How context enriches CX

Deeper insights into customers and employees contribute to robust, frictionless authentication

Habib Hourani
Solutions Engineer, Okta

DURING THE CORONAVIRUS pandemic, the traditional boundaries for security have been dissolved. When government employees could not go into their offices, they needed to be able to do their jobs remotely. But an employee signing in from an iPad at home must be treated differently from the same user signing in on an office computer. That meant agencies had to move security from the boundary of the network to the identity of each individual.

Fortunately, advances in authentication are giving us a deeper understanding of the context around employees' activities, which makes the process more secure without hindering the end user's productivity. In other words, agencies can achieve a higher level of assurance about each individual user's risk.

For instance, we can do risk scoring for users and tap larger datasets to identify known bad IP addresses. By looking at a user's geolocation, we can flag a sign-in attempt coming from, say, Nigeria or North Korea for a government employee who is clearly not in either location. As a result, agencies can start to be more deliberate and prescriptive about how they handle authentications and can enhance their ability to deny suspicious logins.

A best-in-breed approach

Enabling employees to be productive and customer focused is a two-step process. First, the government is increasingly taking a best-in-breed approach to tools. For instance, Okta is laser focused on multifactor authentication and authorization. So rather than agencies trying to build that capability, they can use Okta's solution and always be up-to-date on that aspect of security. We are also seeing agencies move toward adaptive tools that offer additional insight into users' activity and adopting standards that enable interoperability among those best-in-breed tools.

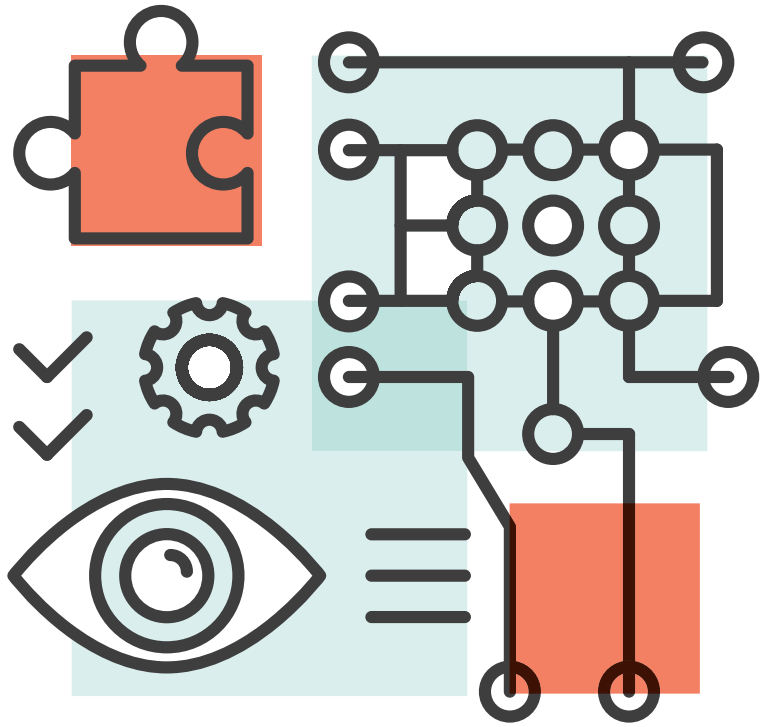
Second, agencies need to build an environment in which those tools can thrive. That's where solutions like Okta's Advanced Server Access come into play. By relying on the OAuth 2.0 framework and zero trust identity and access management, it allows agencies to be more granular about how and what they allow access to.

That approach also enables agencies to automate the process of onboarding new users and deprovisioning accounts when employees leave the agency. It offers an additional layer of security that's not apparent to the end user but is incredibly important for the organization.

Improving access to services

Agencies fundamentally use the same set of tools to authenticate employees that they use to authenticate citizens, but they implement those tools in very different ways.

A citizen who needs to sign into the



By Boo-Tique/Shutterstock/FCW Staff

> **Agencies must take a different approach** to single sign-on and multifactor authentication for citizens and go beyond relying on passwords.

Social Security Administration's website to check on benefits, for example, won't have access to a PIV card or VPN that an agency employee would. Therefore, agencies must take a different approach to single sign-on and multifactor authentication for citizens and go beyond relying on passwords so we can eliminate vectors for threat actors to break into accounts.

The first interaction a person typically has with a government agency involves trying to register for benefits via a website. Unfortunately, according to some estimates, the abandonment rate can be as high as 70% when users encounter friction with that transaction, which creates frustration and phone calls to an already busy support center. That's a staggering number when you think about the importance of the services that federal, state and local agencies provide. Making registration and enrollment easier helps citizens and government staffers in the short and long terms.

Fortunately, with the right tools and strategies, agencies are making those activities both frictionless and secure. ■

Habib Hourani is a solutions engineer at Okta.