Modernizing Authentication in State and Local Government with Hardware-Based MFA

The massive shift to remote work has led to what some experts have referred to as a "cyber pandemic" in state and local government.[1]

Hindered by legacy systems, budget constraints and business processes driven by in-person interactions, many organizations were not prepared for the significant cybersecurity challenges that confronted them during the pandemic, especially regarding strong employee authentication.

State and local governments have traditionally relied on username and password-based authentication. Some agencies have adopted mobile-based multi-factor authentication (MFA), but this may not be the strongest form of MFA, especially for privileged users and administrators.

There are also many employees who can't, don't or won't use mobile devices for MFA because they don't have a smartphone or live in low-connectivity areas. Employees may also balk at the idea of allowing admin access to their personal devices, or compliance issues or union restrictions may actually prohibit using personal mobile devices for work. This creates gaps in governments' security posture and further increases the risk of account takeovers. What's more, mobile-based MFA isn't cost-effective for governments because they must reimburse employees for mobile-related costs.

To ensure 100 percent MFA, state and local governments should consider hardware-based security keys. These are physical, one-touch authentication devices users can input into their computers or tap against their mobile phones to access critical systems and applications. Hardware security keys such as the YubiKey from Yubico are phishing-resistant and help eliminate account takeovers. They're also user-friendly, cost-effective and can serve as a critical enabler of a zero trust security architecture, allowing governments to challenge a user with simple, one-touch authentication when policy dictates the security posture of a user be reaffirmed.

"In today's extremely diverse, large, highly complex and dynamic operating environment, the state of Georgia requires a holistic cybersecurity strategy, one that doesn't rely solely on the individual end user or software-based solutions," says Dean Johnson, the chief operating officer of the Georgia Technology Authority (GTA).

As state and local governments modernize service delivery, a hardware-based MFA solution can help them strengthen enterprise security in three critical areas: remote work, connectivity, and infrastructure and process modernization.

Current Challenges

Remote work and the disruptions of the past year have led to several security challenges for governments.

Employees' homes and devices have become the new perimeter, and usernames and passwords don't offer the robust security defenses governments need in this new work-from-home environment. To strengthen security, state and local governments have had to rapidly switch to 100 percent MFA to obtain more comprehensive coverage.

"Everybody used to work within their own walls, so they were protected," says Frank Snyder, sales leader for the state, local and education markets at Yubico, a leading provider of hardware-based authentication solutions for the public sector. "Now, everybody is trying to come in the front door one at a time. It's just much more complicated. And they have to continuously authenticate to get in, so governments need 100 percent coverage."

Resource constraints, technology silos and an evolving threat landscape also hinder governments. Company-issued devices are often more secure than employees' personal devices, but smaller local governments may not have the resources to provide them. Many governments also still rely on disparate identity platforms, which makes access management more challenging and prevents governments from having complete control and visibility into their security infrastructure.

> **"When governments are looking for an MFA solution, they need one that's like a Swiss Army knife that can handle their legacy applications as well as modern connections."**
>
> Frank Snyder, Yuibico Sales Leader for State, Local and Education

State and local governments are confronting all these challenges at a time when hackers have increasingly targeted these organizations. In 2020, cyberattacks on state and local governments increased 50 percent.[2] These attacks weren't just relegated to software and IT systems. Operational technologies like SCADA systems and air-gapped systems have become prime targets for hackers, too — especially when they're connected to cloud-based monitoring applications.

While governments have turned to a variety of authentication solutions to increase security, many of these solutions are software-based, which can create additional security vulnerabilities. Hardware-based security keys, on the other hand, offer several benefits in terms of more robust security, a better user experience, cost efficiency and authentication modernization.

The Benefits of Hardware-Based MFA

Securing Remote Work and Enhancing Connectivity

As more government organizations embrace hybrid work environments, they'll need to create a secure remote work infrastructure.

Hardware-based security keys offer a range of capabilities to help them achieve this. First, they're typically compatible with some of the leading identity and access management systems, including Microsoft, Okta, Duo Security and Ping. These devices can be connected to multiple identity systems, offering governments more flexibility and scalability. A hardware-based MFA also relies on modern FIDO U2F and FIDO2 authentication protocols that provide strong two-factor and multi-factor authentication; gives users the option to go passwordless; and helps organizations combat phishing attacks because credentials can't be shared across systems, devices or users. This approach also helps reduce man-in-the-middle attacks in which a hacker eavesdrops or alters communications between two parties.

Hardware-based MFA reduces the security risks associated with employees using their personal devices and recycling the same password across their personal and business accounts. The solution also reduces BYOD-related reimbursement expenses for governments.

"A hardware security key wins on a usability standpoint because it's purpose-built for authentication. It has that sole purpose, whereas phones have too many features and apps loaded on to them," says Cody Hussey, a solutions engineer at Yubico. "There's just so much more than could go wrong."

Hardware-based MFA has other usability advantages, as well. Like many organizations, governments are filled with workers from different age groups who have a range of technical abilities. A hardware-based security key levels the playing field because it's as simple as a single touch or the tap of a key.

