JOINT SOLUTION BRIEF

zscaler + ORDR

Comprehensive visibility, contextual intelligence sharing and Zero Trust access across IT, IoT, IoMT and OT

INTEGRATION HIGHLIGHTS

- ✓ Unified device visibility and risk-based insights
- ✓ Dynamic Zero Trust Policies with device context
- ✓ Simplified segmentation across IT, IoT, IoMT and OT

The Market Challenge

As organizations embrace IoT, OT, hybrid IT, and smart infrastructure to drive innovation, they face an explosion of connected assets that legacy security models were never designed to protect. Traditional perimeter-based approaches, VPNs, and hardware-centric solutions fall short in delivering the visibility, agility, and control needed to secure today's dynamic environments. Limited resources and siloed tools leave security teams struggling to manage growing attack surfaces, increasing the risk of breaches and compliance gaps.

The rise of sophisticated threats targeting unmanaged and mission-critical devices only compounds the challenge. To stay ahead, organizations need a modern, cloud-delivered security model that eliminates blind spots, enforces Zero Trust based on real-time device context, and simplifies operations without adding cost or complexity. A unified, scalable approach is essential to safeguard every asset — IT, IoT, OT, and beyond — across any network, any location, and any user environment.

The Solution

Together, Zscaler and ORDR deliver a unified, cloud-delivered security solution designed to protect today's expanding connected ecosystems. The integrations combine ORDR's deep asset visibility, real-time device profiling, and dynamic risk insights with Zscaler's Zero Trust Exchange (ZTE) platform to ensure visibility, compliance and enforce context-based access policies across users, devices, and applications. ORDR AI Protect platform automatically discovers and classifies every connected asset—including IT, IoT, OT, and IoMT devices—mapping communications, identifying risks, and providing actionable intelligence. Zscaler's cloud-native security services deliver inline traffic inspection, advanced threat protection, and secure access to internet, SaaS, and private applications from any location. The seamless bidirectional data exchange, empowers organizations to minimize exposure, block threats at scale, accelerate incident response, and implement dynamic microsegmentation without the complexity of traditional NAC or perimeter-based models. By eliminating blind spots and enforcing Zero Trust principles based on device and user context, Zscaler and ORDR provide a scalable, simplified approach to securing every asset across IT, OT, IoT, and IoMT environments — without costly infrastructure upgrades.

Zscaler and ORDR combine Zero Trust access with real-time asset intelligence to eliminate blind spots, enforce risk-aware policies, and secure every connected device across IT, OT, IoT, and IoMT—at scale and with precision.

©2025 Zscaler, Inc. All rights reserved.

Solution Components Deep Dive

Zscaler and ORDR jointly deliver deep device intelligence and dynamic segmentation to secure every connected asset—whether IT, IoT, OT, or IoMT. ORDR Sensors are deployed passively via SPAN or tap ports to monitor network traffic, identifying and profiling all devices across segments. This telemetry is enriched by the ORDR Systems Control Engine (SCE), which adds contextual intelligence—such as device type, OS, software versions, behavior, and vulnerabilities—and shares it securely with Zscaler's Zero Trust Device Segmentation (ZTDS) platform.

