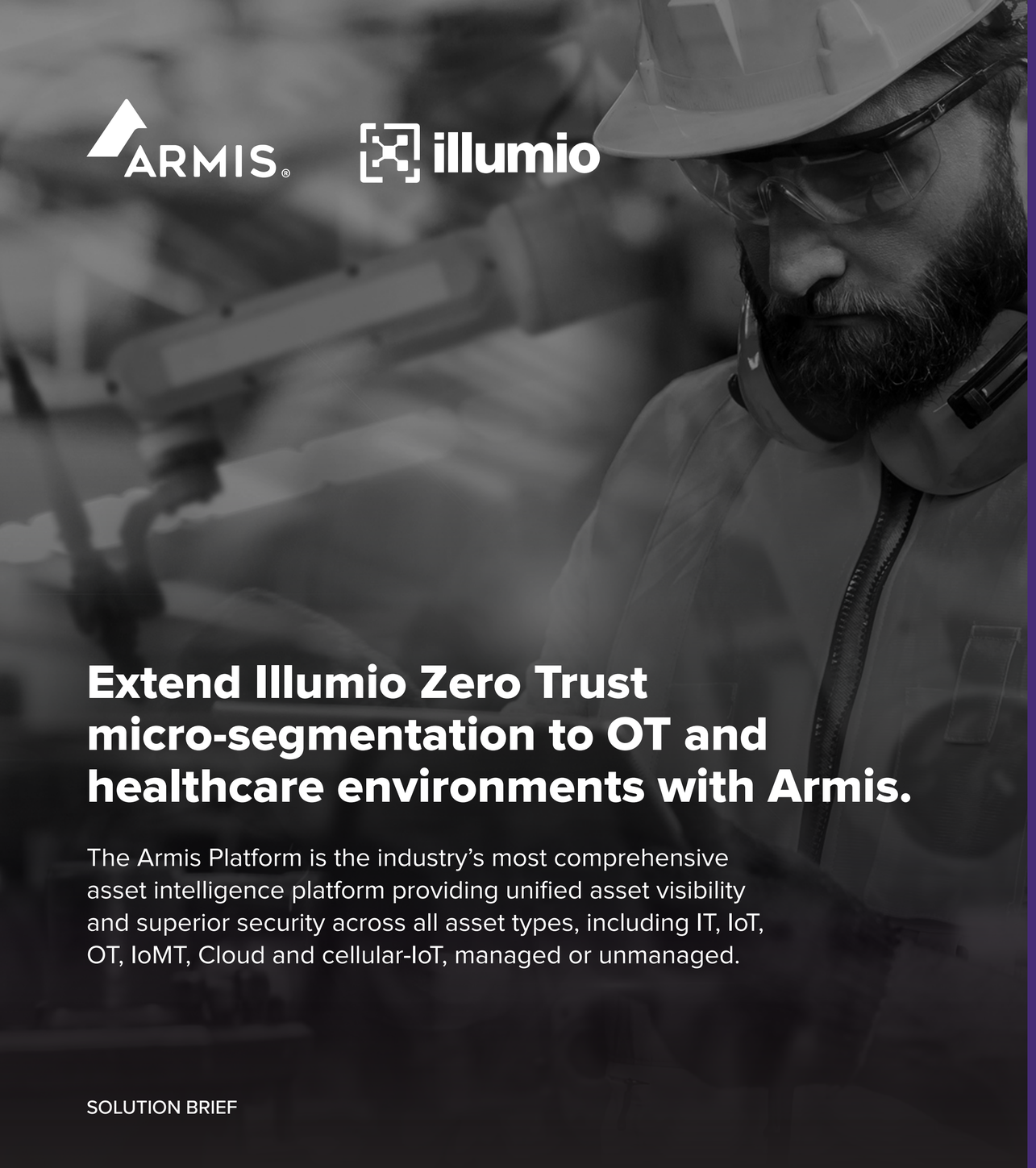

Extend Illumio Zero Trust micro-segmentation to OT and healthcare environments with Armis.

The Armis Platform is the industry's most comprehensive asset intelligence platform providing unified asset visibility and superior security across all asset types, including IT, IoT, OT, IoMT, Cloud and cellular-IoT, managed or unmanaged.

SOLUTION BRIEF

Integration Snapshop

The Armis integration for Illumio Zero Trust Segmentation enables enterprises to extend micro-segmentation across any environment, including OT and healthcare networks

Key Benefits

- Extends Zero Trust micro-segmentation across all environments and asset types, including OT, IoMT, IT, cloud, mobile, and more - without requiring network changes
- Provides deep intelligence into all connected assets and workloads
- Enables quick, efficient, and granular control over dynamic environments that contain both managed and unmanaged assets

The Challenge

Across virtually every type of enterprise, the numbers of connected assets used for increasing efficiencies and driving innovation are exploding just like their related cyber risks. And in healthcare, manufacturing, and critical infrastructure environments, the stakes are especially high:

- **In healthcare**, the new breed of connected medical devices brings the promise of improved patient care, better clinical data, improved efficiency, and reduced costs—but they also introduce unprecedented security risks to healthcare organizations.
- **In OT networks**, the introduction of IoT devices combined with the elimination of the "air gap" between control systems and traditional IT systems is critical for introducing innovative technologies, improving efficiencies and driving growth. However, it also exposes these systems to threats that can lead to various outcomes, from minor production disruptions to hazardous situations that can put human lives at risk.

