MODERN SECURITY CONTROLS FOR A HYBRID WORKFORCE

StateScoop Report

How agencies can establish flexible security and access controls that adapt to changes in their infrastructure and build resilience against modern threats.

The remote work experience over the last year has cemented a lot of changes for state and local agencies and left a trail of before-and-after pandemic stories to tell. One of the most prominent changes — and perhaps most concerning to agency CISOs — is the sheer number of unsecured devices remote employees rely on to access agency resources.

The crisis affected the shape of cloud adoption, application development, user access and identity verification. But most importantly, it affected the focus of security practices surrounding government resources.

"The number one challenge facing agencies today is finding a security solution that gives them visibility into every single device accessing their network. Especially in today's environment where so many of those devices are unmanaged," says Bart Green, Vice President of State, Local and Education at Duo Security, now part of Cisco.

THE INTERSECTION OF SECURITY AND DIGITAL TRANSFORMATION

Where once a majority of access to state and local resources was on site using desktops or laptops that the organization owned and controlled, the majority of the workforce now connects remotely. Where once a majority of citizen services were managed in person at government offices, citizens are now using new applications and platforms to interact with agencies.

Prior to the pandemic, state and local agencies were on a digital transformation journey, and the crisis kicked up the gear in urgency. To meet shifting needs, sometimes expediency was favored over security.

"When you don't have unlimited funds, when you don't have unlimited support or personnel to build and maintain your IT, you need to focus on what you actually have," shares Wendy Nather, Head of Advisory CISOs at Duo Security.

While agencies worked hard to equip their remote workforce, they still were not able to gain visibility of all the devices accessing agency resources. Green says many agencies are lacking "a way to systematically look at all the devices accessing their applications, and determine which ones are safe and which ones are out of date."

To ensure agency networks and data are secure, CIOs and CISOs need a security solution that:

- Works in a hybrid environment
- Works for cloud applications or for software
- Migrates with applications or new networks and hardware
- Checks the health of devices

DYNAMIC AUTHENTICATION POLICIES

Traditionally, enterprise security controls were designed on the basis that IT would deploy and control how the technology is used. But remote work flipped around all these assumptions about security.

Agencies can't afford to manage every device, and they can't request to look into every device. But they can establish dynamic policies that dictate which devices they will allow to connect to their network based on certain criteria that establish trust.

"Almost everyone has become a technology consumer these days. It's time for the security model to reflect that. Part of putting the responsibility on the user [to update their software] is taking away the centralized management mechanism that forces a laptop to reboot," said Nather in an op-ed article on StateScoop in January 2021.

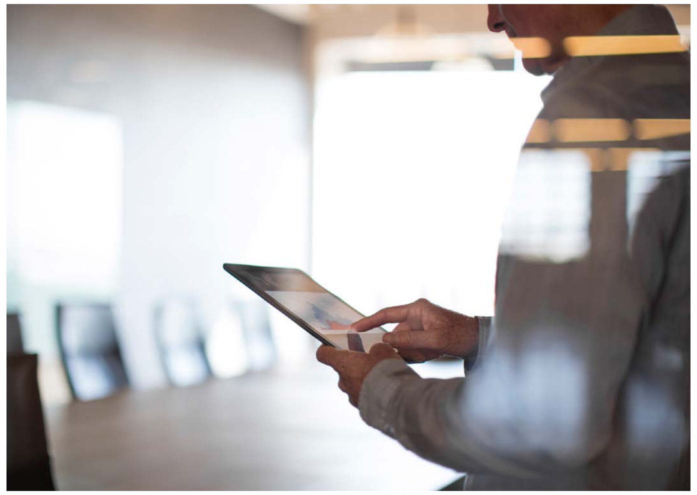
According to Green, recent security incidents illustrate how non-intrusive security controls can help agencies lower their costs of security and improve their overall risk score.

This January, when Apple announced a vulnerability in its iOS 14 operating system, Cisco and Duo used their security platform to immediately react to the announcement.

"In a matter of minutes, we set a policy change for all endpoints and devices accessing our network to get the iOS 14.4 update in no more than 48 hours if they wanted to continue to access our system," says Green.

