity signals from users, workloads, devices, medical equipment, and industrial assets like programmable logic controllers and human-machine interfaces across the enterprise. While Elisity natively discovers assets and learns basic information about them, it lacked deep visibility into the threat landscape, vulnerability data, and detailed component level data. Specifically, Elisity did not have access to attributes such as risk score, the Purdue model for industrial control system security, serial number, firmware version, or known vulnerabilities. These detailed attributes are critical for enriching asset context and building effective policy.

"Our platform is very much focused on the grouping, the classification, and the enforcement of policy," Yanch explained. "With Armis we are able to provide an even deeper level of identification."

Many of Elisity's customers were already Armis customers and had built asset segmentation models using Armis Centrix™ data. These customers wanted the ability to build policy around Armis-specific attributes such as Armis tiers, boundaries, and others. Rebuilding asset groups and policies from scratch would introduce significant friction, and Elisity recognized the value customers place on using a standardized, trusted set of attributes. Integrating with Armis Centrix™ allows Elisity to identify the assets with the highest risk and use that knowledge to put protections in place such as network segmentation, granular LPA, and policies. To support this, integration with Armis Centrix™ was essential.

To deliver the enriched asset intelligence their customers were asking for, Elisity needed access to Armis Centrix™ data. That access came through the Armis API framework—now centralized and expanded through the Armis Developer Portal.

The Solution

The Armis Developer Portal provides structured API documentation, payload examples, implementation guidance, and ready-to-use implementation "recipes" that fast-track Armis integrations. It also includes a community space where developers, technology partners, and Armis experts share integration guidance, best practices, and real-world implementation insights that accelerate building with Armis Centrix™ APIs.

For technology partners like Elisity, the portal represents a scalable, self-serve path to building high-value integrations on top of Armis's cyber exposure management platform.

Elisity first recognized the value of integrating with Armis several years ago, leveraging the Armis Centrix™ API to access detailed asset intelligence. Even before the launch of the centralized Developer Portal, the APIs were clearly structured and well-documented, enabling rapid development. Thanks to Yanch's technical contacts at Armis, he was able to get everything he needed—API data, API payload information, and best practices—directly from his colleagues at Armis. With that clear guidance, the Elisity engineering team was able to build an integration quickly and with confidence. "It worked flawlessly, and has continued to do so ever since," Yanch asserted. Today, the Armis Developer Portal formalizes and expands that experience, making it accessible to the broader developer ecosystem.

© Copyright Armis 2026

"Armis provides valuable data to our customers. The quality of that data is what makes our product work so well."

Dana Yanch,
Director of Product Management, Elisity

Through the integration, Elisity pulls Armis Centrix™ data into Elisity IdentityGraph™ where it is used to create identity-based policy. Customers build policy around Armis Centrix™-specific attributes with Elisity's language-based security model. That data is processed within Elisity's backend and used to identify trends and support large-scale data models, including those that power AI-driven insights.

The integration is bidirectional. Elisity dynamically shares policy enforcement status back to Armis Centrix™. Within Armis Centrix™, a customer can create a report or do a search to see which assets lack enforcement, which assets have enforcement, and what level of enforcement exists, whether basic or custom.

The Results

Yanch reported that customers have been very happy with the integration and find it extremely valuable. "Customers love Armis because it's simple to deploy, rapid to deploy, low touch, completely cloud-delivered," he said. "It causes zero disruption to the network while passively collecting, analyzing, and presenting its data to the customer in a very easily digestible fashion—and that's a big advantage for Elisity's customers."

Once customers see the wealth of granular data from Armis, the Elisity integration answers the question that naturally arises: "How do I use this now?" Elisity helps customers take the next step and enforce policy in a practical, scalable way.

The integration ensures that network segments are properly enforced to prevent lateral movement of ransomware and other threats. For example, if a manufacturing asset is compromised, the threat is contained and prevented from spreading across production sites or the corporate environment.

"There's nothing better than this," Yanch remarked. "With Armis's data and Elisity's control plane for policy, you have the best of all worlds." He emphasized the ease with which customers can build policy, using English language attributes. For example, customers can group all assets at a given site that are within a designated boundary and are exhibiting certain behaviors on the network. "It makes Armis more valuable, and it makes Elisity more valuable. This is very much a bidirectional value proposition," Yanch declared.

This creates a network effect, where the value of both platforms increases as customers build more policy around standardized attributes. As Yanch noted, once a customer has built their entire segmentation model around Armis Centrix™ data attributes, "there's no way they're pulling Armis out of that network anytime soon, whether it's for renewals or competitive reasons."

After Elisity discovers an asset, it leverages detailed Armis Centrix™ data pulled from hundreds of customers into large language models that map out trends in the cyberthreat landscape. This helps Elisity hone policies for its customer to suit their specific use cases.

"You hear the phrase 'garbage in, garbage out,'" Yanch added. "Well, Armis provides valuable data to our customers. The quality of that data is what makes our product work so well together."

© Copyright Armis 2026

10/10
Armis Developer Portal experience rating

2-way
bidirectional data sharing

Zero
post-release rework

Yanch said he would strongly recommend building an integration using the Armis Developer Portal. On a scale of one to 10, “It’s a solid 10,” he said. “It’s straightforward. Anybody with a little bit of experience on how to leverage APIs will pick this up,” he added. Yanch pointed out that the APIs from Armis are better than the APIs from some of the other platforms Elisity integrates with, where they are not clearly defined, lack descriptions and samples of data output, and require a lot of time to figure out independently.

“With Armis we can do a one-and-done,” Yanch said. He noted that rework is the enemy of many developers. They don’t want to have to go back and fix things after the initial release.

Yanch is preparing to expand the integration using the portal’s updated documentation, recipes, and tools sometime over the next year. He expects the portal to be very beneficial in that process. “I love the recipes,” Yanch said.

As Elisity looks to the future, the Armis Developer Portal plays a central role in its roadmap. By enabling structured, scalable, and community-driven API development, the portal empowers partners to continuously extend the value of Armis asset intelligence.

“We’re looking into the future to see what other APIs we can leverage to add additional value,” Yanch said. For Armis partners and customers alike, the Developer Portal represents more than documentation. It’s a foundation for building the next generation of integrated cybersecurity solutions.

ARMIS

See how leading organizations secure their environments with Armis.

See Armis Centrix™ in Action

Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization’s cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, secure, protect and manage all critical assets.

Armis secures Fortune 100, 200, and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies, and society safe and secure 24/7.

Armis is a privately held company headquartered in California.

+1 888 452 4011
armis.com