CASE STUDY

Protecting citizens with IoT Security in the Great Plains

The State of North Dakota partners with Palo Alto Networks to extend its cybersecurity leadership with IoT Security for advanced protection while enabling economic growth and optimized customer experience.

paloalto® NETWORKS

IN BRIEF

Customer

State of North Dakota Information Technology (NDIT)

Industry

Government

Country

United States of America

Products and Services

Technology and service to more than 800,000 citizens

Organization Size

1-500

Website

www.nd.gov/itd

Challenges

- IoT has introduced visibility, risk, and protection blind spots.
- Need security to be part of future IoT device adoption and digital transformation initiatives.

Requirements

- Provide visibility of the IoT landscape across all state institutions.
- Increase security across the network.
- Implement a solution that is scalable with future IoT expansion.

Solution

North Dakota Information Technology selects Palo Alto Networks IoT Security solution for best-in-class ML-powered visibility, prevention, and enforcement.

Extending cybersecurity leadership

The State of North Dakota has a very successful record of applying technology to drive positive transformation, improve state services, and enrich the lives of its citizens. The state's governor, Doug Burgum, is a former tech company executive, and Shawn Riley, state CIO and head of North Dakota Information Technology (NDIT), is an intrepid early adopter of groundbreaking technologies and a passionate advocate for solutions that make a difference for North Dakotans.

The state prides itself on taking a leadership position when it comes to technology adoption, internet connectivity, and cybersecurity. NDIT, part of the executive branch of state government, strives to make North Dakota the most cyber-conscious and secure state in the nation. The agency's tech-forward vision has led it to explore a wide range of innovations that advance the state's mission of transformation through technology.

In fact, the NDIT team has a number of US technology firsts and bests. North Dakota, for example, is a leader in broadband: All the state's residents have access to fiber and benefit from high-speed connectivity at home. And since its earliest days, NDIT has been on a continuous journey to improve and strengthen cybersecurity across the state. Palo Alto Networks has been an important partner on that journey for over a decade, helping NDIT grow its Security Operations Center (SOC) and better secure its network, data centers, and users statewide.

NDIT's goal is to deploy a world-class government experience, securing all government-held data in the state and delivering the most efficient government services in the US. Recently, NDIT has been tackling the next frontier in security and technology—the Internet of Things (IoT)—to further protect users on its network and promote tech innovation for businesses across the state, and ultimately, the nation.

Background

A STRATEGIC PARTNERSHIP LEADS TO TECHNOLOGY WINS WITH NATIONAL IMPACT

NDIT became an early adopter, in 2009, of Palo Alto Networks firewalls, attracted to the potential of gaining visibility over its network without large infrastructure investments.

"I still remember when we deployed our first Palo Alto Networks firewall," says Ryan Kramer, Enterprise Infrastructure Architect with NDIT. "Finally, we could actually see what was going on natively in the firewall. That was a huge moment for us. If you don't know what's on your network, you really can't control anything."

In the years that followed, NDIT deployed Palo Alto Networks Next-Generation Firewall solutions to transform security in multiple areas across the state. First, NDIT deployed the Palo Alto Networks firewall to protect the Bank of North Dakota, the only state-owned bank in the US. Next, the team shored up security within its data centers, deploying the first set of PA 7050 firewalls in the market, serial numbers 1 and 2.

With the data centers secured, NDIT focused on offering similar protections to citizens in a two-year project to put a firewall in front of every user across the state as they accessed NDIT resources. Continuing on this path, it extended security to North Dakota institutions of higher education, bringing firewalls to every campus in the state and providing protection against the unique threats in that sector.

Most recently, NDIT turned its attention to implanting a Zero Trust framework and equipping its SOC team with additional platform tools extending beyond the firewall, including Palo Alto Networks Cortex™ XDR. XDR is the world's first detection and response app that natively integrates network, endpoint, and cloud data to stop sophisticated attacks, accurately detecting threats with behavioral analytics and revealing the root cause to speed up investigations.

In sum, the result is a Palo Alto Networks-enabled Zero Trust security strategy across the entire NDIT network.

Challenge

INNOVATION IN STATEWIDE NETWORK SECURITY REQUIRES A WORLD-CLASS SOLUTION

As the NDIT team matured and expanded its approach to security, it realized that the next important security hurdle was to gain complete visibility into what was actually connecting to the network. The tools the team was using to scan their network for threats weren't providing an accurate picture. For example, an NDIT team might scan a school, expecting to see a variety of devices connecting to the network, but they were not getting reliable results back.

NDIT was also up against the practically exponential expansion of its IoT connectivity, which is projected to grow to two billion devices rapidly—and, eventually, even more. This growth vastly increases the threat surface and creates many more vulnerability entry points to the network that NDIT needs to discover and secure to maintain network security integrity. Driving this explosion is the innovative use of IoT in farming, commercial drone aviation, and other industries, as well as more and more personal and mobile devices in schools and across local and state government departments.

Innovation at NDIT never stands still. As the team continued to explore ways to improve network security, the state also wanted to pursue a number of business automation initiatives to advance commerce in North Dakota and across the US. To meet this challenge, however, NDIT needed a robust IoT visibility and security solution. What, for example, would a fully automated North Dakota farm of the future look like? Or, how could the state benefit from breakthroughs in beyond visual line of sight (BVLOS) drone aviation for public and private use?

Requirements

GOOD GOVERNMENT DEPENDS ON UNDERSTANDING THE TECHNOLOGY LANDSCAPE

To increase security across the network—called STAGEnet and connecting more than 252,000 daily users in a diverse environment for K-12, higher education, a state hospital, city, county, and all government branches, including the courts and legislature—NDIT needed to gain a better understanding of its IoT landscape.

At the same time, any solution it deployed needed to provide complete unmanaged device visibility, assess risk, and afford robust protection against known and unknown threats to enable the state to scale its standards for IoT security.

"Our strategy was to have at least one Palo Alto Networks IoT Security firewall between the network connectivity of any two users or devices, discovering and securing each device and guarding our network against vulnerabilities and attacks," explains Kramer. "We needed to ensure that the state's 'crown jewel' institutions, from banking to education to government, remain protected at the highest, world-class level. The challenge is, this also needs to be a scalable solution that will protect hundreds of thousands of devices today, and billions of devices in the future."

In short, its IoT security solution needed to support NDIT's continuing innovation agenda with a Zero Trust framework, enabling the state to further explore ways that technology can make businesses more efficient and secure while improving all North Dakotans' lives.

> Our strategy was to have at least one Palo Alto Networks IoT Security firewall between the network connectivity of any two users or devices, discovering and securing each device and guarding our network against vulnerabilities and attacks.
>
> **— Ryan Kramer, Enterprise Infrastructure Architect, NDIT**

Solution

THE DECISION IS EASY WHEN THE SOLUTION IS BEST-IN-CLASS

When it came time to select a solution, NDIT's decision was easy: Palo Alto Networks IoT Security solution. IoT Security delivers ML-powered visibility, prevention, and enforcement, surfacing unmanaged device data across the network, providing device risk analysis, and enabling the enforcement of recommended device risk-based policies to minimize risk.

The value of IoT Security was immediately apparent to NDIT, allowing the team to easily scan and see hundreds of thousands of devices connecting to the network—many of which had previously been hidden. The solution quickly became an important mechanism for IoT device discovery to improve network security.

What's more, IoT Security worked well with NDIT's other existing solutions. For example, NDIT used IoT Security to discover devices and set up firewall policies and then extend the device visibility and context to vulnerability management tools, enabling it to detect vulnerabilities across managed and unmanaged devices. Where previously, in a scan of, for instance, a particular K-12 school, prior tools returned unreliable results—an impossible report of zero devices—following deployment of IoT Security, a scan showed 10,000+ IoT devices in place. The Palo Alto Networks solution allowed NDIT to see and secure the previously undiscovered IoT devices. Multiplied by all the schools and other sites and users across the network, this system improvement had a huge impact on strengthening network security.

With Palo Alto Networks sponsorship, NDIT has been able to accelerate its progress and involvement in incubation projects, like the Grand Farm Initiative. This ambitious pilot project is accelerating innovation and research into technology that will enable the farm of the future–impacting North Dakota, the US, and the world by solving challenges and developing new transformation opportunities in the labor-intensive agriculture industry.

"We joke that we have cows on our network, and we do! North Dakota's agricultural community already tags cattle with IoT sensors for remote monitoring and automated husbandry," says Duane Schell, Chief Technology Officer with NDIT. "We expect this to grow as projects like the Grand Farm Initiative expand."

Similarly, NDIT's leadership has contributed to the development of Vantis, a statewide network enabling unmanned aircraft systems (UAS) flights beyond visual line of sight (BVLOS) for pipeline and power line inspection. Vantis is the first such program of its scale in the US. It's positioning North Dakota to become the nation's epicenter of commercial UAS activity and is also a public incubator expected to expand nationwide.