With dynamic policies, it no longer matters if a user has a managed device or not. The policy dictates a course of action which the user can accept or ignore on their own terms. And simultaneously, CIOs and CISOs can establish an assurance of trust for devices connecting to the system based on the criteria they set.

> ❝ Finding the right security partner to work with is critical — not only a partner who can help with the problems of today, but in five or even 10 years from now. ❞
>
> **BART GREEN**
> *VP, State, Local and Education, Duo Security*



"For state and local agencies, if an employee or citizen is using their personal device, they don't want the government to have any insight or control into that phone, tablet or computer. With dynamic policies, agencies can be flexible, adaptable and reduce their risk as the world continues to change, and as bad actors find vulnerabilities in operating systems and devices," Green explains.

A MODERN SECURITY PLATFORM AND PARTNERSHIP

Public sector organizations don't have unlimited funds, support or personnel, but they still need a solution that will allow them to evolve the security tools as fluidly as their enterprise architecture evolves.

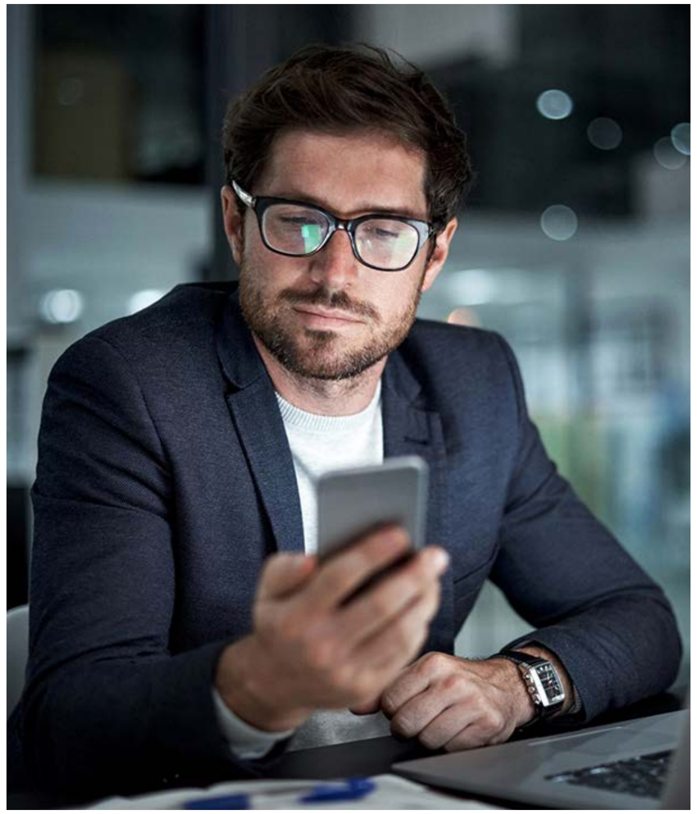
Duo's platform is an out-of-the box tool that allows agencies to establish stronger authentication and dynamic policy controls to prevent unauthorized access to both cloud-based and on-premises applications from any device.

With stronger security tools, CIOs and CISOs can make sure they are protecting all their data at different classifications, gain visibility across the network and establish trust in devices.

"It's not a simple step-by-step strategy," says Green. "Leaders need to break down the security strategy and document all their risk points that they have across all their applications."

Green recommends that leaders ask some of the following key questions to help in the document process to better define their strategy:

- How does my security solution protect my device?
- How does my security solution allow me to adapt and change with new security threats?
- Does my security solution protect my applications that may be on a mainframe, client server application, or cloud environment?
- How resilient is my security solution to provide flexibility and agility as my applications adapt to hybrid environments?



> ❝ When you don't have unlimited funds, when you don't have unlimited support or personnel to build and maintain your IT, you need to focus on what you actually have. ❞
>
> **WENDY NATHER**
> *Head of Advisory CISOs, Duo Security*

"Additionally, finding the right security partner to work with is critical — not only a partner who can help with the problems of today, but in five or even 10 years from now," says Green. "Cisco has a long history of being focused on its customers. We are addressing the same identity questions, the same security questions, the same zero trust questions as our government customers. We are dealing with our own complex environments which helps us as we develop world-class security solutions."

Learn more about how Duo Security, now part of Cisco, is enabling secure and compliant IT transformation for government agencies.

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

STATESCOOP

DUO