



Turn Zscaler telemetry into high-fidelity security insight with Cribl



## INTEGRATION HIGHLIGHTS

- ✓ Retain more Zero Trust telemetry within existing budgets.
- ✓ Reduce noise and false positives with de-duplicated, contextualized signals.
- ✓ Speed triage and investigations with better context across security workflows.

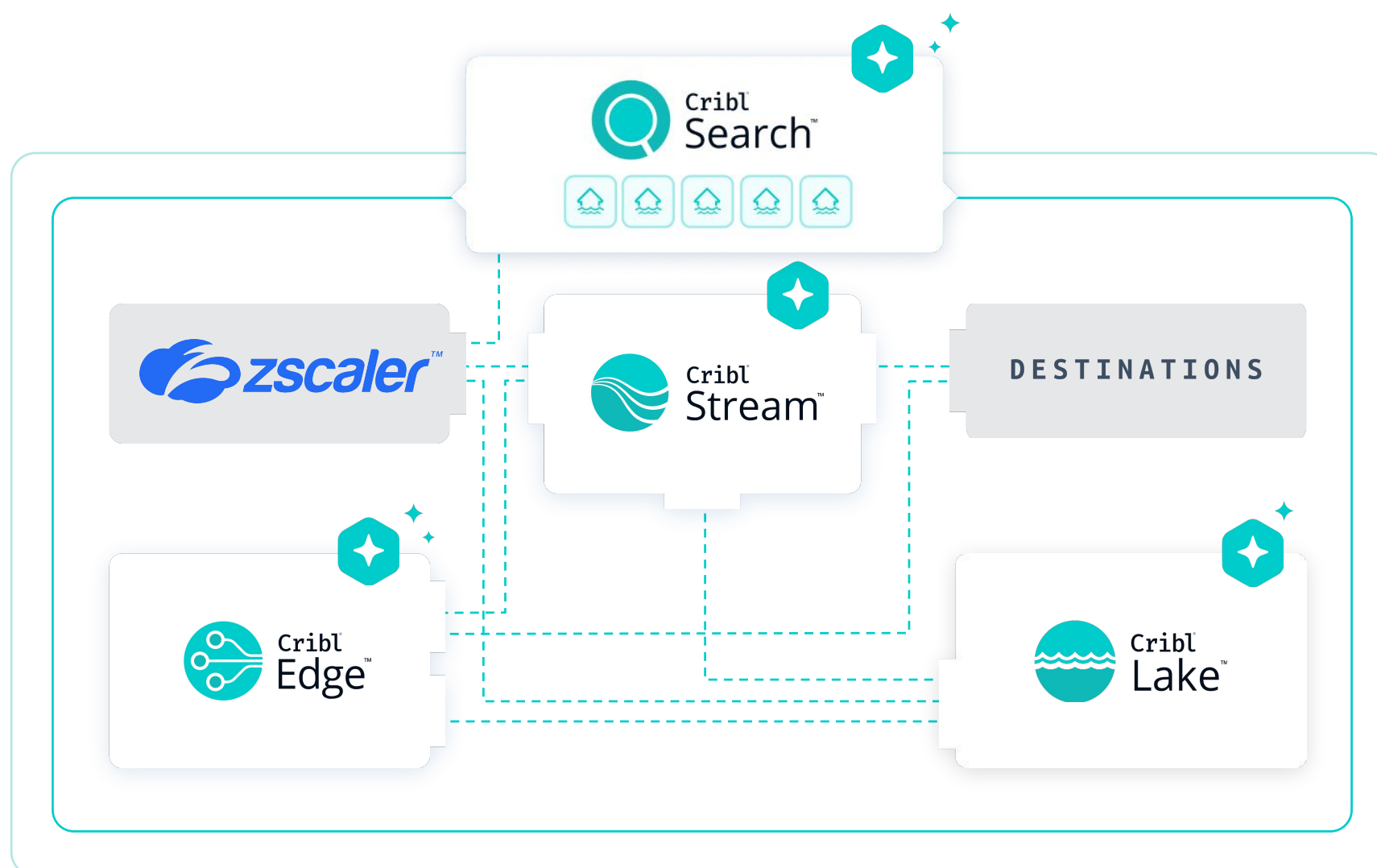
### The Market Challenge

Modern SOCs are flooded with logs from cloud services, endpoints, identities, and networks, but still struggle to see the full picture when something goes wrong. Zscaler produces deep visibility across internet access, private applications, SaaS usage, and data protection, yet pushing all of that telemetry into every downstream tool quickly becomes unaffordable. Teams end up making hard tradeoffs about what to keep, where to send it, and how long to retain it, which leads to noisy alerts, blind spots, and slow investigations.

### The Solution

Together, Zscaler and Cribl turn telemetry into a controllable data stream. Security teams can collect events once, standardize and enrich them, remove redundancy, and then deliver exactly the right data to SIEM, SOAR, security data lakes, observability platforms, and long-term storage. Cribl Search gives analysts direct, search-in-place access to Zscaler telemetry for day-to-day investigations and threat hunting, while Cribl Lake provides a lower-cost layer to keep more history online and replay it into analytic tools when needed.

**Zscaler's Zero Trust Exchange produces high-value telemetry from users, devices, applications, and cloud traffic. Cribl makes that data operational by collecting it once, shaping and enriching it, de-duplicating overlapping signals, and routing it to one or many downstream tools in the formats teams need.**



## The Benefits of Using Zscaler and Cribl

### Cut noise, keep context

Zscaler's Zero Trust Exchange generates high-value signals from every user and application connection. Cribl preserves that rich context while stripping out duplication and low-value events so SOCs are working from sharper signals instead of sifting through repetitive data. Analysts spend more time investigating real issues and less time tuning around noisy feeds.

### Keep SIEM and storage costs in check

Rather than sending every Zscaler log to a single expensive destination, teams can decide what goes where. High-value events feed SIEMs and SOAR platforms for detections and response, while less time-sensitive data lands in more economical storage. This lets organizations expand their use of Zscaler telemetry without constantly renegotiating ingest and retention limits.

