BeyondTrust

Network Security Doesn't Have to Come at the Expense of Usability

BY MIKE WEISS

Mike Weiss has worked in IT for over 20 years in municipal government and healthcare. His passion lies in Information Security where he has spent the majority of his career.

Weiss attained his CISSP in 2006 and his Masters in Information Security Engineering in 2012. He has managed small IT departments since 2004 and enjoys the challenges and atmosphere in municipal government.

We see it time and time again in IT, the more secure an IT environment becomes, the less usable it is. Environments that are too user-friendly have the opposite problem. Open access leaves sensitive networks vulnerable to attacks and increases the risk of a data breach.

It seems inevitable, at some point down the line, IT departments will have to choose: Do we want more security or better availability? We sacrifice one for the other, often with severe consequences.

But what if I told you this no longer has to be the case?

It's rare to see an environment become more usable and more secure simultaneously, but that's exactly what happened for the City of Midlothian, Texas. Midlothian removed its attack vectors, while also making access to systems more straightforward. All it took was a new ecosystem from a reliable partner.

A GROWING AND INCREASINGLY CONNECTED CITY

Just 25 miles south of Dallas, Midlothian has grown from 18,037 residents in 2010 to 35,125 residents in 2020. I've worked for the city for almost 13 years, starting as the IT manager back in 2009. It was just a one-person shop and stayed that way for several years. Today, I am the IT Director with a staff of three full-time employees. Together, we manage the many IT systems in Midlothian across public safety and government.

These systems include water treatment, public works, fire, police, EMS, 911 dispatch, administration, building inspections, and city planning, among others. Our systems are interconnected on a large municipal network. Each department wants (and often needs) to talk to other departments, so we've kept the single network and put some segmentation and other security functions in place to help separate those spaces.

We have around 375 regular users and about 350 desktops and laptops. The network hosts many other devices, including video cameras, door security devices, physical gates, phones, SCADA systems for water monitoring, and even irrigation control systems.

BeyondTrust

> At some point, IT departments face the choice of sacrificing either security or usability, often with severe consequences.

The police and fire departments have added more communication devices and video systems as they've become more digitized. The fire department even has a tracheostomy tube with a camera connected to our network, enabling them to send video to the hospital for a doctor to assess a situation before a patient arrives.

A network this extensive comes with its own set of challenges, and when it came to usability and security, we had quite a few.

THE REMOTE ACCESS PROBLEM

Before 2018, granting access to our third-party vendors and remote workers was a hands-on chore that required multiple touchpoints and tons of cleanup. We used a VPN client from our firewall provider to set up accounts for vendors and third-party users. They would download and run the software client, input their credentials, and gain full access to our network. They were creating a secured tunnel to our systems, but there were no actual security controls in that tunnel. The only way to keep people from logging in whenever they wanted was to disable the account, which also meant we had to reactivate the account as needed.

We used a program called VNC for internal remote access. It worked, but it wasn't a secure application, and we had no additional security controls or wraps around it. Neither our internal nor external access methods provided a way to track or record activity within sessions. We couldn't authorize anything on the fly or limit access to specific machines and servers. It was a disaster waiting to happen.

The City of Midlothian was lucky—we never ran into any significant problems or security issues using these techniques. Unfortunately, there were a lot of other cities that did. We didn't want to be on the news because of a security incident, and we certainly didn't want to let down the people who relied on us most. We know we could do things better, and that prompted us to start looking for solutions.

A SOLUTION THAT CHECKED ALL THE BOXES

While hunting for a solution to our security and usability concerns, I wanted to compare a few vendors that offered the same features, great reviews, and plenty of demos to examine. We wanted to try and "break" each solution, giving the tires a good kick before buying anything outright. I also reached out to other IT professionals to ask how their favorite solutions made a difference in their respective organizations.

BeyondTrust provides one of the first solutions we found, and it had everything we wanted. The company has an excellent reputation, and the Privileged Remote Access product had the potential to solve many of our accessibility problems, immediately. It also has solid support, which is crucial for a small team.

