Elevating SaaS Governance: The New Cribl Search Pack for AppOmni

Integrating AppOmni with Cribl has always been about getting the right data to the right place. But with the latest updates, it's no longer just about moving data—it's about **visualizing and interrogating** that data without the "SIEM tax."

The addition of the **Cribl Search Pack for AppOmni** changes the game for security teams who need to maintain a high level of governance without ballooning their ingest costs.

Visualize Before You Ingest: High-Level Dashboards

The standout feature of this new Search Pack is the ability to generate **high-level dashboards** directly on top of the data residing in **Cribl Lake**.

Traditionally, to see a dashboard of your SaaS security posture, you had to pay to ingest every single log into your SIEM. Now, you can route the full fidelity of AppOmni events into cost-effective storage in Cribl Lake and use Cribl Search to visualize:

- **Top Policy Violations:** See which SaaS apps are trending toward non-compliance.
- **Privileged User Activity:** Monitor administrative changes across Salesforce, ServiceNow, Google Workspace, Workday, and Microsoft 365.
- **Data Exposure Trends:** Track where sensitive data is being shared externally in real-time.

The "Store Everything, Query Anything" Strategy

By pairing Cribl Lake with the new Search Pack, organizations can adopt a tiered data strategy that balances visibility with budget:

1. **Cost-Effective Retention:** Store the "long tail" of AppOmni security events in Cribl Lake. This keeps your expensive SIEM licenses reserved for only the most critical, actionable alerts.
2. **Instant Investigation:** When an anomaly appears on your Search dashboard, you don't have to wait for a "restore from archive" process. Use Cribl Search to perform sub-second queries across your AppOmni data stored in Lake.
3. **On-Demand Rehydration:** If a Search query uncovers a legitimate threat, you can "rehydrate" that specific subset of data through **Cribl Stream** and send it directly to **Google SecOps (UDM)**, **Splunk (CIM)**, **Azure Sentinel (ASIM)**, or transform it into **OCSF** for full-scale incident response.

Updated Packs: Schema Mapping Made Easy

The latest updates to the AppOmni Packs for Cribl Stream ensure that whether you are searching data in Lake or routing it to a SIEM, the schema is handled for you. The heavy lifting of mapping complex SaaS event structures into UDM, CIM, or OCSF is now automated. This ensures that your dashboards in Cribl Search and your alerts in your SIEM speak the same language.

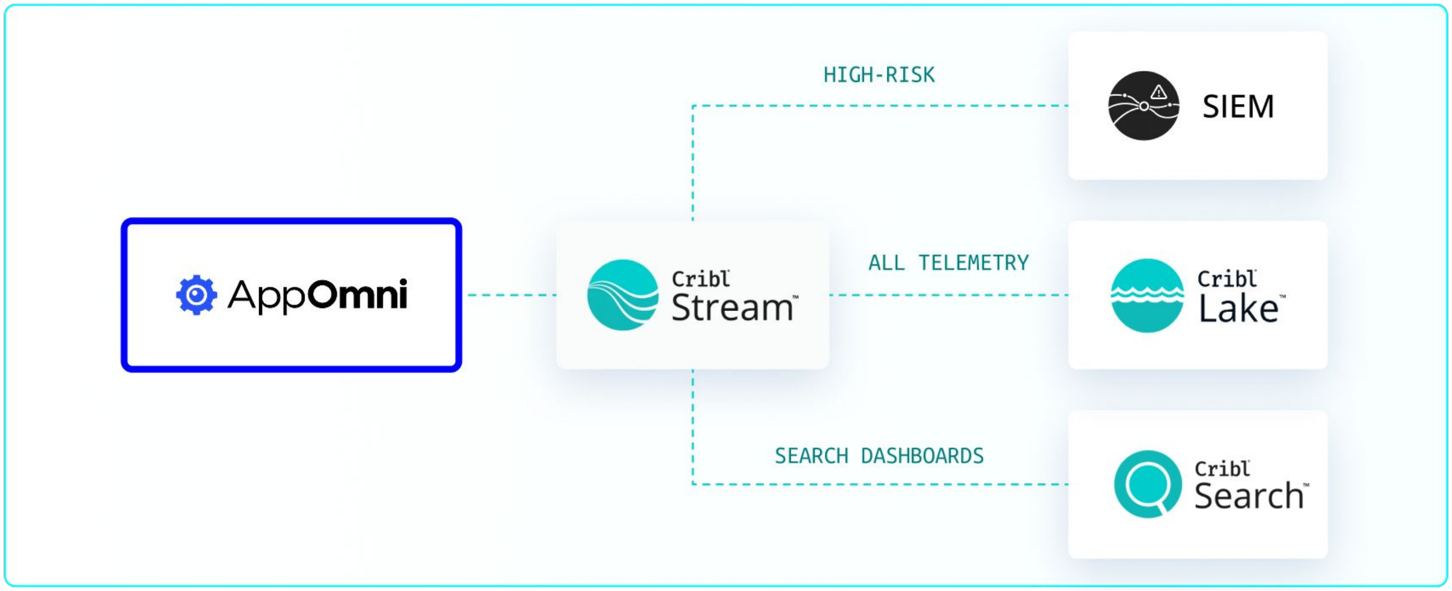
Cribl Lake collects data from AppOmni and stores it for long-term storage. Subsequently, Cribl Search and the new Dashboard Pack for AppOmni provide a high-level overview of the generated data.

KEY TAKEAWAY

You no longer have to choose between "complete visibility" and "budget management." With the AppOmni + Cribl Search Pack, you can keep your data in Lake, visualize it with dashboards, and only pay to move it into your SIEM when it truly matters.

With Cribl and AppOmni

With Cribl and AppOmni, SOC and security teams get faster remediation and see greater SIEM cost reduction.



About AppOmni

AppOmni prevents SaaS data breaches by delivering end-to-end SaaS security. Our platform gives security teams clear visibility into posture, access, third-party connections, AI-related activity, and with built-in discovery to identify unsanctioned SaaS and shadow AI tools. Backed by continuous monitoring and real-time threat detection, AppOmni helps enterprises identify and resolve risks early, keeping their SaaS applications secure. Request a personalized demo at appomni.com/demo or get in touch with one of our security experts at info@appomni.com.

About Cribl

Cribl, the AI Platform for Telemetry, empowers enterprises to manage and analyze telemetry for both humans and agents with no lock-in, no data loss, no compromises. Trusted by organizations worldwide, including half of the Fortune 100, Cribl gives customers the choice, control, and flexibility to build what's next. Learn more at cribl.io.