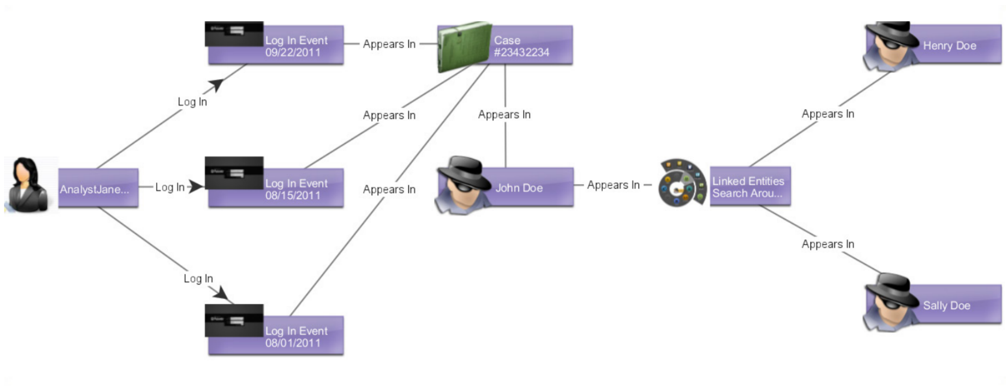
Palantir

100 Hamilton Avenue
Palo Alto, California 94301

PALANTIR AUDIT LOGGING

INTRODUCTION

Palantir features a full, tamper-evident audit log of user and administrative activity and is trusted in many of the strictest security environments in the world, including widely in the defense and intelligence community. Audit logging occurs automatically in Palantir, as the system records every read, write, and other manipulation of data, along with the user, time, date, and action. With configuration, Palantir can expose this audit log to the end user through the user interface and can also source each piece of data back to its origin. Users can also "play the audit trail" forward or backward to see how the data universe has changed through time.



Palantir can be configured to allow users to investigate and analyze audit logs within the platform itself.

SOLUTION OVERVIEW

Configuration and Retrieval

Palantir's audit logging functionality automatically creates a historical record of user and system activities. By accessing the audit logs, authorized administrators can retrieve information about virtually any type of user interaction with the platform, including when a user logged in and out, viewed an object or record, created or deleted an object, printed or exported information, and conducted a search.

Palantir enables users to finely tune the level of detail and context provided in the audit logs based on event category. For example, the audit logs can be configured to track user interactions with sensitive data types at a fine-grained level while limiting the verbosity for other categories of less sensitive data. Palantir can also simply record internal object IDs in the audit records, or include more human-readable details on the objects such as document or object titles.

SOLUTION OVERVIEW (CONT.)

Method & Format

Palantir provides multiple levels of application auditing to capture all user and administrative activity. The primary audit facility is provided by the **Dispatch Service**, which is part of Palantir's server-side architecture. All data access by a client must pass through the Dispatch Service and every call to the service is recorded. As a result, Palantir captures all data loads, searches, object modifications, and typical operations like login and logout. By providing this audit functionality on the server side, Palantir can track all information that is transmitted to a client.

Palantir also provides client-side audit logging to record user operations in the **Palantir Workspace** such as printing, exporting, and viewing documents. Client-side audit logging sits on top of the server-side auditing to provide further detail on user actions. In addition to application auditing, Palantir can configure standard operating system and hardware auditing when requested by customers.

The Apache log4j logging utility is used for logging data. Each Palantir server maintains a log directory and accompanying configuration files. All audit records can also be transmitted in real time to a remote audit server to separate duties. This transmission can be done via a secure SSL/TLS connection. By default, the system logs audit messages in XML format and writes to a .log file. The XML format can be readily reconstituted in any common human readable form (e.g., CSV). The audit logs can also be configured and loaded within a Palantir investigation to allow auditors to conduct the log analysis within the platform itself.

PRIVACY & CIVIL LIBERTIES

We create technology that reflects our commitment to protecting privacy and civil liberties. From the very beginning, we have built privacy and civil liberties protections directly into Palantir's core technologies.

Combined with Palantir's detailed object history (which records every addition, modification, and deletion to a record), the audit logs provide a complete picture of how Palantir is used by analysts. This data can be reviewed at any time to determine whether individuals are misusing data by inappropriately accessing information, conducting overly-broad searches, deliberately or inadvertently entering erroneous information, sharing or exporting information without authorization, or engaging in other activities that could lead to serious violations of privacy and civil liberties.

In addition, this detailed usage information can also help administrators understand how users are conducting analysis, identify inefficiencies, and design training programs to improve the overall effectiveness of individual analysts.