JOINT SOLUTION BRIEF

zscaler™ + Gigamon®

Extend Zero Trust Access With Deep Observability Into Application Activity

Integration Highlights

- Zero Trust access with visibility into east-west traffic
- Faster troubleshooting across users and applications
- Stronger policy validation and lateral movement detection

The Market Challenge

Organizations adopting Zero Trust often solve the access problem first. What remains harder is understanding what happens after access is granted, particularly when application activity and east-west traffic create blind spots across hybrid cloud infrastructure.

Zscaler Private Access provides identity- and context-aware access to private applications without exposing them or placing users on the corporate network.

Gigamon complements ZPA by turning relevant post-access traffic into application metadata and network-derived telemetry for downstream SIEM and security workflows.

The Solution

Zscaler Private Access delivers identity-based access to private applications without placing users on the corporate network. The Gigamon Deep Observability Pipeline turns relevant post-access traffic into application metadata and network-derived telemetry.

Gigamon Application Metadata Intelligence (AMI) correlates this telemetry with ZPA identity context, helping organizations investigate faster, validate Zero Trust policy, detect lateral movement, and troubleshoot application performance using existing SIEM workflows.

How the Joint Solution Works

Secure Access and Post-Access Visibility

Zscaler Private Access delivers identity-based access to private applications without exposing them or placing users on the corporate network. Gigamon monitors relevant post-access and east-west traffic to generate application metadata and network-derived telemetry.

> Zscaler Private Access determines who can securely reach a private application. The Gigamon Deep Observability Pipeline provides the post-access application intelligence security teams need to understand what happens next. Together, Zscaler and Gigamon help organizations investigate faster, validate Zero Trust policy, and detect lateral movement with greater confidence.
>
> **Srinivas Chakravarty,** Vice President, Cloud Ecosystem at Gigamon

How the Joint Solution Works (cont'd)

Application Metadata Intelligence
Gigamon Application Metadata Intelligence extracts application metadata from observed traffic and enriches it with ZPA identity context for downstream SIEM and security workflows.

Operational Visibility Across Hybrid Cloud
The joint solution helps organizations investigate application activity, validate Zero Trust policy, detect lateral movement, and troubleshoot performance across hybrid cloud infrastructure.

KEY USE CASES

Comprehensive Visibility
Combine ZPA identity and access context with Gigamon application metadata intelligence and network-derived telemetry to investigate activity, validate policy, and monitor application behavior across hybrid cloud infrastructure.

Secure Private Application Access
Replace VPNs with Zero Trust access that connects users only to authorized private applications, reducing attack surface without placing them on the corporate network.

Additional Use Cases

Lateral Movement Detection
Monitor east-west communication after access is granted to identify suspicious probing, unauthorized connection, and potential lateral movement.

Application Activity Visibility
Extend visibility beyond access logs with application metadata derived from observed traffic. Gigamon AMI enriches downstream monitoring and security workflows with additional application context.

Faster Incident Response
Correlate ZPA identity context with Gigamon application metadata and network-derived telemetry to connect user activity with application behavior, accelerate triage, and improve response.

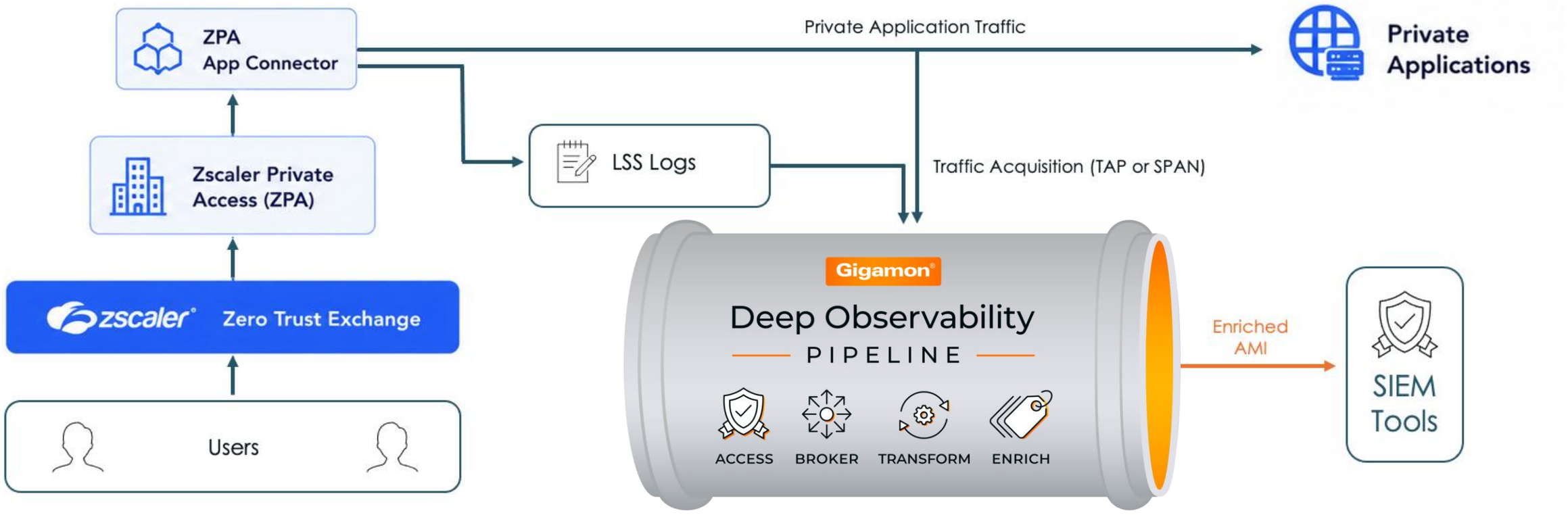

Figure 1. Enriching ZPA identity context with Gigamon application metadata intelligence and network-derived telemetry.

Zscaler + Gigamon Benefits

Action	Description
Reduce Attack Surface	Connect users only to authorized private applications without exposing applications or placing users on the corporate network.
Accelerate Investigations	Correlate ZPA identity context with application metadata and network-derived telemetry for faster analysis and response.
Validate Zero Trust Policy	Monitor post-access application activity to identify unexpected communication and potential policy drift.
Improve SIEM Workflows	Deliver enriched AMI that provides deeper application context without changing established security workflows.

Conclusion

Zscaler and Gigamon combine secure private application access with post-access application intelligence, helping teams investigate faster, validate policy, and detect lateral movement using existing SIEM workflows.

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

©2026 Zscaler, Inc. All rights reserved.