JOINT SOLUTION BRIEF

zscaler™ + ARMIS

Zero Trust security with real-time visibility across IT, IoT, and OT assets to protect every connection

INTEGRATION HIGHLIGHTS

- ✓ Unified visibility across IT, IOT, and OT to eliminate blind spots
- ✓ Real-Time Zero Trust Conditional access with device-aware risk enforcement
- ✓ Accelerate threat detection, containment and incident response

The Market Challenge

Enterprises today operate in a perimeter-less world, where employees, contractors, and devices connect from anywhere, and critical applications are increasingly hosted in the cloud or delivered as SaaS. 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—designed for static networks and managed endpoints—cannot keep pace with the volume and diversity of these connections. 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 access 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 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. The Zscaler Zero Trust Exchange delivers secure, policy-driven access to internet, SaaS applications, and private applications for all users, regardless of device or location. It leverages inline AI-powered traffic inspection for advanced threat protection, dynamic segmentation to control and manage user access, deception-based threat detection to identify and mitigate attacks, and unified vulnerability management to address security risks. 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.

From discovery to defense—Zscaler and Armis automate Zero Trust control across IT, IoT, and OT.

Solution Components Deep Dive

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.

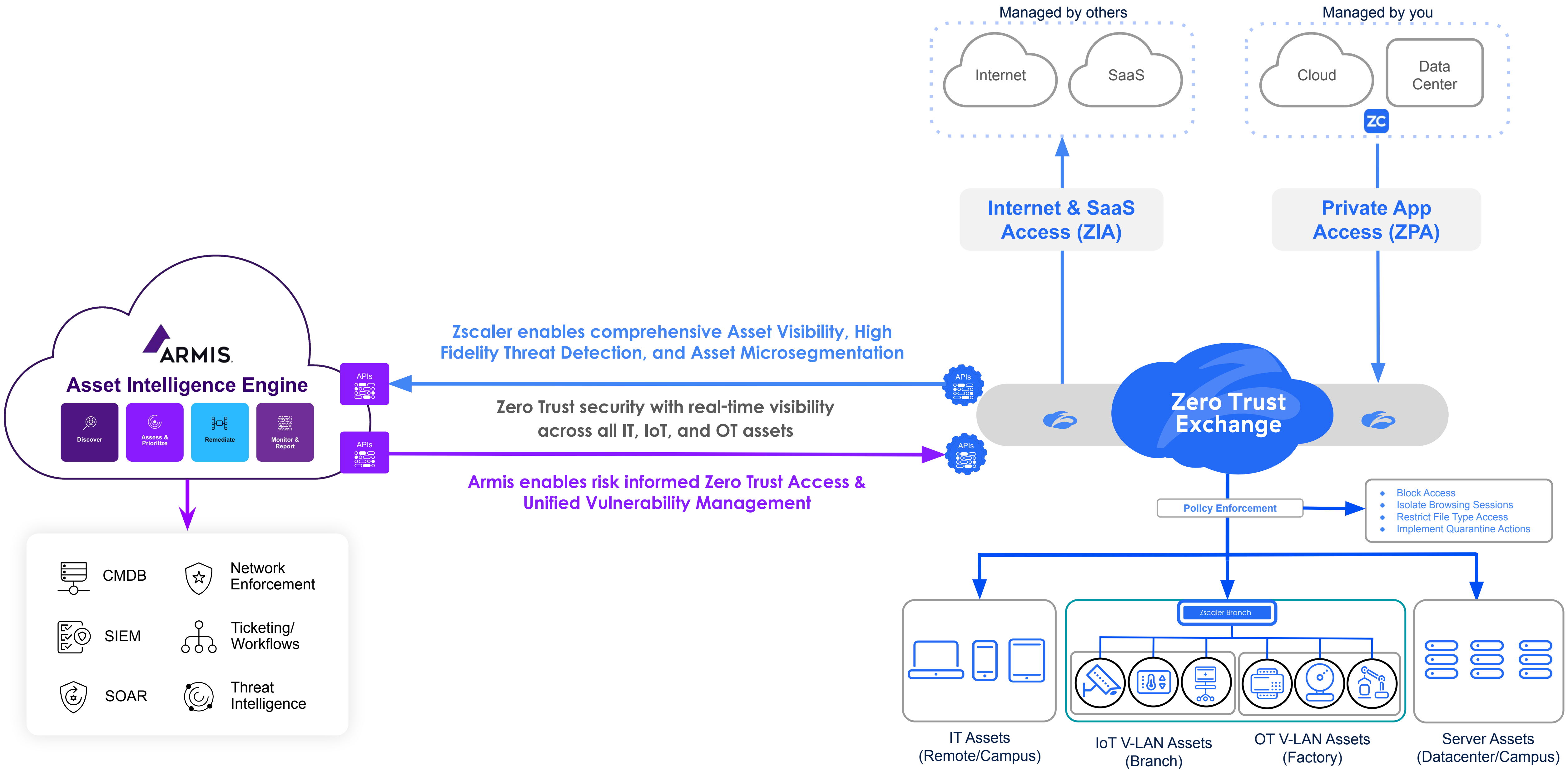
Managed by others
Internet
SaaS
Managed by you
Cloud
Data Center
ZC
Internet & SaaS Access (ZIA)
Private App Access (ZPA)
ARMIS
Asset Intelligence Engine
Discover
Assess & Prioritize
Remediate
Monitor & Report
APIs
APIs
Zscaler enables comprehensive Asset Visibility, High Fidelity Threat Detection, and Asset Microsegmentation
Zero Trust security with real-time visibility across all IT, IoT, and OT assets
Armis enables risk informed Zero Trust Access & Unified Vulnerability Management
APIs
APIs
Zero Trust Exchange
Policy Enforcement
Block Access
Isolate Browsing Sessions
Restrict File Type Access
Implement Quarantine Actions
CMDB
Network Enforcement
SIEM
Ticketing/ Workflows
SOAR
Threat Intelligence
Zscaler Branch
IT Assets (Remote/Campus)
IoT V-LAN Assets (Branch)
OT V-LAN Assets (Factory)
Server Assets (Datacenter/Campus)

