ZERO TRUST ACCESS

Trust-based access controls give state CIOs a powerful mechanism to deter cyberthreats

A surge of ransomware attacks is accelerating the need for state and local governments to deploy and secure modern identity and access management solutions.

By StateScoop Staff

State and municipal government officials don't like to talk about them. But the rising tide of ransomware attacks, and their ability to paralyze state and local government services, have created new urgency for public agencies to rethink their approach to controlling who or what can access IT resources and under which circumstances.

Recent ransomware attacks in Georgia, Maryland, Ohio, New York and Florida – in which attackers encrypted and held agency data hostage unless officials met attackers' demands – are part of a disturbing pattern of escalating cyberthreats, according to data from Recorded Future.

What the majority of these attacks share in common: compromised user credentials. Verizon's latest Data Breach Investigations Report for instance, found that 97 percent of IT attacks on public sector entities involved phishing tactics and 70 percent of these attacks succeeded in compromising user credentials.

Though public officials have generally remained resolute about not giving in to ransom demands, the more distributed nature of government IT systems often makes them easier targets for hackers. Even when governments hold the line on ransom demands, the costs of service interruptions and recoveries are proving nightmarish. Baltimore officials, for instance, estimate the total cost of the RobbinHood attack in May could top $18 million.

That's altering the risk calculus for public and private sector leaders alike. It's also why IT security professionals polled around the world ranked phishing, ransomware, account takeover attacks and malware as their top concerns for the third year in a row among a dozen leading cybersecurity threats, according to the latest Cyberthreat Defense Report.

Security is a must when adopting IAM solutions

State CIOs and security officers have hardly been idle in addressing the need for more robust identity and access management (IAM) and modern authentication controls. Thirty-three states have either established an enterprise IAM solution or plan to perform a product selection, according to the latest Deloitte-NASCIO Cybersecurity Study of state CIOs and CISOs.

Security is the most important reason for investing in IAM solutions, state IT officials say. However, they also see IAM solutions as a strategic lever to accomplish other priorities. For instance, 87 percent of state IT leaders in the Deloitte-NASCIO study said deploying a multifactor authentication (MFA) solution was a key initiative driving their IAM efforts. They also noted that IAM investments make it easier to modernize IT systems for digital transformation, increase operational efficiencies and improve the online experience of end-users, according to state IT leaders.

Their challenge, they say, is how to also deal with competing or higher priorities, funding constraints and the complexity of integrating modern IAM security solutions with legacy systems.

And there's the reality of managing and maintaining controls across a large, diverse and distributed user base, involving all kinds of devices.

