PARTNER BRIEF

Zscaler + Armis: Zero Trust Security with Real-Time Asset Intelligence Across IT, IoT, and OT

The Market Challenge

Enterprises no longer operate behind fixed perimeters. Employees, contractors, partners, and devices connect from anywhere. Applications increasingly live in the cloud, and SaaS has become the default delivery model. At the same time, the number of connected has exploded, with IDC predicting 41.6 billion connected devices generating 79.4 zettabytes of data this year. This creates a massive, dynamic attack surface.

Traditional security tools, built for static networks and managed devices, fail in this environment. They provide limited visibility, lack context, and are often siloed, leaving blind spots for attackers to exploit. Unmanaged devices, ephemeral assets, shadow IT, and flat networks make organizations vulnerable to lateral movement, ransomware, data exfiltration, and operational disruption.

Security teams are left reactive, fragmented, and overwhelmed by alerts, unable to prioritize threats or enforce risk-based policies in real time. To succeed, enterprises need an approach that **unifies Zero Trust enforcement with continuous visibility and risk context across IT, IoT, and OT.**

The Joint Solution

Zscaler and Armis together deliver a new level of protection for the modern enterprise. By combining Zscaler's cloud-delivered Zero Trust Exchange with the Armis Centrix™ platform, organizations gain a single, integrated fabric that brings together enforcement and intelligence. Zscaler enables secure, policy-driven access to applications and services regardless of user, device, or location, while inspecting traffic in-line to detect threats in real time. At the same time, Armis continuously discovers and monitors every asset across IT, IoT, and OT environments, whether managed or unmanaged, and identifies vulnerabilities, assessing posture, and flagging abnormal behavior in a prioritized order based on risk to operational resilience and safety.

This joint solution creates a feedback loop that drives adaptive security. Armis provides the real-time device intelligence and risk scoring needed to understand the true posture of any asset as well as connections, while Zscaler enforces Zero Trust access, segmentation, and remediation based on that context. This ensures that every user and device connection is validated, threats are detected earlier, and risks are contained before they disrupt operations. Together, Zscaler and Armis give enterprises the visibility to see every asset, the intelligence to know its risk, and the enforcement to secure every connection across all assets and devices, whether physical, logical, or virtual.

How It Works

The Zscaler–Armis integration combines Zscaler's cloud-delivered Zero Trust Exchange with the Armis Centrix™ to deliver contextual visibility, adaptive access, and unified continuous threat exposure management (CTEM) via:

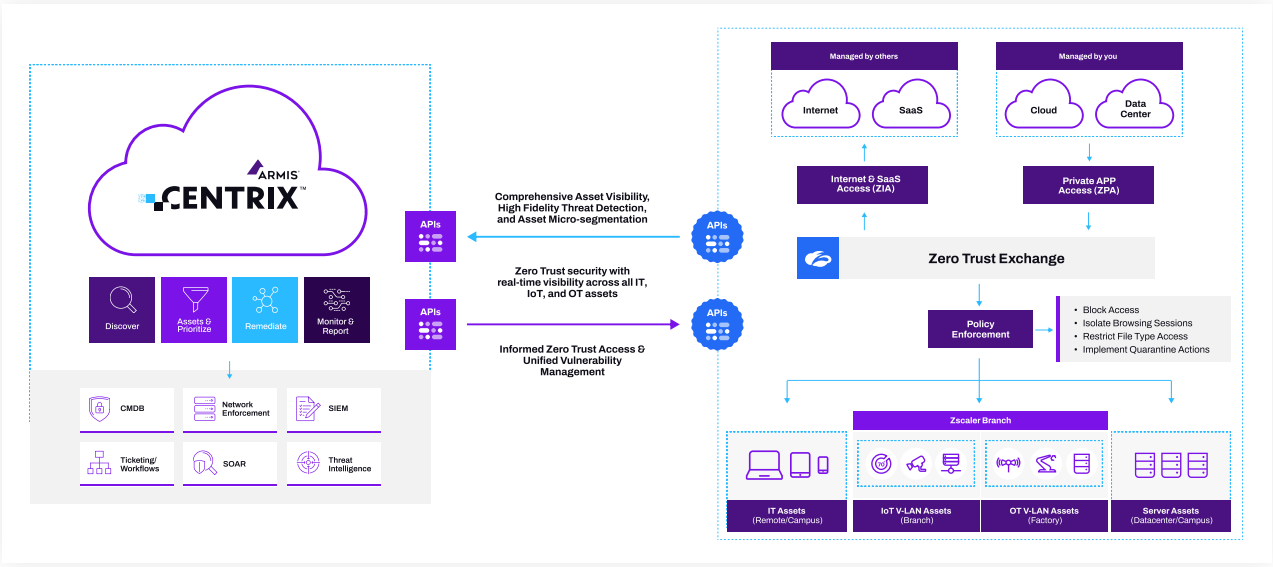
Bi-directional integration - Armis ingests enriched telemetry from the Armis Centrix™ platform as well as, Zscaler Internet Access (ZIA), Private Access (ZPA), and the Zscaler Client Connector (ZCC), correlating user activity, device posture, and network behavior.

