

Washington County Implements a Zero Trust Foundation to Enable Hybrid Work and Adopt AI

**Industry:**

Public Sector

Location:

Washington County,
Wisconsin

Organization:

Roughly 500 full-time employees, plus contractors, third parties, and seasonal workers supporting county services across offices, field locations, squad cars, and remote environments.

Solution:

Cisco User Protection Suite with Standard Support (Secure Access, Duo, Email Threat Defense)

Washington County, Wisconsin provides essential local government services across public safety, health and human services, administration, and community operations. Its workforce includes roughly 500 full-time employees, plus contractors, third parties, and seasonal workers who need secure access from county offices, home offices, field locations, squad cars, and other public-sector work environments.

When COVID hit Washington County, Wisconsin, remote work was not a transformation project. It was an emergency. Before the pandemic, employees were primarily in the office. Then the county had to send people home and make remote access work. “It was just kind of overnight, like boom, here it is, and now we’re working remote,” said Joel Woppert, Director of Information Technology.

The legacy remote desktop environment kept county services moving. To reach the county’s private applications, employees had to connect through a virtual desktop environment (VDI), authenticate again, and work inside that hosted environment. This experience added latency, support tickets, and security questions around who was connecting to what. While this worked as a band-aid, it was not a long-term solution. As offices reopened, some departments came back onsite while others remained hybrid.

“Our users are all over the map,” Woppert said. Around 500 full-time employees, plus contractors, third parties, and seasonal workers needed access that matched the reality of local government: different jobs, different locations, different risk profiles, different access permissions, one IT team responsible for protecting it all.

“It went from taking about five minutes for remote users to log in and load their apps to about 30 seconds. Now they can go home, open the laptop, and use it like they were in the office.”

Dr. Joel Woppert, Director of Information Technology, Washington County

During COVID, the question was, can people connect from home fast enough to keep county work moving? After COVID, the question became, can the county trust the user, limit access, and still make remote work simple?

From Basic Security Hygiene To A Stronger Zero Trust Model

When Woppert joined the team, Washington County was still improving its basic security hygiene. Phishing, web browsing risk, email threats, protecting users, and secure remote access were all on the IT team's radar. The county did not need more disconnected tools. It needed practical controls that could work across a messy public-sector environment with diverse users, applications, and legacy technology.

The county started with identity protection: securing administrator access to critical infrastructure by adding multi-factor authentication for server logins. Next, they focused on meeting new Criminal Justice Information Services (CJIS) requirements for the Sheriff's Office, including squad cars, which became the foundation for stronger authentication across the county.

This was not a simple task. Washington County's environment was not just a cloud-app story. The county had the productivity tools and infrastructure its workforce depended on, but it also needed to protect users accessing data from a variety of devices, including remote desktops, hardware, servers, squad cars, and specialized public-sector workflows. The identity layer had to support those devices and use cases too.

"We looked at other vendors, but Cisco Duo fit the bill for what we needed," Woppert said. "It gave us the flexibility we needed for servers, endpoints, and remote access."

The rollout gave the team an early proof point that stronger security did not have to become a new burden for users. It took two days to roll Duo out to IT. Servers followed a few days later. The Sheriff's Office, with roughly 150 users and complex shift schedules, was enrolled in about a week.

Woppert still remembers how simple the process felt: send the user a link, have them install Duo, and accept the prompt on their smartphone. "That was really it," he said. "I didn't have to type up a long list for our users. It was self-explanatory. They would log in, get the chime on their phone, validate that it was their system, and say yes. It was simple, easy to use, and it did not take a lot of effort to implement."

How Cisco's User Protection Suite secures Washington County's Workforce

Secure Access: Secure Access gives Washington County a simpler way to protect remote work, helping users safely access the internet and private applications by transitioning from a virtual desktop to zero trust network access (ZTNA). Employees get a more consistent work experience, while IT gets more granular control over who can access which resources.

Duo Identity Security: Duo helps Washington County strengthen authentication across critical use cases, from server access to Criminal Justice Information System requirements and remote access across the county. It gives the team a practical way to verify users before they reach sensitive systems.

Email Threat Defense: Email Threat Defense adds another layer of protection on top of Washington County's email provider. The IT team can monitor suspicious messages, investigate issues, and remove threats quickly when action is needed.

The Remote Access Problem Was No Longer Just Remote Access

Identity solved one part of the problem. Remote access was the next.

The virtual desktop environment required users to open a URL, enter credentials, approve an MFA prompt, wait for it to load, then open email, their messaging app, and other applications inside that environment. The desktop alone could take 30 seconds to a minute to load. Fully getting to work could take about five minutes.

The bigger problem was how fragile that flow could be. If a user profile failed to load, if single sign-on did not work, or if one authentication handoff added latency, the whole process could break. The user could be locked out of work, and IT would end up with another help desk ticket. Woppert described the old environment plainly: "Every day was kind of a different adventure."

