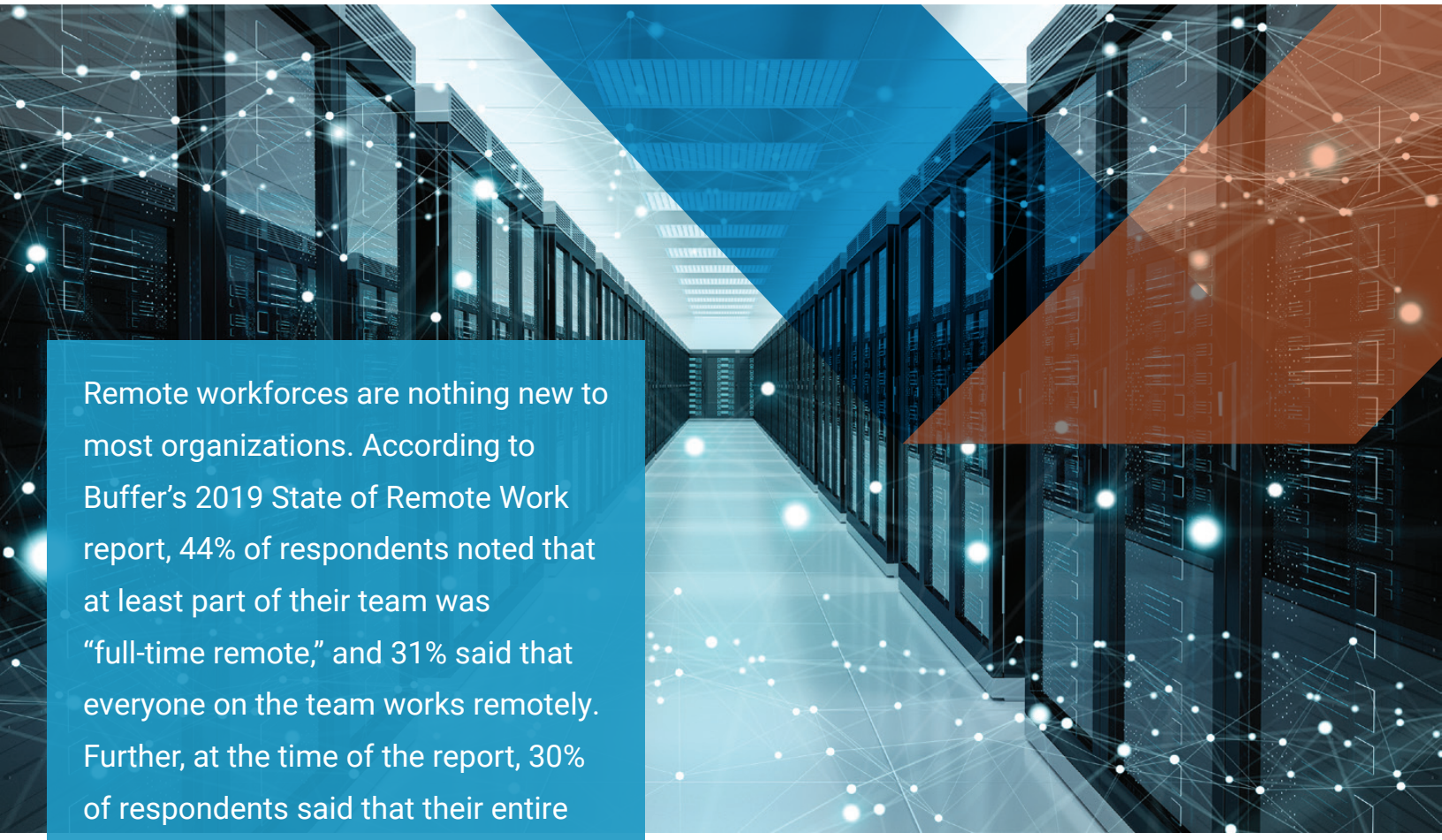
APPSIAN

EXECUTIVE BRIEF

Why Control and Visibility are the Keys to Maintaining ERP Data Security in a Remote Environment



Remote workforces are nothing new to most organizations. According to Buffer's 2019 State of Remote Work report, 44% of respondents noted that at least part of their team was "full-time remote," and 31% said that everyone on the team works remotely. Further, at the time of the report, 30% of respondents said that their entire company worked remotely. However, the COVID-19 pandemic accelerated the work-from-home model. By March 31, 2020, the percent of users working remotely had increased by 15 percentage points since the start of the COVID-19 outbreak. With that in mind, organizations are assessing how they can maintain granular levels of control and visibility when business data is accessed remotely.

