yubico

PARTNER WITH YUBICO TO GO PASSWORDLESS

Rethinking cybersecurity across state and local government

State and local governments around the world are deploying modern authentication using hardware-backed passkeys

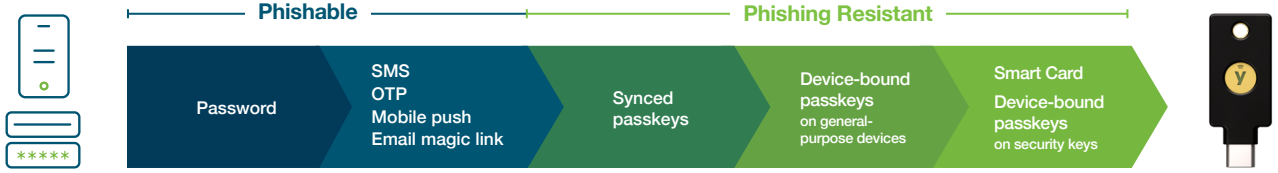
The urgency to harden cybersecurity defenses across state, local, territorial and tribal governments

State, local, tribal and territorial (SLTT) governments are increasingly the target for cyber attacks due to highly sensitive information they hold and critical services they provide. Cyber attacks that utilize weaponized artificial intelligence (AI) to steal user credentials are on the rise and can be highly successful. These can take various forms, such as phishing emails, malware, ransomware, or even social engineering techniques, highly crafted to the target user. With cyber threats evolving, legacy authentication methods are no longer sufficient and agencies need to rethink their cybersecurity postures.

Not all MFA is created equal

While any multi-factor authentication (MFA) is better than a username and password alone, not all forms of MFA are created equal. Legacy mobile-based authentication such as SMS, OTP codes, and push notifications are highly susceptible to phishing attacks, malware, SIM swaps, and attacker-in-the-middle attacks. Mobile-based authenticators create high-risk security gaps in an agency's MFA strategy, when users can't, don't, or won't use mobile authentication due to union restrictions, personal preferences, mobile-restricted locations, financial reasons and more. Additionally, employers may be required to reimburse employees for using personal cell phones for business purposes. Or alternately, are required to purchase and provide work phones and telecom services for employees, both of which can be expensive. Legacy MFA may also increase cyber insurance premiums or reduce payouts. Phishing-resistant multi-factor and passwordless authentication is the need of the hour.

According to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-B4, only two forms of authentication currently meet the mark for phishing-resistant MFA: Smart Card/PIV and the modern FIDO2/ WebAuthn authentication standard.



The YubiKey

A pioneer in modern, hardware-based authentication and Yubico's flagship product, the YubiKey is designed to meet you where you are on your authentication journey by supporting a broad range of authentication protocols, including FIDO U2F, WebAuthn/FIDO2 (passkeys), OTP/TOTP, OpenPGP and Smart Card/PIV.

yubi.co/key

YubiKey as a Service

Get peace of mind in an uncertain world with a YubiKey subscription service that makes supporting new hires, tackling employee turnover and securing remote/ hybrid workers fast, flexible and future-proofed—all with a lower cost to entry.

