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
- Plaintext visibility into encrypted private access tunnels
- Faster detection and response for lateral movement

## The Market Challenge

Organizations adopting Zero Trust often solve the access problem first. What remains harder is understanding what happens after access is granted, especially across hybrid cloud environments where application activity, East-West traffic, and encrypted sessions can create blind spots for security and operations teams.

Zscaler Private Access shows who connected and which application they accessed, but security teams often need more context about what happened during the session. Much of the activity tied to lateral movement detection and policy validation happens inside the environment, not only at the point of access. Analysts also have to piece together identity, application, and network context across disconnected tools, which slows investigations and makes it harder to separate security issues from performance issues when users report lag or application problems.

## The Solution

Together, Zscaler and Gigamon help teams secure private application access and understand what happens after access is granted across hybrid cloud environments. Zscaler Private Access delivers identity-based access to private applications without putting users on the corporate network, while Gigamon turns relevant post-access traffic into application metadata and network-derived telemetry for existing SIEM, log management, NDR, SOC, and observability tools.

Gigamon Application Metadata Intelligence (AMI) extracts rich session context and enriches it with ZPA identity data so teams can connect who initiated access with what happened during the session. Gigamon also provides visibility into relevant traffic before it enters encrypted ZPA tunnels, helping reduce blind spots and support AI-driven security operations, faster investigations, policy validation, and troubleshooting without changing existing ZPA controls or downstream workflows.

**Together, Zscaler and Gigamon give security and IT teams the context to validate policy, reduce blind spots, and resolve issues faster by combining identity-based access with application metadata and post-access visibility across hybrid cloud environments.**

## Solution Components Deep Dive

**Secure Private Application Access**
With Zscaler Private Access, organizations replace legacy VPNs with cloud-native, identity-based access to private applications without putting users on the corporate network.

**Monitor East-West Traffic After Access Is Granted**
Gigamon Deep Observability Pipeline adds visibility into East-West traffic across hybrid cloud environments, helping teams detect lateral movement and reduce blind spots after access is granted.

**Precryption-Based Tunnel Visibility**
Gigamon Precryption® technology provides visibility into relevant traffic before it enters ZPA encrypted tunnels, exposing activity that downstream security and monitoring tools might otherwise miss.

**Identity-Enriched Network-Derived Telemetry**
Gigamon AMI extracts and enriches more than 5,000 metadata attributes from network traffic and combines that telemetry with ZPA identity context to give SIEM, NDR, and SOC workflows more useful investigation context and faster incident response.

**Consistent Hybrid Cloud Deployment Model**
The solution works across on-premises and public cloud environments, providing a common monitoring point for lateral traffic, security analytics, and performance troubleshooting.