Figure 1. The Zscaler and Armis Integration Architecture

With Zscaler and Armis, we're redefining how enterprises secure today's digital perimeter. By merging asset intelligence with cloud-native Zero Trust enforcement, this integration delivers real-time, scalable protection across IT, IoT, and OT environments—empowering customers to stay ahead of evolving threats.

Liron Kaneti
Senior Vice President, Strategic Initiatives

KEY USE CASES

Unified Asset Visibility Across IT, IoT, and OT

Zscaler and Armis integrate to provide expanded asset visibility across IT, IoT, and OT environments, giving security teams a complete view of managed and unmanaged devices. Armis Centrix continuously ingests log data from Zscaler Internet Access (ZIA) and Private Access (ZPA), along with metadata and Hardware Fingerprint data from the Zscaler Client Connector (ZCC). This unique device fingerprinting capability enables organizations to gain deep visibility into network traffic, user activities, and device behavior. This integration unifies device discovery from Armis—covering managed, unmanaged, IT, and OT assets—with Zscaler's inline telemetry on user and cloud access.

This integration unifies device discovery from Armis, covering managed, unmanaged, IT, and OT assets, with Zscaler's inline telemetry on user and cloud access, while adding the crucial context of device hardware identity from ZCC. The result is especially valuable for organizations with distributed workforces, IoT deployments, or operational technology (OT) assets in remote locations. It enables security teams to analyze activities and risks by both user and device, spot unusual activities such as unauthorized device-to-device communication or data exfiltration, accelerate investigations, and strengthen enterprise security across hybrid and edge environments.

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.

Threat Detection and Early Warning with Deception

Zscaler and Armis together enable an Active Defense strategy that disrupts attackers early, exposing advanced threats before they can spread. At the core of this integration is Zscaler Deception, which plants highly realistic "honeypot" decoys—fake endpoints, servers, files, credentials, and network shares—alongside legitimate assets. Because any interaction with these decoys is inherently malicious, alerts generated carry near-zero false positives, immediately signaling adversary presence and intent.

Armis then enriches these deception alerts with deep device context—hardware fingerprint, behavior, identity, and user association—providing security teams with a precise, actionable view of the threat landscape. This combination of reliable detection and rich context streamlines incident triage, speeds containment decisions, and ensures organizations can respond decisively, stopping attackers before material impact occurs.

Dynamic Segmentation and Containment (Zero Trust Device Segmentation)

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.

Zscaler + Armis Benefits

ACTION	DESCRIPTION
Gain complete visibility	Armis Centrix ingests Zscaler Internet Access (ZIA) and Private Access (ZPA) logs, combined with Hardware Fingerprint data from the Zscaler Client Connector (ZCC). This provides verifiable device identity and activity trails across IT, IoT, and OT, eliminating blind spots and delivering visibility that stands up to investigative and compliance scrutiny.
Enforce dynamic, risk-aware Zero Trust access policies	Real-time device intelligence from Armis (identity, posture, vulnerabilities) pairs with Zscaler's policy enforcement to adapt access decisions dynamically. Devices with risky behavior or anomalous fingerprints are immediately quarantined or segmented, ensuring only verified, trusted devices and users connect to enterprise resources.
Prioritize vulnerabilities and accelerate risk remediation	Armis supplies device behavior, vulnerability (CVE), and exposure data that Zscaler UVM incorporates into contextual risk scores. This enables security teams to target remediation efforts on assets with the highest business impact, accelerating patching and reducing cyber risk.
Detect threats early and enable coordinated response	Zscaler Deception deploys decoy assets to catch attackers, while Armis enriches alerts with device and user context. This integration delivers high-fidelity alerts and enables faster, coordinated responses to threats.
Automatically segment and contain high-risk or compromised devices	Zscaler Zero Trust Branch enforces fine-grained segmentation between IT, IoT, and OT environments. When Armis flags a high-risk or compromised asset, Zscaler instantly isolates it from critical systems, reducing lateral movement risk and preserving business continuity.

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.

Learn more at **www.zscaler.com/partners/technology**

Experience your world, secured.

About Zscaler: Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest in line cloud security platform. Learn more at zscaler.com or follow us on X (Twitter) @zscaler.