ARMIS® ELISITY

PARTNER BRIEF

Power Zero Trust Protection and Dynamic Microsegmentation With Armis Centrix™ and Elisity

Enhanced cyber exposure management with identity-based microsegmentation

Landscape

Cyber exposure risks are constantly evolving. Your asset inventory and least privilege access segmentation policies should do the same. Organizations across industries such as healthcare and manufacturing struggle to secure increasingly complex and interconnected digital environments. Traditional security approaches may lack the necessary visibility, granular access control, and adaptability required to mitigate evolving threats. Microsegmentation and automated policy enforcement can support cybersecurity initiatives for sensitive assets.

Armis and Elisity provide a powerful integration that identifies all assets, profiles their behaviors, and performs dynamic microsegmentation to ensure the automatic sequestering of assets at risk. Joint customers can benefit from Armis Centrix™ by gaining comprehensive visibility of all assets, quantification of risk profile, and Zero Trust aligned Least Privilege Access policies with Elisity. The result is comprehensive situational awareness, a strong security posture, and protection of operational resiliency.

With Armis and Elisity, You Can…

Discover and identify all IT, IoT, OT, and IoMT devices across your enterprise network, automatically capturing critical details like manufacturer, model, firmware version, and location.

Enrich asset intelligence by integrating with your existing systems and eliminating manual data entry, creating a comprehensive and dynamic single source of truth.

Quantify security risks with context-aware scoring that enables prioritization based on potential business impact and compliance requirements.

Apply dynamic microsegmentation with identity-based, least privilege access policies that automatically adapt to changing risk levels reported by Armis.

Prevent lateral movement across your network without adding hardware, agents, VLANs, or complex ACLs, containing threats before they can spread.

Streamline security workflows with automated policy enforcement that reduces manual intervention and accelerates incident response time. Easily open remediation tickets and automatically assign ownership.

Simplify compliance with frameworks including HIPAA, NIST 800-207, and IEC 62443 through comprehensive asset visibility and policy documentation.

Achieve Zero Trust maturity in weeks instead of years by leveraging your existing network infrastructure with cloud-delivered security controls.

