>SOLUTION BRIEF_

Zero in on your Zero Trust Observability with Zscaler and Cribl

THE CHALLENGE

Disparate schemas along with the sheer volume of data make creating a **Zero Trust environment** challenging for enterprises today.

THE SOLUTION

Together, Zscaler and Cribl provide unprecedented visibility into your Zero Trust environment while keeping you safe from data leakage and saving costs on retention and ingestion.

THE BENEFITS

- **Simplified Data Collection**
- **Normalization and Transformation**
- **Data Reduction**
- **Flexibility and Customization**

Expand Your visibility with Zscaler and Cribl

The challenge

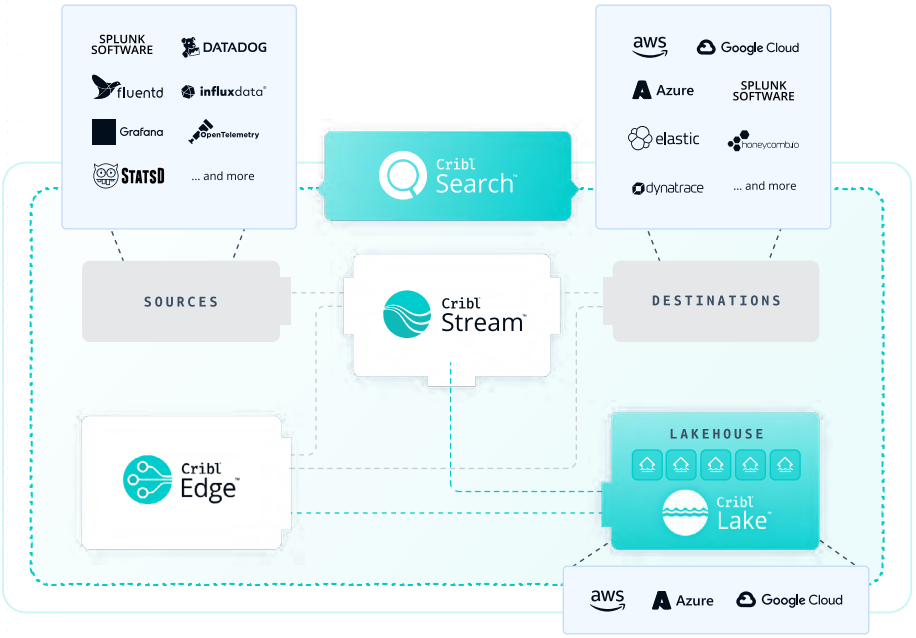
In today's increasingly complex and data-rich environments, the Zscaler Pack for Cribl Stream serves as a beacon of simplicity and efficiency, particularly when it comes to onboarding Zscaler Internet Access (ZIA) logs from NSS Cloud instances. Whether you're looking to simplify your log ingestion or unleash your analytics' full potential, this pack provides a comprehensive framework that can be adapted to your unique use-cases. In essence, consider this pack not just a tool, but a blueprint that showcases the "art of the possible" with Cribl Stream, Zscaler logs, and your creative ingenuity.

This solution works for Splunk but there are some issues:

- **Parsing Cloud NSS logs can be difficult and cumbersome**
- **Transforming Zscaler Logs to OCSF, CIM, ECS is taxing on security resources**
- **Zscaler logs are high in volume and can overwhelm a SIEM**

The Cribl solution

Cribl Stream your best option for achieving this elevated state of operational brilliance? Here's the key: Cribl Stream excels in enhancing observability use cases that complement both your security and DevOps operations. With a wide array of configurable functions in pipelines or full packs, like this Zscaler Pack, you can experiment with different configurations and techniques to make your entire observability ecosystem more stable, more sustainable, and incredibly efficient.



By leveraging this pack, you'll streamline data ingestion and enrich your analytics system, thus ensuring more effective data processing and searching.

The benefits of using Zscaler with Cribl's observability solution

Simplified data collection

The Zscaler Pack offers robust parsing capabilities, designed to work with logs from NSS Cloud instances in a variety of output formats including JSON, CSV, TSV, and Key Value Pairs. Pre-configured parsers (located under Knowledge/Parsers) for each log type are also available, built on field names specified in Zscaler's documentation and are fully customizable to meet your unique requirements.

Normalization and transformation

The Zscaler Pack offers a robust data normalization feature that aligns your log events with both the Common Information Model (CIM) and the Elastic Common Schema (ECS). By doing so, the pack ensures compatibility with industry-standard data models, such as Network Traffic, Network Name Resolution, and Web data models. The true brilliance of this feature lies in its flexibility; you have the option to incorporate the normalized data back into your main log events or use it to update or modify the _raw field. This means you're not just adhering to recognized standards, but you're doing so in a way that aligns with your operational needs. This standardization process not only elevates data integrity but also streamlines downstream analytics and querying, allowing your analysts to dive into data insights without wrestling with incompatible formats or disparate fields.

Data reduction

A standout feature of this pack is its Data Reduction capability. Each field recommended for reduction comes with a comprehensive description, outlining both the value and the potential consequences of its removal from the respective ZIA log types. This facilitates informed decision-making on data minimization.

Flexibility and customization

The Zscaler Pack serves as a blueprint for what is achievable within Cribl Stream. Whether extending basic functionalities or fine-tuning configurations, this pack provides the flexibility needed to tailor features to your unique use-cases and requirements.

Summary

The Zscaler pack is an initial approach to ingest and optimize Cloud NSS Feeds into your system of analysis. Currently, Firewall, DNS, Web and Tunnel logs are being ingested. The Pack is structured as a blueprint to not only showcase what is possible to do within the three pillars of Cribl Stream (Parsing, Enriching and Reducing) but also demonstrate optional functions to unlock new customer use cases.

With Cribl, Zscaler customers can:

- **Simplify their data collection**
- **Normalize and transform their data into common schemas**
- **Reducing data be removing redundant events**
- **Customize the data to fit your requirements**

Together, Cribl observability solutions and Zscaler offer customers unmatched visibility into their Zero Trust environment at an economical cost, thereby ensuring a strong cybersecurity posture.

Get started with Zscaler and Cribl today. The **Cribl Slack Community** is also a great place to connect with leaders from other teams leveraging both <Partner Name> and Cribl.

ABOUT ZSCALER

Zscaler accelerates digital transformation so 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, the SSE-based Zero Trust Exchange is the world's largest in-line cloud security platform.

Learn more at www.Zscaler.com

ABOUT CRIBL

Cribl, the Data Engine for IT and Security, empowers organizations to transform their data strategy. Customers use Cribl's vendor-agnostic solutions to analyze, collect, process, and route all IT and security data from any source or in any destination, delivering the choice, control, and flexibility required to adapt to their ever-changing needs. Cribl's product suite, which is used by Fortune 1000 companies globally, is purpose-built for IT and Security, including **Cribl Stream**, the industry's leading observability pipeline, **Cribl Edge**, an intelligent vendor-neutral agent, and **Cribl Search**, the industry's first search-in-place solution. Founded in 2018, Cribl is a remote-first workforce with an office in San Francisco, CA.

Learn more: **www.cribl.io** | Try now: **Cribl sandboxes** | Join us: **Slack community** | Follow us: **LinkedIn** and **Twitter**

SB-0032-EN-2-0225