JOINT SOLUTION BRIEF

zscaler™ + TREND MICRO™

Real-Time User Risk-Based Access Control with Zero Trust Enforcement

INTEGRATION HIGHLIGHTS

- Real-Time Zero Trust Conditional access control
- Minimize data silos and drive automated enforcement at scale
- Increase efficiency of incident triage and investigation

The Market Challenge

Today's enterprise technology stacks are complex – with distributed applications, users, and endpoints, an ever-expanding list of IoT devices, and new sanctioned and unsanctioned applications being deployed daily. As attack vectors continue to expand—from endpoints to networks to the cloud—security teams face increasing challenges in protecting valuable assets both within and beyond the traditional network perimeter.

The more security controls that security operations teams deploy, the more alerts they get, but too often, the signal is buried in the noise. Security analysts are forced to pivot between tools that do not integrate and fail to connect the dots across the entire technology stack. As a result, security data is collected and analyzed in isolation, without any context or correlation, creating gaps in what security teams can see and detect, leading to longer dwell times.
This complexity has necessitated a new approach to securing access—one that provides frictionless security from endpoint to network to application.

The Solution

Together, Zscaler and Trend Micro unify to provide enterprise security across endpoint, network, and cloud, enabling enhanced end-to-end visibility, accelerated remediation, and secure conditional access. Trend Micro's Trend Vision One continuously protects against threats, detects them, and responds across endpoints, identities, and cloud workloads using unified analytics. The Zscaler Zero Trust Exchange (ZTE) provides secure access to the internet, SaaS apps, and private apps for all users from any device or location, with inline AI-powered traffic inspection and advanced threat protection. As user risk scores increase due to suspicious behavior or threat exposure, Trend Vision One can automatically adjust group memberships in Zscaler through SCIM provisioning. This activates predefined policies in ZIA and ZPA—such as restricting application access, enforcing browser isolation, or blocking downloads—helping to reduce risk while preserving user productivity. With seamless integration between Zscaler and Trend Micro, security teams can minimize risk and block threats outright, security operation centers can triage, investigate, and remediate threats much more efficiently and with greater confidence.

Together, Zscaler and Trend Micro deliver a cloud-based, end-to-end zero trust solution that provides users fast and secure access to the internet, SaaS, and private applications – over any network, at any location, and on any device.

Solution Components Deep Dive

The joint solution hinges on SCIM-based identity synchronization, where restricted user groups are created in the Identity Provider (IdP) and synced with Zscaler Internet Access (ZIA) and Private Access (ZPA). Trend Vision One continuously monitors user behavior and dynamically adds high-risk users to these groups, triggering Zscaler to enforce conditional access policies.

Trend Vision One's automated playbooks use predefined templates such as Automated High-Risk Account Response, with logic built on triggers (e.g., elevated risk score), conditions (e.g., credential compromise), and actions (e.g., add to Zscaler Restricted Access Group). Each workflow is composed of modular nodes—target, condition, and enforcement—that ensure precise, policy-driven responses.

Zscaler then applies the appropriate restrictions—such as URL filtering, browser isolation, or access denial—based on the user's group membership. Combined, these capabilities enable continuous Zero Trust enforcement, accelerate threat containment, and eliminate manual intervention for high-risk user scenarios.

