

Mississippi State Department of Health IT Security Officer Jarad Stout uses AI-powered automation and centralized security operations to help his team detect, investigate and respond to cyberthreats more efficiently.

SEP 08 2025

SECURITY

State Agencies Seek a Streamlined, Actionable View of Risk

Replacing fragmented security monitoring efforts with centralized solutions brings threats into focus.

by Erin Brereton

Erin Brereton has written about technology, business and other topics for more than 50 magazines, newspapers and online publications.

LISTEN 08:43

After a hacker attempted to compromise the Mississippi State Department of Health's executive business email system in 2024, the agency decided to incorporate CDW's Incident Response Services.

"That was a big driver for our wanting to have a managed response capability," says IT Security Officer Jarad Stout. "One of the things I really liked about the incident response package was I could turn remaining contract hours into training and assessments for my team and organization. We just did a tabletop exercise in May."

The public health agency — which performs services ranging from physical exams to childcare facility licensing using Lenovo laptops, Apple iPad devices and other endpoints — had previously deployed Microsoft Defender and Palo Alto Networks' Cortex XDR endpoint detection and response solution.

Also implementing the Cortex XSIAM security operations platform, Stout says, helped unify the agency's tool profile.

Click the banner below to explore today's biggest cybersecurity concerns.



"We're able to grow and put more modules in place that allow us to take advantage of the telemetry and data in our network so we can gain a better understanding of the threat environment as it affects us," he says.

Today's state cybersecurity budgets need to cover rising talent and technology costs — yet 55% received the same funding amount this year as in 2025 or saw an increase of less than 6%, according to a survey by the National Association of State Chief Information Officers and Deloitte. Eight states' cybersecurity budgets were reduced.

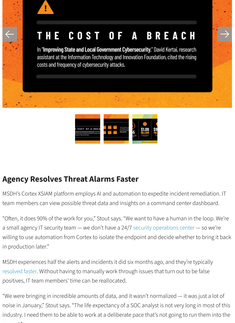
More than half of CISOs (59%) identified insufficient funding as a barrier to effective security, propelling the issue to become one of 2026's top three cybersecurity challenges.

States' other main cybersecurity concerns include a reliance on legacy infrastructure and solutions, and escalating threat sophistication.

Legacy hardware and software can be prone to attacks, while more modern tech tools may be able to mitigate threats; workforce deficits may be another obstacle, says David Kertai, research assistant at the Information Technology and Innovation Foundation and author of an April ITIF report on improving state and local government cybersecurity.

Bad actors are using artificial intelligence to discover new vulnerabilities in government systems, but state agencies can also take advantage of the emerging technology, Kertai says.

"These models could be used to help find those vulnerabilities before the attackers do and make changes," he says.



Agency Resolves Threat Alarms Faster

MSDH's Cortex XSIAM platform employs AI and automation to expedite incident remediation. IT team members can view possible threat data and insights on a command center dashboard.

"Often, it does 90% of the work for you," Stout says. "We want to have a human in the loop. We're a small agency IT security team — we don't have a 24/7 security operations center — so we're willing to use automation from Cortex to isolate the endpoint and decide whether to bring it back in production later."

MSDH experiences half the alerts and incidents it did six months ago, and they're typically resolved faster. Without having to manually work through issues that turn out to be false positives, IT team members' time can be reallocated.

"We were bringing in incredible amounts of data, and it wasn't normalized — it was just a lot of noise in January," Stout says. "The life expectancy of a SOC analyst is not very long in most of this industry. I need them to be able to work at a deliberate pace that's not going to run them into the ground."

North Dakota Centralizes Endpoint Protection

Several years ago, North Dakota Information Technology — which provides equipment, IT support and other services to state agencies — also began overseeing a cybersecurity strategy for public higher education institutions, school districts and local governments.

Those entities, which had previously managed their own cybersecurity systems, now have access to a centralized endpoint protection platform, vulnerability scanning solution and other resources.

"We were able to develop a common toolset and bring all of that logging and telemetry into one place," says CISO Chris Gergen. "We got much better visibility into the threats coming at North Dakota. It also put us in a position to build playbooks and leverage automation in a way we otherwise would not have been able to do."

The state, which had used Palo Alto Networks' next-generation firewalls for more than a decade, replaced its traditional security information and event management product with Cortex XSIAM in 2024, allowing it to automate actions that had historically been manual, thereby increasing operational efficiency, says Gergen.



> "We're willing to use automation from Cortex to isolate the endpoint and make a decision whether to bring it back in production later."
>
> **Jarad Stout, IT Security Officer, Mississippi State Department of Health**

Identity and access management, email and other data are fed into the platform. Analysts don't have to comb through tens of thousands of alerts spread across multiple tools; standardized dashboards show incidents and alerts, broken down into different queues.

Analysts can immediately identify, for example, if malware has been seen anywhere else in the environment. Their actions and any notes they leave in the platform when investigating alerts are logged, facilitating collaboration.

"Our security operations center sees roughly 70,000 cases a year, and the team that's responding is fewer than 10 people," he says. "There's really no way we would have been able to do that without the automation we've been able to build from this platform."

Palo Alto Networks also provides other cybersecurity assistance, including threat intelligence feeds that help NDIT stay up to date.

"The attack surface has certainly exploded. There are more endpoints, remote work, cloud adoption and data sprawl," Gergen says. "The increased reliance on third-party vendors has caused us to shift the way we think about security. Years ago, we were very heavily focused on the network perimeter. