Solution Overview

Transform Cloud Log Data into Business Intelligence

Improve transparency of cloud security and event management data with Global Log Receiver for F5 Distributed Cloud Services.

Data Overload

Cloud operations teams need to secure and optimize the digital experience for their users, ensuring an application's security, reliability, availability, and performance. To do this, they may employ a solution found in the F5® Distributed Cloud Web Application and API Protection (WAAP) service to keep apps protected against emerging threats and secure APIs from vulnerabilities and attacks.

But these solutions can produce a lot of data in the form of access, application, security, and audit logs. This data begins to accumulate and consumes compute resources through its retention. This accumulation presents a challenge to the cloud operations teams who need to synthesize the data into intelligence they can use to optimize the app experience for their users and, in some situations, maintain regulatory compliance. Are apps safe for users? Are they vulnerable to bad actors? Are they slowing down or causing unnecessary friction in a user's experience? Could a team pass an audit from a regulatory body if called upon to do so? If the teams lack access to the data that will inform the answers to these questions, they won't be able to optimize and secure their apps in an efficient manner.

These real-world questions highlight the complexity cloud teams must manage, so the tools they use must be up to the task. The log data can also be used for business intelligence that further enables teams to optimize the application they're supporting. Therefore, developing a process and a tool to understand the performance and functionality of their cloud assets continues to be a top priority. While log collectors (also known as Security Information and Event Management, or "SIEMs") like Splunk and Datadog provide a place to store that log data, cloud ops teams need a tool to move that data from their distributed cloud solutions to a collector.

Secure, Efficient Log Data Transportation and Management

Global Log Receiver (GLR) for F5 Distributed Cloud Services can stream all system and application logs of a tenant at both Regional Edge and Customer Edge sites to third-party SIEM collectors like Splunk, Datadog, Amazon CloudWatch, and Amazon S3. This ability to offload cloud log data to SIEM collectors allows teams to free up local storage and extend the length of time logs can be retained logs in those collection systems. These collectors effectively act as libraries of cloud log data that can be utilized later for postmortems, performance optimization, or security hardening purposes.

Key Benefits

Extend log data storage for regulatory compliance
Send log data telemetry to remote logging services to retain critical data for longer periods of time, enabling more complete regulatory compliance where required.

Enhance visibility of log data
Analyze logs and security events on your Security Information and Event Management (SIEM) hours, days, or even weeks after an event.

Expand integration compatibility
Securely stream log data to the industry's top log collection systems like Splunk, Datadog, QRadar, and Sumo Logic.

Automate easily and efficiently
Automate responses to security and infrastructure events more efficiently and effectively with log data gathered through GLR.

Deploy in minutes
Configure and provision GLR alongside F5 Distributed Cloud WAAP solutions with just a few clicks to begin log data capture.

Are apps safe for users? Are they vulnerable to bad actors? Are they slowing down or causing unnecessary friction in a user's experience?

Key Features

Stream diverse log types
Includes request and security event logs (e.g., WAF, Distributed Cloud Bot Defense, API security, L7 DDoS, service policy, and malicious user events) as well as audit logs.

Maintain multiple delivery streams
Offers vendor-specific, public cloud storage, and generic HTTP(s) delivery options. Logs are also exported in common JSON format.

Export from the edge
Users can export log data from Regional Edge or Customer Edge locations.

These collection systems effectively act as libraries of cloud log data that can be utilized at a later date for postmortems, performance optimization, or security hardening purposes.

The enhanced retention that these log collectors provide enables teams to more easily comply with audits associated with regulatory frameworks like HIPAA and PCI-DSS. Ready access to secure, long-term storage for data logs can help to avoid penalties and build trust with customers and users. Logs are also useful for reviewing events like database access records, server logins, or successful and failed API requests. Access logs in particular can help answer troubleshooting questions like, “Who did what, when, and how did that impact the application or system?” This facilitates faster time to diagnosis and resolution, leading to improved uptime for users.

