North Dakota IT safeguards citizens with integrated, AI-driven security operations

RESULTS Platform strategy accelerates security response and optimizes IT spend.

99.6%
Decrease in open alerts, from 16,000 before Cortex XDR to ~50.

60%
Of total incidents are resolved automatically with Cortex XSOAR.

Minutes
To find a true positive with Unit 42 MTH vs. weeks previously.

The State of North Dakota Information Technology (NDIT) supports the technology needs of state government, K–12, higher education, cities and counties. As the internet service provider (ISP) of choice for its citizens and state agencies, NDIT has always seen its mission as driving digital innovation across the state.

In 2019, North Dakota state leadership made a shift to unify all IT services across the state to lower costs and operational complexity. NDIT security leadership saw an opportunity not just to unify its approach to security operations statewide but also to modernize for greater efficiencies, increase visibility, and improve threat detection and response.

CUSTOMER
State of North Dakota Information Technology

INDUSTRY
Government

COUNTRY
United States

PRODUCTS & SERVICES
- Cortex XSOAR®
- Cortex XDR®
- Cortex Xpanse®
- Cortex XSIAM®
- Unit 42® Managed Threat Hunting
- Unit 42® Retainer
- Prisma® Cloud
- Next-Generation Firewalls

CHALLENGE

Reining in costs while fighting sprawl.

- Scale security from 20,000 endpoints to 250,000 without increasing security staff.
- Unify over 600 state entities, overcoming siloed security tooling and unique processes.
- Enable both broad and granular visibility of the threat landscape–statewide or at the level of a single entity.
- Reduce the burden of handling tens of thousands of daily incidents for security operations staff.
- Strengthen and accelerate detection and response to cyber threats.

Path to platformization

Network security	Endpoint security	Incident response automation	Attack surface management	SOC transformation	Managed services and incident response	Cloud security
Next-Generation Firewalls	Cortex XDR	Cortex XSOAR	Cortex Xpanse	Cortex XSIAM	Unit 42 Managed Threat Hunting Unit 42 Retainer	Prisma Cloud

SOLUTION

Platform strategy drives statewide consistency and visibility.

NDIT chose the Cortex platform as the foundation for its next-generation Security Operations Center (SOC). The ability to extend platform protections from the network to the cloud was non-negotiable to achieve its goals. After 20 years as a Next-Generation Firewalls customer, moving to Cortex and adding Prisma Cloud allowed the organization to do just that. Cortex transformed operations, enhanced threat detection and response, and Prisma Cloud delivered a centralized view of the state's cloud assets, enabling better management and oversight of security posture across various cloud services.

Unification streamlines processes and lowers costs

By moving to the Palo Alto Networks platform, from the SOC down to the level of each state entity, NDIT was able to standardize everything from dashboards to policies and drive new automations. This made it possible to implement a statewide strategy for threat prevention and detection and response. The shift has not only streamlined the state's approach to its security operations, it's also yielded significant cost savings. NDIT CISO Michael Gregg notes, "While we're about the size of a Fortune 30 company, we operate at half the cost."

Automation dramatically reduces manual tasks

The Cortex platform helps NDIT comfortably manage security for over 250,000 endpoints while poised to scale to support the needs of the state's future growth. With the reduced volume of alerts for analysts, NDIT teams can focus on highest-priority incidents in a timely manner, making a bigger impact on safeguarding the state's digital resources. The streamlined workflow for SOC staff has allowed NDIT to achieve operational efficiencies equivalent to 8-10 SOC analysts.

Streamlined work makes for happier employees

Using AI and machine learning to automate many tasks that were previously manual has reduced analyst burnout, with NDIT staff experiencing improved job satisfaction. The state is seeing that translate to longer tenures: The average tenure for NDIT security operations staff has grown to three years, double the industry average of 18 months.

From 16,000 daily alerts → <60

196 playbooks help close over 60% of incidents

57% reduction in false positives for phishing incidents = 21,000 fewer incidents per year

> "The Cortex portfolio has really helped our SOC mature. With so many threats coming in, having that toolset has really been a big benefit for us."
>
> **Michael Gregg**, Chief Information Security Officer, North Dakota IT

Shift to proactive threat defense

Cortex Xpanse provides NDIT's red team greater visibility into North Dakota's attack surface. Those insights allow the team to better map where to test for vulnerabilities across the state. Through Unit 42 Managed Threat Hunting (MTH) services, NDIT has a team dedicated to monitoring threats around the clock and pulling in information from other attacks so the state is better positioned to respond to similar activities. Before Unit 42 MTH, the NDIT team could spend months working through many false positives before they would find a true positive, whereas now they're notified of incidents instantly. In addition, a Unit 42 Retainer gives NDIT peace of mind with incident response experts on call any hour of the day should an incident occur.

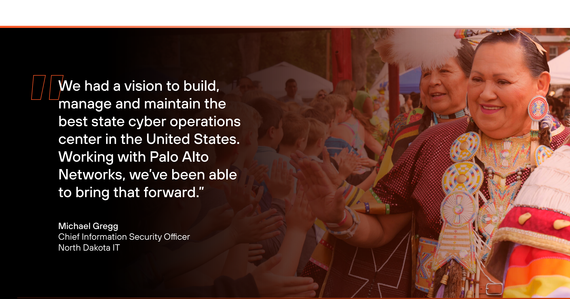
Interstate collaboration for greater security

Modernizing security operations has allowed North Dakota to share threat intelligence more effectively with other U.S. states. After working with North Dakota's elected officials to adapt state law allowing interstate IT communications, the CISO pitched leaders in other states on the vision of a joint-state SOC. Cortex XSOAR has made it possible to quickly integrate data from multiple states into a shared environment so participating states can compare threats and see how others are responding to them. Now, nearly 20% of states in the U.S. participate in the Joint-Cybersecurity Operations Command Center (J-CSOC) and achieve greater visibility and faster response to evolving threats.

Modernization is an ongoing journey.

Going forward, NDIT plans to continue building on its security transformation as AI and other technologies bring new challenges and threats. It recently adopted Cortex XSIAM as part of a strategy to fight threats with AI detection and response, which will enable greater levels of automation across its security operations.

Find out more about how Palo Alto Networks best-in-class solutions can improve security for your organization. Learn more about Cortex, Unit 42, Next-Generation Firewalls, and Prisma Cloud.



> "We had a vision to build, manage and maintain the best state cyber operations center in the United States. Working with Palo Alto Networks, we've been able to bring that forward."
>
> **Michael Gregg**
> Chief Information Security Officer
> North Dakota IT