JOINT SOLUTION BRIEF

zscaler + Plixer

From secure connections to clear answers: Validated security. Explained performance. A single source of truth.

PLIXER

INTEGRATION HIGHLIGHTS

- Detect C2, credential abuse, and sensitive data movement within encrypted sessions
- Prove every incident: Jump from alert to timeline in minutes with clear evidence
- Validate Zero Trust outcomes: report on enforcement and user experience

The Market Challenge

As organizations adopt encrypted, Zero Trust access, traditional network visibility changes. Together, Zscaler and Plixer give SecOps and NetOps the operational context they need, without decryption, to see attacker behavior, validate policies, and explain performance. The result: earlier detection, faster investigations, and clearer answers across teams.

Analysts already face a flood of alerts without enough proof to prioritize. Network teams are pressed to explain outages and slowdowns across hybrid networks and encrypted sessions. The result: longer dwell times, missed SLAs, and unproductive cycles of cross-team escalations.

Delivering this context requires more than access control. Organizations need observability that complements Zero Trust by making encrypted traffic explainable. Plixer and Zscaler together deliver that clarity, turning encrypted sessions into actionable insight.

The Solution

Zscaler and Plixer together extend visibility in Zero Trust. Zscaler enforces secure access to internet, SaaS, and private applications. Plixer enriches ZIA and ZPA telemetry to make encrypted sessions explainable, without decryption. The result is a single source of truth that SecOps and NetOps use to detect attacks faster, prove policies are working, and assure performance.

Plixer One transforms Zscaler logs into enriched, flow-like records that surface attacker behaviors such as command-and-control, lateral movement, and account misuse. Security teams scope incidents with confidence, while network teams validate service quality and pinpoint slowdowns with evidence.

With direct integration, Zscaler and Plixer reduce alert noise, extend visibility, and cut investigation time from hours to minutes. Every Zero Trust connection becomes both secure and explainable, giving teams proof they can act on.

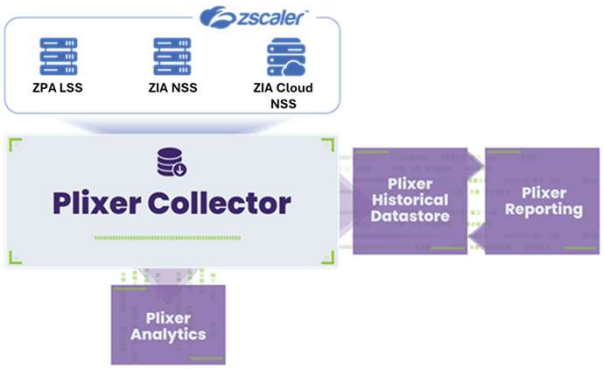
Together, Zscaler and Plixer make every Zero Trust connection secure and observable on any network, from any location, and on any device. Teams detect earlier, investigate faster, and prove outcomes.

Solution Components Deep Dive

Strengthen Zero Trust with observability through ZIA and ZPA
Add visibility to encrypted Zero Trust sessions without agents or decryption. Plixer enriches ZIA and ZPA telemetry to reveal user, app, and connector activity.

Validate policy effectiveness in real time
Prove Zero Trust rules are working. Plixer maps sessions to users, destinations, and connectors, highlighting drift or connector issues before they become outages.

Continuously monitor experience and behavior
Track service quality and attacker behavior. Plixer correlates ZIA and ZPA telemetry with flows to surface anomalies, detect C2 indicators, flag credential abuse, and identify sensitive data movement within encrypted sessions. Incidents roll up into clear timelines and tickets that make Zero Trust explainable.



KEY USE CASES

Comprehensive visibility for faster triage

SecOps surfaces attacker behaviors such as command-and-control, credential abuse, and sensitive data movement without decryption. NetOps validates service quality by correlating user, app, and connector activity. Together, teams cut investigation time from hours to minutes, moving from alert to timeline with the context to close cases quickly.

Experience assurance across applications

By correlating Zscaler telemetry with flow context, Plixer pinpoints whether slowdowns stem from policy configuration, connector status, network path, or application responsiveness, so teams resolve issues faster and confirm Zscaler policies are performing as intended. Reports confirm service quality and verify that Zero Trust policies are working. NetOps gains clarity, users get faster answers, and leadership sees proof of outcomes.

Zero Trust isn't just about keeping threats out. It's about knowing what's happening within. Together, Zscaler and Plixer make every connection a source of truth, giving enterprises the confidence to move fast and prove security at every layer.

Paul Piccard
Chief Technology Officer, Plixer

Zscaler + Plixer Benefits

ACTION	DESCRIPTION
Surface activity in encrypted sessions	Zscaler secures access. Plixer adds observability by ingesting ZIA and ZPA logs, surfacing user activity, app access, and anomalies within encrypted sessions.
Accelerate investigations with clear evidence	Plixer correlates Zscaler telemetry with flow context so analysts trace scope, connections, and root cause in minutes. Cases close faster with timelines that prove what happened.
Validate Zero Trust policies continuously	Plixer analyzes ZIA and ZPA patterns to highlight rule drift, unused policies, and connector health. Teams quickly confirm policies are enforced and effective.
Assure user experience across applications	When apps slow down, Plixer correlates Zscaler traffic with network paths and connectors to show if issues stem from policy, path, or responsiveness. Reports confirm service quality and speed resolution.
Unify operations across SecOps and NetOps	Plixer turns Zscaler activity into a single view. Shared dashboards and context-rich reports reduce duplication and give all teams clarity they can trust across operations

Conclusion

Zscaler secures access while Plixer adds observability. By transforming ZIA and ZPA telemetry into enriched records, Plixer provides the context to understand users, applications, policies, and performance in encrypted sessions, without decryption or agents. Security and network teams work from a single source of truth to detect earlier, investigate faster, and validate outcomes.

The result: earlier threat detection, faster investigations, validated policies, and a better user experience. Security and network teams act from the same source of truth, reducing risk and ensuring every Zero Trust connection delivers proven security and assured performance.

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

+1 408.533.0288

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

©2025 Zscaler, Inc. All rights reserved.