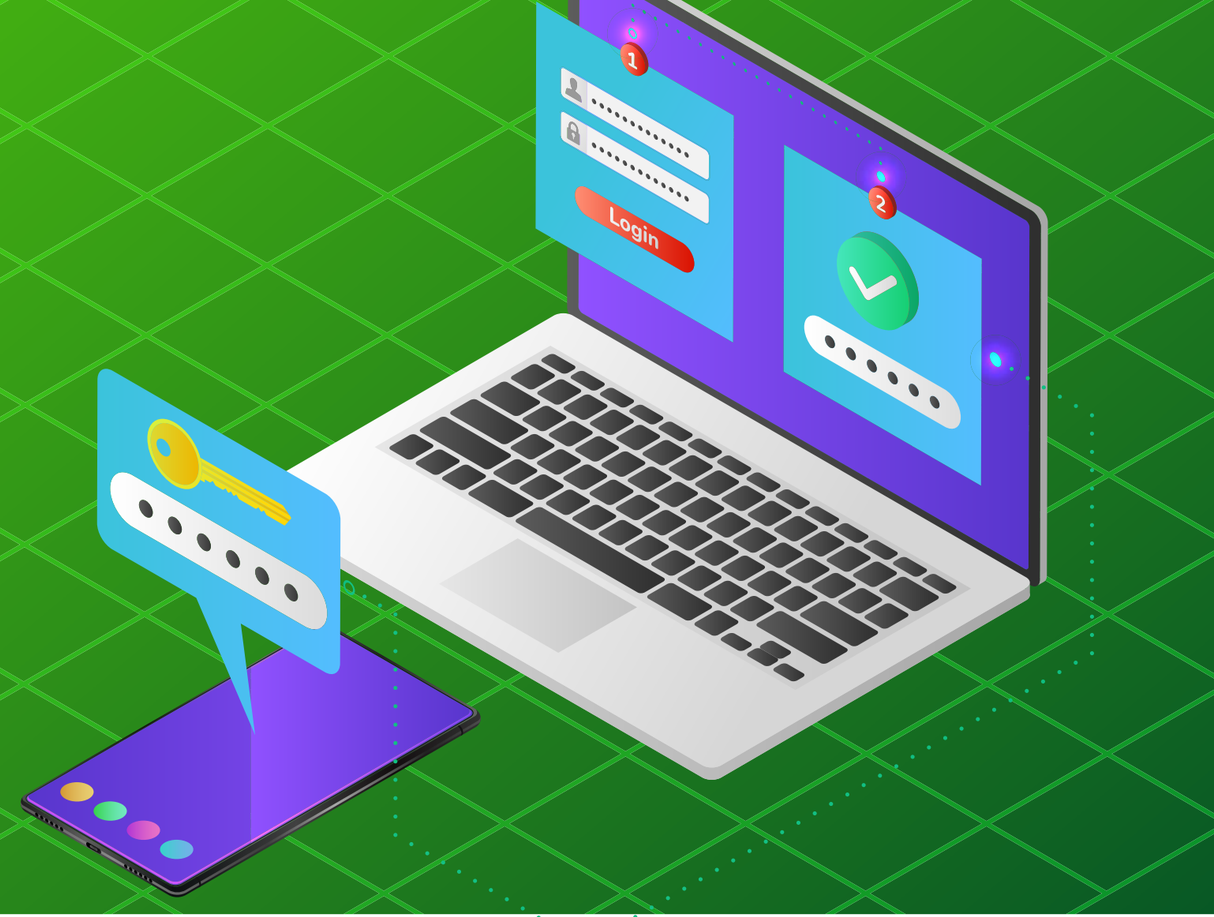
State Agencies Look to Multi-Factor Authentication to Augment Security

Login credentials, like user IDs and passwords, are ineffective on their own to protect against cyberattacks, leading IT leaders to move to stronger identity authentication technology.

By StateScoop Staff



State and local government agencies are well aware of the threats that ransomware and security breaches pose. Their concerns are expanding as election systems and voter registration databases represent increasingly attractive targets for attackers.

The rising number of attacks on state and local agencies have prompted IT leaders to prioritize protective measures and give increased attention to identity and access management controls and solutions such as two-factor authentication (2FA) or multi-factor authentication (MFA) that improve their security posture.

According to a recent Deloitte-NASCIO survey, 87% of state chief information security officers said that implementing an MFA solution was their top choice priority among ongoing identity and access management initiatives.

Security experts assert that today's 2FA and MFA authentication technologies are essential to provide stronger protections for agencies because they require users to verify their identity with secondary credentials. Agencies can also place greater limits on what information users can access in real time.

"State and local governments, which are still largely using username and password security measures, are most at risk to attack," says Dean Scontras, vice president, U.S. public sector for Duo Security. He cited a 2017 Verizon Data Breach report that found more than 80% of hacking related breaches were due to weak or stolen passwords.

And high-profile attacks, like those in Virginia, Maryland, Georgia, Florida and Texas that garnered national news coverage, have only highlighted the disruption to government services that breaches can cause and the costs to recover locked systems and data. While the causes of these breaches vary, their impact still signals the need for state agencies to better protect enterprise systems and access points.

