



CASE STUDY



At a glance

30,136 residents

500 city staff

Key results

Protects all city employees from phishing attacks

Streamlined, passwordless authentication

Compliance level exceeding requirements of CJIS, EO 14028

Reduced support calls for password resets

YubiKeys deployed

YubiKey 5C NFC FIPS



Attacks against state and local governments are increasing and becoming more difficult to combat. The best way to combat attacks is with security policies and the implementation of passwordless methods and multi-factor authentication.”



Jason Rucker |
Director of IT |
City of Southgate

City of Southgate levels up cybersecurity with passwordless authentication and the YubiKey

Celebrating small cities with strong ideals

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. Municipalities help keep citizens secure, a responsibility that the City of Southgate extends beyond police, fire or public works to include the requirement to defend critical infrastructure and citizen data against cyber threats.¹

Cyber threats against state and local governments on the rise

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 Federal Bureau of Investigation (FBI) warned state, local, tribal and territorial (SLTT) governments that an increase in ransomware attacks has led to “disrupted operational services, risks to public safety and financial losses.”

City of Southgate Mayor Joseph Kuspa, the longest serving Mayor with 15 years of experience, and nearly lifelong resident of Southgate, recognized that the evolution of the City and its technology created a new risk to public safety, one that required active management.



Today, perpetrators don’t have to come to our premises to gain access to important documents. Now we have external threats that could impact our water systems or citizen data. It was important to us to shore up any weaknesses.

Mayor Joseph Kuspa | City of Southgate

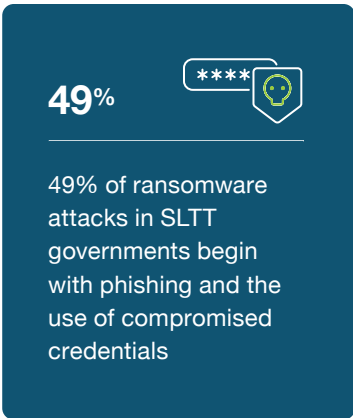
To that end, Mayor Kuspa elevated long-time consultant Jason Rucker to Director of IT for a new Department of Information Technology (DoIT) to oversee and secure technology systems, ensure compliance with state and federal partners, and to work closely with the city administration and the Director of Public Safety, Joe Marsh, to support public safety needs.



Unfortunately, threat actors don't wait for cybersecurity plans to be implemented before they attack. In 2023, cyber threat actors infiltrated the City of Southgate police department through a shared police system.

“ The cyber attack demonstrated a threat to public safety. I was worried about what kind of sensitive information was possibly obtained about cases or citizens. It was important to safeguard that and to make sure those entry points are no longer there.”

Joe Marsh | Director of Public Safety | City of Southgate



Modern multi-factor authentication (MFA) part of a top 1% innovative strategy to secure city infrastructure

Recognizing that SLTT governments have limited resources to mitigate cyber attacks, the federal government created the State and Local Cybersecurity Grant Program.² Using this grant, the City of Southgate executed a cybersecurity strategy that combines the YubiKey with Microsoft Entra certificate-based authentication (CBA) to help achieve a compliance level that's ahead of federal mandates, placing them in the top 1% across the public sector.

Recognizing that 49% of ransomware attacks in SLTT governments begin with phishing and the use of compromised credentials,³ Rucker knew that multi-factor authentication (MFA) would be a critical part of securing city infrastructure. The ideal solution needed to support the highest assurance security and varied authentication scenarios and work seamlessly across both cloud infrastructure (e.g., Microsoft 365) and Microsoft Entra ID (previously Azure Active Directory).

“ Our mission is our citizens. It's our responsibility to build a fortress wall between threat actors and citizen data with enhanced methods of multi-factor authentication.”

Jason Rucker |
Director of IT |
City of Southgate

“ Although we were on the path to finding the best way to be secure. The attack propped us up and we clearly identified that the YubiKey could have prevented the attack. It helped support our decision.”



Mayor Joseph Kuspa |
City of Southgate

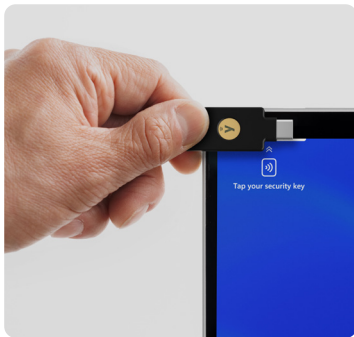
Although no data had been lost in the 2023 cyber attack, the incident heightened the awareness of cybersecurity risk and provided the impetus for the city council to approve the deployment of the YubiKey.