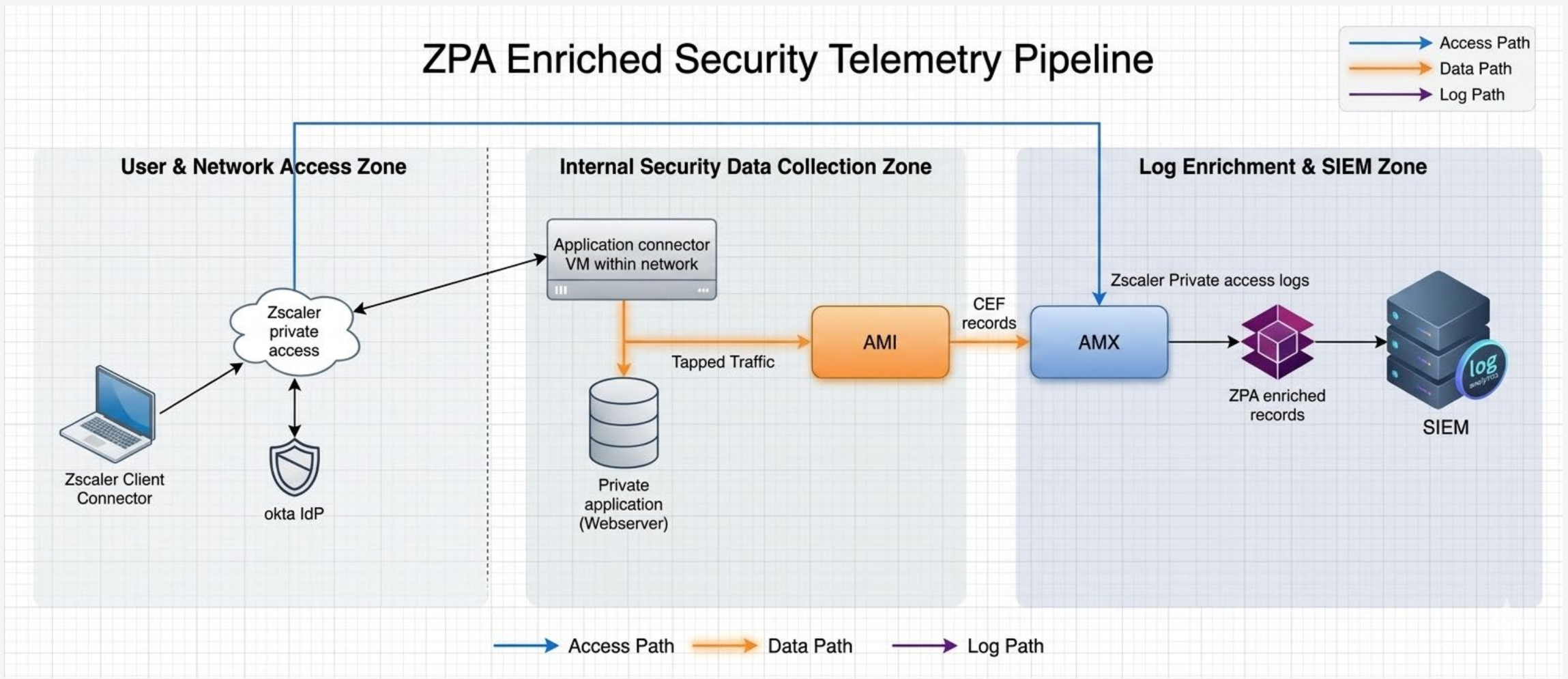


**Figure 1**. ZPA enriched with network-derived telemetry and Application Metadata intelligence from Gigamon.

## KEY USE CASES

### Comprehensive Visibility

Zscaler and Gigamon integrate for expanded visibility to provide security teams with a holistic understanding of threat context and user attributes, allowing them to quickly triage and respond to attacks. While Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) offer secure internet, SaaS, and zero trust network access, the Deep Observability Pipeline continuously provides network telemetry for complete visibility and accelerated investigation.

### Secure Private Application Access

Replace legacy VPN architectures with Zero Trust access to private applications, giving users direct connectivity to only the applications they are authorized to use without placing them on the broader corporate network. This reduces attack surface while improving the user experience for employees, contractors, and third parties.

## Additional Use Cases

**Lateral Movement Detection**
Extend security monitoring beyond initial access by observing East-West traffic between applications and workloads. This helps security teams detect suspicious probing, unauthorized communication, and signs of compromise that may occur after a user or workload has been granted access.

**Encrypted Tunnel Visibility**
Reduce blind spots created by encrypted application tunnels with visibility into traffic before it is encrypted by ZPA. This allows teams to inspect activity that might otherwise be hidden from downstream monitoring and analytics tools.

**Faster Incident Response**
Improve investigations by adding enriched metadata from Gigamon to ZPA identity context, to help analysts connect user activity with network behavior more quickly. This context supports faster triage, better prioritization, and more efficient response to lateral movement and other suspicious activity.

**Hybrid Cloud Consistency**
Apply a common access and visibility model across on-premises environments and public cloud infrastructure, including VMware-based data centers and AWS or Azure deployments. This gives security teams a more consistent way to monitor traffic and feed optimized telemetry to centralized security tools.

## Zscaler + Gigamon Benefits

| ACTION | DESCRIPTION |
| --- | --- |
| **Reduce the Attack Surface** | Ensure zero trust access with risk-based authentication that securely connects users directly to authorized apps without accessing the network to prevent the lateral movement of threats. |
| **Richer Context for Security Investigations** | Enrich ZPA access data with application metadata and network-derived telemetry to accelerate investigations across SIEM, NDR, SOC, and related workflows. |
| **Improved Zero Trust Visibility and Operations** | Validate least-privilege policies, reduce blind spots created by encrypted tunnels, and isolate issues across users, applications, and hybrid cloud infrastructure. |
| **Better Signal Quality for Existing Security Tools** | Send higher-value metadata and telemetry to current SIEM, log management, and observability tools so teams can focus on more useful signals. |
| **Faster Troubleshooting Across Users and Applications** | Use latency and response-time telemetry to help determine whether an issue sits with the user, the application, or the access path. |
| **Consistent Monitoring Across Hybrid Cloud Environments** | Apply the same visibility model across on-premises and public cloud environments to support centralized analytics and more consistent operations. |

## Conclusion

Zscaler and Gigamon bring secure private application access and post-access insight together in one joint solution. By combining identity-based access with application metadata, network-derived telemetry, and visibility into encrypted traffic, the solution helps security and IT teams investigate faster, validate policy, reduce blind spots, and get more value from existing tools across hybrid cloud environments.

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