netskope + Cribl

Solution Brief

Maximize investments and consolidate data where it needs to go effectively with context-rich logs generated by Netskope's Intelligent SSE (Security Service Edge) and SASE (Secure Access Service Edge) platform. Shape or route valuable Netskope telemetry using a joint solution with Cribl Stream to monitoring, dashboard, or storage locations with governence, speed, flexibility and control.

Key Benefits

- **Enrich Netskope logs with Cribl Stream:** Get the right data to the right location, in the right format from SSE and SASE products
- **Flexibility and scale:** Stream events, metrics, and traces from any Netskope source to any monitoring or dashboard service in any format
- **Eliminate risky business:** Encrypt, obfuscate or remove sensitive data from in-flight and at-rest data. Enforce data policies, standards, and formats across tool-sets
- **Maximize investments and reduce costs:** Receive once and scale or fan out logs, infinity

Netskope provides seamless integration capabilities for high performance log export for timely response and investigations.

The Challenge

Existing enterprise IT and security teams are facing increased volumes of personnel and machine-generated data that take on many forms and exist in various tool-sets– becoming unwieldy and difficult for teams to manage and analyze. Organizations of all sizes continuously seek to optimize the most out of their security and IT investments without increasing or adding new infrastructure costs. Security teams are also short on resources and may lack the ability to send data to third-party platforms that can simplify detecting, correlating and responding to incidents and alerts.

Notwithstanding a great set of tools and solutions, organizations need to adhere to privacy and regulatory standards that cause further strain on existing infrastructure.

- How can I take advantage of my existing SSE and SASE investments in order to correlate data to other sources, like my XDR tool(s)?
- My organization generates a large amount of data, how can I pick which data to keep and send to the appropriate team?

The Netskope One & Cribl Solution

Netskope's high-performance integration capabilities enable organizations to send all or a selected subset of rich customer tenant events and alerts logs to security information and event management (SIEM), data lakes, and extended detection and response (XDR) platforms. When integrated as a solution with Cribl Stream, organizations can optimize IT, security, observability, and telemetry data without the tradeoffs of budget, flexibility, and visibility. Cribl Stream helps organizations gain the choice and control of getting the right Netskope data you need, in the formats you want, and sent off to the destinations required.

Enrich Netskope One logs with Cribl Stream

Paired together and further connected to existing security and IT investments, Netskope One and Cribl Stream enable the exportation of rich event logs from Netskope inline and out-of-band security solutions into SIEMs, data lakes, and syslog formats.

Security operations centers (SOCs) and XDR/MDR services can extend their depth of visibility and context with Netskope Intelligent SSE, NG-SWG, CASB, ZTNA, CSPM/SSPM, and CFW solution logs.

With Cribl Stream, a vendor-agnostic data collection, reduction and enrichment instrument, organizations can smoothly control and enforce data policies, standards and formats across toolsets to:

- Optimize existing security IT infrastructure through data ingestion, tool performance and people hours
- Add rich, contextual, expansive, and detailed Netskope event and alert data to enable SOC teams to quickly understand and investigate cloud applications, data, users, and devices
- Streamline data onboarding and collection to surface data previously unforeseen

Flexibility and scale across existing infrastructure

Together with Cribl Stream, organizations can shape and mold real-time processing of logs, metrics, traces, IT and security-relevant data efficiently.

The solution is built to give teams the flexibility to collect the data they want, and shape it into the formats they need, send it exactly where it needs to go, and replay data on-demand. Furthermore, of the billions of transactions that organizations generate on a daily basis, the solution simplifies and paints a complete picture of the data by enriching Netskope logs and third-party findings–providing actionable insights and metrics for analysis.

