yubico

CASE STUDY

Landeshauptstadt
München
IT-Referat

Industry

City government

Protocols

FIDO for SSO & VPN access

NFC capability for follow-me printing

OTP for legacy processes

PIV for future document signing

Products

YubiKey 5 NFC

YubiKey 5C NFC

Munich protects itself from cyber attacks with YubiKeys

Phishing-resistant authentication secures city government

Tradition runs deep in the Bavarian capital of Munich, Germany. However, the city's IT team knew existing solutions were no longer enough to secure critical systems and infrastructure against ever-evolving cyber threats. To safeguard technological assets, residents and visitors, as well as over 43,000 city employees, the City of Munich turned to the YubiKey for modern phishing-resistant MFA.

At a glance

1.6M residents

8.5M annual visitors

43K city employees

Key results

32K YubiKeys deployed

Enhanced security

Faster, simpler authentication

"We are definitely more secure. We are really fond of the YubiKey for strong authentication. It's much more reliable and secure than any non-Smart-Card-based factor."

Matthias Wagner | IT Architect & Director | Cybersecurity Center | City of Munich

Securing Munich's digital future

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. Munich is also the annual host of Oktoberfest, the largest public festival in the world, and its city administration is tasked with providing valuable information and services to the approximately 8.5 million tourists the city welcomes every year.

Public sector organizations, such as the City of Munich, face many of the same cyber threats as those in the private sphere, but can be even more enticing targets for cyber criminals who want to disrupt crucial public services or cause financial harm. In 2023, Germany's Federal Office for Information Security (BSI) recorded an average of two ransomware attacks per month on local governments or municipal businesses,[1] a threat that continues to grow.

"We don't have a business that you can break down into hard currency," says Matthias Wagner, IT Architect & Director of Cybersecurity Center at the City of Munich. "But we have a lot of customers within our organization and also, of course, the citizens of Munich, who would be deeply impacted if there was a serious ransomware attack."

The City of Munich has been in a process of implementing digital transformation over a number of years, which has necessitated new approaches to cybersecurity.

> "Cyber threats have increased and become highly professional. There have also been geo-political shifts in the past couple of years, and the pandemic in particular was a challenge. Like any other organization, moving a lot of people to home offices has changed the way we work and the way we manage our devices."
>
> **Matthias Wagner** | IT Architect & Director | Cybersecurity Center | City of Munich

Historically, many services were not built on web technologies, adds IT Service Owner Markus Weber. "Previously, most people were working in the office so it was easy to put everything behind a gateway and provide a virtual desktop. Since a few years ago, many business applications have been deployed as web applications. Our customers need to access these via the Internet."

In 2017, the city implemented Single Sign On (SSO), replacing LDAP-based authentication for many services. This was a crucial moment for the overall strategy, and it was soon decided that the new SSO architecture required stronger authentication.

> "We previously used hardware-based OTP tokens, but only for the VPN gateway, a special jump service for administrative purposes and very particular web applications. We were aware that this wasn't the strongest solution, as there was no phishing-resistance."
>
> **Matthias Wagner** | IT Architect & Director | Cybersecurity Center | City of Munich

[1] Bundesamt für Sicherheit in der Informationstechnik, The State of IT Security in Germany in 2023

“We had a good feeling about the procurement chain and how the sales channel was working. That Yubico is a European manufacturer was also a factor in our decision.”

Matthias Wagner | IT Architect & Director | Cybersecurity Center | City of Munich

Fortifying SSO with modern FIDO2 authentication from Yubico

The city’s IT leadership began market research into a new MFA strategy aligned with their multifaceted setup: an identity management system in the backend, a Windows domain with Active Directory and an SSO endpoint.

“Phishing will always be a big threat for us, so it was important to find Smart-Card-level security. Legacy MFA would not offer phishing-resistance. If a user is bombarded with push notifications, they will eventually just press the button because they don’t want to be annoyed anymore. And, for instance, alternatives like SMS-based authentication are just obviously not as secure.”

Matthias Wagner | IT Architect & Director | Cybersecurity Center | City of Munich

While mobile authentication methods were considered, Wagner and team were keen to have a separate factor, and so they began investigating the vendor landscape for FIDO2 hardware security keys. They considered different vendors, and ultimately opted to purchase the YubiKey 5 Series, with contactless NFC capability, in both USB-A and USB-C models. In addition to Yubico’s proven and innovative authentication solution, that the company was European, with headquarters in Stockholm, Sweden was also a key consideration.