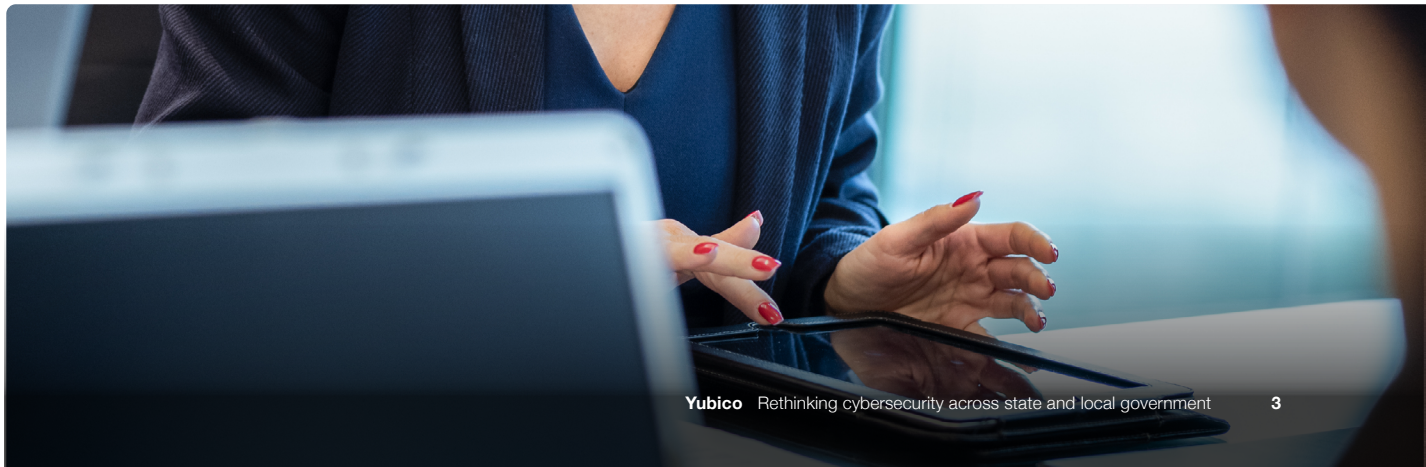
This service provides priority customer support, ease of form factor selection, backup key discounts, and replacement stock benefits.

yubi.co/subscription

YubiEnterprise Delivery

Accelerate your journey to phishing-resistant MFA with an end-to-end domestic and international YubiKey delivery service. Let Yubico and our global partners worry about the logistics so you can focus on bigger business issues.

yubi.co/delivery



Advancing Zero Trust and passwordless at the City of Southgate

The City of Southgate, Michigan is a municipal government that supports a population of just over 30,000 residents and is a growing business community that's a part of the Downriver fellowship of communities south of Detroit.

In the past ten years, private and public sector organizations alike have faced increased levels of cyber attacks, including phishing and ransomware. For public sector organizations such as the City of Southgate, who provide critical utilities as well as police, fire and civil services, these attacks threaten both citizen data and critical infrastructure.

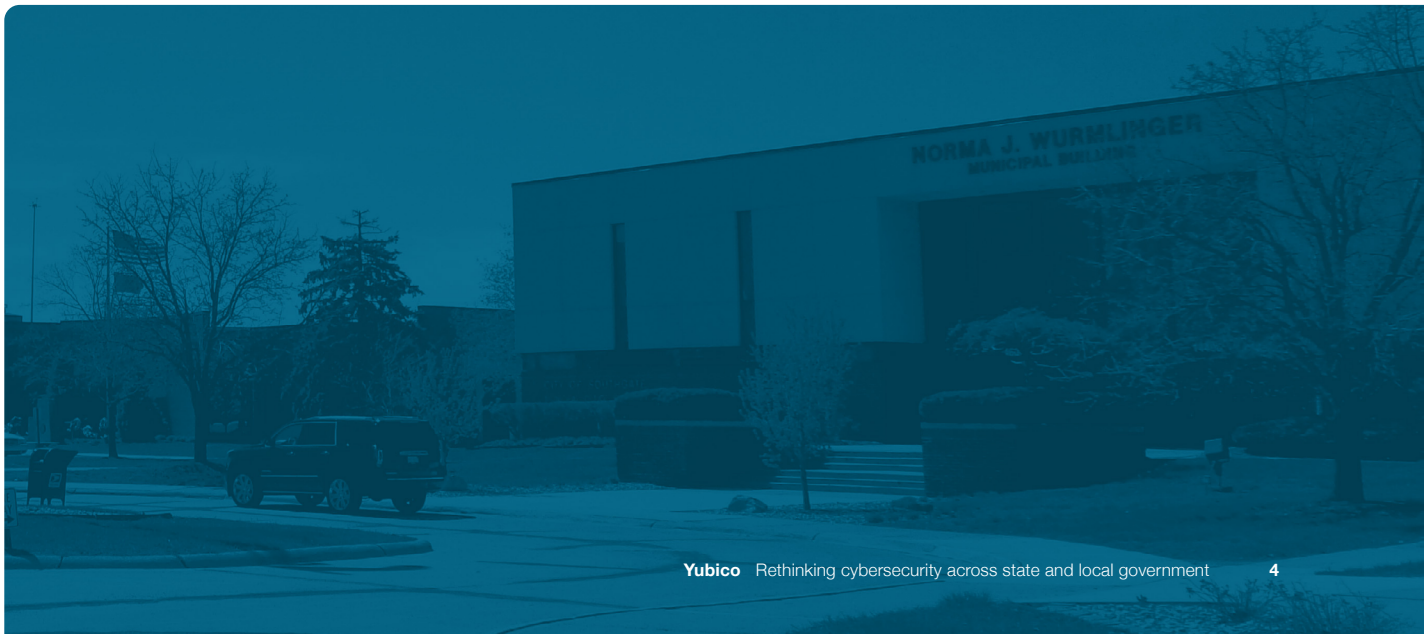
The City of Southgate executed a cybersecurity strategy that combines the YubiKey with Microsoft Entra certificate-based authentication to help achieve a compliance level that's ahead of federal mandates such as CJIS, OMB M-22-09, EO 14028 and PCI DSS, placing them in the top 1% across the public sector.

