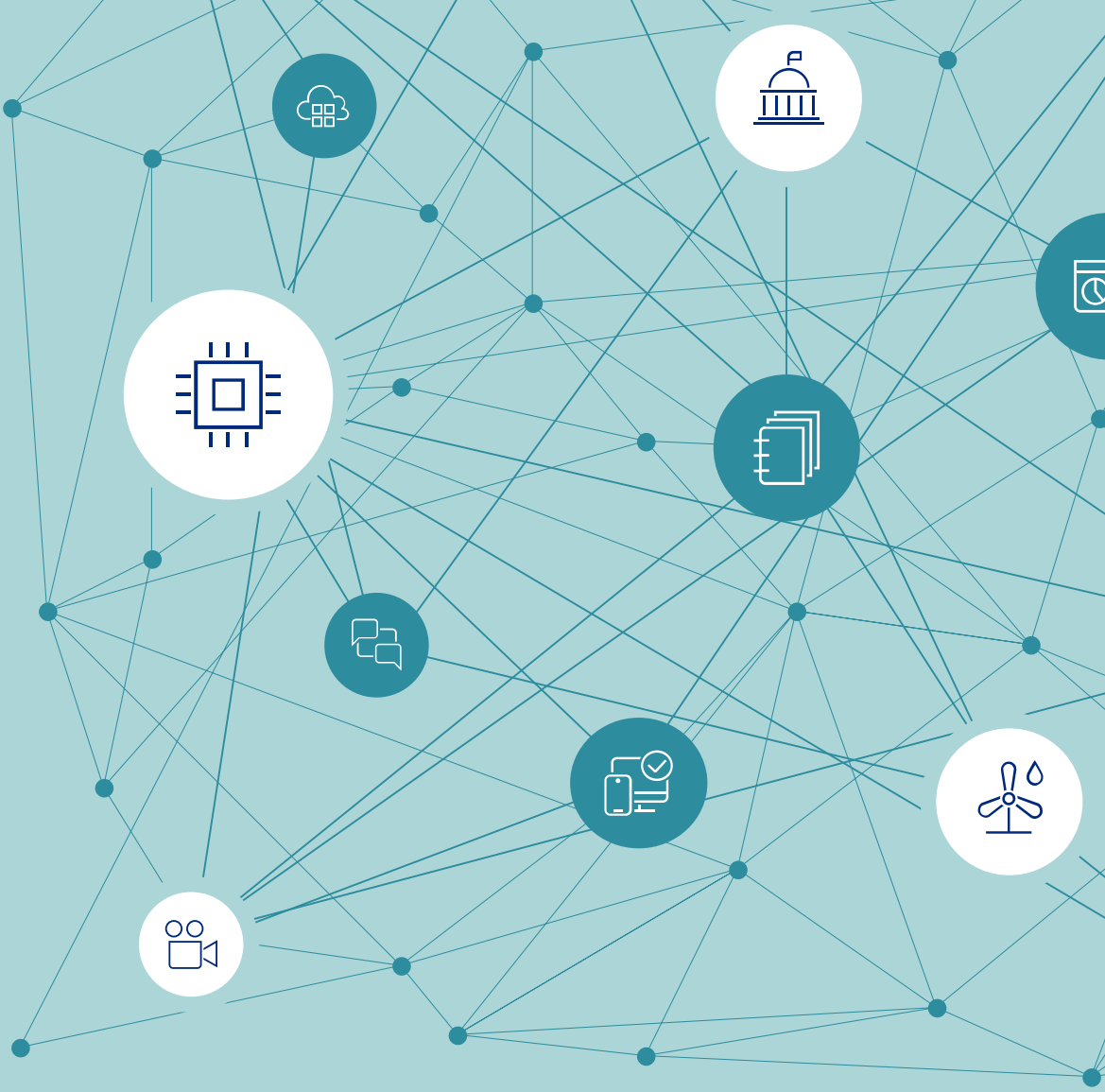

okta

The 3 Tenets of Enabling a Remote Government Workforce

As agencies begin to support a more permanent remote future, it's critical that they build security in every step of the way — starting with access and identity.

> **“We always have to be thinking in the back of our mind how to not just deliver that capability, but deliver it securely.”**
>
> Sean Frazier | *Federal CSO, Okta*

Even as a possible end to the coronavirus pandemic is on the horizon, there’s no doubt that telework is here to stay for the government workforce. In many ways, 2020 served as an unintentional proof of concept, demonstrating that workers can be just as productive away from the office as inside it. Going forward, many employees are likely to begin looking for the flexibility and ease that remote work offers even as the pandemic wanes, turning many previously in-person government workplaces into hybrid ones.

