451 Research® Now a Part of S&P Global Market Intelligence | Business Impact Brief

Secure Work From Home With Zero-Trust Access

The 451 Take

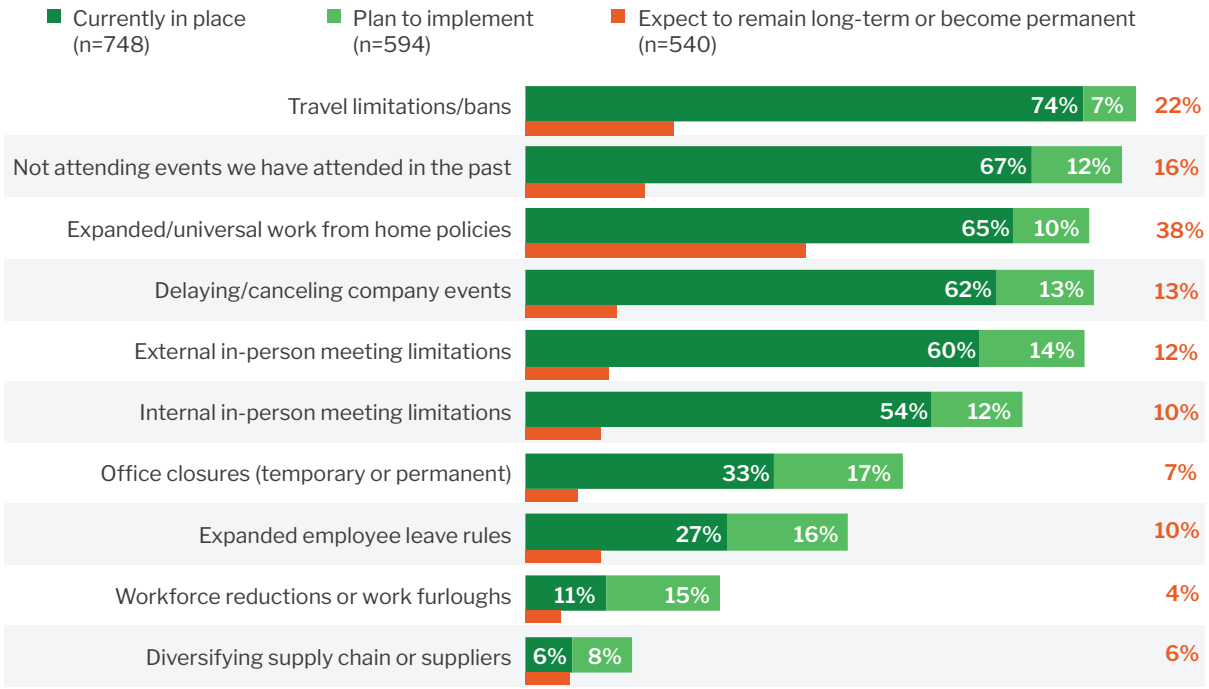
One of the short-term consequences of the COVID-19 pandemic has been a massive controlled experiment in the viability of work-from-home (WFH) strategies. Indeed, many enterprises went from having a small fraction of their employees working from home (28% work some or all of their week from home, according to 451 Research's Voice of the Enterprise [VotE] survey data) to, in many cases, over 95% – often in a matter of weeks, if not days. Indeed, additional VotE survey data shows that an expansion of WFH policies was among the top three responses to the pandemic (65%) among enterprises, trailing only reduced event attendance (67%) and travel restrictions (74%).

The surprising success with which many large companies have made the WFH transition has long-term implications as well. Executives at multiple large enterprises have suggested there may be a degree of permanence to these moves, with some announcing plans to permanently close a substantial portion of their remote locations and generally rethink their overall strategy regarding work locations. Indeed, 451 VotE survey data shows that 38% of respondents expect WFH policies to become permanent – the number one choice of all responses.

Organizational Policy Response to the Pandemic

Source: 451 Research's Voice of the Enterprise: Digital Pulse, Coronavirus Flash Survey March 2020

Q. Has your organization put any of the following new policies/changes in place as a result of the circumstances surrounding the coronavirus outbreak? Q. Do you expect your organization to put any of the following new policies/changes in place? Q. Do you expect any of these new policies/changes to remain in place long-term and/or become permanent? Please select all that apply.



451 Research Now a Part of S&P Global Market Intelligence | Business Impact Brief

Business Impact

ADAPT TO THRIVE. The reality is that most firms may never go back to the old ways of doing business. The upshot is that in addition to short-term tactical responses, companies need to have a long-term strategy focused on remote work that can adapt to this new reality and allow for business agility as well as continuity. In simpler terms, we need to embrace new means of access to resources that take into account more flexible ways of conducting business that go beyond what legacy technology like VPNs or secure web gateways offer.

MULTIPLE ACCESS SCENARIOS REQUIRE A UNIFIED APPROACH. Historically, access to traditional on-premises applications has been managed separately from access to SaaS applications and apps running in public cloud environments. A unified approach to access management can help enterprises that are managing a mix of on-premises apps, virtualized apps, web apps and cloud apps, but also a wide range of users (employees, partners, contractors and customers) across a mix of network access solutions (VPN, Wi-Fi, VDI and zero-trust network access) and devices (PC, Mac, iOS, Android) – with better end-user experience, tighter security and reduced overall cost of managing multiple vendor solutions. Also, it's important to note that true unified access is not just about access to apps, but also to data and files residing either on premises, in the cloud or in other resources.

SECURITY POLICIES MUST BE CONSISTENT ACROSS ALL ASSETS. In such mixed scenarios, complexity can increase, which in turn increases the need for context across users, networks and devices across all assets, as well as visibility across all platforms, both cloud-based and non-cloud. To avoid gaps in coverage, security policies also need to be consistently and continuously applied, which implies automated, contextual processes, as opposed to manually 'stitching together' legacy policy frameworks.

Looking Ahead

Not surprisingly, the increase in WFH has led to an initial surge in VPN usage, since most established firms already have VPNs in place. However, over the long run, existing VPN infrastructure is not optimized for this emerging new world. For starters, VPNs can be a challenge to deploy, particularly with more than 90% of employees working remotely. More importantly, VPNs also present security challenges, in the sense that they provide broad access to an entire flat network segment rather than to just the applications and resources that employees need to do their jobs.

A new approach to security, known as zero trust, has gained momentum in the past year and has the potential to become the new standard for security in this emerging reality. At its core, zero trust is an extension of the principle of least privilege – access is granted to only those resources that a user requires to do their job, and nothing more. And in the zero-trust model, access to resources is based more on your identity than what network you are on.

In such an approach, access policies should not be imposed just at login, but should continuously monitor and evaluate user sessions to make sure they remain in compliance with adaptive and contextual security policies, often by leveraging user behavior analytics, AI or machine learning. The latter implies extensive use of MFA, device posture and risk profiling to make more intelligent decisions about which users to grant access to which resources. If done correctly, a unified approach to zero trust can both help reduce risk and improve security, but also enable a better overall user experience from more consistent, 'invisible' security and access policies.