In terms of connectivity, hardware-based MFA can extend the capabilities of security solutions such as a VPN, which many governments implemented as a stopgap in the beginning of the pandemic. Though many organizations continue to use VPNs, the quality of these solutions vary by provider and may not offer the highest levels of encryption. As governments adopt a cloud or hybrid cloud infrastructure to support remote connectivity, a hardware-based MFA solution can serve as an effective second authentication layer for a host of digital workplace collaboration tools, including videoconferencing and email applications.

For those reasons and more, the state of Georgia selected Yubico to provide hardware MFA services.

"Given the varied regulatory requirements that state agencies are required to comply with, the GTA views Yubico's hardware security option, Yubikey, as vital to helping protect mission-critical systems and state data from both external and internal threats, while at the same time doing so in a very cost-effective way," Johnson says.

"The Yubikey solution brings multiple benefits to state agencies. It provides greater security than mobile authenticators: The physical device prevents 100 percent of account takeovers which is the threshold that GTA was targeting."

Driving Infrastructure and Process Modernization

Many of the same capabilities that make hardware security keys so beneficial for remote work also make them optimal for infrastructure and process modernization within state and local government.

Relying on newer FIDO authentication protocols enables strong authentication across legacy and modern infrastructures and applications that facilitate citizen-facing digital services. This is crucial for budget-strapped governments that may not yet have the resources to rip and replace legacy systems or prefer to operate in a hybrid cloud environment for the long term.

In 2020, cyberattacks on state and local governments increased 50 percent. These attacks weren't just relegated to software and IT systems. Operational technologies have become prime targets for hackers, too.

"When governments are looking for an MFA solution, they need one that's like a Swiss Army knife that can handle their legacy applications as well as modern connections," Snyder says.

Hussey adds that as governments modernize, it's critical for them to shift their security mindset.

"As governments move toward modern infrastructure, more streamlined processes and methods of tackling projects with cloud technologies, they've realized that modern authentication is needed to protect those resources," he says. "It's now important for organizations to move away from a network perimeter as their main means of security and move towards identity as the new perimeter, especially with a modern zero trust architecture."

A Roadmap for the Future

As state and local governments work to strengthen enterprise security, they should keep the following best practices in mind:

Think long term. Governments should consider their near-term operational goals and long-term initiatives as they assess MFA solutions — whether they plan to permanently adopt a hybrid work model, launch more self-service applications or digitize the majority of citizen services. The right MFA solution should be future-proofed to meet evolving needs and should authenticate across all platforms.

"The solution should be ubiquitous," says Michael Santini, a sales leader for the state, local and education markets at Yubico. "You shouldn't have to redo your infrastructure, undergo a massive overhaul or engage in a massive spend to implement stronger authentication."

Focus on strong authentication. While any MFA solution is better than no MFA, not all are created equal. For the greatest levels of protection, governments need to deploy strong authentication using phishing-resistant hardware security keys to stop account takeovers.

Focus on usability. User experience can make or break adoption, so the solution should not require a steep learning curve for employees to use it effectively. In a remote environment, this is especially critical to ensure compliance and greater endpoint security.

That was an especially important factor for Georgia in adopting the Yubikey solution, says Johnson.

"A big selling point for GTA was the fact that the hardware solution does not need network connectivity to be functional. A large number of the state agencies operate across Georgia's 159 counties. Many of these agency sites are in very remote, rural geographies where maintaining a consistent network connection all of the time can be virtually impossible. Having ease of access to a Yubikey device that facilitates functionality regardless of where the end user is located is significant."

Collaborate with the right partner. A provider and an organization should share the same long-term vision, both for technology and for the partnership itself. The provider's vision and products also should align with federal cybersecurity guidance and priorities, such as NIST 800-207, which provides a framework for establishing a zero-trust architecture.

> **"The GTA views Yubico's hardware security option, Yubikey, as vital to helping protect mission-critical systems and state data from both external and internal threats."**
>
> Dean Johnson, Chief Operating Officer
> of the Georgia Technology Authority

Snyder says the threat landscape has changed so much that modern authentication is no longer just about software. Something supposedly as analog as physical security has become just as critical to creating a modern, multifaceted security architecture that thwarts hackers.

"Because modern hackers have gotten so sophisticated, your endpoint security measures have got to involve human interaction, a human gesture," Snyder says. "There has to be proof there's a human on the other side of that authentication. And the only way to do that is with a hardware token."

In Georgia, Johnson says, hardware MFA keys have already become an important part of the state's overall cybersecurity strategy.

"The use of Yubikeys, along with other approved MFA methods, the use of complex passwords, and regular end-user security awareness training help ensure the state of Georgia can maintain a high degree of confidence that our end users and the state's data are being properly secured."

This paper was written and produced by the Government Technology Content Studio, with information and input from Yubico.

Endnotes:
[1] https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html
[2] https://gcn.com/articles/2020/09/04/cyberattacks-state-local-government-climbing.aspx

Produced by: government technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education. **www.govtech.com**

For: yubico

Yubico puts an end to account takeovers for businesses and individuals. The YubiKey — the world's #1 hardware-based security key — is the most secure, easy-to-use, and affordable multi-factor authentication. The world's largest governments, technology companies, and financial institutions trust Yubico to secure their most important information, accounts, and applications. **Learn more at www.yubico.com**

IMAGES PROVIDED BY SHUTTERSTOCK.COM