Benefits

INCREASED INSIGHT ENABLES STRONGER SUPPORT FOR MORE USE CASES AND THE NEEDS OF CUSTOMERS

Using IoT Security, NDIT has increased its ability to understand, secure, and manage network traffic loads. The agency can now better understand peaks and troughs of network usage—connecting between 250,000 and 400,000 devices, a user base equivalent in size to a Fortune 30 company.

That insight allows NDIT to better plan how to support and secure its network, particularly as it gains visibility over new kinds of devices accessing the network. "Once we were able to see what was connected to the network, we discovered an interesting range of devices," Kramer recalls. "We have sensors in agricultural sites, Amazon Alexa™ virtual assistants in school classrooms—we even found some networked Roomba vacuum cleaners!"

"As a CTO, I can easily manage known risk but what keeps me up at night is the unknown risk," laments Schell. "Inherently we knew we had IoT devices on our network but couldn't easily identify, quantify, or classify the devices or risk associated with them. Having Palo Alto Networks IoT Security in place provides that visibility and affords us the ability to manage the risk appropriately."

With greater visibility into the types and quantities of devices and equipment connecting to the network, NDIT can better prepare to support the specific needs and use cases of its customers. Increased visibility also affords the team opportunities to be a consultant to its community. NDIT, for example, recommends specific DVR camera systems for use in traffic monitoring and for security by multiple state agencies that are both affordable and compatible with the state's IoT network.

The ability to make these kinds of informed recommendations on network-optimized hardware peripherals enables NDIT to be more efficient and productive—and to promulgate best practices in support of the state's needs.

Palo Alto Networks IoT Security solution leveraged NDIT's firewall investment for comprehensive and integrated security posturing. Running in conjunction with the capabilities of the firewall, IoT Security automatically recommends and natively enforces security policies based on the level of risk and the extent of untrusted behavior detected in IoT devices.

Taking into account that trust is nothing but a vulnerability, the Palo Alto Networks solution directly aligns with the principle of Zero Trust to enforce policies for least-privileged access control. This significantly reduces the pathways for adversaries, whether inside or outside of the organization, to access critical NDIT IoT assets.

"Working closely with Palo Alto Networks, we've learned that Zero Trust is even more than a technology," says Kramer. "It's also about personnel. It's ideation that people have to adopt. Perhaps as much as a technology shift, it's meant a culture shift for our team, our vendors, and our users."

> As a CTO, I can easily manage known risk but what keeps me up at night is the unknown risk. Inherently we knew we had IoT devices on our network but couldn't easily identify, quantify, or classify the devices or risk associated with them. Having Palo Alto Networks IoT Security in place provides that visibility and affords us the ability to manage the risk appropriately.
>
> **— Duane Schell, Chief Technology Officer, NDIT**

UNBEATABLE IOT SECURITY IS THE KEY TO ECONOMIC GROWTH AND INFLUENCE WITHOUT BORDERS

North Dakota is justly proud of its leadership among states in cybersecurity and tech innovation. Palo Alto Networks IoT Security solution is now enabling the state to research new frontiers in IoT, aviation, farming, and other industries.

NDIT leaders have shared their learnings and North Dakota's noteworthy progress with other US states' IT agencies through meetings of the National Association of State Technology Directors (NASTD). Palo Alto Networks has partnered with NDIT in these efforts and is a NASTD sponsor organization.

"One of our mantras is, 'Continuous improvement,'" Kramer remarks. "We're never going to be done. We fully understand that; otherwise, we wouldn't be doing our job. We're always looking for automation opportunities and ways to strengthen security and improve our state's network."

Palo Alto Networks has helped NDIT build its SOC from the ground up; today it's world-class. Palo Alto Networks has also supported a groundbreaking multi-state SOC spearheaded by NDIT for cybersecurity and threat-hunting across boundaries, including tribal lands.

And with the pivot to remote work required by COVID-19, NDIT has implemented Palo Alto Networks Global Protect to ensure the security of always-on connectivity for its network and data. Also more secure and better protected are 500 NDIT team members, 8,000 other state workers, and almost 800,000 North Dakota citizens—in total more users than are supported by many leading US corporate enterprises.

Visit us online to find out more about how the industry's most comprehensive IoT Security solution delivers ML-powered visibility, prevention, and enforcement in a single platform for unmanaged devices. Start a free trial and see the benefits of IoT Security in your own environment.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com