Now, as agencies begin to look out at a more permanent remote future — at least for some of their staff — it has come time to consider the infrastructure modernization that will need to occur in order to ensure each agency can remain both secure and productive. That’s a tougher road for some agencies than for others.

“Prior to the pandemic, some agencies had already adopted the cloud, moved many of their workloads there, embraced zero trust and were forward-leaning in terms of their infrastructure. But a much larger number were not all prepared,” says Sean Frazier, Federal CSO at Okta. “These agencies were suddenly forced to very quickly stand-up legacy services and scale themselves so that people could connect to data centers, bulk up VPN concentrators so all users could enter the firewall from the outside.”

Where that leaves agencies now, says Frazier, is much further down the road to modernization than they would have been otherwise. But in order to serve both an evolving workforce and ensure they can weather any coming storms, agencies will need to continue down that road and change both their infrastructure and their mindset accordingly. A focus on security will be key to those efforts.

“Agencies need to modernize access — no one can work if they don’t have access — but also security, because attackers never standstill. While we’re contemplating our move from A to B, malicious actors are constantly attacking our assets. We always have to be thinking in the back of our mind how to not just deliver that capability, but deliver it securely,” says Frazier.

1. It All Starts with Identity

So, what can agency and IT leaders do to stay ahead of possible disruptions and growing threats as they continue to adopt the cloud?

For a start, it's crucial for organizations to practice basic security hygiene. This includes: zero trust security principles — a key tenet of cloud security; keeping an inventory of assets, applications and data to ensure IT teams are aware of everything they need to protect; and encrypting data at all times. To get there, however, agencies will need to lay the groundwork starting with the user, or, more specifically, identifying the user.

"Nothing happens until a user requests access to something; prior to that it's all theoretical. So, the natural place to start with modernization is with identity," says Frazier.

Modernizing the identity stack can help an agency adopt zero trust and set them up to implement critical modern day security tools, like multi-factor authentication and encryption. It can also help them make use of evolving technologies, like PKI 2.0, one of the most effective authentication technologies available.

"There's a real opportunity to innovate into PKI 2.0 and implement things like web authentication and other pastoralist technologies that are also PKI based, but have a much better user experience, are more modern and are also supported by platforms like Okta," says Frazier. "Moreover, as that open standard evolves and gets stronger, we can build that strength in without the agencies having to go kind of custom build that strength."

2. Keep a Focus on Usability

The truth, however, is that none of these tools or policies are useful unless the employee actually uses them. And if gaining access or practicing cyber hygiene becomes a hassle, staff will naturally find ways around it.

For example, when security flaws were revealed in popular video conferencing platforms early in the pandemic, many agencies went about layering security software on top of it. But that meant that it took people minutes instead of seconds to log in and start a meeting, Frazier explains. Unsurprisingly, people were eager to get to work and many ended up using their personal accounts to log into meetings instead — meaning they were even less secure than before.

"Today, users have choices. They have iPhones and personal computers that they're comfortable on and so if we don't provide the secure, easy to use platform, they've already got choices, they've got the easy-to-use platform in their personal life and they're not afraid to use it," says Frazier. But this can leave organizations more vulnerable than ever, particularly at

a time when telework means that employees are closer to their personal devices than ever before.

This is one of the reasons why Okta's identity, credential and access management (ICAM) platform focuses on fostering a seamless, rictionless user experience, while also keeping up with the changing security landscape.

"At Okta we do one thing, and that's provide a cloud-native identity solution, and that laser focus allows us to be always on, always accessible and, importantly, to be really agile. Agility is important because much of the platform technology — like Google, Apple or Microsoft — updates very quickly," says Frazier, noting that agencies who have home grown ICAM platforms may invest a significant amount of time and money in order to keep up with all these updates.

Okta, however, has an in-house team designed to stay one step ahead and seamlessly deliver these updates back to the agency. That means agencies can refocus their time and resources toward serving citizens.

"It's designed to serve people today and work with the way we live and breathe," says Frazier.

3. A Seat at Every Table for Security

When it comes to making these changes, it will take more than just new tools; it will also require a shift in mindset across the entire organization to put security first.

"Mindset couldn't be more important," says Frazier. "Security needs a seat at every table." As the threat landscape continues to accelerate and mature, agencies will need to build security into their DNA to minimize vulnerability.

"Your agency's going to be making risk-based decisions every single day, and they're not always going to get it right," says Frazier. "But if you build in the muscle memory of security and it's always a common thread, meaning that every time you go and build an application and you're writing code, you're thinking about security, you can stay ahead of threats."

Learn how Okta's ICAM platform can help your agency stay secure and productive in the age of telework at www.okta.com/government.

At Okta we do one thing, and that's provide a cloud-native identity solution, and that laser focus allows us to always on, always accessible and, importantly, to be really agile."

Sean Frazier | *Federal CSO, Okta*