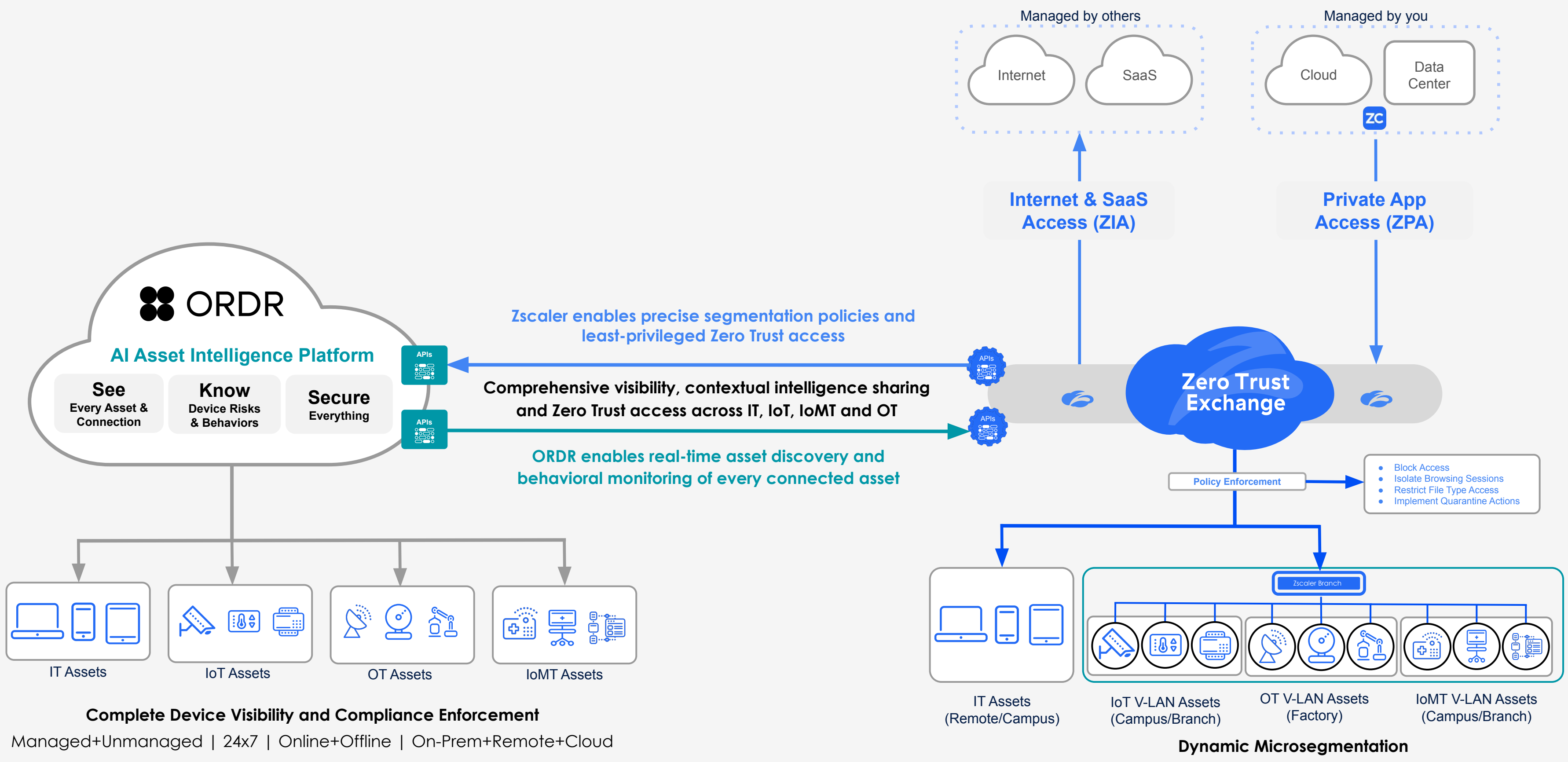
Managed by others
Internet
SaaS
Managed by you
Cloud
Data Center
ZC
Internet & SaaS Access (ZIA)
Private App Access (ZPA)
ORDR
AI Asset Intelligence Platform
See
Every Asset & Connection
Know
Device Risks & Behaviors
Secure
Everything
APIs
APIs
Zscaler enables precise segmentation policies and least-privileged Zero Trust access
Comprehensive visibility, contextual intelligence sharing and Zero Trust access across IT, IoT, IoMT and OT
ORDR enables real-time asset discovery and behavioral monitoring of every connected asset
APIs
APIs
Zero Trust Exchange
Policy Enforcement
Block Access
Isolate Browsing Sessions
Restrict File Type Access
Implement Quarantine Actions
Zscaler Branch
IT Assets
IoT Assets
OT Assets
IoMT Assets
Complete Device Visibility and Compliance Enforcement
Managed+Unmanaged | 24x7 | Online+Offline | On-Prem+Remote+Cloud
IT Assets (Remote/Campus)
IoT V-LAN Assets (Campus/Branch)
OT V-LAN Assets (Factory)
IoMT V-LAN Assets (Campus/Branch)
Dynamic Microsegmentation

