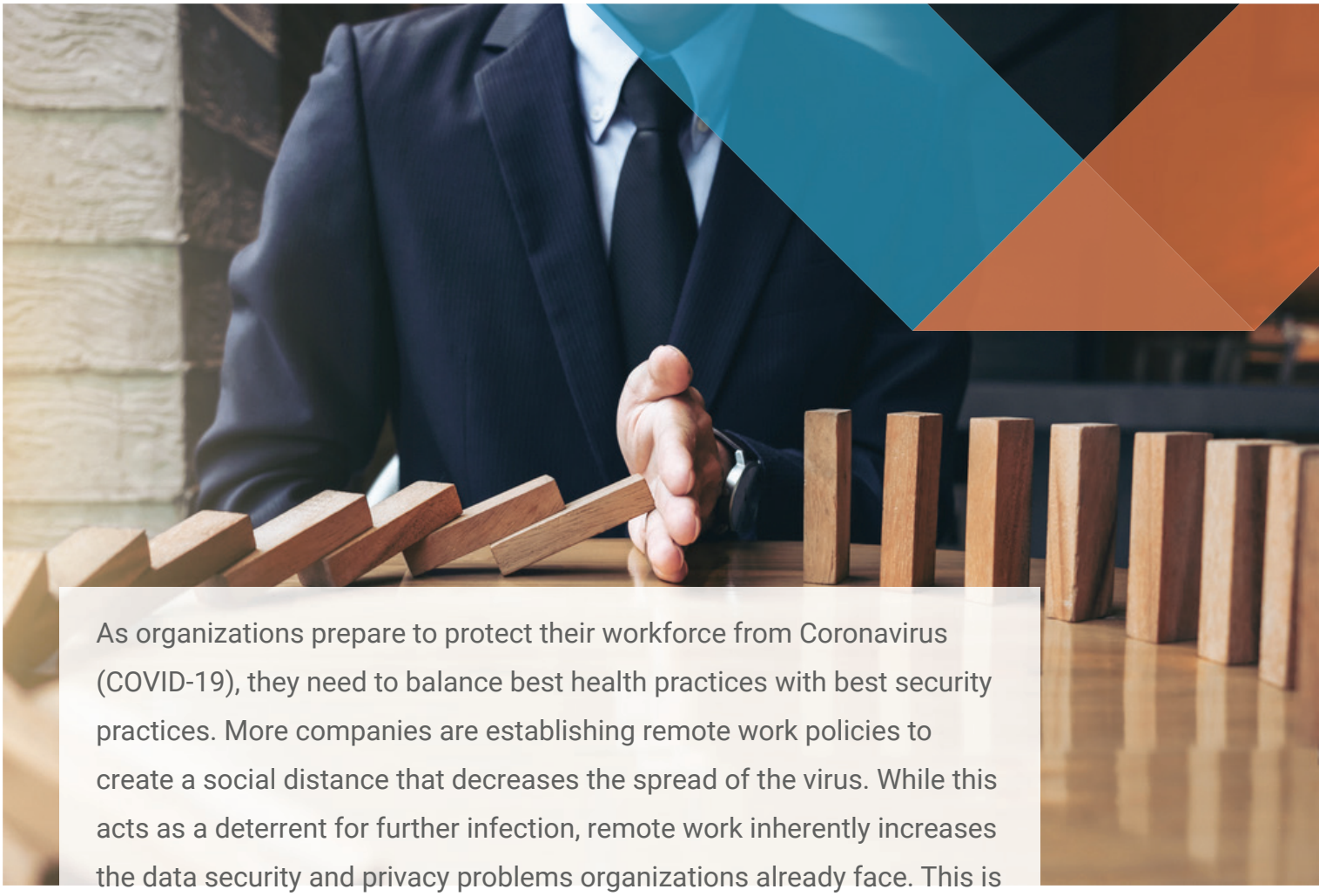
APPSIAN

EXECUTIVE BRIEF

Maintaining Business Continuity During Coronavirus (COVID-19): Securing Critical ERP Functions For Remote Access

Piyush Pandey • CEO



As organizations prepare to protect their workforce from Coronavirus (COVID-19), they need to balance best health practices with best security practices. More companies are establishing remote work policies to create a social distance that decreases the spread of the virus. While this acts as a deterrent for further infection, remote work inherently increases the data security and privacy problems organizations already face. This is mostly due to the increasing attack surface that comes with remote access to critical business applications. Organizations are responding to this new threat by scoping strategies to limit access, create timebound access policies, and establish data visibility controls. If an organization can create a “remote workday” that allows them to secure remote access during the Coronavirus outbreak, then this increased attack surface should be mitigated. But is that nearly enough?

