Silverfort

CASE STUDY

Staying ahead of the threat: How the City of Grapevine builds citywide Identity Security with Silverfort

BASED
US, TX

INDUSTRY
Local government

USERS
~780 to 1,200 (seasonal)

ENVIRONMENT
Active Directory, Microsoft Entra ID
Nutanix virtual environment
Microsoft Authenticator

Grapevine, Texas, is home to about 51,000 residents. The City of Grapevine provides core services for its community, including public safety, water and utility services, parks, and a public library.

THE CHALLENGE:

Protecting water treatment and public safety systems, privileged access, and service accounts in an on-prem environment with no real-time visibility or identity-based policies.

- Inability to see who was accessing OT/SCADA systems at the water treatment plant, even with network segmentation in place
- Need to replace existing MFA solution to meet CJIS requirements to protect police officers' access to criminal justice databases
- No visibility into shadow admins, excessive privileges, or dormant service accounts accumulating across the environment

THE SOLUTION:

Gained real-time visibility and enforced identity-based policies to protect water treatment and public safety systems, privileged access, and service accounts in the city's on-prem environment.

- Closed the visibility gap on OT/SCADA systems at the water treatment plant, enforcing MFA for authorized users and deny policies for everyone else
- Replaced the existing MFA solution to meet CJIS requirements, enforcing MFA for police officers accessing criminal justice databases from patrol vehicles
- Discovered shadow admins, excessive privileges, and dormant service accounts, applied virtual fencing to the service accounts the city relies on, and established a process to map each one to an owner

The challenge: Limited visibility and no real-time controls left the city's critical systems, privileged access, and service accounts at risk

The City of Grapevine runs its operations on an on-prem Active Directory (AD) environment, supported by a small IT team. Darryl Austin, the city's IT Security Administrator, chose NIST as the city's guideline and set Zero Trust as the direction, but putting either into practice required visibility and controls the city did not have.

"When I came on board in 2020, we didn't really have visibility throughout the security space. Nothing was actually real time, and we didn't have any policies that we could put in place to really protect the actual user authentication and identity." said Darryl

That gap mattered most where the city's critical infrastructure was at stake: the operational technology (OT) and supervisory control and data acquisition (SCADA) devices at its water treatment plant. Darryl wanted to close it before an incident forced the issue.

> "We're already in the process of protecting our operational technology and our SCADA devices by doing various different segmentations on the network. But that alone didn't provide the visibility of who's accessing those devices."
>
> — Darryl Austin, IT Security Administrator, City of Grapevine

Public safety brought a different kind of pressure: compliance. The police department must meet Criminal Justice Information Services (CJIS) requirements, which means an officer who pulls over a suspect must verify their identity with MFA before reaching a federal criminal justice database, including from a patrol vehicle. The city's existing MFA solution was nearing the end of vendor support, which put its ability to meet that requirement at risk.

Inside the network, privileged access had grown without formal oversight. The risk was shadow admins: accounts that hold admin-level rights without being officially designated as administrators.

Service accounts added to the risk. Most had been created years earlier and were dormant. The city had no view into what they were doing, and in some cases the person who created one had left the city without passing on its purpose. Because these accounts carry high privileges, an attacker who gained a foothold could use them to cause real damage.

Finding the right Identity Security platform

One of these requirements had a hard deadline: vendor support for the city's existing MFA solution was ending in September 2024. The police department needed a replacement before then to stay CJIS compliant.

"Our public safety team was just looking for an MFA solution, but I wanted to see if we could do something more." said Darryl

Darryl evaluated other MFA platforms, but they were early-stage products with a limited history in identity and access management, so he leaned toward Silverfort for public safety. Vetting Silverfort changed the scope of the decision.

> "I chose Silverfort because the platform provides a solution for identity visibility from a single platform for our normal business as well as our operational technology networks."
>
> — Darryl Austin, IT Security Administrator, City of Grapevine

The city chose Silverfort, which could cover far more than MFA: access to OT/SCADA systems, service accounts, and shadow admins on one platform. As a public body, it also needed City Council approval, which took about two months. The deployment then moved quickly.

The solution: Real-time visibility and identity-based access control for the city's critical infrastructure

The rollout took about 25 days, with Silverfort's engineers working alongside the city's IT team. The first phase focused on MFA for the police department, the group facing the CJIS deadline.

> "The biggest challenge was our public safety vehicles. We had to work with some changes that we needed to make in Active Directory to trigger MFA to a moving vehicle. The device inside the vehicle can't be configured the normal way, which is DHCP automatic IP assignment ... So, we changed them all to a static IP, then developed a rule in our Authentication Firewall using that IP address."
>
> — Darryl Austin, IT Security Administrator, City of Grapevine

Per CJIS requirements, access control lists (ACLs) on the network switches keep that traffic segmented and send it to a RADIUS server, the network service that handles authentication.