Know who is on your system

Phishing campaigns continue to be one of the methods attackers used most frequently to gain access to user IDs and passwords. Additionally, with the availability of compromised password databases, and the low cost of brute force computing, attackers are not limited by their ability to guess at correct combinations, according to security experts.

"A lot of agencies are not using 2FA [or MFA], and that is the lowest hanging fruit that they can do in terms of their cybersecurity," says Sean Frazier, advisory CISO, public sector at Duo Security.

> **State and local governments, which are still largely using username and password security measures, are most at risk to attack.**
>
> **Dean Scontras**
> Vice President, US Public Sector
> Duo Security

Identity authentication isn't just another box to be checked in security, says Frazier. He points to established identity management practices detailed in the National Institute of Standards and Technology's (NIST) Cybersecurity Framework. Those practices include fully understanding what information the agency relies on and what level of security that information requires in order to protect, defend and mitigate cyber risk. The framework lists identity as one of five core functions agencies need to practice in order to manage their cybersecurity risk, which makes it imperative for agencies to implement identity and access management tools in their overall cybersecurity strategy.

"Part of [securing identity] is single sign-on, part of it is centralizing your identity systems. The other part is laying security on top of that with credential security, like 2FA," Frazier explains.

Multi-factor doesn't mean complicated authentication

The simplest way an organization can increase its assurance that an entity requesting access to a system is who, or what, they say they are is by using multiple forms of identity verification.

In the past, poor user experience was one barrier to adopting 2FA and MFA. Today, the wide adoption of smartphones has largely removed that barrier by allowing enterprises to execute push notifications for identity verification via applications.

But state and local agencies must serve a diverse population of users who may not have access to smartphones.

Since everyone may not be able to authenticate in the same way – for example, if a user doesn't have a smartphone – they still need a method through which to authenticate, says Bart Green, vice president for Duo Security's state, local and education markets. Duo's platform helps address that, by providing multiple options on how users can authenticate, such as using hardware tokens, SMS passcodes, bypass codes or biometrics, he said.

Two-factor and multifactor authentication require two different categories of credentials to verify a user's identity, such as:

SOMETHING THE USER KNOWS
Information that a user must be able to provide in order to log in

SOMETHING THE USER HAS
Such as an item in their possession in order to log in; i.e. security token, one-time password token, ID card

SOMETHING THE USER INHERENTLY IS
A biological trait the user has that are confirmed for login

THE USER'S LOCATION
Current location with an IP address or geolocation markers

TIME FACTORS
verification of the user's IDs against known working hours

"Modern tools such as Duo allow agencies to deliver the same user experience across all applications," says Green. "Duo's MFA solution adds a second layer of security to applications, but uses a single logon to give the user the ability to authenticate identity in the same manner, independent of what application they are trying to access."

An MFA solution ultimately gives federal agencies better assurance that only trusted users and trusted devices can access protected applications.

Duo is not only solving the issue of providing a single MFA solution, but we are solving it consistently across the entire organization...

Bart Green
Vice President, SLED
Duo Security

The benefits of an enterprisewide access security solution

Historically, the cost of integrating 2FA and MFA solutions has been an additional barrier for organizations. Fortunately, the adoption of cloud-based applications and platforms, and APIs, give agencies the ability to more rapidly integrate identity and access management (IAM) services with existing applications, without a heavy investment in setup and configuration.

Scontras explains that an enterprisewide access solution goes a long way toward "democratizing security," so anyone can use it and roll it out. This would help agencies reduce costs by lowering the volume of help desk trouble tickets due to password resets and by requiring minimal administrative resources for IT management.

Additionally, a solution like Duo MFA gives IT leaders the ability to fully manage user and device access controls. This opens up an opportunity to influence a holistic approach beyond MFA, including single sign-on (SSO), device trust or even adaptive authentication – the ability to use contextual factors such as user location, IP address ranges or devices security.

"Duo is not only solving the issue of providing a single MFA solution, but we are solving it consistently across the entire organization, with multiple easy ways to authenticate so you can get high adoption rates," Green says.

Getting Started

In the meantime, CIOs and CISOs should continue to lay the foundations of security modernization by:

1. Investigating where gaps exist in knowing exactly who, or what, is on their network and or where potential vulnerabilities exist.
2. Prioritizing strategies and investments to reduce if not eliminate those gaps.
3. Identifying which systems and processes require continuous monitoring and access controls and the means to establish more stringent access controls.

Additionally, Green encourages state and local agencies to start with Duo Security's "proof-of-concept" installation to learn the basics of administering 2FA. IT leaders can gain operational experience with the solution over a 45-day time period and see first-hand how it interacts with the organization's existing infrastructure.

"There is a wealth of MFA solutions in the market, but we can offer a single solution which works across all use cases," says Green.

Learn more about how Duo Security's MFA solutions can accelerate your agency's security strategy.

This StateScoop report was produced for, and sponsored by, Duo Security.

statescoop DUO