Reveal security

Solution Brief

Reveal Security for Yardi

Continuously Monitor User and IT Admin Activity to Detect Insider Threats in Yardi

YARDI

Benefits

- **Accurate Detection:** Patented Identity Journey Analytics™ using unsupervised machine learning continuously learns all the typical Yardi usage patterns and accurately alerts on anomalies.
- **Eliminates Alert Fatigue:** Surfaces true anomalous behavior so security teams can focus only on incidents that require investigation.
- **Reduced MTTD and MTTR:** Enables early detection of incidents and speeds investigation, reducing the mean time to detect (MTTD) and mean time to respond (MTTR).
- **Full Visibility:** Provides comprehensive visibility across Yardi business processes.

Overview

Many leading real estate firms use Yardi ERP as their financial and accounting platform to streamline and optimize their financial operations. Tailored specifically for real estate, Yardi ERP provides functionality, from financial planning and strategy to accounts payable, accounts receivable, managing rent rolls, tracking expenses and ensuring accurate rent collection. It integrates with many other critical systems across the business ecosystem to facilitate smooth data exchange and cohesive operations.

This makes Yardi a rich target for threats - including insider threats, internal fraud, third-party risk, and external attackers using stolen credentials. Although Yardi offers secure access controls and permissions management, enterprises should monitor the usage of the Yardi application to detect any unusual or suspicious activity. Yardi provides audit logs on the changes performed by its users in the Yardi database, which should be analyzed to detect unauthorized changes performed by users.

Writing detection rules to monitor Yardi logs is tedious. It requires knowledge of the log format and content, as well as the definition of all possible unauthorized changes needing detection. Compounding this issue is that these types of detection rules typically generate many false positives, contributing to alert fatigue and often resulting in ignored alerts. Fortunately, there is a more effective solution for detecting unauthorized activity and changes to the Yardi database.

Comprehensive Threat Detection for Yardi

The Reveal Security platform addresses the challenges of Yardi ERP security monitoring by leveraging unsupervised machine learning to help detect unauthorized and accidental changes.

Reveal Security seamlessly ingests and analyzes Yardi logs to automatically learn typical user behavior and detect anomalies, focused on unauthorized CRUD operations in Yardi tables. Anomalies are most often indicative of unsanctioned activity in the application, such as:

Fraud: Misconduct related to financial transactions, including paying invoices, changing bank account information, and altering leasing terms.

Unapproved IT Administration: Unauthorized activities on important tables, such as configuration and administration tables, and changing user permissions.

How Reveal Security Works

Step 1
Builds Journeys

The Reveal Security platform analyzes Yardi logs and builds "journeys," which are sequences of CRUD operations performed by users.

Step 2
Learns Typical Journeys

The Reveal Security platform uses a patented unsupervised machine learning technique to automatically learn all the typical journeys of CRUD operations performed by Yardi users according to their roles in the organization.

Step 3
Detects Anomalous Journeys & Assigns Risk Scores

The Reveal Security platform compares the similarity of each new journey to the learned journeys of Yardi users by role. If an anomaly is detected, a risk score is assigned based on its impact to the business

Step 4
Streamlines Investigation

Reveal Security provides clear visibility of every change that occurs within Yardi, streamlining incident investigation, including a detailed timeline of what CRUD operations were performed and their details, enabling the analyst to understand the anomaly to define how to handle it.

About Reveal Security

Reveal Security quickly and accurately detects insider threats and identity-based attacks in and across SaaS, cloud and on-premises applications. The Reveal Security platform is the only solution in the market based on patented Identity Journey Analytics™ technology that uses unsupervised machine learning to learn the usage patterns or typical "journeys" of human and machine identities in applications and uses it to detect anomalies. This approach delivers a superior level of accuracy and context, reduces alert volumes by orders of magnitude, and enables the business to respond quickly before a material breach can occur.

For more information, visit www.reveal.security