APPSIAN

SOLUTION BRIEF

Enhance Legacy ERP Logging to Gain Direct Visibility into User Activity

Capture granular, structured, and actionable user activity logs to fast-track incident response and establish compliance for your ERP applications.

Abstract

ERP applications house an organization's most important data - financials, corporate records, personally identifiable information (PII) of employees, customers, vendors, associates, job applicants and more. With the advent of enterprise mobility, ERP applications can now be accessed from any device and any location, allowing users to interact with your most sensitive data at any point in time.

The increase in the scope of access has resulted in the expansion of the network boundary which is now extended to users and their mobile devices - making user identity the new perimeter. The easiest way for malicious parties to gain access to sensitive data is by compromising an end-user's identity and ERP login credentials. Threat trends show that social engineering attacks are at an all-time high, followed by insider data leakage and privilege misuse - reaffirming that most attacks to ERP system data are likely to originate from the exploitation of valid login credentials.

Additionally, organizations all around the world are recognizing data privacy concerns. Regulatory mandates like General Data Protection Regulation (GDPR), The California Citizen Privacy Act (CCPA), etc. have become extremely strict and require direct visibility into how organizations store, use and process PII. Under these regulations, organizations are required to respond to audit requests and report breaches in a stipulated amount of time or face monetary fines. Therefore, organizations must be tracking and logging granular data access information at all times, for example – which users are accessing particularly sensitive data fields in ERP applications, where are they accessing it from, to what frequency, and more. By combining added regulatory pressure and the changing threat landscape, it is clear that the new common denominators for information security awareness are identity and activity.

Considering the expansion of access, the shift to user-centric threats, and strict regulatory mandates, organizations must be equipped with deep visibility into user activity. Monitoring and recording user activity within ERP applications can allow organizations to assess the usage of ERP applications, build real-time auditing and reporting capabilities, and provide security teams with actionable information for faster threat discovery and incident response.

Challenges

Legacy ERP logging was not designed for user-activity monitoring

Legacy ERP logging features were designed primarily for debugging and troubleshooting. Designed in an era before the proliferation of user-centric threats, legacy ERP logs lack the capabilities necessary for today's evolved security and compliance requirements.

Out-of-the-box, ERP logging is system-focused, bulky, and unstructured – OK for testing and development, but impractical for use in production environments. Due to the performance impact and amount of "unactionable" data they generate, most organizations will turn off logging in their production environment or limit logging to its most basic functions such as recording credential login and logout activity. Since native logs aren't intended to provide details into user activity and any related contextual data - they limit an organization's capability to respond to user centric threats.

Although triggers can be added through custom development, these custom triggers show data changes, but provide no insight into data exposure (whether a user has viewed a data field). Additionally, these custom triggers add additional work to application upgrade cycles.

Logs provide limited data for compliance and auditing

Data privacy regulations such as the GDPR, CCPA, and more have defined strict guidelines for how personal data is stored, processed, and used by organizations. Since ERP systems have personally identifiable information (PII) in abundance, they are a vital component of an organization's compliance strategy.

Non-Compliance with Data Privacy Regulations can cost companies significantly in terms of fines and remediation efforts. Most of these mandates are broad-reaching and can impact businesses despite their geographic location (i.e., companies in the USA have to comply with GDPR if they have data of EU citizens, despite their location).

To stay compliance audit ready, organizations must have direct visibility into the user activity inside their ERP applications. For example – who is accessing what data, when, and from where on which devices. Unfortunately, default logs from legacy ERP systems *do not* provide that information.

Some data privacy regulations (ex. GDPR) allow data subjects to request an audit at any point in time. These subjects can seek details on who is accessing their data, what are they doing with it, and even online identifiers such as IP addresses. However, in the absence of user-centric transaction logs, organizations will not be able to respond to these audit requests, putting them at risk of non-compliance. Organizations also need to be prepared to address multiple requests simultaneously – a tedious, unsustainable process with existing logs.

Poor incident response capabilities

In recent years, threats have become increasingly targeted toward attaining users' login credentials. Brute force attacks, Phishing and other social engineering techniques are the top source of breaches, followed by insider threats such as privilege abuse or unintentional data leakage. Verizon's Data Breach Investigations Report also states that 81% of data breaches originate from misused or stolen credentials.

Without a complete audit trail of user activity, locating questionable transactions and discerning suspicious activity can be like finding a needle in a haystack. Security teams are often required to manually analyze network and database logs and then make assumption-based decisions. As a result, identification of suspicious events becomes a time-consuming task, delaying incident response and remediation efforts in the event of a breach.

In summary, existing legacy ERP logging capabilities can pose the following constraints:

- Key pieces of information are missing
- Insufficient data to identify or investigate a breach accurately
- The data captured is unstructured / unactionable
- Auditing access and update activity requires extensive customization
- Fully leveraging native logging features can have a negative impact on system performance

Solution

Appsian's Application Security Platform (ASP) enables granular logging and user activity monitoring for your ERP applications. By plugging directly into the ERP web server, ASP can provide transaction-level user activity data that efficiently highlights security lapses, and helps maintain real-time data that is ready to use for audits and regulatory compliance. With ASP, customers can capture user-activity data backed with contextual user information such as device, location, IP address, etc.

Establish Stronger Compliance Strategies

With granular transaction-level data, ASP's detailed logging feature allows customers to respond to audit requests promptly and fulfill regulatory reporting requirements. Organizations can maintain real-time logs of PII processing/usage activities and establish best practices for a compliance ready ERP environment. Using ASPs immersive user-activity logs, customers can efficiently track access to PII and remediate or even prevent security incidents, thus avoiding crippling monetary fines.

Rapid Incident Response

With application-level user activity logging, organizations can embark upon incidence response with a well-defined starting point. ASP enables your security team to correlate access with changes to the database, thus, providing them accurate guidelines on where to focus. Without ASP, organizations are left to sort through network/firewall activity manually, to locate anomalies in transaction logs that indicate unusual activity and can be tied to changes in the database.

How does it work?

ASP takes a different approach to logging and uses a token-based architecture to generate logs in a structured, actionable format. Only the information specified in its flexible configuration is recorded, and in doing so, avoids the large file sizes and performance implications often found with legacy ERP logging. Furthermore, since ASP resides natively within the web server, it is inline and avoids networks hops that delay performance. Load tests return results within the margin of error of normal installs.

The log files created in ASP can be either set to a size threshold (ex. 100mb), or rolled over to an existing SIEM or data warehouse immediately. The structured data format allows customers to readily extract insights.

The logs produced by ASP include detailed information on who is accessing the data, what information is being accessed, where it is being accessed from, user ids, IP address involved and more. With Appsian's platform, customers can customize the information they need to collect in security logs. Based on their specific business needs and industry standards, organizations can setup logs to address their exclusive priorities such as threat remediation, incident response or audits.

Appsian can also employ click-to-view masking features for sensitive PII such as social security numbers, medical ids, address, direct-deposit info and more. As a result, when a user views that specific record their actions are recorded, and any malicious activity can be traced back to them.

APPSIAN

8111 Lyndon B Johnson Fwy. Dallas, TX 75251

(469) 906-2100

info@appsian.com