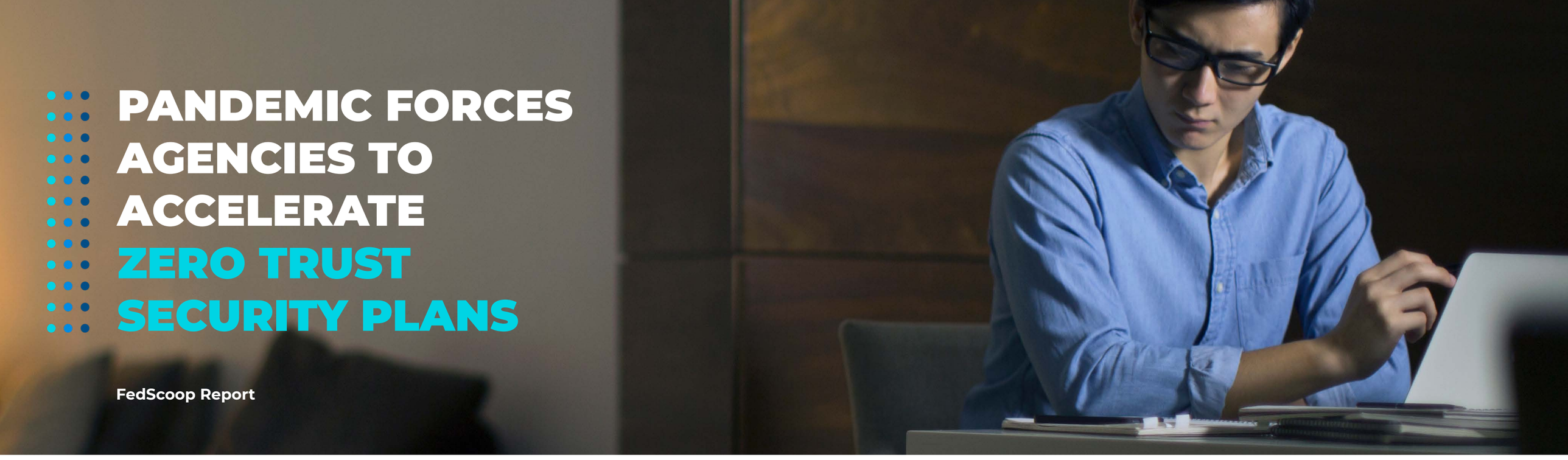


PANDEMIC FORCES AGENCIES TO ACCELERATE ZERO TRUST SECURITY PLANS

FedScoop Report

How work-from-home initiatives and the loss of physical access controls in 2020 are driving agency leaders to reprioritize zero trust strategies.

When organizations lost the ability to manage devices and verify identity with physical tokens, it created visibility gaps on the networks that gave threat actors new opportunities to breach government systems.

In the past, getting buy-in from agency leaders to invest in zero trust security has been challenging. Though federal guidance requires using a strong multi-factor authentication (MFA) tool, it doesn't require the use of zero trust principles. With countless other mandates to meet, CIOs and CISOs are often left checking boxes for security requirements, rather than building strategies that will future-proof the agency against new threats.

Leaders threw their security and access planning assumptions out the window when the majority of their workforce was sent home. Under these new working conditions agencies lost much of their ability to manage devices, control software updates and establish trust when users attempted to access government systems.

"For many organizations — not just the federal government — that means reprioritizing what security and access controls look like when establishing trust for both users and devices," says Helen Patton, Advisory CISO at Duo Security, now part of Cisco.

THE SCOPE OF IDENTITY AND SECURITY TODAY

A recurring security story continued to play out in 2020 and early 2021, which CISOs cannot ignore: compromised privileged accounts allow for the lateral spread of breaches across the network.

According to Patton, this is especially true with shared administrative accounts. In those admin accounts, agencies give multiple users access to a primary username and password. Unfortunately, they often lack strong MFA controls that provide an identity assurance of who is accessing the resource. These are the kinds of weaknesses threat actors hope to exploit to gain access and move laterally across the network.

The Federal Identity, Credential and Access Management (FICAM) policy attempts to guide agencies on ways to protect against compromised accounts using dynamic security models, while still ensuring accessibility and interoperability. But those guidelines weren't always enough to help agencies address the shift to so many remote users.

"Federal agencies need to think in terms of workforce — people and devices; workloads — application and micro services; and workplace — things like printers that are attached directly to the network," explains Patton. "Each of these needs to be evaluated for security posture at the time of authentication to ensure remote and on-premises workers and systems are properly secured."