The City of Southgate's cybersecurity plan would "harden the fortress walls," Rucker notes, including upgrades to city networking infrastructure, Microsoft Entra certificate-based authentication, 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. With the help of the State and Local Cybersecurity Grant Program, Rucker was able to purchase two YubiKeys per person, with the second backup key to be secured in a central location.



The city infrastructure and security are my baby. Why would I want to put my baby outside without a coat in hand? Going with MFA using hardware tokens, the YubiKey, is a no brainer for me, it's that much more secure."

Jason Rucker |
Director of IT |
City of Southgate



Staying ahead of Zero Trust and MFA compliance requirements with YubiKey and Microsoft Entra CBA

The YubiKey first came onto Rucker's radar during a Criminal Justice Information Services (CJIS) audit two years ago. "We passed our audit rule," says Rucker, "But we were warned that standards would soon enforce two-factor authentication." Having experienced several data breaches personally, Rucker became convinced that he needed to "skip to the next level" with regards to MFA in order to not just comply with CJIS (which now does require MFA⁴), but to stay ahead of other compliance mandates including PCI DSS,⁵ Executive Order (EO) 14028⁶ and Office of Management and Budget (OMB) Memo M-22-09.⁷ "If they're calling for MFA, what's the next thing?," says Rucker. "There's always a 'next thing.' The YubiKey was our solution for the requirements of today—and beyond."

The YubiKey helped meet the specific CJIS Advanced Authentication requirements (section 5.6.2.2) for the Southgate Police Department, providing highly portable, phishing-resistant user access to critical data for police operations. While deployment of the YubiKeys to the police department took priority, implementation has continued incrementally across all departments and users. The YubiKey is ideal for a variety of scenarios, including remote and field work, because it doesn't require external power, batteries or a network connection—a user can use a single YubiKey for secure access to Microsoft Entra ID protected workstations, applications and services, as well as over 1,000 other products and applications, with the secrets never shared between services.



We've worked collectively to strengthen our security posture. The YubiKey is instrumental for me as the Director of Public Safety. It gives me a sigh of relief because the one thing that we don't want to do is repeat history."

Joe Marsh | Director of Public Safety | City of Southgate

Future-proofing the City of Southgate's MFA security investment and staying ahead of compliance requirements

Looking to that "next thing," Rucker knows that many City of Southgate departments include state and federal tie-in systems and that it won't be long before the phishing-resistant MFA requirements of OMB M-22-09 extend to SLTTs, particularly as they fall within the "partner" category for federal agencies.

In order to future-proof the city's compliance requirements, Rucker chose the most secure form factor of the YubiKey, the YubiKey 5 FIPS Series, which offers validation to the Federal Information Processing Standards (FIPS) 140 standard⁸ and meets the highest AAL3 requirements.



There's only one company that offered FIPS validation that I needed, and that's Yubico. We're a lot further along in securing our future by using the YubiKey. I'm one step higher than being compliant, I'm ahead of the game. I know that in my next audit, I'll pass with colors—in fact, I look forward to being audited."

Jason Rucker | Director of IT | City of Southgate



They are the gate to your castle walls and you don't want them to let threat actors in. I can now tell my users if you click a link and it asks for a password, you don't have a password. You know that that link is fake."

Jason Rucker |
Director of IT |
City of Southgate



The multi-protocol support of the YubiKey is an important bridge solution for the city to ensure secure access to all systems, even those that don't yet support FIDO2. The YubiKey also supports both types of phishing-resistant authentication for cloud environments, FIDO2 and Microsoft Entra CBA.

Entra CBA allows the city to use x.509 certificates for authentication directly against Entra ID. The YubiKey helps improve the experience for certificates by enabling the user to authenticate simply on any supported device. The YubiKey is currently the only external device that supports Entra CBA on Android and iOS and is the only FIPS-certified phishing-resistant solution available for Entra ID on mobile.

The combination of Microsoft Entra CBA and YubiKey has placed the City of Southgate on the forefront of the country for public sector security posture and has put the city firmly on the path to Zero Trust. A Zero Trust strategy reduces risk by assuming all users, devices, applications and transactions are potential threats that should be verified and authenticated before access is granted.