Eric Mesa, IT Infrastructure Manager and Information Security Officer, saw the same pain from the operations side. The county was carrying license cost, third-party consulting cost, integration cost, and help desk load around a remote access model that was becoming harder to support. "It was a lot of management overhead," Mesa said.

As Washington County evaluated its options, they were careful about the human side of the architecture. "I didn't want to impact the end user," Woppert said. Another tool, another login, another visible change would make adoption harder. The win would have to be security that mostly disappeared into the background.

Security In The Background, The Same Work Day In Front Of The User

Cisco's role in the story was not a cold start. Washington County already had pieces of the foundation in place, including identity and internet security. Then the account team asked a simple question: why not bring those ingredients together into a broader zero trust access model? The county saw a demo of Cisco Secure Access, set up a trial, and began testing the solution.

Mesa expected the transition from the legacy environment to take far longer. "I was expecting a multi-year phase-in," he said. "We had an operating environment for our team within a month."

The pilot clarified the bigger point. This was not just a remote access replacement. It was a different access model. Users could be verified once, work from wherever they were, and get a consistent experience.

"Once they're enrolled and they were off site, their experience was the same no matter what," Mesa said.

For Woppert, the message to users became almost too simple: "I can tell them, 'Go home and use it as if you were in the office.' They ask, 'Really, that's it?' And I say, 'Really.'"

For the IT department, it gave them the tools to enforce least-privileged access. "We can control access per user, per department, and even down to specific port numbers for on-prem resources," Mesa said.

“The user only gets access to precisely what they need and authorized to get to, and it is pretty locked down. Plus, strong authentication is on top of all that.”

That combination changed the tradeoff. Users got less friction. IT got more control. “The amount of control and security that we can put behind that was just hands down the win-win solution for me,” Woppert said.

The Results

The team easily configured more than 30 private resources and is rolling the solution out to the workforce in a phased approach. The user experience changed just as clearly. “I sign in, approve the login on my laptop, and I’m working,” Woppert said. “If it’s 30 seconds for the client to kick in, that’s it. I’m ready to go for the day.”

The feedback from users has been direct and practical. “Now they use their computer as one stop,” Woppert said. “The days of waiting around, or not being able to log in, that’s gone. It does not exist anymore.”

For IT, the benefit is not just fewer complaints. It is a more manageable security program. “The monitoring and reporting are so intuitive that we basically have our entire team in there,” Mesa said. “We’re able to look at all of that data to figure out where the problem is. If it’s a network setting or something else, all the information is right there.”

The same theme showed up in email security. Washington County layered Cisco email protection on top of their existing email security and found the setup straightforward enough that they could easily monitor and maintain it. When suspicious messages had to be pulled back, the team could search, select, and remove them “within minutes,” Mesa said. After a review with Cisco, the team learned its settings were already aligned with best practices. Woppert credited the documentation: “I remember setting that up with Eric and I was thinking, boy, that’s it. That’s all we had to do.”

Using A Strong Security Baseline To Help Enable An AI Future

Washington County’s progress comes back to the basics. That’s what makes zero trust access useful: verify the user and endpoint, limit access, secure web and email activity, and make the experience consistent enough that users can keep doing their jobs.

That baseline matters in local government, where the security bar keeps rising. For example, under updated CJIS access requirements, Washington County could no longer treat squad cars as a default trusted location. Deputies needed to authenticate before reaching criminal justice data and systems. In addition, Health and Human Services brings HIPAA obligations. Sensitive public data and PII are part of the mission.

AI adds another layer to that reality. Woppert expects requirements to keep getting more stringent as AI evolves and attacks increase. But the point is not to shut down new tools. It is to make sure the county can enable them with the right visibility, policies, and protection for county data.

For generative AI use, Washington County is steering employees toward a vendor that aligns with government data and privacy requirements. But IT also knows employees may test other AI tools. The goal is to maintain enough visibility to shape policy and decide where stronger controls may be needed, without defaulting to hard blocking or shutting down useful AI work.

“Everything is going to have some sort of AI module built in that can talk to other tools,” Mesa said. “We just need to be prepared for that. We will continue to watch what security tools Cisco has to offer to make sure we have good insight into what’s happening in our environment.”

That is the balance Washington County is trying to strike: not blocking useful tools, but making sure AI adoption is approved by the county, visible, and aligned to county policy.

“I don’t want to block people from AI,” Mesa said. “We’re trying to get things in line: policies, how do we control this, what tools are out there, how do we train our end users.”

Mesa is also watching the evolution of Cisco Cloud Control, calling the dashboard “very intriguing”.

Specifically, he was interested in the idea of a shared canvas for human and agentic workflows that could create efficiencies and help speed up troubleshooting.

That is why the Washington County story matters beyond remote access. The county is not waiting for AI to become an urgent security problem before fixing the basics. It is building the controls that will make safer AI adoption possible when the county is ready to move further, without dragging users through the machinery of security every morning.

For Washington County, zero trust is becoming what good security should be: better for users, better for IT, and stronger security.