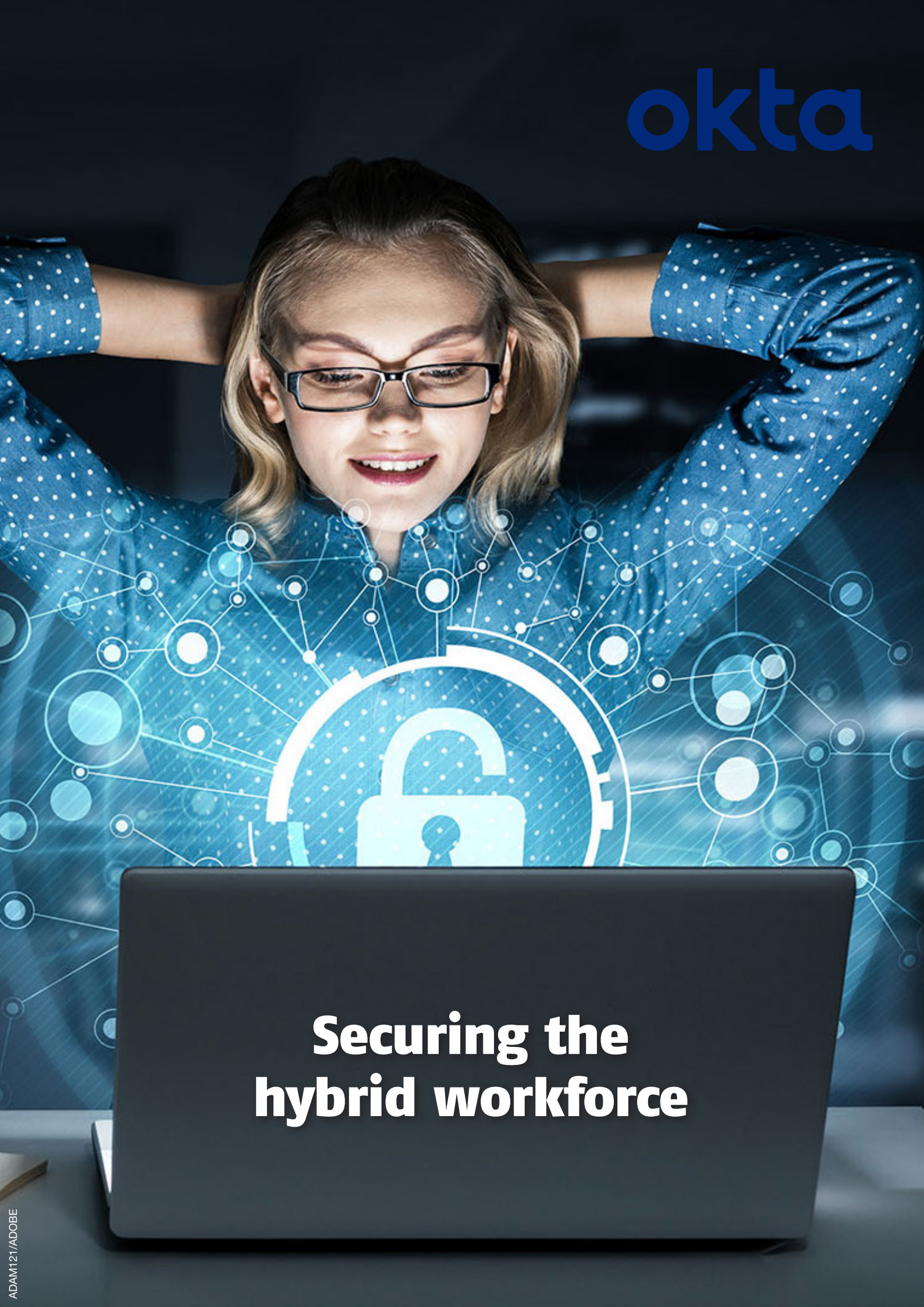


ADAM121/ADOBE

Establish trust to secure dynamic working for post-pandemic business

Organisations need to understand and plan effectively for the next phase of the post-pandemic workplace, with identity and security woven in. Fortunately, help is at hand to help them do this

The Covid-19 pandemic has revolutionised the way we work. Many employees swapped an office space where their IT systems were protected by perimeter security, for a home or remote environment with uncertain connectivity and security challenges.

