CASE STUDY

Bakersfield Police Department locks down remote access

City meets compliance requirements and ensures secure remote access

Key Facts

Company
City of Bakersfield

Industry
Local Government

Employees

13,000

Country
United States

Website
www.bakersfieldcity.us

Challenges

To increase security of mobile computing devices used by the city's police department and other field personnel, as well as comply with federal requirements to provide secure remote access.

Results

- Met compliance requirements
- Increased security of remote access
- Leveraged existing infrastructure
- Easily scaled with 100% increase in users
- Delivered a low-maintenance twofactor authentication solution

Products

Identity and Access Management

Located in the southernmost reach of the fertile San Joaquin Valley, the City of Bakersfield is the ninth largest city in California with approximately 370,000 people and expected to reach 1 million by 2020. Managing this tremendous growth in population and suburban infrastructure is a huge task for the city government and its police force. Of course, communications, the collection of and access to data, as well as providing security are critical to smooth management for the city.

Tasked with keeping the city's technology resources running smoothly and securely is a team of 38 IT professionals, among them are David Hecht, director of IT for the City of Bakersfield, and Gregory Pronovost, the city's assistant director of IT.

ONE IDENTITY

"We found Defender to be a robust, feature rich solution that was competitively priced."

David Hecht Director of Information Technologies, City of Bakersfield

Department of Justice Requirements

In 2008, the U.S. Department of Justice (DOJ) updated requirements that mandated two-factor authentication for remote access to DOJ systems. A stipulation of this mandate was that the second factor had to be a device – such as a hardware token – that is separate from the computer accessing the DOJ systems.

This new regulation meant the city needed to enable two-factor authentication for all of the mobile computers inside the police vehicles. Hecht and Pronovost, who were both working in more handson technical roles at the time, were tasked with researching solutions to fulfill this DOJ requirement.

The search for an authentication solution

They didn't have a large set of requirements for the two-factor solution, but two of their key objectives included Active Directory integration and the need for hardware tokens. "We use Active Directory as our primary identity store and wanted to ensure any solution we implemented was tightly integrated with it," said Hecht."

Another concern was a need for hardware token support. "We liked the idea of software tokens on mobile devices," said Pronovost. "However not all of our staff has a city-supplied phone, so a mobile-based solution wouldn't work for us.

"We were looking for ease of management and installation," said Pronovost. "And, of course, being a government agency, cost is always a primary concern." Finally reliability was a key concern as the police officers' quick and secure access to systems is a matter of personal and public safety. "Our systems cannot fail," said Pronovost.

In their search for solution, Hecht and Pronovost looked at a number of different vendors but ultimately found many advantages to Defender – and purchased and implemented the solution.

Defender - an easy choice

When comparing Defender to competitive solutions, they found it had all the features they required and its competitive priced made it an easy decision. "We found Defender to be a robust, feature-rich solution that was competitively priced," said Hecht. After conducting an on-site proof of concept (POC) it was very clear that Defender was the ideal solution. "The pre-sales technical support for the POC was excellent and a key factor in our selection process as the level of support is paramount for a solution has a potential effect on public safety" said Pronovost.

After purchasing Defender, the rollout was quite simple and - with the occasional phone and email support - the implementation took less than a week. Defender enables administration via a web interface

ONE IDENTITY

or through Active Directory Users and a computer's ADUC. For the city's IT team, the option to use ADUC simplified training and eased ongoing administration. "Our help desk associates were already using ADUC. The ability to manage Defender through the same console made supporting a new authentication method a lot easier," Hecht said.

Continued Growth

Since the city had so much success with the police department rollout, they decided to extend it to all of their remote-vendor access, as well as to admins with privileged account access. "We are always looking for ways to increase the security of our networks, extending Defender to some of our high-risk users just made good security sense," Hecht said. Pronovost agreed: "We definitely feel more secure with our remote access today." Since the initial rollout in 2008, the city has doubled use of Defender and it continues to grow annually.

"After years of use, Defender has proven itself to be a solid, robust solution," said Pronovost. "I can't think of any time that it's ever failed. I don't have to worry about it. And it has become so much a part of what we do and so easy to use that we don't think of it as a separate solution."

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