A fast and easy user experience with passwordless

Rucker had two primary goals when deploying MFA: security and ease of use. Rucker's vision, passwordless authentication, achieves both, eliminating the need to remember or change long passwords, and entirely eliminating the risk of the human element.

Leveraging the YubiKey and FIDO2 (passkeys) credentials, Rucker is able to support passwordless login across the city's Microsoft infrastructure and every system that accepts passwordless, with ongoing updates. The City of Southgate employees received training in how to use their YubiKey as well as regular security training and phishing exercises. Since primary systems are all passwordless, it's very easy now to explain to users that any request for a password is a phishing attack.

“ 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.”

Jason Rucker | Director of IT | City of Southgate

Authentication with the YubiKey is fast and secure with a simple touch and PIN. Employees are encouraged to use their YubiKey for personal accounts, reinforcing strong security habits and how they should carry over into their personal lives.

Staff have been passionate about the change, becoming huge fans within a matter of days. “Staff come to me saying ‘I hate my password, I'm tired of remembering it, when am I getting my YubiKey?’” says Rucker. “It makes me happy because I'm making their lives professionally easier.” From a support perspective, passwordless has also eliminated calls for password lockouts.

But for the Southgate Police Department, passwordless authentication is not just about security or ease of use, it also relates to officer safety.

“ Officer safety is the number one thing on our minds. We want our officers to be safe. We can't have them distracted by typing on a keyboard or delayed by using passwords to access information that they need.”

Joe Marsh | Director of Public Safety | City of Southgate



When you're looking at passwordless and Zero Trust, everything I do becomes the same security. I'll just keep circling around, expanding passwordless and thinking outside the box to keep my fortress secure."



Joe Marsh |
Director of
Public Safety |
City of Southgate

Sources

1. FBI Cyber Division, [Private Industry Notification 20220330-001](#), (March 30, 2022)
2. DHS, [Biden-Harris Administration Announces \\$1 Billion in Funding for First-Ever State and Local Cybersecurity Grant Program](#), (September 16, 2022)
3. Sophos, [The State of Ransomware 2024](#), (April 2024)
4. FBI, [Criminal Justice Information Services \(CJIS\) Security Policy v. 5.9.4](#), (December 20, 2023)
5. PCI, [PCI DSS: v4.0](#), (March 2022)
6. The White House, [Executive Order on Improving the Nation's Cybersecurity](#), (May 12, 2021)
7. OMB, [M-22-09](#), (January 26, 2022)
8. NIST, [FIPS 140-3 Security Requirements for Cryptographic Modules](#), (March 22, 2019)

As a small IT department, Rucker has personally overseen the technical integrations, setup and deployments across each YubiKey user group. Given the vast quantity of complex systems a government works with, Rucker worked with Yubico's Professional Services team when technical questions arose and to gain insight on best practices.



Yubico has been a strong partner. They were always there and just seeing how they could support me."

Jason Rucker | Director of IT | City of Southgate

The City of Southgate an example of security best practices for other cities

The City of Southgate is ahead of the curve in terms of security and compliance for the public sector, a feat that has not gone unnoticed. "As a city, we're on the cutting edge in a lot of things, and now we can say that about our security," says Mayor Kuspa, "I am very proud of my staff and Jason [Rucker] for trying to identify the best possible program to prevent future breaches of our system." Rucker is equally proud and is happy to share his insights with other cities and IT professionals who heard about his strong security posture and have sought out advice.



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

While there are many instances of federal agencies implementing the YubiKey, Rucker feels like he has a unique perspective of what it's like to use the YubiKey at the SLTT level. "If someone is nervous about going passwordless," says Rucker, "I encourage them to do it: to select a small group and see how easy it is."



If our small city can do it, despite budget constraints, there's no excuse for any government entity or business not to do it."

Jason Rucker | Director of IT | City of Southgate

For Marsh, the reason to encourage other SLTTs to implement strong MFA with the YubiKey comes down to public safety. "You don't want to be the people in the crisis."

Looking to the future to advance Zero Trust and Passwordless

As Rucker noted, there is always a "next thing" in cybersecurity too. There will always be new threat actors and new kinds of cyber threats. Looking to the future, Rucker plans to continue the journey to Zero Trust.



[Learn more](#)

yubi.co/customers

yubi.co/contact



Yubico (Nasdaq First North Growth Market Stockholm: YUBICO) is the inventor of the YubiKey, the gold standard in phishing-resistant multi-factor authentication (MFA). The company 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.