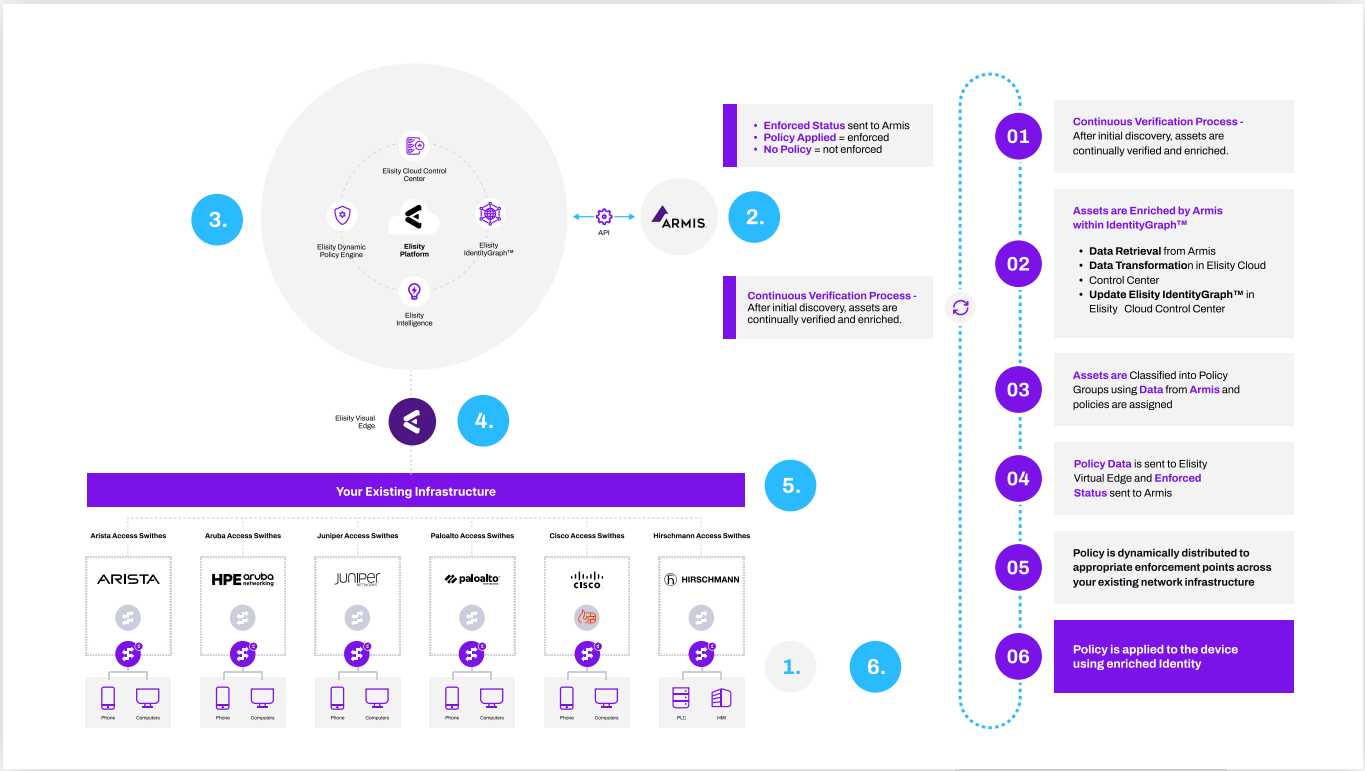
Joint Solution

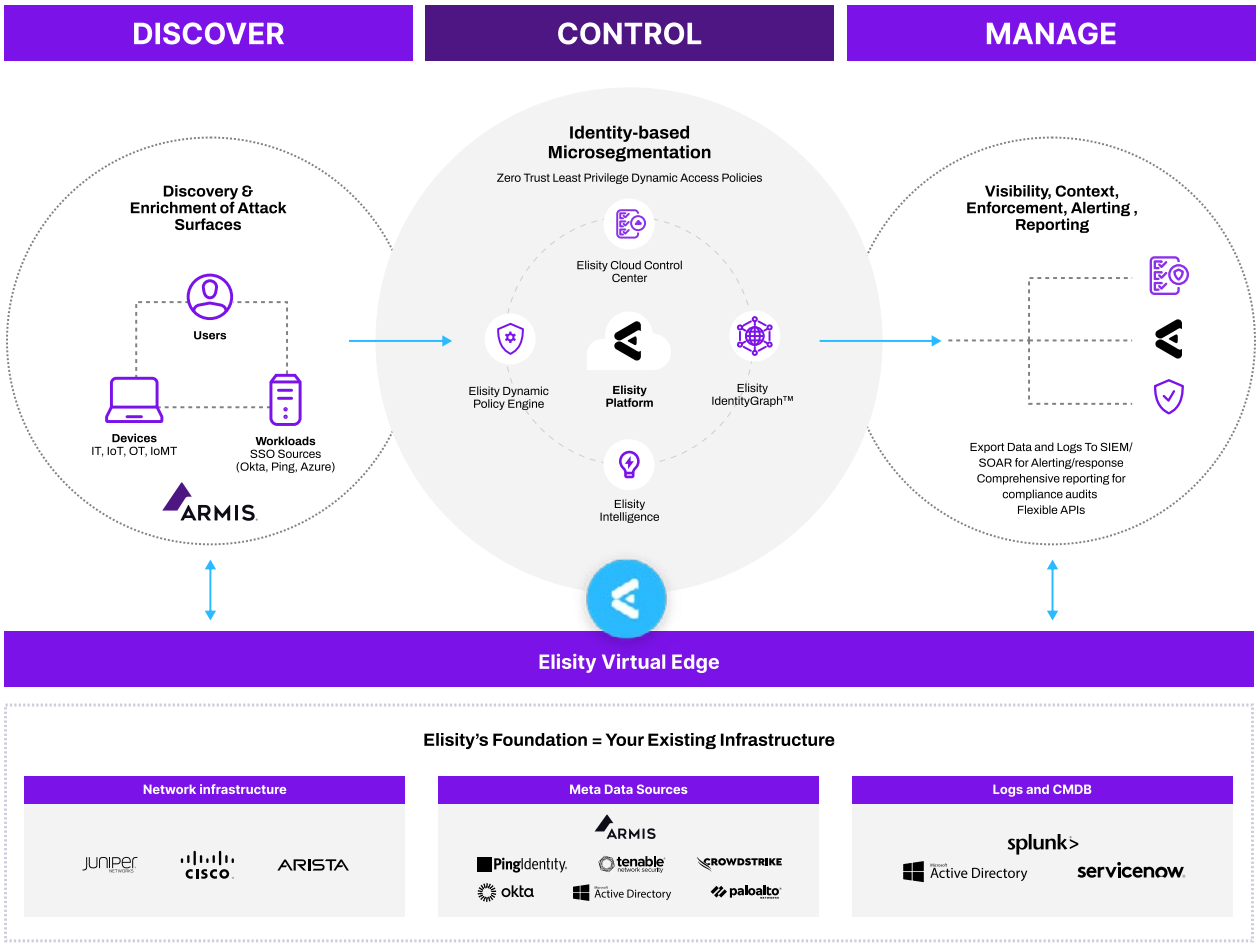
Armis Centrix™ and Elisity have partnered for a bidirectional integration and streamlined approach to microsegmentation. Asset intelligence and security information is synchronized between Armis Centrix™ and Elisity for comprehensive visibility of every asset in a single location. Similarly, Elisity's microsegmentation capabilities and dynamic policy engine can enhance security with least-privilege access policies based on Armis attributes and other metadata. The partnership enables greater security and strengthens defenses against evolving threats.

