ENTRUST

# PERFECTING THE HYBRID WORK MODEL

Report 1 of 3: Securing the New Hybrid Workplace

# INTRODUCTION

The surge of COVID-19 cases driven by new variants is challenging enterprises' development of long-term hybrid work models that meet the needs of their businesses and employees. As organizations consider their approach for a sustainable work environment in this transition, Entrust wanted to know: What is needed to secure the world's hybrid workplaces?

To determine the security needs of the new hybrid workplace, we surveyed 1,500 leaders as well as 1,500 full- and part-time employees from 10 countries across four global regions, including the United States, Canada, the United Kingdom, Germany, Australia, Saudi Arabia, the United Arab Emirates, Indonesia, Japan and Singapore. We asked leaders from the manager level to the C-suite about their current approach and plans for a new hybrid workplace. In addition, we engaged employees at the entry and associate levels to gauge their feelings about the new hybrid workplace and how pandemic-induced work arrangements have affected their perspectives on operations as employees.

This first report of a three-part global data series explores what is needed to perfect the new hybrid work model for sustainability and actions the enterprise should consider to secure data in its infrastructure.

01

# A NEED TO GO BEYOND BASELINE SECURITY MEASURES

The majority of leaders (64%) and employees (54%) surveyed said their company is currently using a hybrid work model. In addition, 16% of leaders and 21% of employees said their enterprise is fully remote but considering a hybrid work model.

There is a clear trend toward a more distributed workforce with less emphasis on traditional offices. As such, the need for a high standard of security has never been greater. And as the results showed, employees at least say their employers have made inroads to shoring up security. Ninety-five percent of leaders said their policies discuss data security and privacy best practices. In addition, 89% of leaders and 87% of employees said they feel confident their company's data is secure when people work outside the office.

But is this confidence warranted?

Leaders who were confident in data staying secure outside of the office credited baseline protections like **multi-factor authentication (MFA)** and **virtual private networks (VPNs)** for their confidence — a finding that was confirmed by employees (Figure 1 and Figure 2).

But there's a contradiction here. Leaders may believe company data is protected with standard solutions. Yet leaders cited the security of home

internet connections, leaked sensitive company information and cyberattacks from bad actors as their top security concerns — all of which are closely tied to data remaining secure outside the office and potential challenges to the hybrid work model (Figure 3).

If organizations are going to use hybrid work models successfully over the long term, then they will need to further invest in their security strategy. MFA and VPNs, while important, are part of a larger strategy for data security in a hybrid work model. Throughout the pandemic, bad actors have exploited security deficiencies of remote environments such as insecure home tech hardware, poor password hygiene and employee use of unapproved tools. These cyberattacks will only continue if organizations neglect data security and don't use data encryption to protect the integrity of communications across hybrid connections.

Figure 1. **What technology/tools have you put into place to ensure confidence in your company's data security when employees work outside of the office? Leader answers broken down by country**

| | Multi-factor authentication | Virtual private network | Single sign-on | Passwordless tech |
|---|---|---|---|---|
| United States | 78% | 58% | 43% | 35% |
| Canada | 64% | 69% | 48% | 17% |
| United Kingdom | 63% | 68% | 41% | 22% |
| Australia | 70% | 58% | 57% | 34% |
| Germany | 67% | 49% | 25% | 29% |
| Saudi Arabia | 89% | 44% | 48% | 37% |
| United Arab Emirates | 70% | 39% | 46% | 54% |
| Indonesia | 80% | 47% | 55% | 51% |
| Japan | 48% | 60% | 41% | 36% |
| Singapore | 65% | 56% | 47% | 31% |

Figure 2. **Tools and technology being used for data security in a hybrid work model**

**From leaders:**
What technology/tools have you put into place to ensure confidence in your company's data security when employees work outside of the office?

**From employees:**
What security technology/tools has your company introduced to accommodate a hybrid work model?

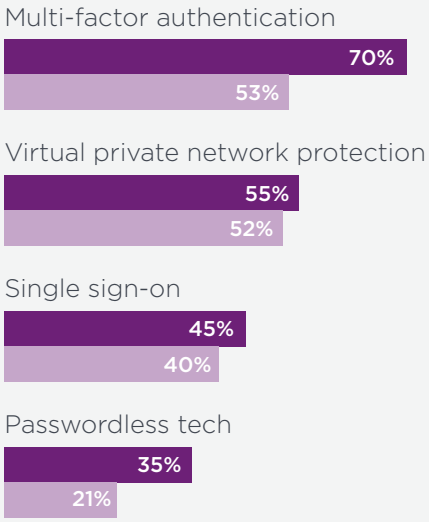


Figure 3. **Biggest security challenges facing hybrid work models, ranked by leaders**

| | |
|---|---|
| Security of home internet connection | 21% |
| Leaked sensitive company information | 20% |
| Cyberattacks from bad actors | 18% |
| Poor data protection methods | 15% |
| Lack of privacy in the home | 8% |
| Phishing attack | 8% |
| Poor password management/hygiene | 4% |
| Compliance violations | 3% |
| Other | 1% |

02

# GREATER EFFICIENCY FOR SECURE REMOTE ONBOARDING

The majority of leaders (68%) said they're considering hiring talent that resides in geographically diverse locations. A seamless and secure onboarding experience is a great first step toward ensuring these employees from other cities, states and countries feel welcome and gain confidence from day one.