The City of Southgate's cybersecurity plan hardens the fortress walls, including upgrades to city networking infrastructure, Microsoft Entra certificate-based authentication (CBA), and the YubiKey 5 FIPS Series, a FIPS 140-2 validated hardware-based solution that supports multiple authentication and cryptographic protocols including FIDO2 (passkeys) and Smart Card/PIV to protect access to computers, networks and online services.

READ THE CASE STUDY

> "By moving to passwordless, you're eliminating the forgetfulness of users. You don't have to worry about them getting locked out, writing passwords on a piece of paper, or falling prey to a phishing attack. You remove the human element. Everyone wants to know, 'well, what do you do?' and I say 'Well, I just use YubiKey and it's easy."

Jason Rucker
Director of IT
City of Southgate



Landeshauptstadt
München
IT-Referat

YubiKeys securing City of Munich's digital future

> "You cannot access anything from outside our own network without the YubiKey as a second strong factor… We wanted phishing-resistant two-factor authentication: FIDO2."

Matthias Wagner
IT Architect & Director
Cybersecurity Center
City of Munich

As Germany's third largest city by population, the City of Munich's various departments oversee education, healthcare, transportation, social support and other critical services and infrastructure for over 1.5 million residents.

As part of their 2018 market research on the realignment of their MFA strategy, the City of Munich began vetting manufacturers of FIDO2 hardware keys that would allow a smooth migration for the city's legacy processes. They also needed a key that worked with their multifaceted setup: an identity management system in the backend, a Windows domain with Active Directory, and a Single Sign On (SSO) endpoint. As a result, they did a comprehensive analysis of the vendor landscape, arrived at Yubico through various channels as part of manufacturer meetings, and determined that the YubiKey looked solid.

A traditional username and password provide the first layer of security, while the YubiKey provides foolproof assurance that the user is who they claim to be. The city's centralized IDP ensures that all users have a consistent login experience for all the applications and IT services they require to perform their roles. This has improved user experience and bolstered the acceptance of the YubiKey among city staff.

READ THE CASE STUDY

Government of Nunavut turns to phishing-resistant Yubikeys after ransomware attack

In November 2019, the Government of Nunavut was the victim of a sophisticated spear phishing attack, which ultimately led to ransomware that took down critical servers, phone lines, and applications. The Government of Nunavut looked to rebuild their infrastructure and regain trust by leveraging Microsoft's Azure Active Directory (Azure AD) and M365 solutions. Protecting identities and access to applications and services became the top priority. The Government of Nunavut rebuilt their network over the course of six weeks, and began to look for additional security measures to protect user identities and credentials.

Due to inconsistent cellular networks across Nunavut communities and the constant threat of phishing attacks, the Microsoft Detection and Response (DART) security team recommended Yubico's phishing-resistant multi-factor authenticator (MFA) called the YubiKey. The YubiKey is a hardware security key that requires no network connection, no power source, and no client software. These factors made the YubiKey easy-to-use in extreme and inconsistent environments, while also significantly reducing phishing attack vectors.