How Organizations are Responding to CDC, OSHA, and HHS Coronavirus Guidance

The Centers for Disease Control (CDC) issued a Coronavirus Interim Guidance for Businesses and Employers in March 2020 while the Occupational Safety and Health Administration (OSHA) and Health and Human Services (HHS) issued a joint guidance of their own. At their core, both guidance recommendations suggest social distancing as a basic infection prevention measure.

Social distance, or separating people to limit the spread of infection, led many organizations to implement more flexible remote work strategies. OSHA/HHS specifically suggested:

Employers should explore whether they can establish policies and practices, such as flexible worksites (e.g., telecommuting) and flexible work hours (e.g., staggered shifts), to increase the physical distance among employees and between employees and others.

While this strategy decreases the spread of Coronavirus, it leaves IT and security teams in an unenviable position. Taking applications away from corporate networks/firewalls and exposing them to the internet can lead to many concerns – most of which surround the secure authentication of users.

Prompting a Move Towards a Zero Trust Model

Zero Trust acts as a best practices model when attempting to secure user authentication to critical systems. Thus, treating all users, both internal and external, as potential malicious actors – and not granting high-privilege access to anyone by default. While you may trust your employees, you also need to recognize the potential risk for credential theft (ex. phishing) that a remote workforce creates.

For instance, someone working from home may have a home wireless connection that lacks encryption or other security protocols. While a VPN can provide some confidence, not all users may have the VPN on a home laptop or other personal device. After all, the fundamental risk created by remote access comes from personal devices accessing sensitive data.

Using an adaptive multi-factor authentication (MFA) solution can help control access to sensitive information. For example, organizations using PeopleSoft can use an adaptive MFA solution that takes into account the context of access like location, device, or time of day. This solution becomes more effective when integrated at page, component, and field levels of particularly sensitive transactions and as users move between applications. With contextual controls as part of your remote workforce policy, you gain greater control over access to sensitive information such as payroll data, vendor payment data, or corporate financial information. A secondary benefit is a decrease in user friction, as remote users are only challenged when the context of their access deems it necessary.

Simulate a “Workday” with Time-bound Controls

Although organizations normally consider timebound controls part of their emergency access and firefighter access or joiner, mover, and leaver processes, they can also help simulate “workday” appropriate access for a remote workforce.

As more remote users work from home, organizations should establish timebound access controls that limit access outside of a given “flexible workday.” For example, if your current flexible schedule allows employees to arrive at the office as early as 7 AM and leave as late as 7 PM, then you can establish timebound organizational access based on application criticality to simulate this.

By disabling access between 7:01 PM and 6:59 AM, you limit the risks associated with credential theft and internal privilege misuse. Limiting access to certain times of the day means that you can worry less about the anomalous 2:00 AM access that might indicate a malicious actor with a stolen credential or a workforce member accessing information inappropriately.

Continuously Monitor User Access to Sensitive Information

While most organizations monitor user access requests or user behavior, creating specific dashboards as part of Coronavirus remote workforce preparedness provides an additional layer of security. From a security

standpoint, the biggest risk with remote workers is maintaining visibility into activity around sensitive data. Organizations need a way to view and monitor data access in real-time. Some of the key variables that should be tracked are geographic location of access, device used, and access volume on specific data fields (salary, social security, direct deposit, etc.)

Lastly, you may want to consider monitoring failed authentication trends and triangulating them with geographic location. This data can quickly identify brute force attacks that may not be apparent at the application level – but may only be showing up as anomalies and errors taking place with your identity provider.

Protecting Workforce Health While Maintaining Data Health

As organizations face the distinct possibility of the Coronavirus requiring nearly all workforce members to do their jobs remotely, balancing data health and employee health becomes a concern. Fortunately, today's advanced technologies provide a variety of solutions.

The Coronavirus may be acting as a catalyst for organizations to change their approach to managing user access to sensitive information. Unfortunately, many companies that once required employees to work on-premise when they manage sensitive data are having to reconsider policies and scramble to maintain business continuity.

How Appsian Can Enable Secure Telecommuting

Appsian delivers the control and visibility that traditional ERP applications like PeopleSoft and SAP (ECC or S/4HANA) inherently lack. As access becomes increasingly mobile, having the ability to dynamically control access and gain deep visibility into user behavior is increasingly necessary. The Appsian Security Platform combines a sophisticated suite of solutions designed to enhance user authentication, apply contextual access policies, fine-grained data security controls and provide granular logging with real-time analytics.

For more information about how Appsian can help accelerate your remote workforce access strategy, contact us today or schedule a demo.

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