But even after nearly 18 months of operating in remote and hybrid environments, leaders and employees indicated the process can still be improved.

Our data indicated that leaders and employees aren't aligned on what constitutes a best-in-class onboarding experience. Leaders said the first key to improving remote onboarding was improving new employee training. Conversely, employees ranked this same tactic in the bottom half of their list of ways to improve remote onboarding. Employees instead listed new or improved collaboration tools as the best way their organization could improve the onboarding process (Figure 4).

Leaders and employees not seeing eye-to-eye on remote onboarding indicates a larger problem of inefficiency. Employers are leveraging a range of tactics to improve remote onboarding. However, instead of making scattered improvements across the entire process, employers should instead focus on making incremental improvements

that streamline the foundations of security and productivity.

For example, before the onboarding process formally begins, **digital identity proofing** can help enterprises confirm the identity of newly hired remote employees — ensuring workers hired are who they say they are. In addition, a secure system for **mobile ID issuance** enables employers to remotely issue new employees a physical or digital ID card before they even first step foot into the office. This solution streamlines onboarding to connect digital and physical employee identity, making it easier for employees to "enter the workplace" — both the physical office and the digital applications required for work.

Businesses in Saudi Arabia (89%) and the United Arab Emirates (87%) were the most willing to consider hiring talent that resides anywhere in the world. Businesses in the United States and Singapore are the next most likely to hire talent anywhere in the world, with 73% of leaders in each country indicating they would be willing to hire global talent.

Figure 4. **Tactics organizations have implemented to improve remote onboarding practices for new employees**

# INNOVATIVE SOLUTIONS TO PERFECT THE HYBRID WORK MODEL

Tools to level up security in a hybrid work environment can give organizations a leading edge. And for IT and security professionals who know the pain of a broken remote onboarding process, a seamless solution for mobile ID issuance can be a welcome efficiency.

There are four key solutions you can count on to raise your security standard and streamline remote employee onboarding:

## PASSWORDLESS WITH SINGLE SIGN-ON

Strengthen your MFA and VPN by incorporating a passwordless with single sign-on (SSO) solution. A strong solution uses PKI credentials and biometric authentication to ensure an employee logging in is in fact an employee logging in. Additionally, a high-assurance passwordless solution effectively blocks 80% of today's cyberattacks.

## ADAPTIVE RISK-BASED AUTHENTICATION

Ensure only authorized employees access your company network by leveraging adaptive risk-based authentication. This technology engine adds a layer of security for network login attempts by assessing contextual attributes of users such as biometrics, geolocation and device reputation in real time to grant, block or challenge access.

## DIGITAL IDENTITY PROOFING

A digital identity proofing solution can help streamline onboarding while ensuring a trusted identity from new hires. Through a cloud-based identity proofing system, you can automate the onboarding of new employees to enable access to your company's network, apps and websites. In addition, accelerating this process can make the overall employee onboarding process **8x more efficient** with a modernized identity proofing solution.

## SELF-SERVICE PASSWORD RESET

Enable a frictionless network user experience with a self-service password reset tool. By empowering employees to reset passwords on their own, they can securely solve the problem without any involvement from your IT team. Leveraging this solution can also help reduce costs, as password resets often account for 20 to 50% of IT help desk calls.

At Entrust, we're leading the way in developing solutions built for the new hybrid workplace. With our **Passwordless Login**, **Single Sign-On**, **Adaptive Authentication**, **Mobile ID Proofing** and **Password Reset** offerings, you can solve the challenges pressing today's leaders and employees — and take your hybrid work model to the next level.

# LAYING THE FOUNDATION FOR THE NEW — AND FUTURE — HYBRID WORKPLACE

Using scattershot tactics to secure your hybrid work model and improve remote onboarding leaves your organization unprotected and inefficient. A better approach? Taking the necessary steps to defend your network against evolving cyberattacks and making a universal process, like mobile ID issuance, seamless, secure and scalable across your entire organization.

Entrust can be a partner in protecting the data that's vital to your company's operations and optimizing new hire processes through secure, streamlined onboarding. **Get in touch with our team** to see how we can help perfect your hybrid work model for the new hybrid workplace of today, and set your organization up for the hybrid workplace of tomorrow.

## ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us. For more information, visit **entrust.com**.

## SURVEY METHODOLOGY

Entrust surveyed 1,500 leaders and 1,500 employees from the United States, Canada, the United Kingdom, Germany, Australia, Saudi Arabia, the United Arab Emirates, Indonesia, Japan and Singapore in June 2021. Leader respondents worked at the manager level up to the C-suite and employee respondents worked at the associate and analyst levels. All respondents in both groups encompassed a variety of companies that employed anywhere from 1,000 to 50,000+ employees. In addition, all respondents in both groups worked at organizations that currently use a hybrid work model, formerly used a hybrid work model or are fully remote but considering a hybrid work model.