Key flexibility and control capabilities include:

- Streaming events, metrics, and traces from any Netskope source or existing security and IT toolsets to any monitoring or dashboard service in any format
- Additionally add any analytics tools without adding new clients or agents to enhance log findings
- Encrypt, obfuscate or remove sensitive data from in-flight and at-rest data.
- Enforce data policies, standards and formats across toolsets

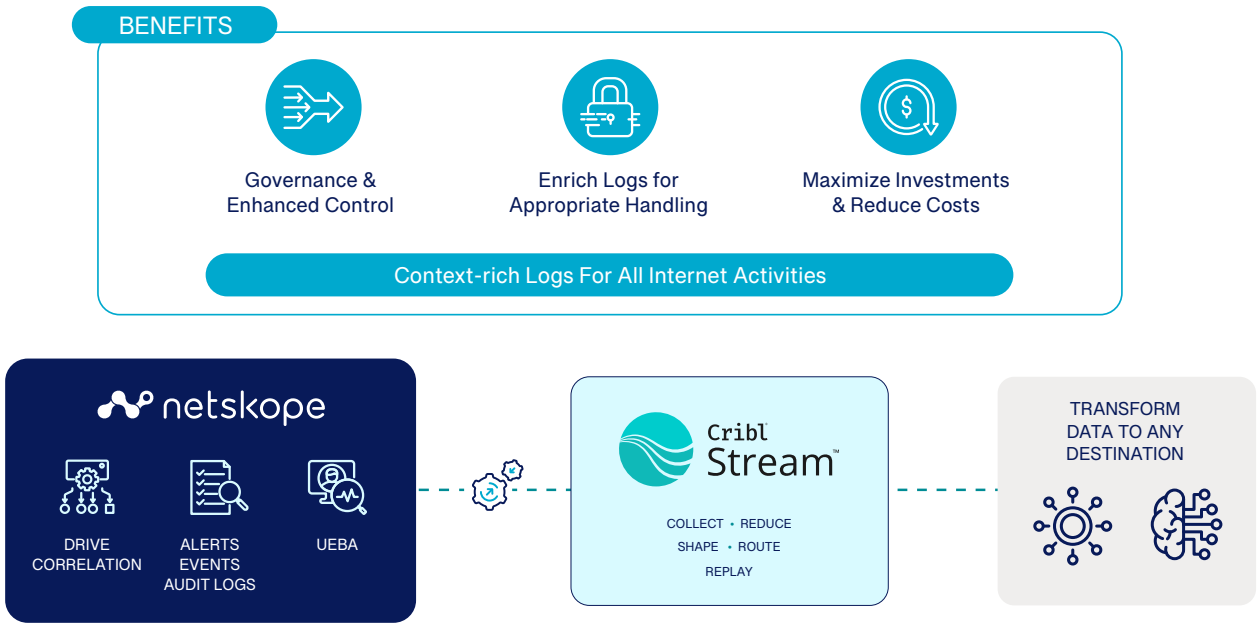
> Cribl Stream helps you get the data you want, in the formats you need, to wherever you want it to go.

Maximize investments and reduce costs

The Netskope One and Cribl Stream joint solution both integrates with—and extends—existing investments to maximize efficiency and enhance capabilities in a way that simplifies and strengthens an organization's overall security posture and improves operational efficiency and effectiveness.

Through improved and automated process workflows, organizations can send the data required for SecOps investigation queues so that systems can instantiate investigations on a single platform without creating multiple configurations. For example, organizations can further direct Netskope One, CrowdStrike Falcon Platform, or Splunk data where it thrives best–offloading to Cribl Lake or other destinations for long-term retention.

Netskope One & Cribl Stream



By translating or formatting data into any tooling schema, organizations can deliver the right data to the right department without adding new costs generated by new agents or forwarders.

Together, the Netskope One and Cribl Stream solution allow organizations to:

- Receive data once and scale out, infinitely and affordably
- Send data to low cost storage and recall as needed for enhancing security, operational outages, and service interruptions–on-demand
- Eliminate the need to deal with raw API output and minimize API calls and connector rebuilds
- Troubleshoot less and immediately see savings without writing a single expression, regex, or lookup

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 to 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, Cribl Search, the industry's first search-in-place solution, and Cribl Lake, a turnkey data lake. Founded in 2018, Cribl is a remote-first workforce with an office in San Francisco, CA.