Nunavut's healthcare organizations, education system, and first responders all had various Windows-based systems which used different authentication protocols. While this normally would increase complexity and cost, the YubiKey's multi-protocol functionality allowed government employees to use a single YubiKey to authenticate in their existing systems as a smart card as well as in modern cloud-based systems using the passwordless FIDO2 protocol, which was pioneered by Yubico and Microsoft.

READ THE CASE STUDY

> "The YubiKey is the ideal 'bridge to passwordless' solution. We are able to provide our staff with phishing-resistant hardware authentication in the traditional environments, while also enabling the transition to passwordless workstation logins within Azure AD across all of Nunavut."

Martin Joy
Director Information
& Communications Technology
Government of Nunavat

michigan
child support

The Michigan Office of Child Support secures and streamlines access to state-wide systems with the YubiKey

The State of Michigan's Office of Child Support (OCS) is a critical lifeline for families because it establishes, enforces, and distributes child support payments throughout the state and helps parents establish a financial partnership through structured child support.

The catalyst for change was OCS' transition from an on-premise SharePoint platform to a cloud-based solution that required multi-factor authentication (MFA). OCS needed a solution that could accommodate a wide range of needs without overwhelming users. Many OCS users were unfamiliar with MFA altogether, and some county-managed offices had restrictions on the use of personal devices, which limited the MFA options available to them.

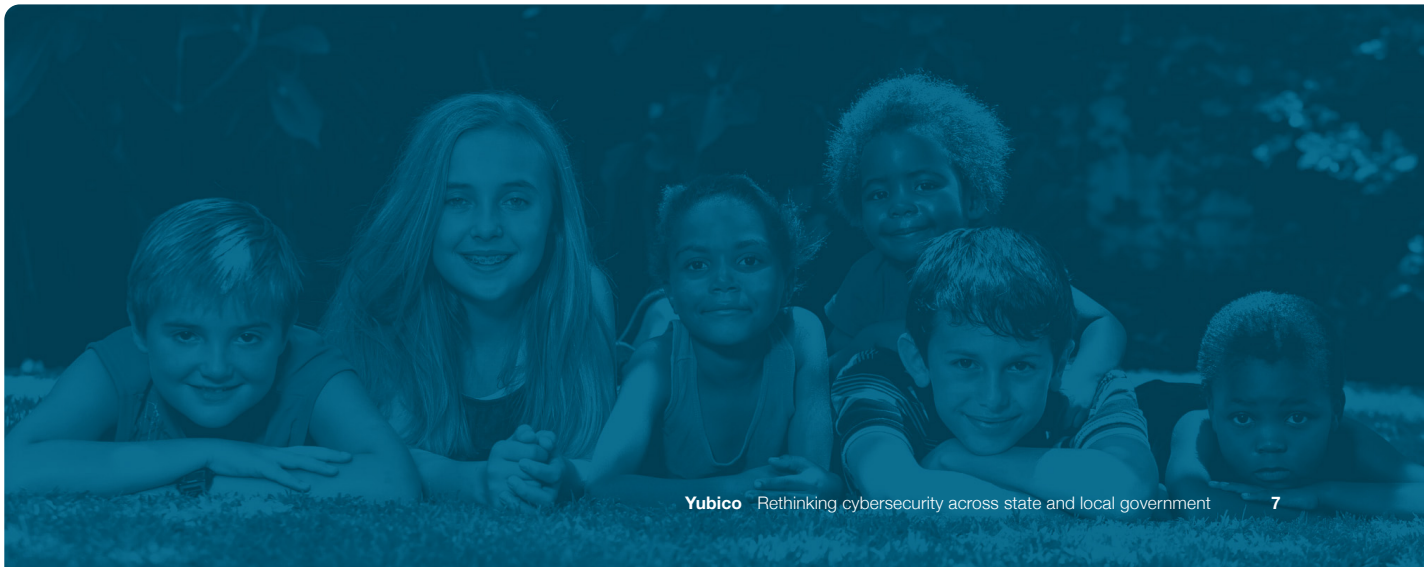
All of the challenges made the goal crystal clear: implement a solution that would work across these varying environments, that also maintained the highest security standards, that would also be incredibly user-friendly.