The initial task for IT leaders was enabling this switch at speed. With rules now easing, the next objective is how to build on this dramatic change and create flexible access to systems and data to enable employees to work securely wherever it suits them.

The transition has inherent risks if organisations get it wrong, but huge advantages if they get it right. CIOs want to avoid data breaches, but the business can benefit from this new dynamic office model – lower real estate costs, happier staff with a better work-life balance, and access to talent unconstrained by location, are just some of the potential gains.

But how can IT chiefs secure data while allowing the necessary flexibility of access to applications and systems to ensure a good work experience, wherever users are? For a start, they need to build a hybrid workplace that securely connects the right people to the right technology at the right time – and they need a partner with the understanding and real-life experience of this new dynamic working environment.

Digital identity provider Okta understands the security challenges faced by organisations and can deliver the technology solutions to meet them

Post-pandemic working

Trusted digital identity provider Okta has more than 10,000 customers globally and understands the security challenges faced by organisations, with the experience of how to deliver the technology solutions to meet them.

Okta's expertise in the use of key technologies, such as identity and access management, zero-trust security and multifactor authentication, is providing a path for many organisations to establish their post-pandemic working arrangements.

"During lockdown, many organisations had a knee-jerk reaction where they had to implement security technology to enable their workforce to work from home," says Ian Lowe, director of solutions marketing EMEA at Okta.

"But now we have a real juxtaposition among organisations. Some are championing a hybrid or digital-first approach where they allow employees to work from wherever they choose," he adds. "Others are taking a step back and reviewing the technology they implemented in that knee-jerk and looking holistically at their approach to identity management to enable flexibility. Another group are requiring their workforce to return to the office as if it was pre-pandemic."

Many organisations chose multifactor authentication to securely access cloud applications, but are now realising there is more to be gained by evolving towards a workplace which is hybrid and dynamic.

Trust at work

While some organisations want to encourage employees back to the office, the reality is that most are grappling with a new reality that combines multiple working environments, choices of technology, and styles of working that best suit employees' individual needs.

Other staff, meanwhile, are pushing back against employers that want to return to the same old pre-pandemic environment. Lowe says that up to 70% of employees want to continue to have a choice. Organisations must evaluate how to make this new dynamic approach work for them to provide that flexibility but also mitigate risk.

"Whatever way we look at this, there's a pivotal foundation piece that organisations must put in place, which Okta calls 'trust at work'," says Lowe.

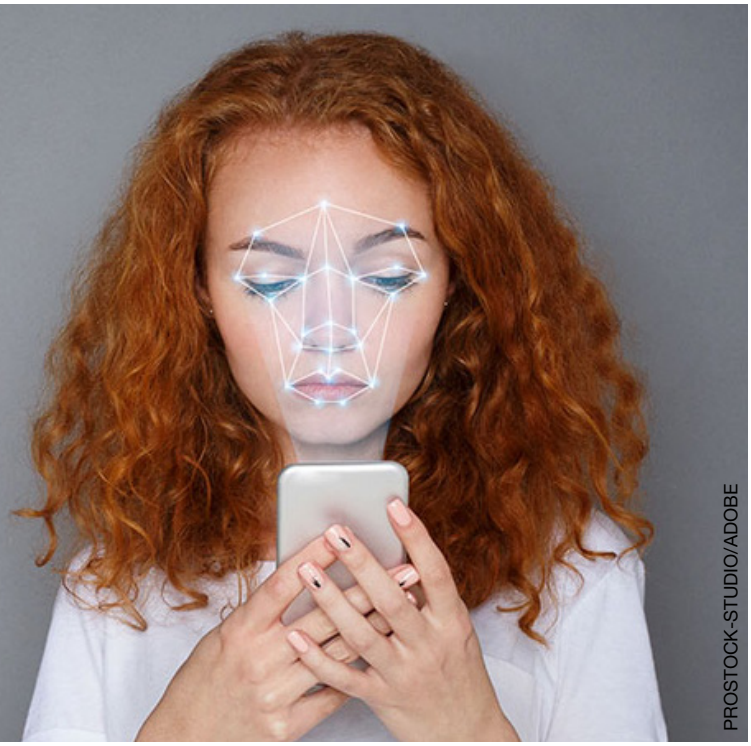
To deliver the technology that supports this "trust at work" approach, Okta's zero-trust framework gives organisations a holistic view of their identity and security strategy.

Gartner defines zero-trust security as "never trust, always verify". The aim is to secure every user, wherever they are at any time, irrespective of the device they are using.

"Zero trust is pivotal even for organisations that want to return to a pre-pandemic working environment because they still have contingent workers who may not be able to come in or are using their own devices. Zero trust is also vital in delivering the hybrid or digital-first approach where employees can work from anywhere," says Lowe.

Every organisation had to shift quickly at scale during the pandemic – changing policies and making upgrades and updates to their technology stack to enable remote working. Further adoption and scaling up of collaborative technologies such as Zoom or Slack, for example, became common practice and increased the security challenges when sharing data across a distributed work environment.

Lower priority applications can be protected with a simple username and password, while mission-critical apps can have extra protection through multifactor authentication or biometric authentication



PROSTOCK-STUDIO/ADOBE

According to Okta's *Businesses at Work* report, its customers use an average of 88 applications, with use of Zoom alone growing over 45% between March and October 2020.

"If you look at digital transformation and collaboration in the workplace pre-pandemic, most of those projects were taking, on average, over 200 days to deliver a new collaboration tool into the business," says Lowe.

"When the pandemic hit, those 200-day projects were delivered in just 10-and-a-half days – a significant acceleration. The IT team had to move from lightspeed to ludicrous speed. Without the security in place to support this transition, many organisations had little choice but to increase their licences for multifactor authentication."

"Zero trust is vital in delivering the hybrid or digital-first approach where employees can work from anywhere"
Ian Lowe, Okta

Opening up the perimeter

Many of those fast-paced implementations were point solutions, and now organisations are stepping back to look holistically at how the perimeter of their organisation has opened up.

"New apps have been introduced that require controls to be put in place. People are working at different hours from different locations and via IP addresses never seen before. There's a plethora of security challenges that we're now faced with. Complexity and speed of change have dramatically increased," says Lowe.

He says a question each IT leader must ask is, "What is the ideal experience I am looking to deliver?"

Organisations must secure multiple identities and deliver a seamless solution for users, whether accessing applications or providing sign-up or onboarding for systems. Working with Okta, companies can consolidate different identity databases and integrate them with the required applications.

"Consolidation gives you a complete 360-degree view of identity and security and simpler implementation of policy across different applications. You can increase security by pulling in information from other systems more easily, because you have a central database of identity, so you can pull in risk signals from different applications through better integration," says Lowe.

For example, plant breeding company KWS worked with Okta to help with a secure roll-out of Office 365 for 4,500 users globally who use single sign-on and multifactor authentication. Okta coordinated all user identities while making it easy to use the new system securely.

The benefits included saving 125 hours per month on onboarding tasks and enabling 187 integrated applications ready for use in the cloud and on-premises.

A holistic view

Providing this holistic view of identities and validating them remotely is a game-changer for many organisations which previously relied on manual processes to onboard and authenticate new employees. Often, they would be required to go into the office with some form of identity, such as a driving licence, and meet an HR representative before being given access to buildings and IT systems.

"If you have a holistic view and integrations already done, and control of the lifecycle management of the identity in place to support remote onboarding, you can have a better experience than pre-pandemic. You can automate the starter-leaver-moving process and reduce the burden on the IT helpdesk," says Lowe.

However, reducing the support burden and enabling productivity from day one are only worthwhile if security is in place.

“In the remote working environment, we have a huge number of potential attack vectors that have opened up, including phishing and malware attacks. Having a holistic view of identity allows you to implement different security policies for different applications,” says Lowe.