### Search fast, tier smart

With Cribl Search, security teams can query Zscaler telemetry directly, without waiting for it to be copied into yet another system. Cribl Lake serves as a cost-efficient tier for broader Zscaler history so that data stays available for months or years instead of days. When deeper analysis is required, teams can selectively replay the right slices of data into SIEMs or other tools instead of re-ingesting everything.

**As organizations accelerate their modernization and Zero Trust efforts, they require solutions that give them choice, control, and flexibility over their data, not added complexity. The integration between Zscaler and Cribl turns the complex task of managing high-volume telemetry into a seamless experience that helps customers accelerate time-to-value within the Zscaler ecosystem.**

**Vlad Melnik**

VP, Alliances and Business Development at Cribl

## The Benefits of Using Zscaler and Cribl

### One integration, many destinations

By treating Zscaler as a first-class telemetry source, Cribl lets teams onboard the integration once and fan out the data to multiple tools. As new platforms are added or older ones are retired, the Zscaler pipeline stays consistent. Security and platform teams keep control over formats, routing, and policies instead of wiring up one-off point connections.

### Power AI-driven security workflows

Clean, well-structured telemetry is a prerequisite for effective automation and AI. Cribl ensures Zscaler data is shaped, enriched, and ready for advanced analytics, while Cribl Lake provides the historical depth those approaches require. Zscaler's MCP Server can then expose Zero Trust Exchange insights to AI agents, allowing teams to build more automated, consistent workflows on a curated data foundation rather than raw, noisy feeds.

## Conclusion

Deliver better business results with Zscaler and Cribl

Organizations do not need more raw security data. They need a better way to operationalize the Zero Trust telemetry they already have. Together, Zscaler and Cribl help security teams collect once, reduce noise, retain more data cost-effectively, and investigate faster across the tools they already use. The result is stronger security outcomes, lower data-management friction, and a more flexible foundation for modern SecOps.

Learn more at [www.zscaler.com/partners/technology](https://www.zscaler.com/partners/technology)



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](https://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.