This conversation is indicative of a larger trend among agencies where leaders are taking steps to understand where they are in their zero-trust journey and their next steps. Patton describes what that path might look like for a typical organization.

CENTRALIZE AUTHENTICATION TO SUPPORT A ZERO-TRUST MODEL

Centralized authentication is a key for managing modern authentication. This capability, by itself, doesn't mean you have a zero-trust model. It does, however, provide the necessary visibility to know what is connected to, and happening across, the network. And it's one of the reasons this type of security control is required in programs like Continuous Diagnostics and Mitigation (CDM) and Trusted Internet Connections (TIC) 3.0.

"The result of centralizing authentication is to make the user experience easier, to have the ability to see where authentication is occurring and to enact policy engines where they will be the most effective," explains Patton.

In some ways, centralizing authentication becomes even more important than looking for flexibility in types of authenticators, she says, because "moving away from fragmented authentication policies will result in greater speed to react to risks and threats as they emerge."

Once centralized authentication is in place, organizations can enact other key principles of zero trust, including policies that govern user and device trust and adaptive access.

DIGITAL IDENTITY AND DYNAMIC AUTHENTICATION POLICIES

The ability to authenticate digital identity at time of request, and to continue to evaluate the security posture of the requestor, is a core tenet of zero trust. Centralizing that capability "ultimately gets organizations to a point where we've got strong policies that have been set up for unique groups of users, for applications and for the organization as a whole," says Patton.

To look at digital identity more holistically, Patton says that a central platform can capture that security data and start to gain insight to what the network looks like — including where the perimeter is and what devices are actually on the network. That process of discovery around digital identity will help agencies figure out what types of policies they need to enact and enforce.

Ideally, agencies want to get to a place where it doesn't necessarily matter what credential an employee was issued, or whether or not the employee is using a managed device. With strong MFA and identity assurance, the organization can centralize a policy engine in such a way as to determine whether or not access should be granted.

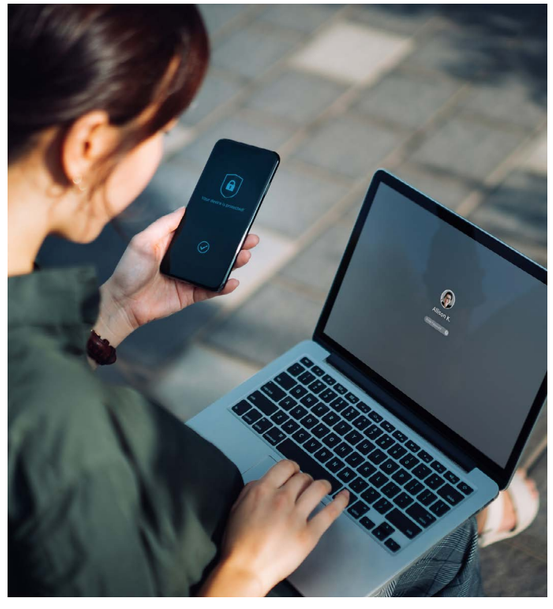
Referring back to the problem around shared administrative accounts, Patton explains that along with establishing identity assurance, this is where a strong multi-factor authenticator — that is unique to each individual — will start to build some semblance of trust back into the security model.

"If agencies are still using accounts with just a password and no multi-factor enacted, they are missing critical controls to authenticate that the user is who they say they are. Only after establishing strong multi-factor authentication with some identity assurance across all its accounts can CISOs look at digital identity more holistically," she explains.

TYING IT ALL TOGETHER

Security risks for distributed work environments are top of mind, and while the problem may seem overwhelming, Patton explains that there are out-of-the box tools that allow agencies to establish stronger authentication and dynamic policy controls.

She pointed to an incident this past January, when Apple made a rare announcement that security vulnerabilities in iOS 14 may have been actively exploited. Though details about the vulnerabilities were scarce, organizations who have built out a dynamic authentication system were able to act quickly.



"When the iOS 14 vulnerability was announced, Duo's parent company, Cisco, implemented a policy change for access authentication. In a matter of minutes, Cisco rolled out the policy to all of it's protected applications accessed by more than 400,000 endpoints making it a requirement for devices to install the iOS 14.4 update before they were able to connect to the network," explains Patton.

It didn't matter if the user had a managed device, and Cisco didn't need to push out an update across the system. They simply required users to act on their own — or not — to make an update if they wanted to access the company's resources with their devices.

Learn more about modernizing authentication controls to allow your agency to react quickly to the next security threat.

This report was produced by FedScoop and underwritten by Duo Security.

FEDSCOOP

DUO