Elisity delivers identity-based microsegmentation through its cloud-delivered policy management platform that works with your existing network infrastructure, eliminating the need for new hardware, agents, VLANs, or complex ACLs. The seamless integration with Armis Centrix™ enhances the Elisity IdentityGraph™, a comprehensive device, user, workload identity, and attribute database. Leveraging

Armis' extensive Asset Intelligence Engine, spanning over 6 billion assets, provides detailed asset information such as risk score, boundaries, device type, manufacturer, model, operating system, firmware version, and network segment. These enriched attributes provide crucial information for Elisity's classification and policy creation and enforcement, enabling precise, context-aware security policies across the network.

How It Works





"The synergy between Armis and Elisity has fortified defenses against targeted cyber threats, improving overall operational efficiency with added layers of security and visibility… Microsegmentation is a key strategy for accelerating our Zero Trust program."

Aaron Weismann

Chief Information Security Officer for Main Line Health

Key Use Cases

1 | Enhanced Visibility

- **Comprehensive Asset Discovery:** Armis uncovers previously unknown assets and application traffic, protects the entire attack surface, and manages cyber risk exposure in real-time. This enhances Elisity's segmentation capabilities through real-time detailed visibility of every asset in the digital footprint.
- **Real-Time Asset Intelligence:** The Armis Asset Intelligence Engine is a collective AI-powered security data lake, that monitors billions of assets world-wide in order to identify cyber risk patterns and behaviors. Device profile information can include site and boundary location, model, operating system, risk score and more. These early indicators of risks facilitate faster response and bolster defenses against evolving threats. Then, Elisity IdentityGraph™ combines Active Directory, CMDB, Armis, and EDR metadata with network flows for an automated, single source of truth for asset identities which is used by teams to have confidence as they create and apply policies.

2 | Greater Cybersecurity Control

- **Granular Policy Enforcement:** Enforce access policies and align with Zero Trust initiatives with identity and context-based least privilege access policies, independent of network infrastructure. Security teams can rapidly implement least privilege access by leveraging Elisity's pre-built policy templates as a starting point, or create highly granular, dynamic microsegmentation policies that automatically adapt based on device identity, behavior, and risk score.
- **Dynamic Access Management:** Utilize enriched asset attributes to create and enforce adaptive, context-aware security policies. Elisity leverages Armis risk scores to automatically adjust access policies when device risk levels change, ensuring dynamic microsegmentation that adapts to evolving security postures.

