Forcepoint

Splunk Integration

with Forcepoint CASB

Key Benefits:

- Continuously inspect all traffic for on-site and remote users.
- Coordinate security log analysis across all security controls.
- Reduce time to analyze and remediate threats.
- Monitor and orchestrate risk dynamically across the organization.

Achieving integrated visibility in today's business world is highly challenging. With the rise of cloud, BYOD, remote work, IoT and countless other phenomena, there are more avenues for data leakage than ever before.

When administrators are tasked with managing multiple, disjointed tools to achieve visibility, it becomes a time-consuming, frustrating endeavor. Consequently, security personnel want a single hub where they can visualize all the log data that is generated across their organization. When administrators are provided with a single dashboard that accomplishes this, they are better equipped to make rapid, informed decisions that ensure better cybersecurity, data privacy and regulatory compliance.

Splunk

Splunk is a leading Security Information and Event Management (SIEM) tool that can ingest any form of complex dataset, quickly analyzing the load and displaying it in a manner that enables users to take necessary action. By deploying Splunk, users can search, monitor and analyze machine-generated data from across their organization.

Splunk users are typically deeply interested in using collected data to gain insights into problems so that they can solve them quickly and efficiently. The capabilities within Splunk's product essentially convert information into answers for users, generating tangible insights across numerous disciplines such as cybersecurity, IT, and DevOps.

Forcepoint CASB

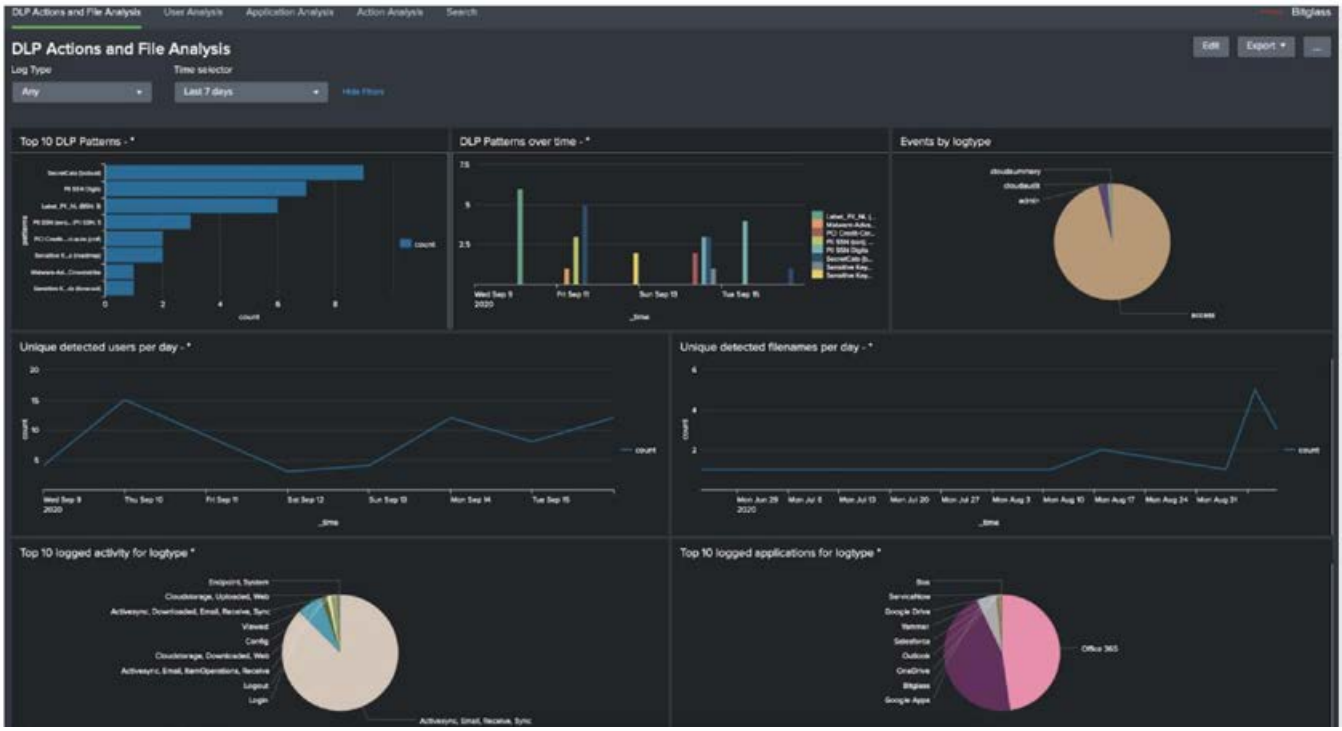
Forcepoint CASB (Cloud Access Security Broker) is a cloud-native solution that provides deep visibility, control, and protection for data across sanctioned SaaS applications. This multi-mode, cloud-native offering generates logs that detail all activity between any devices and the managed SaaS applications.

Forcepoint CASB provides valuable insights about user logins, uploads, downloads, locations, device types and shares, as well as sensitive data patterns detected at rest or in motion.

The Integration

The integration between Splunk and Forcepoint CASB combines these vendors' best-of-breed solutions to deliver comprehensive visibility in a single location with easily digestible reports. By using Forcepoint CASB in the Splunk platform, joint customers can have Forcepoint CASB logs streamed directly to the SIEM. This affords Splunk insights from the Forcepoint CASB SASE platform, a powerful source of information about what users are doing in the cloud and on the web, two areas where granular visibility is typically lacking.

Likewise, it allows administrators to see this Forcepoint CASB data directly in the Splunk dashboard so that they can generate the reports and charts that they want and review it in the context of their other data sources, as well. For example, the dashboard below shows top DLP patterns, activities, apps and more.



By interlacing the Forcepoint CASB ability to capture unique data points with Splunk's distinct focus on visualizing said data, organizations can maximize the usability of the information that they collect. This enables administrators to configure more effective security policies, leading to enhanced data privacy and regulatory compliance.

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, X and LinkedIn.