Even though organizations are connecting more assets and asset types to networks, it doesn't mean all assets should communicate with one another. To better control dynamic environments and the rapidly expanding attack surfaces, many organizations are turning to Zero Trust solutions. Micro-segmentation is a key Zero Trust technique for protecting against cyberattacks by restricting lateral movement and reducing the attack surface. However, lack of visibility into OT and healthcare assets remains a barrier to fully controlling Zero Trust network access (ZTNA).

The Solution

The Illumio Zero Trust Segmentation solution offers efficient, granular control over dynamic environments. Since it is a host-based solution and independent of the underlying infrastructure, Illumio allows quick implementation of micro-segmentation without requiring any network changes—one of the main barriers to implementing ZTNA. However, Illumio Zero Trust Segmentation only covers IT networks and lacks visibility into OT and IoMT networks and assets.

The Armis platform is an agentless SaaS platform that automatically collects and analyzes data through meaningful integrations, delivering the industry's most comprehensive asset intelligence platform. Armis provides complete and continuous real-time visibility into every type of asset—including OT assets and medical devices—enabling Illumio to properly segment and/or microsegment them appropriately.

How the Armis and Illumio integration works

Armis automatically generates a wealth of information that includes much more intelligence than other "visibility" products generate. Armis shares this information with Illumio to support proper network segmentation.

Being aware that devices exist isn't enough. For Zero Trust security, you need to know whether a device represents a risk. This is what Armis tells Illumio. After discovering and identifying each device, the Armis platform analyzes and calculates its risk score. The score is based on multiple risk factors. Armis' cloud-based risk analysis engine compares observed device characteristics and behavior against real-

63% of healthcare delivery organizations have experienced a security incident related to unmanaged and IoT devices over the past two years.

—Forrester

time intelligence from our Collective Asset Intelligence Engine, which contains a baseline of what we know to be normal behavior for each type of device.

The integration between Armis and Illumio extends ZTNA across all environments and asset types, including OT, IoMT, IoT, IT, cloud, mobile, and more. The integrated solution provides complete visibility into all connected assets and workloads—agented or not—and provides contextual intelligence to enable risk-based prioritization and implementation of controls.

ASSET INFORMATION

- Asset type
- Manufacturer
- IP address
- MAC address
- Computer name
- User name

ENDPOINT BEHAVIOR

- Stationary vs. moving
- Communication timing
- Communication volumes
- Cloud services accessed
- Tunnels utilized
- Encryption usage

CONNECTION INFORMATION

- Connection type (e.g., wired, Wi-Fi)
- Connection point (e.g., corporate, guest, rogue)
- Traffic volume and timing
- Internet domains accessed

SOFTWARE INFORMATION

- OS type and version
- Applications

WI-FI INFORMATION

- Access point (AP) name
- AP CPU utilization
- AP bandwidth utilization
- AP OS version

SWITCH INFORMATION

- Switch name and location
- Switch CPU utilization
- Switch configuration
- Internet domains accessed

The Difference

Gain Zero Trust control from your workloads to your endpoints

Decoupled from the infrastructure, the combined Armis and Illumio solution empowers healthcare, manufacturing, and critical infrastructure enterprises to “go faster, safely” with ZTNA, without changing their existing infrastructure.

See and stop ransomware

Armis relies on real-time insights into asset behavior and context to quickly identify ransomware and reduce the risk of operational downtime and reputational damage.

Block lateral movement

Armis enables you to isolate assets or kill OT or medical device connections if an asset is seen as high risk. You can granularly segment all systems and assets, even if they are not high-risk, to help maintain a minimized attack surface and mitigate malicious lateral movement.

Contain cyberattacks and reduce risk

Automatically contain and remediate cyber threats as they happen in real-time, reducing overall operational risk and downtime.

Enable Zero Trust with full confidence

The Illumio Zero Trust Segmentation solution offers industry-leading micro-segmentation capabilities for protecting your organization. Although OT assets and medical devices present unique Zero Trust-related challenges, the Armis Asset Intelligence Platform enables you to take full advantage of Illumio micro-segmentation in healthcare, manufacturing, and critical infrastructure environments.

Illumio + Armis:

Complete Visibility, Intelligence, and Enforcement

It is now possible to see, analyze, and apply micro-segmentation across your network of IT, OT, and IoT systems within a single, interactive dashboard.

Visit: www.illumio.com/partners/tap/armis or www.armis.com/illumio

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.

1.888.452.4011 | armis.com

20221116-1

ARMIS.