Adopting Contextual Controls to Protect Data

Most organizations already leverage role-based access controls. These controls, which align access privileges and job function resources, provide a baseline for data governance. However, they often lead to excessive data access and, in turn, present additional risk. Contextual controls allow organizations to dynamically manage access with varying contexts of access, often aligning to least privilege best practices.

Migrations to cloud applications are largely due to contextual controls being a business requirement, simply because the interconnected applications require a more dynamic approach.

With the move to a remote workforce, organizations need to create more detailed and dynamic access controls. Attribute-based access controls (ABAC), allow a company to incorporate additional context (such as geolocation, time of day, and IP address) to ensure the appropriate user is accessing the resources, and to prevent users from having more access than they need. For example, if the organization knows that an employee should be working from Connecticut, ABAC can restrict access to resources if the user's location is suddenly California – or a foreign country.

Contextual controls provide both the prevention of access policy violations, along with alignment between business requirements and security protocols. Because the organization can limit access according to the principle of least privilege, it reduces the risk of data leakage and financial fraud. Meanwhile, by creating more granular, data-centric access privileges, an organization can ensure that users do not get too much or not enough access – limiting the potential adverse effects of restricting access excessively.

User Activity Monitoring for Security and Managing Productivity

Monitoring users' access to resources, and tracking how they interact with data provides an additional benefit as businesses move towards a remote model. Most organizations recognize the benefit of monitoring user access – but not just instances of logging in and logging out of applications. Understanding data access and usage is now an essential requirement when maintaining visibility over business data. Organizations are turning to analytics platforms that include granular access details and visualization elements (for example, SIEM). Data is only as useful as the insights it provides, and rapid aggregation and visualization of user access data is a crucial requirement for data security.

Using “Virtual” Work Hours

Looking at a common security use case, many organizations leverage “virtual” work hours to detect anomalies. For example, an employee usually works between the hours of 8 AM and 6 PM. In this case, monitoring and alerting to activity around sensitive data at 3 AM can be indicative of unauthorized behavior. This uncharacteristic behavior may be an anomaly, but the organization needs to monitor user activity closely. If the user denies accessing the information at 3 AM, the organization needs to focus its monitoring and have the employee change their password. If the organization detects additional unusual activity, it may need to review the employee’s actions or investigate a potential data breach.

Monitoring User Productivity

From a workforce management perspective, organizations can leverage these insights to review employee productivity. Two use cases present themselves. First, many organizations have contracts that stipulate late payments incur a late fee. If the organization knows that employees should be processing payments ten days prior to the payment date, then they can leverage these reports to ensure that employees meet their timelines, even from a remote location. Additionally, by tracking resource usage data, organizations can monitor whether workforce members are appropriately prioritizing their workdays. If the employees are only accessing a business application at the end of the month, then they are likely waiting until the last minute to input payment information. Preventing these potential revenue losses or rush projects in other areas by speaking with the employee enables the organization to stay on top of its financials.

Enabling Visibility for Business Applications Has Never Been More Critical

Creating trust within and across distributed workforces ensures productivity. However, continued status update meetings across multiple time zones decrease workforce efficiency. Organizations already monitor user access to their systems, networks, and applications. As part of a robust security posture,

organizations should apply protections at the new perimeter – user identity. Rather than micromanaging employees via emails or chats, managers can gain valuable insight into how users are accessing resources and prioritizing work by reviewing data and resource usage.

In an unprecedented time, companies need to find ways to enable their levels of control and visibility over business data. Whether a business application is on-premise or in the cloud, enhancing these solutions should be a mission-critical.

Risks against an organization are prevalent in a remote environment, whether those risks are security-related or employee-related (vis fraud, theft, or error). The keys to maintaining data security ultimately lie in your ability to provide oversight for your data, and the time to act is now.

Written by

Piyush Pandey, CEO at Appsian is a technology executive with 18 years of global experience in strategy, sales, mergers & acquisitions, and operations within software companies. Over the last 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

8111 Lyndon B Johnson Fwy. Dallas, TX 75251

+1 (469) 906-2100

info@appsian.com

www.appsian.com