Figure 1. The Zscaler and ORDR Integration Architecture

In parallel, ORDR integrates with Zscaler Client Connector via API, pulling device-level data to enhance visibility, detect agent gaps, and assess endpoint risk posture. Zscaler ZTDS uses this contextual data to orchestrate and enforce segmentation via the ZTDS Gateway, dynamically isolating high-risk devices and enforcing least-privilege access without network redesign.

KEY USE CASES

Unified Asset Visibility and Compliance Enforcement

Zscaler and ORDR deliver real-time visibility into every connected asset—across IT, OT, IoT, and IoMT—while continuously exchanging contextual intelligence. This integration enables security teams to identify unmanaged or non-compliant devices, streamline regulatory compliance (e.g., HIPAA, CJIS, FedRAMP). The integration of Zscaler and ORDR provides organizations with unparalleled visibility and control over their entire connected devices ecosystem spanning IT, OT, IoT and IoMT.

By combining ORDR's real-time asset discovery and behavioral monitoring with Zscaler's Zero Trust Engine (ZTE), security teams can automatically detect, profile, and assess the risk associated with every device in the environment. Contextual information about devices and their behavior is continuously shared between ORDR and Zscaler—so if ORDR identifies a device behaving abnormally or failing to meet security standards, it immediately notifies Zscaler. This allows for rapid identification of unmanaged or non-compliant devices, ensuring that no asset goes unnoticed or unsecured. This integration empowers organizations to enforce Zero Trust access controls across all device types, allowing only authorized devices to access critical applications. At the same time, it streamlines regulatory compliance efforts for standards such as HIPAA, CJIS, and FedRAMP, simplifying the ongoing challenge of maintaining compliance in complex, ever-evolving connected environments.

Dynamic Microsegmentation with ZTDS

Using ORDR's granular device intelligence and real-time insights into risk posture, Zscaler's Zero Trust Branch dynamically enforces least-privilege access across the network and swiftly isolates high-risk assets. Organizations gain the ability to define precise segmentation policies for every device—without the need to redesign their network—with each device limited to only the resources and applications it truly needs. This dynamic approach sharply limits lateral movement if a device is compromised, dramatically reducing the potential impact of a security breach.

At the same time, the combined solution ensures secure operational continuity across even the most diverse and mission-critical environments. Security teams can respond immediately to changes in device risk, maintaining tight controls and supporting business operations without disruption.

> **Our partnership with Zscaler empowers organizations to see every device, enforce precise Zero Trust controls, and contain risk instantly—delivering operational resilience and compliance across even the most complex IT, IoT, and OT environments.**
>
> **Srinivas Loke**
> Head of Products, ORDR

©2025 Zscaler, Inc. All rights reserved.

Zscaler + ORDR Benefits

ACTION	DESCRIPTION
Gain Real-Time Asset Visibility	Unified view across IT, IoT, OT, and IoMT assets through ORDR's passive monitoring and Zscaler Client Connector context ingestion.
Enforce Risk-Aware Segmentation	Zscaler ZTDS dynamically enforces least-privilege access policies based on ORDR-provided device intelligence and behavioral risk insights.
Accelerate Compliance	Identify unmanaged or non-compliant assets and automate policy enforcement to support frameworks like HIPAA, CJIS, and FedRAMP.
Reduce Lateral Movement Risk	Isolate high-risk devices without core network changes using Microsegmentation that leverages joint telemetry and enforcement logic.

Conclusion

Together, Zscaler and ORDR help security teams minimize risk, accelerate threat response, streamline compliance, and reduce operational overhead. With scalable, cloud-delivered security and real-time device insights, organizations can protect their expanding digital ecosystems—across IT, IoT, and OT—with confidence, speed, and simplicity.

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

zscaler™ | **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.

©2025 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, and ZPA™ are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

©2025 Zscaler, Inc. All rights reserved.