

Scaling for long-term telework success

How agencies can focus on mission, not location

Before the COVID-19 outbreak, just 40% of federal employees and only 4% of state and local employees were authorized to telework. When the almost-overnight move to near-total telework happened, organizations and employees were faced with unfamiliar work environments and the need to revisit priorities.

Shifting a workforce from in-office to majority-telework requires more than just adding new collaboration tools, explained Kelsey Nelson of Okta's Zero Trust division. "It also means adding on new processes and new styles of work, and having the technical components you need to support and enable your teams."

The key to managing the shift, Nelson said, is the ability to enable security that is "people-centric rather than network-centric. You need to make sure that the right people have the right level of access to the right resources and in the right context—and to assess it all continually."

Some level of telework is certainly going to persist after this crisis, and organizations are starting to orient toward what that will look like in the longer term. In this "new normal," said Nelson, "productivity has continued or even increased."

Organizations want to know how to continue this trend. Those that are starting to enable this approach for the longer term are the ones that are moving toward greater IT agility—able to balance the productivity and the rapid transition from office to telework with its shifting security perimeter. They are moving away from a traditional network-centric model to one that is more rooted in identity and zero-trust. Okta's goal, said Nelson is to "not only enable our users, but also help our users understand what this new networking work life looks like from a security perspective."

Many government agencies were struggling with authentication, Nelson said. In one case, the terminals that employees were using from home were not Personal Identity Verification (PIV)- or Card Authentication Key (CAK)-enabled.

The solution was Okta Verify, she said, adding, "we're seeing a blend of other factors as well, including SMS and voice, and using a hard token or physical key. Okta Verify is a multifactor type (FIPS 140-2 validated factor) used to verify the end user's identity via mobile app, that also allows flexibility for sequencing."

For end users, technology should be an enabler, not a point of friction. "I think this is why we saw such a huge spike in Okta Verify adoption and use over last few months. It is quick to deploy. Getting a physical token to a user can have supply chain challenges and take more time. In terms of process, an app like Okta Verify, that you can download to your phone, is much less of a lift for the user."

"The organizations that are enabling a distributed workforce for the longer term are the ones that are able to drive IT agility." These organizations are asking about how to automate on- and off-boarding for devices and for users when they are not actually in the office. They are implementing stronger security tools, such as context-based access policies, that are less network-



specific and extend access controls.

This agility is crucial for interagency and public/private partnerships, Nelson noted. "Take COVID-19. Different agency working groups have been trying to coordinate about how to respond to this crisis: information sharing, being able to know who has access and to what data so they have what they need without sending documents around email, which is not the most efficient way to collaborate."

The core goal, said Nelson, is "to enable secure access for all users and on any network and device; to bring that zero-trust and use it as a guiding star toward where we can go in the future."

It is not just how we work, said Nelson, but also what we want to enable our agency teams to do. First, how can we ensure that our teams are able to fulfill their mission—and not only productivity, but also translate this into services. From there, she said, we identify the quick wins, ways to deploy custom applications and portals for digital services, ways to make things more efficient for the people these agencies serve.

"As you start to build out, make sure that you are scaling appropriately," Nelson advised. "That is critical, especially in terms of citizen services, and the dynamic digital traffic expected over the next few months. Make sure that those citizen services are seamless, they are omnichannel experiences, that they're tailored for the use cases of the constituents you are trying to serve."

"The organizations that are enabling a distributed workforce for the longer term are the ones that are able to drive IT agility."

— KELSEY NELSON, SENIOR PRODUCT MARKETING MANAGER, OKTA

SPONSORED BY :

okta