We opted for the training bundle and deployment bundle, which included a week-long course on the ins and outs of the solution. This course took the guesswork out of everything and provided a great foundation for our new way of working. We also got great value from the BeyondTrust technicians, who quickly answered our questions and followed us down rabbit holes as we discovered something new or didn't remember something from the training class. After the testing phase, we moved our internal and external agencies over in just a few weeks.

BeyondTrust

> Automating remote network access for third parties saves countless hours and headaches for IT staff.

HOW AUTOMATION IMPROVES SECURITY AND REDUCES HEADACHES

Now that we use Privileged Remote Access, third-party access requires both an internal and external request. Our IT team can scope access to specific systems, too. When vendors log in with their credentials, they can only request access to the systems that we have pre-approved, and they can't see anything else.

Once I saw how easy it was to use Privileged Remote Access, I started looking into BeyondTrust Remote Support for internal use. Remote Support allows our technicians to jump into employees' computers to help troubleshoot. This ability was a big help when the pandemic hit, as restrictions limited close proximity, and we didn't want to be using each other's keyboards. Remote Support also allows us to draw in other people or other resources, if necessary. So, if one of my staff needs to pull me in for some additional expertise or if we have to pull in someone with specialized knowledge, it's no problem to get someone on a screen share and allow them to participate in the conversation.

As our IT department grew, I segmented tasks among staff as it was increasingly important to enhance security around remote access. It was also getting difficult to keep track of multiple passwords and ensure everyone was up to date on password changes. And after some external pen tests, I wanted to make our system more secure against unwanted visitors.

BeyondTrust Password Safe offers a solution to all those issues, while enabling more features in Privileged Remote Access and Remote Support. Password Safe can auto-inject credentials when remoting into a server, rather than having those credentials written down somewhere or saved in a password file or shared location. We can now automate that with Password Safe, integrate it with Remote Support and Privileged Access, and make it easier for our staff to get in under common logins.

When we auto-inject credentials, vendors don't know the password (and it changes on a set schedule). If they lose their credentials and somehow get into the system through another means, that account doesn't have access to anything. Before, a vendor would get admin rights on a specific server once they logged in. Now, they can't log into a server as an admin. We saved a ton of administrative overhead by automating the process, and the separation and segmentation improved security.

We also saved time and money by preventing external vendors from logging in whenever they wanted to perform their updates. That was a big headache for my IT team, who often had to go in after the fact and fix whatever the updates broke. Password Safe allows us to record sessions rather than escort vendors while in the system. This feature has saved countless hours for the entire team.

BeyondTrust

> With Privileged Remote Access, Password Safe, and Remote Support, we've ensured privileges aren't left unchecked, preventing users from becoming entry points for attacks.

MAINTAINING AN ECOSYSTEM OF SECURITY AND USABILITY

We have improved visibility and control over all vendor access to the municipal network. Our technicians enjoy easier access with more granular control over their rights, and we have more control over internal server passwords with the automated cycling of passwords. Vendors no longer remote in unannounced, nor do they update their software without telling us. We can set parameters for how long their access can be granted and have plenty of forensic evidence that proves vendors did what they said they did. With Privileged Remote Access, Password Safe, and Remote Support, we've ensured privileges aren't left unchecked, preventing users from becoming entry points for attacks.

It's always a challenge to prove security. How can you prove yourself against an attack that didn't happen? But we have become less vulnerable to things that affect other cities in our area. Around the time we implemented the BeyondTrust solutions, more than 20 cities in our area got hit by an attack that compromised their vendor's systems. This gave attackers direct access to more than 22 police departments with 24/7 remote access to their systems. So, while I can't prove outright that using BeyondTrust has prevented any attacks on the City of Midlothian, I can say that we have eliminated attack vectors, which helps everyone sleep better at night.

Today, the BeyondTrust ecosystem has removed vulnerabilities while ensuring everyone has access to what they need. It's significantly increased our security posture and scalability as the city adds more residents and more people depend on our network.

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. We are trusted by 20,000 customers, including 70 percent of the Fortune 500, and a global partner network.

beyondtrust.com