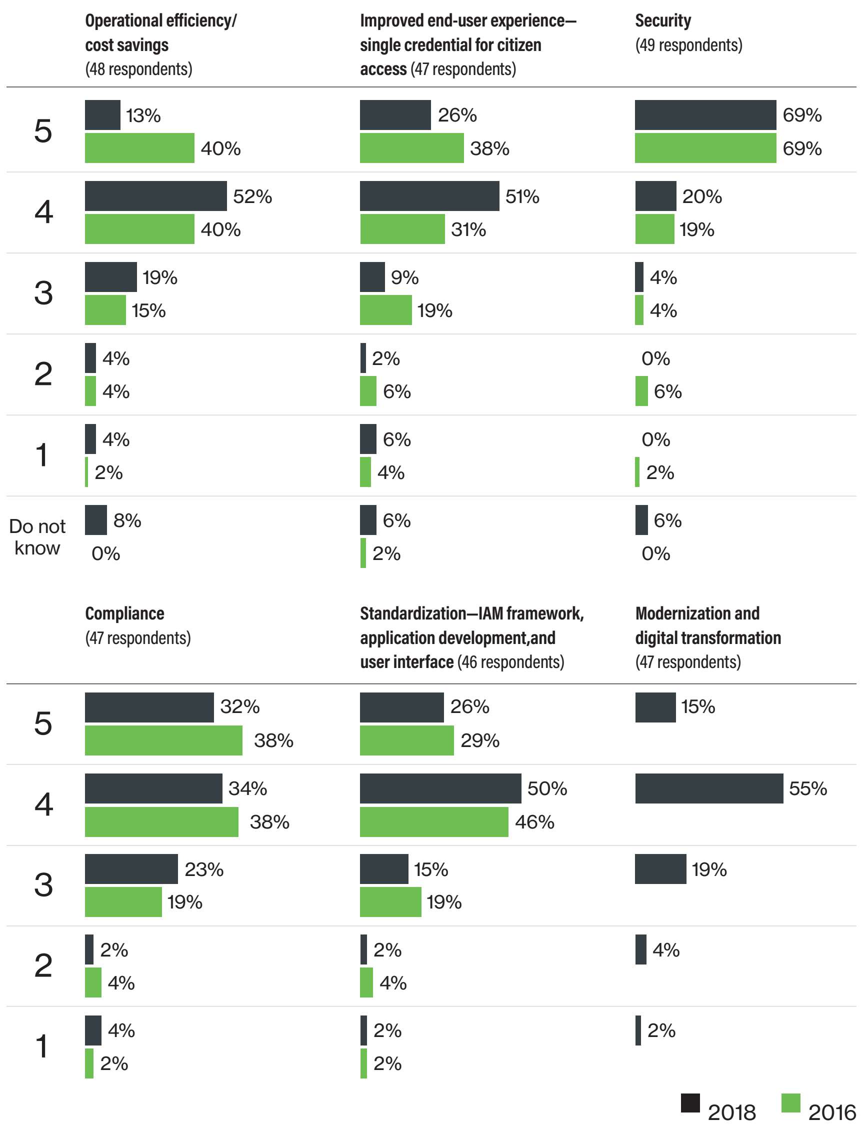
Getting serious about 'Zero Trust'

Security experts, however, point to a deeper challenge: Identities are no longer limited to people; they also represent devices, workloads, services, APIs and machines. That means control mechanisms capable of granting or blocking access privileges must extend beyond the confines of infrastructure, databases and network devices – and manage access to the cloud, DevOps automation, big data projects and potentially hundreds of containers or microservices and applications.

"The next big step is how do we get to 'zero trust' at an enterprise level as we move more towards cloud and mobile," says Sean Frazier, advisory CISO, public sector at Duo Security, a leading provider of trusted enterprise access solutions.

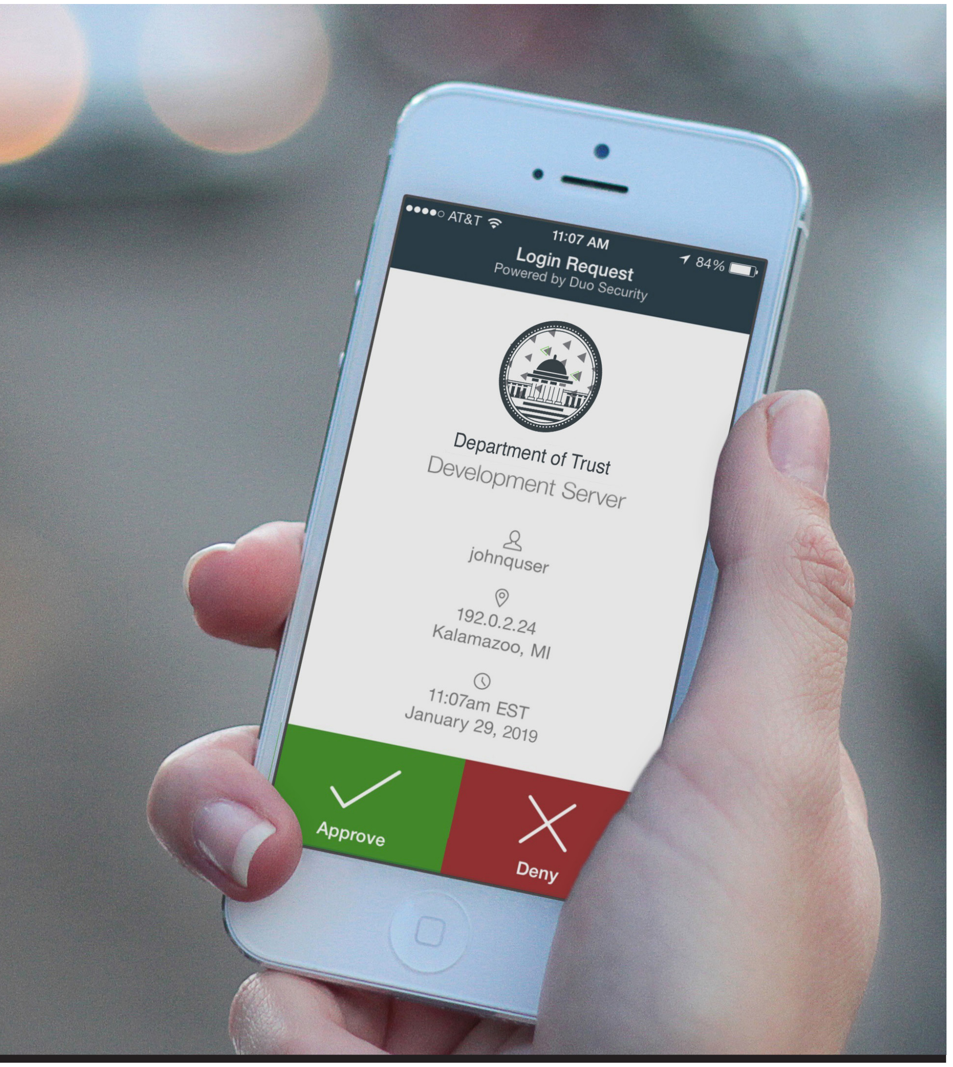
Security is the most important reason for making IAM investment decisions