3 | Enhanced Security Posture

- **Proactive Risk Management:** Identify, deduplicate, contextualize, prioritize, assign, and mitigate risks and security findings using Armis's risk scores and attributes for robust threat protection and prevention. Make the most of tailored, actionable policies for each risk-factor type, accessible directly through the Armis console or via the Elisity integration.
- **Comprehensive Risk Identification:** Armis Centrix™ provides comprehensive visibility and risk profiles for all asset types, including OT, IoT, medical, physical, and virtual. Armis provides a consolidated view of risks including exposure to cyber threats, device recalls, end-of-support operating systems, unencrypted traffic, and potential business impact to the organization. Security teams can view contextual data-based scores that help them understand the risk factor and determine which findings to remediate first.
- **Risk Score Explainability and Prioritization:** Armis provides greater transparency and explainability on risk scoring decisions and connects the "fix" with the findings discovered. Organizations remain in control with the ability to edit, disable, or create additional custom Risk Factor types, and add tailored risk identification rules to facilitate more targeted micro-segmentation campaigns.

4 | Simplified Process Management

- **Rapid Deployment:** SaaS-based, rapid deployment of the integrated solution over existing infrastructure, leveraging existing security stacks for immediate value without extensive network configuration changes, agents, or new hardware.
- **Simplified Segmentation:** Automate and simplify segmentation projects using detailed asset data, reducing operational complexity and costs. Armis and Elisity support both simple microsegmentation policies for single or small batches of devices and complete automation based on device properties like Type, Manufacturer, Model, Version Number, and Risk for faster incident response.
- **Easily Contain Potential Threats:** Identify early indicators of potential threats or risks. Assign policies based on asset context and behavior and automatically assign policies for rapid containment, preventing lateral movement and attack proliferation.

Benefits of Armis Centrix™ Integration with Elisity

Zero-Trust Architecture for Operational Efficiency: The integration between Armis and Elisity creates a powerful security framework, enabling organizations to implement true zero-trust architecture on an ongoing basis, protecting assets from both internal and external threats.

Enhanced Security Posture: By effectively cataloging assets, identifying risks, and carrying out remediation and automated dynamic microsegmentation policies.

Dynamic and Continuous Protection: With enhanced device profiles, policy automation, and microsegmentation technology that are continuously updated, your operations are protected and future-proofed against cyber threats.

Precise, Context-Aware, Rapid Enforcement: Combining Armis's in-depth asset visibility and risk scoring with Elisity's network analytics and dynamic policy management, organizations gain immediate insight into their network environments.

Compliance and Regulatory Adherence: Armis and Elisity's integrated solution helps organizations achieve compliance with HIPAA, NIST 800-207, and IEC 62443 by providing comprehensive asset intelligence and automated microsegmentation across medical devices, industrial controls, and IT systems. By incorporating Armis's detailed asset risk scoring into Elisity's dynamic policy engine, organizations can enforce and demonstrate granular access controls that automatically adapt to device vulnerabilities and risk levels – a key requirement for modern cybersecurity frameworks.

Summary

Together, Armis and Elisity redefine enterprise security by providing a seamless, integrated solution that ensures detailed asset management, proactive risk mitigation, and compliance—all while maintaining the strategic agility needed to respond to today's complex threat landscape.

ELISITY

Elisity is a leap forward in network segmentation architecture and is leading the enterprise effort to achieve Zero Trust maturity, proactively prevent security risks, and reduce network complexity.

Designed to be implemented in weeks, without downtime, upon implementation, the platform rapidly discovers every device on an enterprise network and correlates comprehensive device insights into the Elisity IdentityGraph™. This empowers teams with the context needed to automate classification and apply dynamic security policies to any device wherever and whenever it appears on the network. These granular, identity-based microsegmentation security policies are managed in the cloud and enforced using your existing network switching infrastructure in real-time, even on ephemeral IT/IoT/OT devices.

ARMIS

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. 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 stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website
Platform
Industries
Solutions
Resources
Blog

Try Armis
Demo
Free Trial