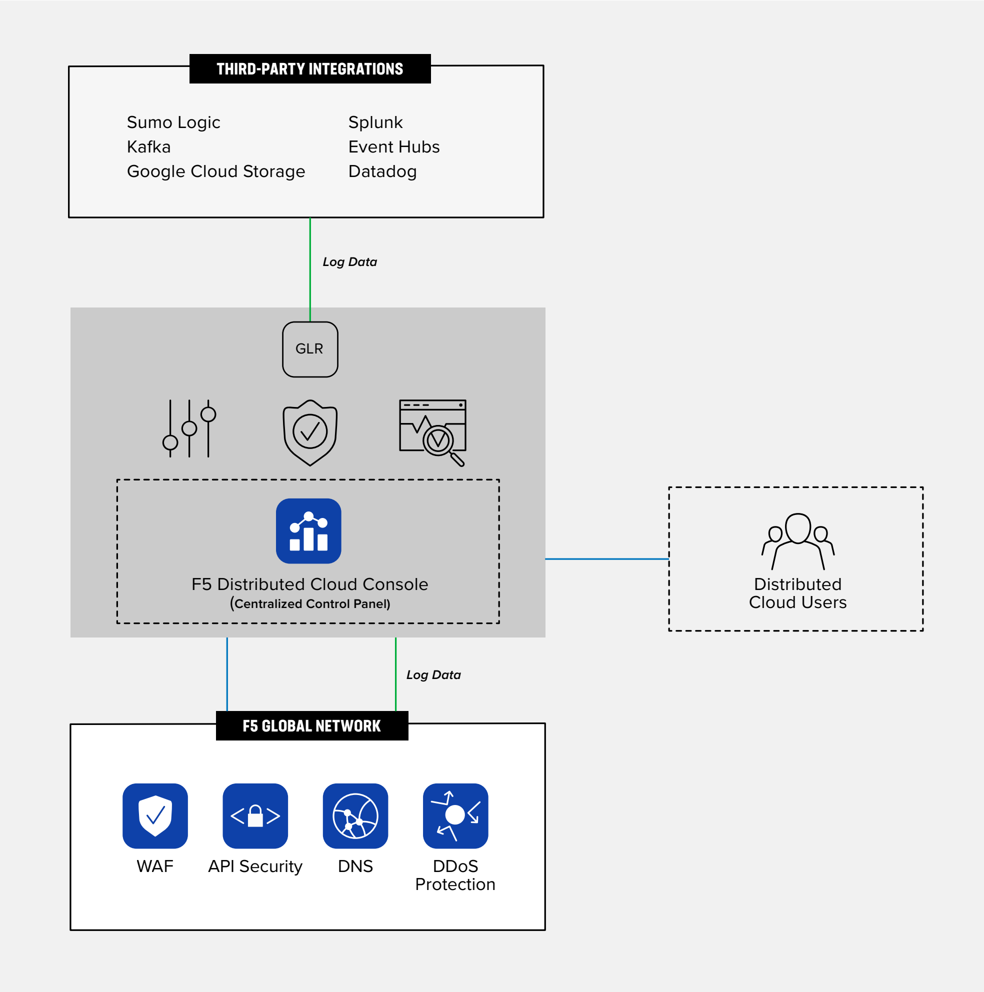

Figure 1: A reference architecture for Global Log Receiver for F5 Distributed Cloud Services

It is...crucial to have a service in place that can gather this data, safeguard it, and securely forward it to a dedicated SIEM collector.

Point A to Point B

Application users are raising the bar on their expectations. Performance, availability, security, and safety are necessities, not luxuries, and users expect the apps they rely on to provide nothing less.

But applications have evolved from monolithic structures to API-based systems that span every type of deployment model, from data centers to multicloud environments, to edge platforms. Because of this distributed, evolved landscape, visibility and insights that provide intelligence across platforms are critical, not just advantageous, to teams who aim to optimize and secure their applications. Therefore, it is equally crucial to have a service in place that can gather this data, safeguard it, and securely forward it to a dedicated SIEM collector. GLR for F5 Distributed Cloud Services, a native element in the F5 Distributed Cloud Platform is easy to activate, configure, and integrate into workflows, enabling organizations to harness actionable insights for strategic decision-making in mere minutes.

Global Log Receiver for F5 Distributed Cloud Services is available for select F5 Distributed Cloud solutions. For more information, please contact sales@f5.com today.