Lower priority applications can be protected with a simple username and password, for example, while mission-critical apps have extra protection added with multifactor authentication such as a unique password sent to a user’s phone, or biometric authentication.

“Having this level of flexibility is critical when employees are no longer in the office and you have no understanding of the perimeter,” says Lowe.

The security burden can be eased because it is possible to have an automated single password reset policy, for example, which further reduces the workload on IT support.

Planning for best practice

To help with planning, Okta can provide professional services and best practice guides. There are key steps businesses must take to ensure a dynamic workplace environment, which include asking questions such as:

- What does my identity landscape look like and where do my identities sit?
- What does my technology ecosystem look like?
- What is the HR process and the ideal onboarding experience?
- What does my ideal workforce application access experience look like?
- What is the business culture and how does that affect the experience?

PROSTOCK-STUDIO/ADOBE

"Once you define your experience and have an understanding of your application and identity landscape, you can start to look at what technology you need to implement to support that vision," says Lowe.

Once organisations have a unified view of identity and security, they can plug in different technologies that will look at risk signals, such as the time of day employees are logging on, or typical and atypical IP addresses, so they can build a profile of employee identity.

"Okta supports multiple partners that give us these insights and organisations can start to automate responses to unusual user behaviour and risk signals," says Lowe. "Access can be blocked without human intervention or authentication can be stepped up with more validation required before an employee gains access."

Multinational company Imerys, which specialises in the production and processing of industrial minerals, worked with Okta to reduce its operational burden when it embraced digital transformation with a global cloud-based approach for 13,000 employees.

Okta helped secure identity management and lifecycle management and sped up employee onboarding and offboarding through automation. Access rights are handled in a targeted way with single sign-on and multifactor authentication providing advanced security measures based on device, location, or network contexts. Employees are not locked out from accounts unnecessarily and the burden on IT support is reduced, while security has been improved.

Once organisations have a unified view of identity and security, they can plug in different technologies that will look at risk signals – such as the time of day employees are logging on, or typical and atypical IP addresses – to help build a profile of employee identity

Okta Integration Network

Many organisations have a complex hybrid environment with a mix of on-premises and cloud applications, but employees don't care where their data resides, they just want seamless access to get the job done.

By choosing Okta, organisations can benefit from enabling dynamic working for their employees by authenticating identities in a cloud or on-premises environment. Okta can also support customer identity management for e-commerce websites on a single platform.

The Okta Integration Network offers over 7,000 applications integrated out of the box, including marketing applications and collaboration suites such as Google Workspace, Office 365 and Slack.

"This is a unique differentiator for us, as is our support for open standards. This enables us to integrate with other cloud applications for single sign-on and multifactor authentication. Okta also works with legacy standards for on-premise integration," says Lowe.

Organisations can take packaged products such as multifactor authentication, lifecycle management or universal directory straight out of the box, which allows unified security and identity.

If an organisation wants to integrate an application that is not supported by Okta, developers can use Okta applicatoin programming interfaces (APIs) and software development kits (SDKs) and extend where they see fit, so there are no limits to application choice, capitalising on the 2021 acquisition of AuthO.

"We have a whole developer portal and support network to enable this," says Lowe. "Most organisations don't have development teams that are experienced in security or identity. We can enable developers to become

experts through those toolsets. Where we enable organisations is through our technology platform to help them deliver security and identity to whichever use case they have."

Advertising agency WPP used Okta to establish a minimum baseline of security and standardise access controls. Post-pandemic, the company can provide rapid, secure access to a range of new remote-working solutions for colleagues.

Choose your work policy

The upside for organisations that work with Okta is that employees can work in a way that suits them, and premises are freed up which reduces rent. The foundation of the "trust at work" approach allows organisations to deliver any kind of work policy they want – in-office, remote or hybrid.

