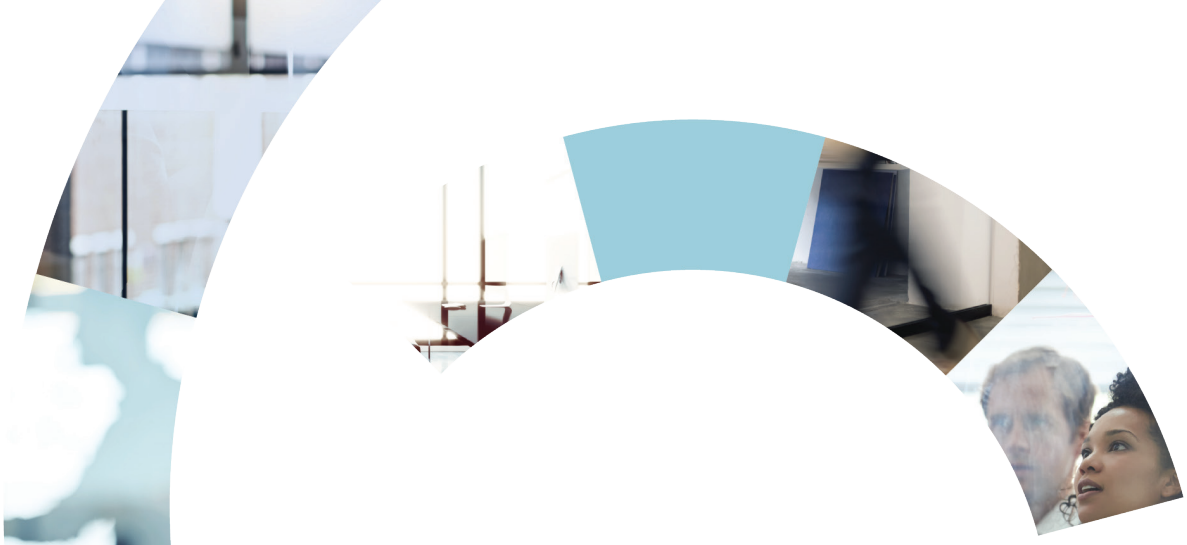
CASE STUDY



# Protecting citizens — physically and digitally

The City of Golden, Colorado, shields citizens' data, increases employee efficiency and mobility, and avoids spending two-thirds more for security with One Identity

**Key Facts**

**Company**
City of Golden, Colorado

**Industry**
State & Local Government

**Country**
United States

**Website**
www.cityofgolden.net

## Challenges

Golden, Colorado, must ensure that only authorized staff can access specific types of government data, including police reports, criminal records and citizens' credit card numbers.

## Results

- Facilitates protected mobile IT access and regulatory compliance
- Saves time for officers, business employees and IT staff
- Avoids paying 66% more for two-factor authentication

## Products

Defender

Increasingly, city governments are equipping staff with IT that helps improve the physical safety of citizens as well as service levels and staff efficiency. However, government systems contain classified data about citizens, including their police records and, sometimes, their credit card numbers. And while it's easier to lock down IT inside a building, patrol officers and other city staff need remote access to applications and databases via laptops.

To protect citizens' digital identities in the face of IT threats introduced through mobile system access by city employees, the federal government mandates specific security measures. For example, police departments must comply with the Criminal Justice Information Services (CJIS) Security Policy. It requires officers to provide a second form of authentication to access an unsecured laptop that connects to local, state and federal systems

ONE IDENTITY


"We can make sure our officers can access IT from remote locations .... Whether it's CJIS, PCI or other security requirements, **Defender** gives us the centralized security tools we need to comply with laws — and the reports to prove it."

*Ken Grimes, Network Administrator, City of Golden, Colorado*

containing law enforcement data. When the first iteration of CJIS was released some years ago, the City of Golden, Colorado, didn't take advantage of the lengthy compliance lead time and instead sprang into action. IT staff reviewed proposals from security experts for solutions that provide second-factor authentication, evaluating offerings for effectiveness, reliability and ease of use for all staff.

## More capabilities for one-third the cost

After narrowing its selection to products from two vendors, the city made its decision. Ken Grimes, network administrator of the City of Golden, explains, "We chose a solution that included One Identity Defender for two-factor authentication. The other vendor's product didn't have all the capabilities Defender has and, at the time, Defender was one-third the cost. We also appreciate how we only need to buy software tokens once, and we like how Defender integrates with Active Directory." IT staff decided to use software tokens instead of hardware tokens because they found them easier to work with.

## Setting up two-factor authentication

The city implemented Defender itself. "There were a lot of moving parts to manage. Our virtual private network is Cisco-based. Our server network is Microsoft-based. We did it, though. The Defender documentation is excellent. It includes many different configuration choices and screen shots that showed us how to configure our diverse technologies. One Identity support was also very helpful in answering questions."

## Cuts risk and boosts efficiency

Because of the seamless integration between Defender and Active Directory, the city's IT personnel can manage identities and tokens from one console. "We can program, monitor and revoke tokens in a couple of minutes from Active Directory," says Grimes. "It's terrific. Once you learn the process, programming a token for someone is so easy."

Managing security reports is also streamlined. "We access the audit trail we need to demonstrate regulatory compliance from Defender," Grimes says. "This includes records about users' connection times and where people logged on and off systems."

## The flexibility to support change

The initial deployment involved complying with CJIS regulations. However, the city has been agile in meeting new requirements, too, including Payment Card Industry (PCI) regulations that require second-factor authentication to remotely access networks that support credit card transactions. "When PCI passed, we were able to quickly comply because we had Defender in place," Grimes explains. "All we had to do was provide users who needed access to PCI resources with Defender tokens."

ONE IDENTITY

## Stands the test of time

It's been six years since the City of Golden implemented Defender. "I've only had to contact support once in the last six years because Defender just runs," says Grimes. "And with it, we can make sure our officers can access IT from remote locations including the courthouse, a crime scene or driving in a squad car. So whether it's CJIS, PCI or other security requirements, Defender gives us the centralized security tools we need to comply with laws — and the reports to prove it."

## About One Identity

The One Identity family of identity and access management (IAM) solutions, offers IAM for the real world including business-centric, modular and integrated, and future-ready solutions for identity governance, access management, and privileged management.

**Learn more at OneIdentity.com**



ONE IDENTITY