Contextual intelligence - This data is mapped against the Armis Asset Intelligence engine to validate asset identity, detect anomalies, provide early warning alerting, and surface vulnerabilities across IT, IoT, and OT environments.

Adaptive enforcement - The joint solution applies Zero Trust Device Segmentation (ZTDS) and Unified Vulnerability Management (UVM), and can dynamically isolate, quarantine, restrict and mitigate high-risk assets and/or behaviors.

Coordinated response - Deception technology generates early warnings of adversary activity, which is further enriched with device and user context to prioritize remediation based on value/risk to the business.

This joint solution ensures consistent policy enforcement across cloud, data center, campus, and factory floor, delivering a scalable, risk-informed Zero Trust strategy for today's hybrid enterprise.



Key Use Cases

1. Unified Asset Visibility Across IT, IoT, and OT

Most organizations struggle with blind spots created by unmanaged or shadow devices. Armis eliminates this problem by delivering continuous discovery of all assets, while Zscaler adds the dimension of inline user and application telemetry. When combined, this integration produces a unified view that correlates user identity, device behavior, and network activity across the enterprise.

Consider a healthcare provider with thousands of connected medical devices in its hospitals. With this integration, unmanaged infusion pumps, printers, and tablets are discovered alongside clinical applications, physician workstations, and cloud services. Security teams gain full visibility into how these devices are behaving, who is accessing them, and whether activity is normal or suspicious. This complete picture allows teams to identify risks faster and address them before they can be exploited.

2. Threat Detection and Early Warning with Deception

Deception technology places realistic decoys throughout the environment, fake servers, files, credentials, and network shares, that no legitimate user should ever touch. Any interaction with these decoys is inherently malicious and immediately signals the presence of an attacker. Because these alerts are free from false positives, security teams can respond with confidence.

The joint solution enhances this process by enriching each alert with deep context about the device and user involved, including hardware fingerprinting, behavioral baselines, and network associations. Instead of just knowing that an attacker touched a decoy, security teams now know exactly which compromised device was involved, how it behaved before and after the event, and what risk it poses. This enriched intelligence makes it possible to triage incidents faster, contain the threat decisively, and prevent attackers from gaining a foothold or causing material damage.

3. Dynamic Segmentation and Containment

Flat networks make lateral movement easy once attackers establish a beach head. By combining Zscaler's Zero Trust Device Segmentation with Armis's comprehensive asset intelligence, organizations can eliminate this risk by dynamically segmenting devices based on their posture and behavior. Armis identifies high-risk or compromised assets in real time, and Zscaler immediately applies segmentation policies to isolate them or restrict their communications.

In a manufacturing environment, for example, a programmable logic controller might begin communicating in an unusual pattern that suggests compromise. Armis would detect this anomalous activity and flag the device as high-risk. Zscaler would then automatically contain it, preventing communication with production systems or sensitive data. This minimizes downtime, preserves business continuity, and shrinks the internal attack surface.

4. Context-Aware Zero Trust Access

Traditional access models often treat all devices the same, regardless of their risk. The Zscaler–Armis integration changes this by continuously evaluating device posture and adapting access accordingly. Armis provides ongoing assessments of device health, vulnerabilities, and behavior, while Zscaler uses this information to grant or restrict access in real time.

For instance, if a contractor's laptop suddenly shows signs of compromise, Armis will surface the issue and raise its risk score based on business risk. Zscaler then automatically adapts by quarantining the user, blocking access to sensitive applications, or rendering the apps in a restricted browser session. This ensures that access decisions are not static, but dynamic and contextual, based on the actual risk a device poses at any given moment.

5. Automated Response to Exposures

The joint solution also transforms how organizations approach unified vulnerability management. Armis continuously identifies vulnerabilities across all assets, including early warning if impending issues "left of boom" as well as those unmanaged devices that traditional scanners miss. The joint solution, calculates risk scores, and prioritizes remediation based on the real-world exposure each vulnerability presents.

Rather than overwhelming teams with long lists of CVEs, this approach ensures focus on the small subset of vulnerabilities that truly matter. A financial services company, for example, might discover thousands of outdated IoT cameras across its branches. With Armis providing detailed vulnerability data and Zscaler prioritizing by risk, the security team can quickly address the highest-impact issues first, dramatically reducing overall exposure without wasting resources.

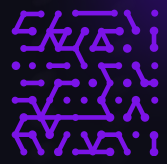
Conclusion

With Zscaler and Armis, organizations gain the visibility to know every asset, the intelligence to understand risk, and the enforcement to secure every connection.

By merging Armis's real-time asset intelligence with Zscaler's cloud-native Zero Trust Exchange, enterprises can:

- **Shrink the attack surface** across IT, IoT, OT and medical devices
- **Detect and stop** attackers earlier in the kill chain
- **Prevent** lateral movement with dynamic segmentation
- **Accelerate** remediation with contextualized risk insights
- **Safely embrace** digital transformation with confidence

Zero Trust starts with knowing what you have. Zscaler and Armis make it real, relatable to the business and actionable.



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