

# Next-Gen Threat Management

Streamline Your Digital Defense With the AppOmni and CrowdStrike Falcon LogScale Integration

## Challenge

Organizations are inundated with data from a multitude of sources, including security, IT, and DevOps. But managing and interpreting this data is increasingly difficult, especially when you consider the fact that organizations must now normalize and consolidate log data from various SaaS applications into a unified system to enable long-term data retention, analysis, and proactive threat hunting. Traditional infrastructures may struggle to handle the sheer volume of data, which can reach petabyte scale, and that makes it difficult to maintain a comprehensive security posture.

The integration of SaaS applications also adds complexity because each app generates its own audit logs that must be monitored and correlated to maintain security and compliance. The ability to quickly search and retrieve complex query results is critical for making informed operational decisions and responding to security incidents. Additionally, financial considerations such as infrastructure costs, licensing, and data management expenses are significant challenges that organizations must navigate.

To address these challenges, organizations require a solution that streamlines the process of correlating log data across their SaaS ecosystem, reduces total ownership costs, and enhances their ability to manage cybersecurity and compliance complexities.



### THE CHALLENGE

- Data consolidation across SaaS apps is complicated by manual setup processes and diverse audit log configurations.
- The sheer volume of log data from various sources overwhelms organizations and complicates effective management and analysis – jeopardizing their security posture.
- The financial burden of infrastructure, licensing, and data management for cybersecurity and compliance is a considerable challenge for organizations.

# Solution

The AppOmni and CrowdStrike Falcon LogScale integration provides a unified system for data storage, analysis, and retention to address the challenges of managing and securing vast amounts of data across numerous SaaS applications. AppOmni's advanced scanning and monitoring capabilities, combined with CrowdStrike's index-free architecture and advanced compression, enables organizations to efficiently manage and correlate massive amounts of data across their SaaS estate.

With real-time streaming and index-free searching, teams can quickly access complex query results to improve operational decision-making and incident response. Teams also benefit from real-time alerting on security threats and performance issues, which promotes proactive anomaly detection.

AppOmni and CrowdStrike Falcon LogScale simplify compliance management and offer a low total cost of ownership. The integration's affordable licensing options and significant data compression reduce infrastructure and licensing expenses. The deployment through CrowdStream accelerates log management adoption, enabling organizations to maximize their investment while maintaining security and compliance within their SaaS applications.



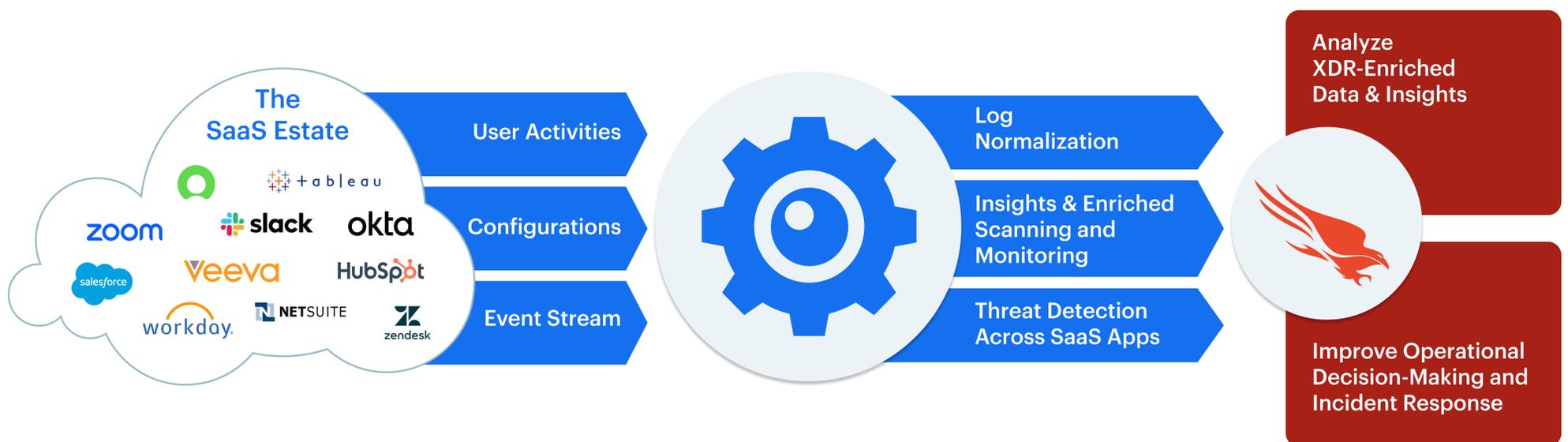
## THE SOLUTION

- Simplify complexity with normalized SaaS event data and long-term data retention.
- Proactively hunt for threats across SaaS applications.
- Enable immediate operational and security insights with rapid querying.
- Maintain compliance through visibility into policy deviations and guided remediation.



## KEY FEATURES

- Normalized SaaS Event Data
- Threat Detection
- Data Access and Analysis
- Simplified Issue Resolution
- Compliance & Risk Management



## KEY FEATURES

Feature	Description	Use Case
Normalized SaaS Event Data	Leverage the combined power of AppOmni's precise continuous scanning and CrowdStrike Falcon LogScale's comprehensive visibility to manage and analyze large amounts of data across your SaaS applications.	A healthcare provider uses AppOmni and Falcon LogScale to scan Salesforce Health Cloud and their digital infrastructure. With the integration, the provider can analyze data in real-time for security and compliance.
Threat Detection	Enhance your security posture with AppOmni's real-time threat detection — bolstered by Falcon LogScale's advanced analytics — for immediate identification and response to cyber threats.	An e-commerce company uses AppOmni's Microsoft 365 threat detection, with Falcon LogScale's attack pattern identification to proactively respond to cyber threats.
Data Access and Analysis	Integrate AppOmni's comprehensive data access insights with Falcon LogScale's centralized log management to gain a holistic view of user activities and system interactions across your SaaS environment.	A financial institution leverages AppOmni and Falcon LogScale to monitor Workday and gain critical insights into financial record access to ensure regulatory compliance.
Simplified Issue Resolution	Use AppOmni's workflow integration to easily set up and manage your security response processes. AppOmni works hand-in-hand with Falcon LogScale's affordable log management to quickly fix security problems and manage expenses.	A software firm uses AppOmni's automated remediation with Falcon LogScale for efficient issue resolution in their ServiceNow ITSM and benefits from optimized costs and tracing capabilities.
Compliance & Risk Management	Enhance your compliance efforts with AppOmni's monitoring capabilities and enforcement of regulatory standards such as NIST, HIPAA, Sarbanes-Oxley and more, which are seamlessly integrated with Falcon LogScale's detailed log retention for a comprehensive audit trail.	A biotech company employs AppOmni for HIPAA compliance in Microsoft 365 and leverages Falcon LogScale to get a detailed audit trail for data access and modifications.

**AppOmni for your SaaS Estate**

AppOmni is the leader of SaaS Security Posture Management (SSPM), enabling customers to achieve secure productivity with their SaaS applications. AppOmni prevents SaaS data breaches and secures mission-critical data from attackers and insider threats. Over 25% of the Fortune 100 and enterprises across industries trust AppOmni to secure their SaaS applications.

(© 2024 All Rights Reserved)

<https://appomni.com>.