The city applied the same approach to the OT/SCADA devices at the water treatment plant, gaining a view of who was accessing them and enforcing MFA for authorized users.

> "Only those who are interacting with the operational technology get a triggered MFA in order to gain access. But for everyone else, there's no reason to gain access, including our systems administrators."
>
> — Darryl Austin, IT Security Administrator, City of Grapevine

An Authentication Firewall deny policy enforces the rule, and anyone who needs access has to ask permission first. **The city applied the same model to a very different kind of system: its long-term storage device.**

"One of the really big improvements on that is that device can be air gapped. It's maintaining our quarterly, monthly and yearly storage, but no one can gain access to it without MFA. Everyone else is denied except for myself and the systems administrators. There's no Microsoft Authenticator app or Silverfort agent on it. We're able to put that policy on just by IP address." said Darryl

Segmenting access by role and responding to risk

With MFA and deny policies in place, the question was now how a small IT team could keep them up to date. For public safety, Darryl built the policies around AD organizational units (OUs). Officers are placed in OUs by role, such as criminal investigators, sergeants, and lieutenants, and each OU is set up in Silverfort as a policy that determines what the group can reach and when MFA triggers.

“The OU groups help because I don’t have to constantly go into the Silverfort platform and add or remove users. It’s automatically done because it’s based on Active Directory.” said Darryl

The same OU mechanism handles departments with different needs. Fire crews, whose vehicle consoles connect to city systems, want devices that simply work, so Darryl is setting up a process that places each driver in an OU. The console then operates for drivers and stays locked to everyone outside that group.

Role-based rules cover the expected cases. For the unexpected ones, Darryl added a policy based on risk that applies to all employees: when an account’s risk level reaches critical, Silverfort triggers MFA.

> "That [risk-based] policy then alerts the user that something’s wrong. At the same time, it allows me to know, when I look in the logs, exactly how the user reached critical status."
>
> — Darryl Austin, IT Security Administrator, City of Grapevine

One case shows what that looks like. An employee on vacation in another country began receiving MFA prompts she did not approve, and she called Darryl. The logs showed that four laptops were authenticated under her name, and one was running a PowerShell process with her old password. Most cases have similarly routine causes, such as a device still holding an old password or a test machine left logged in.

Extending visibility to privileged access and service accounts

Silverfort’s Identity Security Posture Management (ISPM) module showed Darryl unknown exposures, including seven shadow admins, two of them stale accounts created in 2015 and 2018, as well as legacy authentication such as NTLMv1 and old operating systems that were never decommissioned.

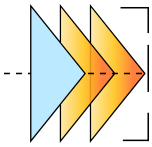
“We’re working with departments on decreasing the shadow admins, old authentication practices, stale accounts … once we gain that visibility, we’ll work with them to understand why they need to change.” said Darryl

Visibility into service accounts has also changed what the city can do. Silverfort detected 159 service accounts and showed what each one is doing, so Darryl could retire any the city no longer needed. With this visibility, he could also place virtual fencing around vital service accounts to ensure they can only perform the actions they—and the city—need them to. So far, 98 of them are protected.

Ownership matters as much as visibility. Silverfort supports multiple owners per service account, and Darryl aims for two on each one. He has already assigned owners to about 75 percent of the city’s service accounts, working department by department.

> "There’s never just one person who’s responsible for a service account. There are always going to be two people, so that if somebody leaves, we still have somebody on board who knows what that service account does."
>
> — Darryl Austin, IT Security Administrator, City of Grapevine

Looking ahead: Extending Identity Security to AI agents



Silverfort has grown from MFA for the police department into the platform the city relies on across the water plant's OT devices, its service accounts, and its privileged access exposures. For Darryl, it is also where the day begins.

> "At the start of my day, my standard operating procedure is to go to Silverfort. Let's check all the authentications and anything within the logs that may be suspicious. ... Being able to have that visibility and know that it's functioning and protecting the way that we intended is really a wonderful tool to be able to go to daily."
>
> — Darryl Austin, IT Security Administrator, City of Grapevine

AI agents are next on their roadmap. The city plans to look at adding Silverfort AI Agent Security in the future, and Darryl wants to apply the same ownership approach he uses for service accounts.

"We don't want to give agents the same privilege as the users who own them. They need their own privileges, their own ability to be protected, and their own authentication process." said Darryl

About Silverfort

Silverfort secures every dimension of identity. We deliver end-to-end identity security that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity, analyze exposures, and enforce protection inline to stop lateral movement, ransomware, and other identity threats.

Learn more