APPSIAN

SOLUTION BRIEF

Location-based Security for ERP applications

Significantly reduce the probability of a breach with dynamic privilege management controls

Abstract

The rise of modern enterprise applications being accessed remotely via the public internet (and on mobile devices) has caused a dramatic shift in the security landscape. Organizations have now entered the age of the borderless network where user identity is the front-line defense – and most organizations are not prepared.

Cybercriminals are increasingly using tailored social engineering attacks to capture valid credentials and breach enterprise systems, with 81% of hacking-related breaches leveraging stolen and/or weak passwords(1). Additionally, 90% of organizations feel vulnerable to insider attacks(2) as the number of insider breaches attributed to accidental data leakage or privilege abuse has significantly increased.

These statistics carry weight as remote access becomes standard in the workplace. Enabling employees to stay connected and complete tasks from 'wherever they are' can do wonders for your organization's productivity. However, it can significantly increase the burden on security teams who now have to manage and report on application access from multiple locations/devices/endpoints.

To meet today's advanced security needs, traditional network security is no longer effective on its own. Many organizations are finding that their legacy ERP applications simply don't have the security capabilities necessary to address the evolving threat landscape. What was once fine behind a corporate firewall is now insufficient to combat the user-centric, application-level breaches seen today.

Rather than the traditional outside-in approach security teams have used, focused primarily on protecting networks, a shift in strategy must happen to bring attention on securing applications and users. Efforts around user-level security must be increased to minimize attack surfaces and eliminate unnecessary privileges. Starting from the bottom-up, making enhancements to privilege management capabilities is a foundational component to maintaining a secure, modern ERP environment.

Challenge

Modernized Access Control

A mobile and connected workplace has become a fundamental demand of modern users but requires additional efforts to keep secure. With multiple devices connecting to an enterprise network from scattered locations, cybercriminals now have numerous access points to enter your ERP applications, and consequently, enjoy an increased probability of success.

Sensitive information is abundant in ERP applications like PeopleSoft and SAP. And with the emergence of mobile access, PII and sensitive corporate data can now be exposed remotely on phones, tablets, and laptops – all outside an organization's traditional scope of control. As modernization brings a new freedom of access for users, ERP applications become more vulnerable to a variety of threats such as accidental data leakage and privilege abuse, as well as face an increased risk of damaging breaches from external threats.

Legacy ERP security controls are no longer effective on their own

While ERP applications are built to be inherently robust and secure, they often lack the fine-grained security controls and granular visibility necessary to combat challenges brought by modern, remote access. Breaches today have become extremely user-centric, and most threats stem from compromised or misused user credentials.

The coarse-grained, role-based access controls that legacy ERP applications use are limited to static enforcement policies and broad parameters like groups or permission lists. There has been drastic change in the work environment since the mid-90's when ERP frameworks were popularized. Access is now decentralized, mobile and remote. Legacy ERP security alone cannot minimize the attack surface of remote access or dynamically assign least privilege. Without enhancements, organizations are left with unnecessary risk and bottlenecks in productivity.

Static Rules Force a Catch 22

The inability to apply customized permissions for users based on contextual parameters like location of access, IP address, or device-type force organizations to choose between robust security and user accessibility. With static rules, users can access all the sensitive information or nothing at all.

For example, self-service transactions such as benefits enrollment or expense submissions are great productivity boosters, especially when employees can complete these tasks on their own time, from wherever they are. However, with legacy ERP access controls, organizations have no way of restricting remote access to only these low-risk

transactions; users would still have their normal privileges and could access sensitive data that should never be exposed outside the work environment.

This leaves organizations vulnerable to both insider and outsider threats. Malicious insiders aside, even well-meaning employees could accidently cause a breach by simply running a report on their home computer. And as cybercriminals continue to breach ERP systems with compromised credentials, once inside, they would have unfettered access to all of a user's privileges.

Solution

Dynamic Privilege Management

Appsian's Application Security Platform enables customers to establish dynamic privilege management based on a user attributes such as the location of access. Organizations can entirely or partially block access, limit access to specific modules or transactions, prompt users with MFA-gated checkpoints and more when an access attempt is made from outside a secure corporate network. By reducing the scope of access based on the context of a particular login session, organizations can significantly reduce the risk posed by both outsider and insider threats.