On a scale of 1 to 5, how important are the following reasons to your IAM investment decisions? **(5 = most important, 1 = least important)**



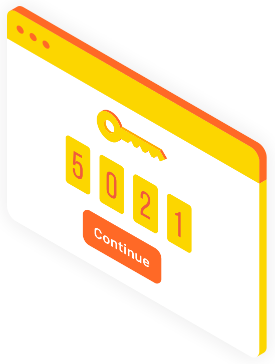
After security, state CIOs cite improved end-user experience and standardization among their top priorities when investing in IAM projects.

Source: *2016 and 2018 Deloitte-NASCIO Cybersecurity Studies.*



"That ultimately means replacing piecemeal IAM applications with a modern, centralized approach, capable of managing multifactor authentication and access control at an enterprise level," he says. Among other capabilities, Frazier suggests agencies begin investing in solutions that can:

- Verify who or what is requesting access, using strong multifactor authentication.
- Evaluate the trustworthiness of every device, application and workload accessing your environment.
- Define and enforce adaptive and contextual access policies, granting "least privilege access" as appropriate across your IT environment for each access request.
- Enable secure connections and deploy access proxies (APIs) to all applications.
- Audit user and device activity, leveraging analytic tools to detect anomalies.



Democratizing security

The other factor essential to getting to enterprisewide zero trust is making it simple to roll out and reliable for users across your entire IT operating environment, says Dean Scontras, vice president for public sector business at Duo Security.

"When it is easy to roll out, you increase the participation pool, effectively democratizing security," he says. "You want everyone to enroll in MFA without a lot of difficulties along the way. Once you start using a centralized system, it is the same workflow and authentication process for every application – on-prem and in the cloud."

"Getting everyone involved in the security conversation," adds Frazier, "means, one, you don't scare away users, by making it easy and transparent to do their job, and two, you don't scare away developers from integrating security."

Deploying a centralized access management solution with multifactor authentication not only lowers the total cost of ownership across all your IT systems, it also puts state and local government agencies in a stronger position to embrace emerging standards aimed at improving security, Frazier says.

Emerging authentication standards

"One of the most important things going forward is being able to leverage biometric sensors for doing multi-factor authentication," he says.

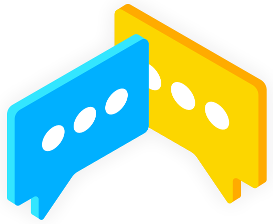
He points to efforts by the FIDO alliance and a consortium of leading technology vendors to develop the Web Authentication API, known as WebAuthn, that takes advantage of public-key cryptography and biometric sensors built into users' devices to authenticate users.

