SOLUTION BRIEF

Turn Zscaler telemetry into high-fidelity **security insight** with Cribl

Cribl helps security teams collect, shape, enrich, route, and retain Zscaler telemetry so they can improve detections, reduce SIEM cost, and get more value from their Zero Trust data.

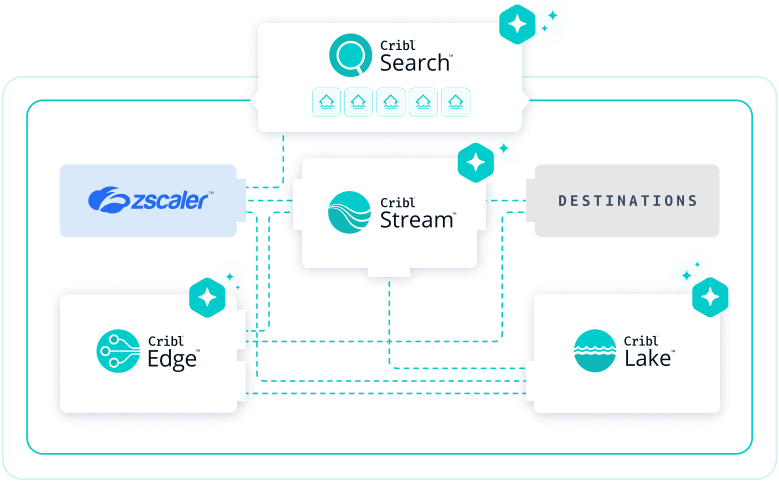
The challenge

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

Cribl Stream turns Zscaler 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.



The challenge

Security operations centers are overwhelmed by fragmented, duplicative telemetry from dozens of tools. That drives up SIEM and storage costs while still leaving teams with alert fatigue, inconsistent context, and slow investigations.

The solution

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

- 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.
- Build a cleaner path to AI-driven analytics and automation.

Benefits

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.

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.

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.

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.

Summary

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.

Cribl | zscaler

Get started with Cribl and Zscaler today

Visit Cribl.io to get started today. The Cribl Slack Community is also a great place to connect with leaders from other teams leveraging both Zscaler and Cribl.

Cribl

The AI Platform for Telemetry

Learn more at cribl.io | Join our Slack community
Try Cribl Sandboxes | Follow us on LinkedIn and X

SB-0074-EN-1-0626