To make adoption just as seamless, OCS developed much of its rollout plan from Yubico's documented best practices and insights from their Customer Success Manager. OCS started with an initial activation of internal champions, followed by a rollout to statewide users.

READ THE CASE STUDY

> "Sometimes not hearing anything is good. What I have heard has been positive, they're using the keys. We've had some thank yous, specifically from IT people saying 'Thank you for helping us,' or little emails, things like that. But I think no news is probably the best news."

Menny Marlat
Help Desk Manager
OCS



City of SACRAMENTO

Building a more secure remote work infrastructure at City of Sacramento

> "The biggest benefit is that you don't have to use your phone and wait for that phone call or wait for that text message with the OTP. This is such a simpler solution where I just plug it in, tap the button and I'm done."

Curtis Chiuu
Principal Systems Engineer
City of Sacramento

Remote work can introduce new security risks with employees using potentially unsecured home-based WiFi networks. Even if remote employees use a virtual private network (VPN), they might still connect unauthorized personal devices or apps to this network, which jeopardizes security for the agency.

To strengthen authentication security across their remote work environment, the City of Sacramento implemented the YubiKey. Previously, the city relied on a mobile-based voice and text OTP for authenticating employees. But that approach became a challenge once more employees had to work remotely as not every employee had a government-issued mobile device.

Sacramento had previously adopted the YubiKey for a smaller number of remote employees who needed access to critical infrastructure, as well as for field workers who didn't have access to government-issued mobile devices. But with one-third of its workforce remote during COVID-19, the city needed to leverage the solution more broadly to ensure secure VPN connectivity and application access for remote employees.

Hardware-based MFA eliminates device-based authentication and bring your own device (BYOD)-related reimbursement expenses. Each employee also gets their own key, which also helps protect data at shared workstations. All these capabilities are critical as government organizations like Sacramento shift to a hybrid work environment.

READ THE CASE STUDY

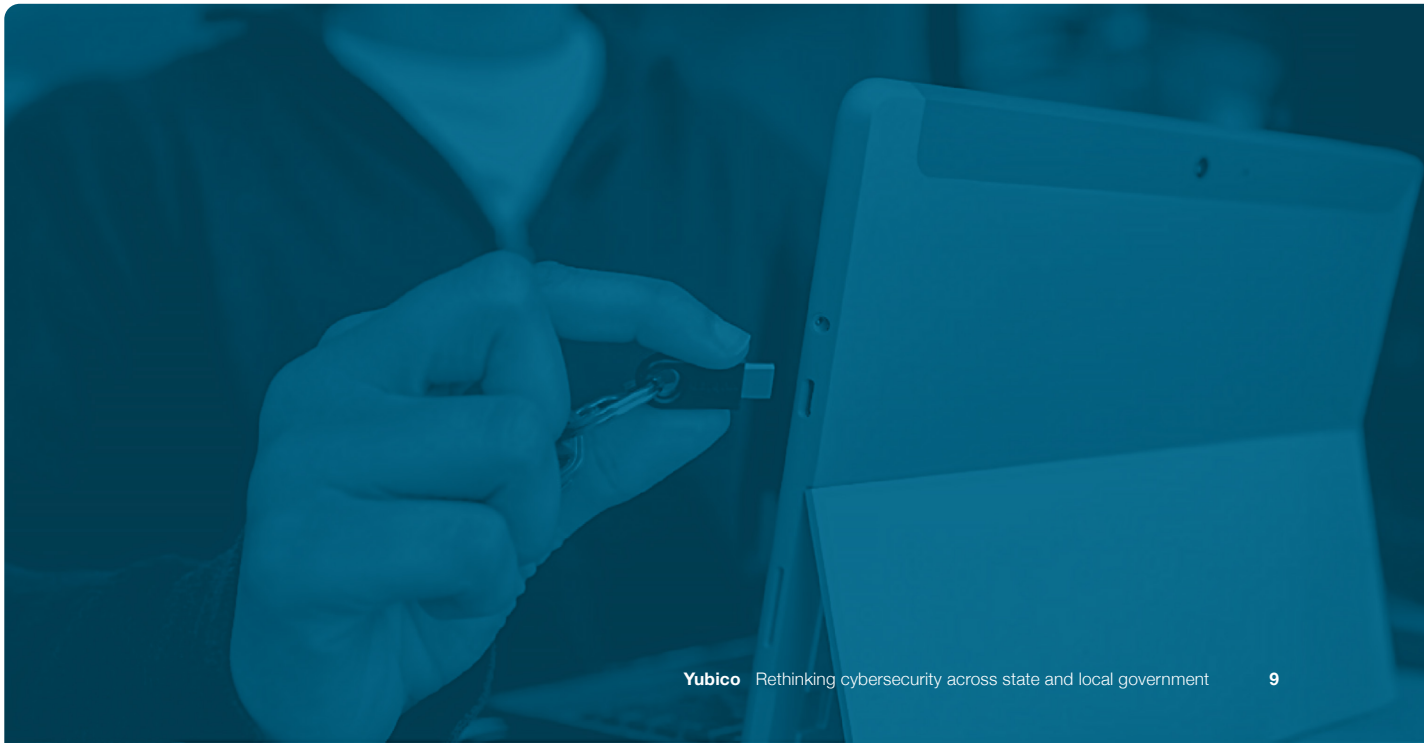
Modernizing authentication across State of Georgia