The goal of WebAuthn specifications, which have been ratified by the World Wide Web Consortium (W3C), is to replace the reliance on passwords altogether, he says, as well as a "mish-mosh" of smart cards and other tokens that state and local governments have cobbled together over the years to control access to their IT systems.

"We've already rolled out early adoption capabilities with Chrome browsers on MacOS and will expect to see proofs of concept on other platforms accelerate over the next year. I fully anticipate wide adoption of this standard in the next 12-18 months," said Frazier. "This is the future," he added. "It provides a common language which will allow a lot of different technology companies, like us, and just about everybody else, to integrate (IAM protocols) even more effectively than we can today."

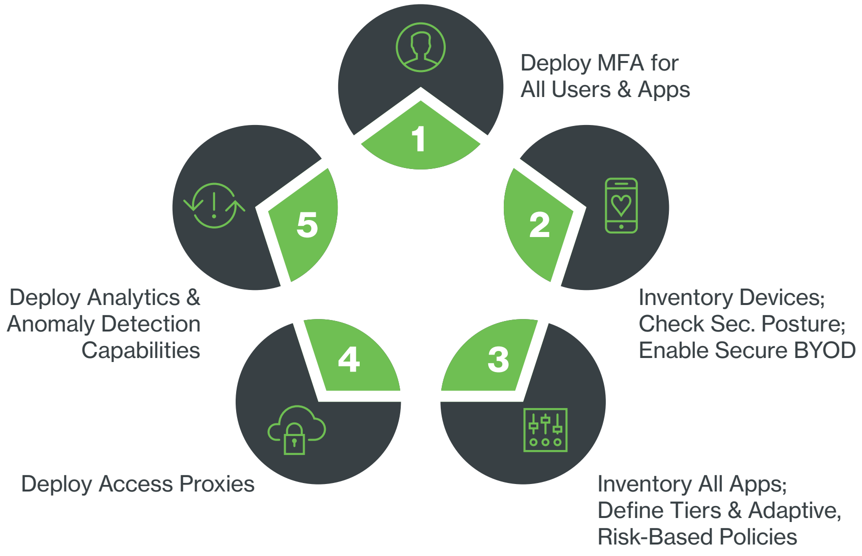
Getting started

In the meantime, Frazier encourages state and local agencies to continue laying the groundwork for deploying a centralized IAM security solution that can manage access controls across multiple IT environments and that also supports compliance with multiple regulations. Duo Security's platform, for instance, meets a variety of compliance regulations, including PCI-DSS, HIPAA, CJIS, NIST SP 800-171 and ISO 27001. And the company says FedRAMP approval is imminent.



> **"The next big step is how do we get to 'zero trust' at an enterprise level as we move more towards cloud and mobile"**
>
> **Sean Frazier**
> Advisory Chief Information Security Officer
> Duo Security

Zero Trust is an approach, not a product, that begins with a 5-step process.



1
Deploy MFA for All Users & Apps
2
Inventory Devices; Check Sec. Posture; Enable Secure BYOD
3
Inventory All Apps; Define Tiers & Adaptive, Risk-Based Policies
4
Deploy Access Proxies
5
Deploy Analytics & Anomaly Detection Capabilities

__Source:__ 2016 and 2018 Deloitte-NASCIO Cybersecurity Studies.

When implementing MFA, he also recommends agencies enforce National Institute for Standards and Technology (NIST) authentication assurance levels 2 and 3 (defined in NIST Special Publication 800-63-3.)

But he ultimately urges state and municipal governments to truly embrace enterprisewide zero trust access, taking prescribed steps to:

1. Deploy multifactor authentication for all users and applications.
2. Inventory devices. Check their security posture. Enable secure BYOD.
3. Inventory all applications. Define tiers and adaptive, risk-based policies.
4. Deploy access proxies.
5. Deploy analytics and anomaly detection capabilities.

As long as humans are one click away from opening a deceptive email or web application, hackers will keep trying to exploit users' credentials. The good news for state and local government officials is, the tools now exist to make it significantly harder and more costly for hackers to gain access to government's most exploitable assets. ■

Learn more on how Duo Security can help your agency achieve enterprise-wide Zero Trust Access.

DUO

statescoop