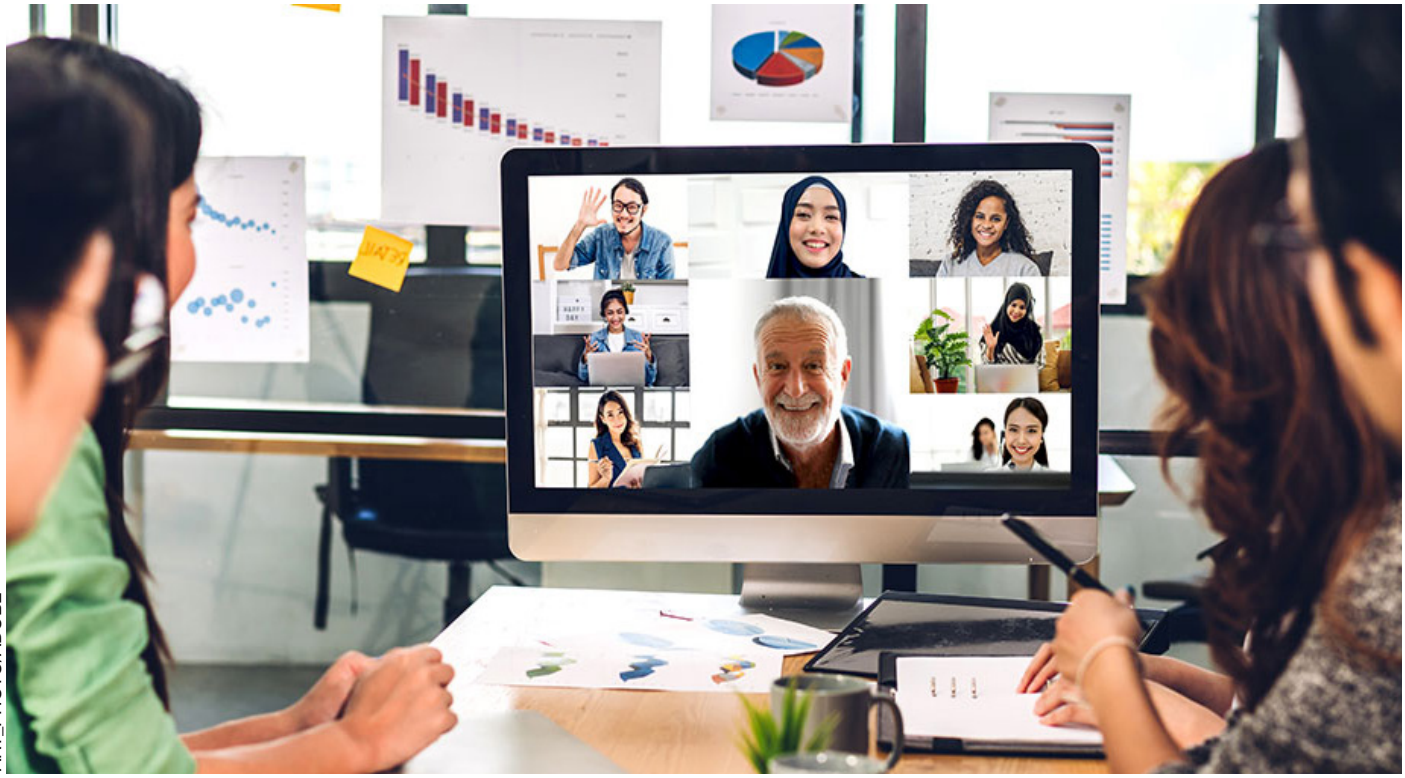
"Dynamic working is about the flexibility to establish different access policies depending on what you're doing, whether you're at home or in an office, so you can adapt the access policies as the risk varies depending on location," says Lowe.

This unified approach to identity is central to creating a dynamic environment and a positive user experience.

"If an organisation has a blanket multifactor authentication policy to access every application, it becomes a pretty terrible user experience," says Lowe.

Working with Okta, organisations can understand and plan effectively for the next phase of the post-pandemic workplace.

Lowe concludes: "We've gone through an evolution of working life from pre-pandemic in the office to remote working and now a dynamic, hybrid environment. To deliver the flexibility and scalability required for this new environment, you need a foundational approach – trust at work rooted in zero-trust security." ■



ART_PHOTO/ADOBE