> 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."
>
> **Georgia Technology Authority**

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.

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.

READ THE CASE STUDY



MISSION VIEJO
Make Living Your Mission

Enhancing security for digital services at Mission Viejo

The city of Mission Viejo has embraced digital services, allowing constituents to report complaints and submit service requests to different departments, attend virtual meetings and access city records online. The city even has its own mobile app—the MV Life App—that provides timely updates and allows citizens to report public safety issues. These and other digital services involve collecting citizen data and reviewing it on the back end, which means employees must have secure access to systems—whether they're in the office or working remotely. The city previously relied on complex password requirements for authentication, but decided to adopt a hardware security key-based MFA solution to strengthen its security posture.

The city deployed hardware security key-based MFA using the YubiKey across 12 different locations, including its library and community center. All of its departments are required to use the solution to log in. YubiKeys help the city meet high security standards, but it's also more cost effective compared to other MFA solutions. And because it doesn't require password changes as often, it provides a more frictionless experience for government employees.

READ THE CASE STUDY

"We have seen several attacks against user accounts, but they've been unsuccessful. If you're not using MFA, you must find the budget to adopt this solution. It adds a much-needed layer of protection and provides protection against password exploitation."

Jackie Alexander
Director of IT
Mission Viejo

The path to passwordless

No matter where you are on your MFA journey, we'll meet you there. You can accelerate your zero trust approach and gain a bridge to a passwordless future. With a tried and true process that many state and local governments have followed already—and with a 'YubiKey as a Service' model—it's not a matter of if you'll be successful but when you'll be successful in raising your bar for security with modern, hardware-backed passkeys such as the YubiKey.

