APPSIAN SECURITY

EXECUTIVE BRIEF

How to Detect Modern Data Security Risks in Legacy Systems

To battle today's subtle cybersecurity threats, you need visibility to monitor user behavior, data access, and use.

Piyush Pandey • CEO

When organizations were forced to expand access to remote and mobile users because of COVID-19, there was a rush to install authentication protocols, such as VPNs, multifactor authentication (MFA), and single sign-on (SSO). Although these were necessary and vital steps for cybersecurity, user authentication is only a small part of the data security conversation. The rest of that conversation involves having the visibility to monitor user activity and understand user behavior, data access, and use. Frankly, many legacy systems are not up to the task.

Legacy applications were originally designed for easy data access. As organizations move to cloud-based systems -- under the assumption that cloud-based systems provide enhanced security -- many use on-premises systems to manage critical business workflows. Investment in these systems can take decades of effort and tens of millions of dollars mainly to customize workflows to exact business specifications. Although this adds tremendous value to operations, these applications were originally designed to provide easy access to data -- not taking addressing many of the data privacy, security, and compliance demands that have emerged in recent years.

From the perspective of monitoring user activity, traditional applications feature logging solutions that focus on troubleshooting system errors. They were not designed for understanding the "who," "what," and "why" around user access of specific data elements -- especially data deemed highly sensitive.

Remote Workforces Increase Demand for Data Access and Usage Visibility

Monitoring data access and tracking how users interact with data provides an essential benefit as organizations move towards securing remote and mobile environments. With the expanded threat surface that comes with remote access, organizations must go beyond merely tracking how users log in and log out of applications and track what data users access.

To meet these requirements, organizations are turning to analytics platforms designed to capture [data access and usage information and send alerts based on granular data access and usage behavior. To make this level of granular detail actionable, visualization solutions are becoming essential. After all, data is only as useful as the insights it provides, and rapid aggregation and visualization of user access and data use are a crucial requirement for data security, breach detection, and rapid response.

This additional level of visibility can also highlight internal access misuse and credential theft, which put the organization's data and financial security at risk. Continuously monitoring for outlier and anomalous access patterns reveals how high-privilege users interact with sensitive data.

However, visibility into the data is only as useful as the insights it provides. For example, application-level logging (aka monitoring front-door access) cannot detect if a hacker or malicious insider changes employee direct deposit information to route that week's payroll run into an offshore account. Only field-level logging (aka transaction-level logging) can capture data access and provide quick insight into irregular activity.

Modern threats are subtle. Hackers are aware these visibility gaps exist. They understand that staying hidden inside an application provides a vulnerability they can exploit. Risk mitigation must evolve to combat these modern threats.

Data Security Does Not End at Authentication

A strict authentication process on its own is no longer sufficient for maintaining data security. If scores of users are accessing company data from different locations, using potentially compromised devices and access points outside of working hours, lacking complete visibility into who is doing what, when, and why can be incredibly damaging. Thus, the need for transaction-level logging. Transaction-level visibility is ultimately the most effective way to identify a threat that has entered your environment, compromised an account, and ultimately leads to fraud or theft.

The good news is solutions exist solely to retrofit legacy applications with the visibility necessary to combat modern data security compliance risks. Research such solutions specifically designed for your system.

In the end, the keys to maintaining data security ultimately lie in your ability to provide oversight for your data, and the time to act is now.

About the Author

Piyush Pandey CEO of Appsian Security, has 18 years of global experience in strategy, sales, mergers and acquisitions, and operations within software companies. During the past 10 years, he has worked with enterprise software companies including Oracle, Epicor, Concur, Citrix, and Microsoft on various transactions. He has held various leadership positions at Procera, Deutsche Bank, Stifel, Wipro Technologies, and a wireless startup.

APPSIAN SECURITY

8111 Lyndon B Johnson Fwy. Dallas, TX 75251

+1 (469) 906-2100

info@appsian.com

www.appsian.com