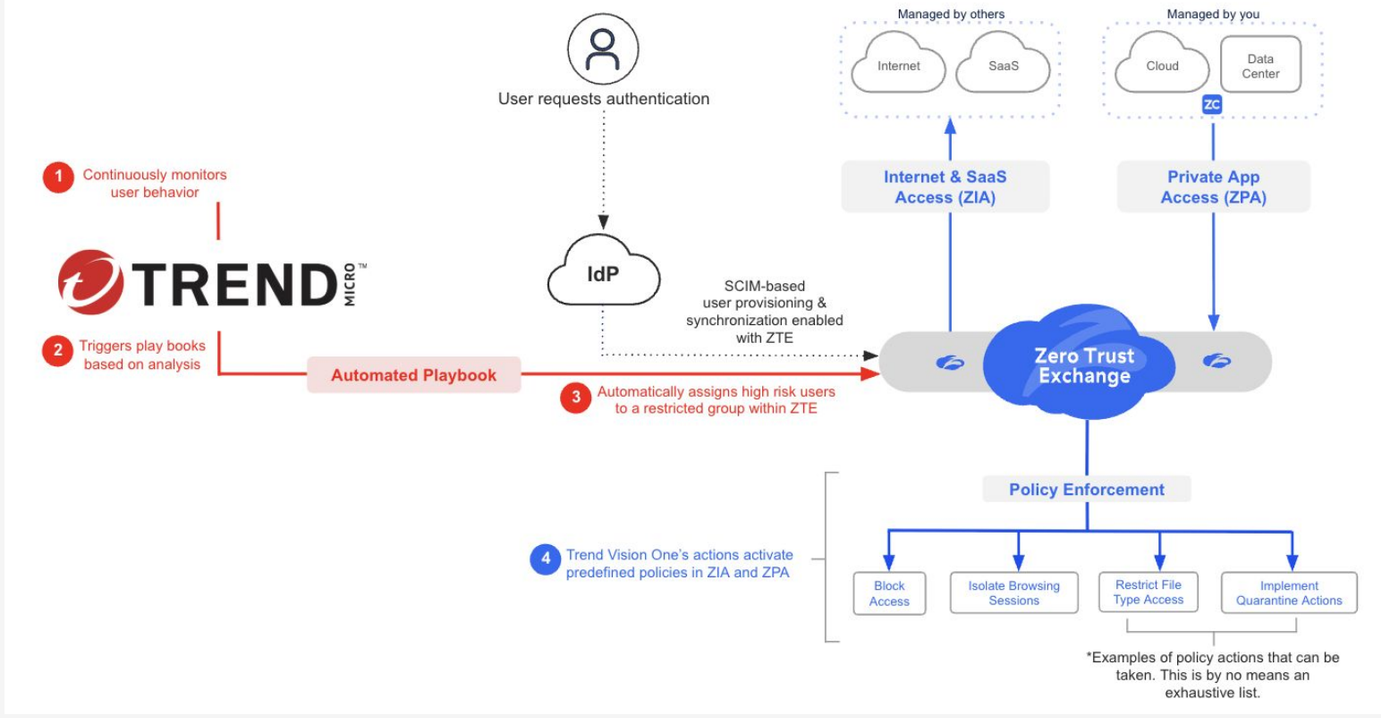

Figure 1. The Zscaler and Trend Micro Integration Architecture

KEY USE CASES

Dynamic Policy Enforcement for High-Risk Users

Trend Vision One actively monitors user behavior to detect risky activities, such as unusual access patterns, potential compromises, or any behavior indicative of a threat. Based on this analysis, it automatically adjusts the user's group membership within the Zscaler environment.

When a user's risk level increases and they are moved to a restricted group, Zscaler enforces predefined policies to limit the high-risk user's access. These measures can include blocking access to specific resources or services, isolating browsing sessions to reduce exposure, restricting file-type access to prevent the transfer of executable files or sensitive documents, and implementing quarantine actions that further restrict network and resource access, preventing lateral threat movement within the environment.

Automated Response to Threat Activity

Trend Vision One empowers security teams to manage threats with both manual enforcement and automated workflows. By leveraging triggers, conditions, and actions, teams can design automated playbooks that respond to incidents in real time, reducing the need for manual intervention. Detailed audit logs are generated for every automated response, providing valuable data for forensic analysis and continuous improvement of threat management strategies.

Zscaler + Trend Micro Benefits

ACTION	DESCRIPTION
Proactive Risk Mitigation	Automatically restrict access for users exhibiting risky behavior or compromised credentials, reducing the potential impact of threats before they escalate.
Seamless Zero Trust Enforcement	Aligns with Zero Trust principles by dynamically adjusting access policies based on user risk — ensuring least-privilege access to both internet and private applications.
Improved Operational Efficiency	Reduces the need for manual policy updates and incident response steps, freeing up time for SOC teams, Incident Responders and Threat Hunters to focus on high-value investigations.
Unified Security Posture	Leverages the combined power of Trend Vision One and Zscaler's access controls to create a tightly integrated, context-aware defense strategy
Faster Incident Containment	High-risk users are immediately isolated or have their access reduced, helping contain threats early in the attack chain

Conclusion

Together, Zscaler and Trend Micro's Trend Vision One deliver adaptive, risk-based access control that aligns with Zero Trust principles. By unifying threat detection and dynamic policy enforcement based on defined user risk threshold, organizations can reduce dwell time, contain threats faster, and minimize operational overhead. This joint solution empowers security teams to respond with speed and confidence—protecting users, data, and applications across the enterprise.

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.

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

©2025 Zscaler, Inc. All rights reserved.