Reduce Your Attack Surface

Account takeovers through social engineering and brute force tactics are becoming increasingly common. Using location-based security, organizations can implement least privileged access in their ERP systems to safeguard sensitive information even if a cybercriminal gains access through valid credentials. Organizations can also control what type of transactions can be performed while accessing applications from external locations and limit sensitive ones to authorized locations only. As a result, the remote access attack surface is significantly reduced and the extent of damages a successful breach could create is minimized.

Protect Against Unintentional Data Leakage

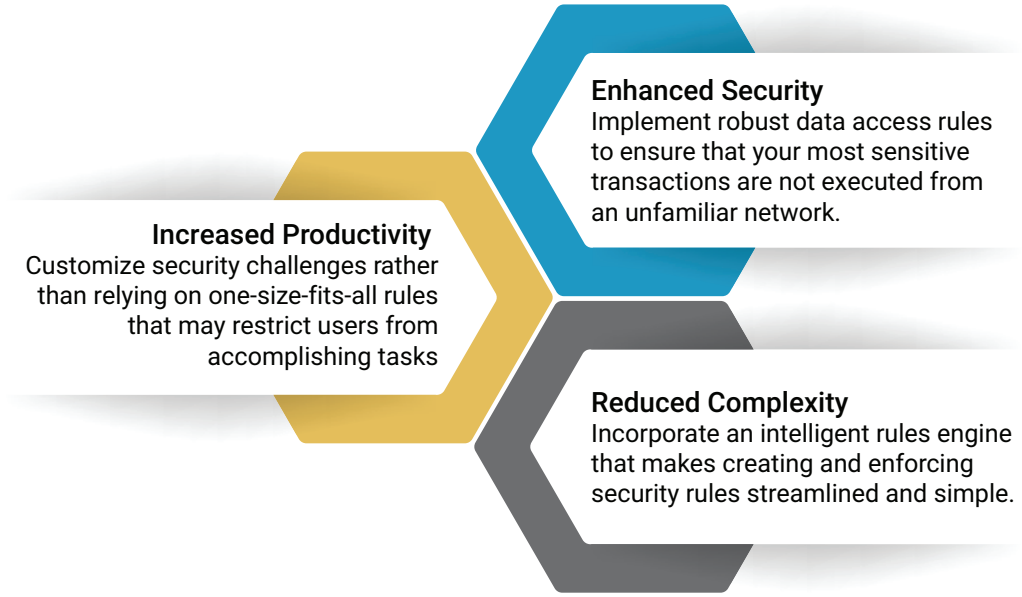
By limiting the scope of access outside a corporate network, organizations can reign in the risk of unintentional/accidental data leakage. With location-aware contextual rules, even authorized insiders will not be given a chance to accidentally jeopardize corporate data – for example, by running a report on their home computer. Thus, improving data loss prevention (DLP) controls for ERP systems.

Prevent Privilege Abuse

Using dynamic privilege management, access from external locations can be restricted to high-level information only and sensitive records such as social security numbers, direct deposit information, etc. will remain concealed. Organizations can limit sensitive transactions for high privilege users who could potentially abuse their authority to access and exfiltrate sensitive data when outside of work. Which means that despite their privileges, users will not be able to accomplish tasks such as downloading reports using queries, perform financial transactions, or view personally identifiable information outside of their normal work environment.

How does it work?

Using a contextual rules-based engine, Appsian's Application Security Platform allows ERP systems to distinguish between trusted and unknown locations of access and assign privilege accordingly. Whether a user is accessing ERP applications from a secure network or the open internet, organizations can decide precisely what they can view and what transactions they can execute. Using dynamic privileged management rooted in contextual awareness, organizations can better align with the principle of least privilege to reduce unnecessary privileges, shrink their attack surface, and provide secure remote access to their ERP applications.



(1) https://www.knowbe4.com/hubfs/rp_DBIR_2017_Report_execsummary_en_xg.pdf

(2) https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf

8111 Lyndon B Johnson Fwy. Dallas, TX 75251

(469) 906-2100

info@appsian.com