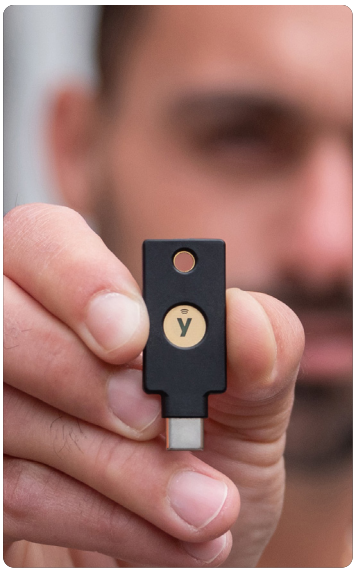
The YubiKey 5 Series is a multi-protocol hardware security key, supporting FIDO U2F and FIDO2 (Passkey) authentication, as well as Smart Card (PIV), and a range of legacy protocols. This meant that the YubiKey could work across a broad range of use cases, and allowed the City of Munich to easily migrate their legacy OTP processes to modern phishing-resistant authentication.

An accelerated city-wide deployment

The team began to deploy YubiKeys within their own IT organization in 2019, but the goal was always to expand the rollout to the full range of employees city-wide with an IT account. This meant over 30,000 employees, in a broad selection of departments ranging from HR and finance, to waste management and education. When the COVID-19 pandemic required that many staff be urgently moved to remote work, the YubiKey rollout was accelerated to ensure no security risks arose from staff remotely accessing city services, applications or information.

Two-factor authentication is now not only required for remote access and administrative access. “We are putting more and more web applications into a position where you need to have the YubiKey to access data, especially if it’s directly accessible from the Web and not through the VPN,” says Wagner. “You cannot access anything from outside our network without the YubiKey as a strong second factor.”

A traditional username and password provide the first layer of security, while touching the YubiKey provides foolproof assurance that the user is who they claim to be.



> The rollout and transition was a big success. Users accepted the token and registered it quite easily. No FIDO PIN is necessary in our setup as we use YubiKeys for login only as a second factor. This makes it also easily accessible for our disabled users and minimizes support costs."
>
> **Markus Weber** | IT Service Owner | City of Munich

> The biggest plus point that YubiKeys provided for us is the versatility. As the YubiKey is a multi-protocol token we use it for FIDO authentication, and are currently integrating business processes to utilize the PIV/Smart Card protocol for signing invoices and other documents."

Markus Weber | IT Service Owner | City of Munich

Expanding access beyond IDP

The versatility of the YubiKey means that the same key can be used for many different use cases. The City of Munich has introduced a Follow Me printing infrastructure, using the device's NFC compatibility, so staff working in the city's offices can simply tap their YubiKey to one of the city's printers to release their project.

The team also sees great potential in using the YubiKey's Smart Card (PIV) capability for document signing. In the future the City of Munich plans to sign external documents with official signatures.

Ensuring cyber resiliency into the future

By implementing YubiKeys, the City of Munich is a pioneer in ensuring business continuity and cyber resiliency against modern AI-based cyber attacks that are increasingly sophisticated. Looking back more than five years, the City of Munich is pleased with the decision to implement FIDO authentication across the organization. "We are definitely more secure," says Wagner. "We are really fond of YubiKey for strong authentication. It's much more reliable and secure than any non-Smart-Card-based factor." For Weber, the biggest plus point is the YubiKey's versatility: "It's a multi-protocol token, so we are always able to expand how we use it."

Weber and Wagner both use YubiKeys for several of their personal accounts, and the YubiKeys issued by the City of Munich are employees' to keep, even after they leave the organization. "It's a gift from the employer to the employee," says Wagner. Staff are encouraged to use the YubiKey to secure their own personal accounts, enhancing their cyber resilience not only in their professional but in their personal lives as well.

As threats to critical infrastructure organizations grow, and ways of work continue to transform, the City of Munich's dedication to the highest assurance, phishing-resistant authentication continues to protect not only their IT team and employees but also the welfare of the city's many residents and visitors—and contributes to a more secure and trusted digital world.

Learn more | yubi.co/customers | yubi.co/contact

yubico

Yubico (Nasdaq 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.

© 2025 Yubico