Plan

Ensure readiness by clarifying use cases and user populations

Validate

Confirm the process with a small group of users before broader rollout

Integrate

Ensure key apps and services are YubiKey-ready

Launch

Distribute keys to users with turnkey delivery services or channel partners

Adopt

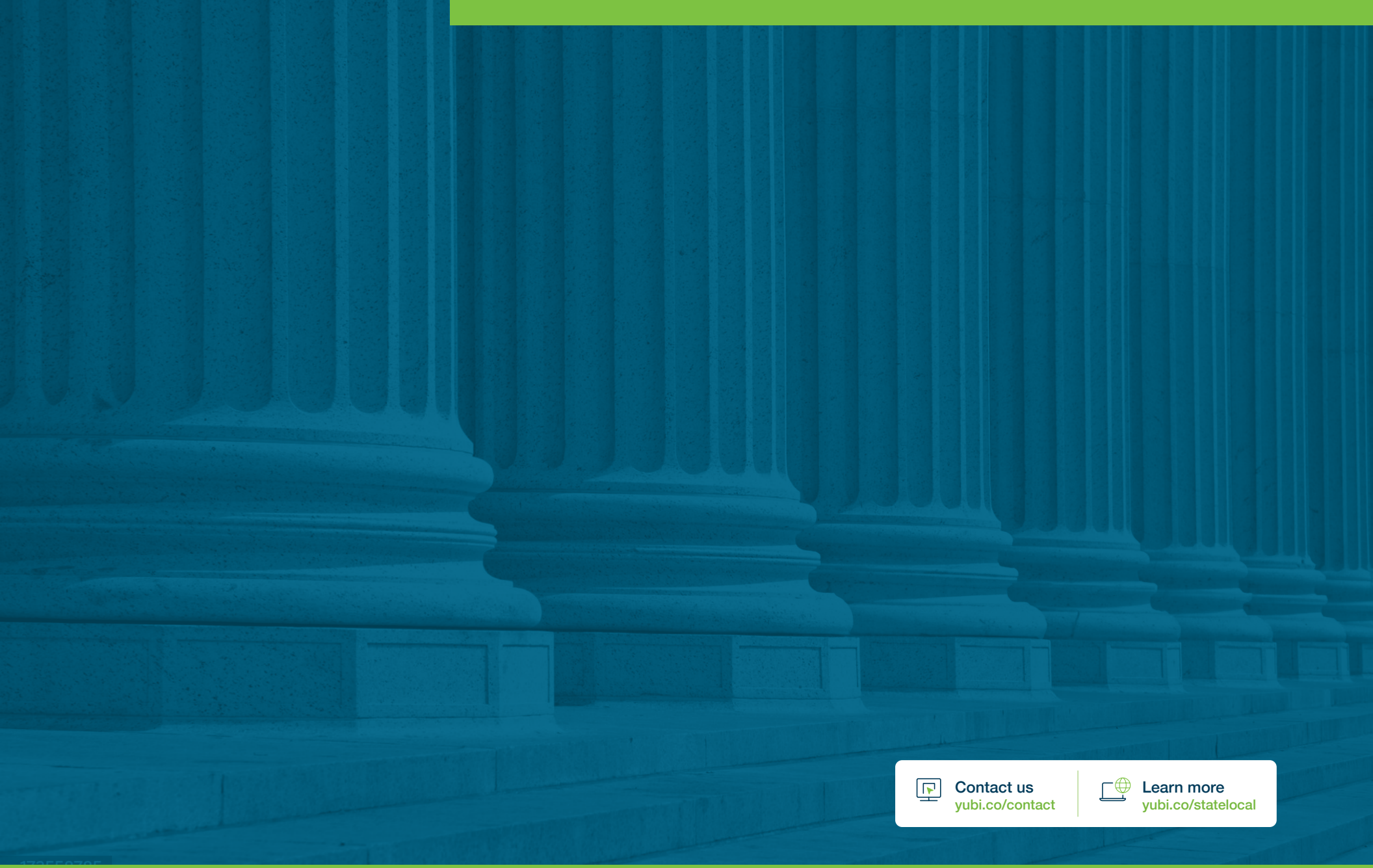
Drive adoption with best practice training and support

Measure

Report on security and business value impact

The YubiKey 5 Series–from left to right: YubiKey 5 NFC, YubiKey 5C NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano and YubiKey 5C Nano

The YubiKey FIPS series—from left to right: YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS and YubiKey 5C Nano FIPS



Contact us
yubi.co/contact

Learn more
yubi.co/statelocal

yubico
The key to trust

Yubico (Nasdaq Stockholm: YUBICO) is the inventor of the YubiKey, a hardware security key that is the gold standard in phishing-resistant multi-factor authentication (MFA). Yubico's solutions offer organizations and users deployment expertise and operational flexibility as YubiKeys work across hundreds of consumer and enterprise applications and services.

Yubico is a creator and core contributor to the FIDO2/passkey, WebAuthn, and FIDO Universal 2nd Factor (U2F) open authentication standards, and is a pioneer in delivering hardware-based passwordless authentication using the highest assurance passkeys to customers in 160+ countries. For more information, visit: **www.yubico.com.**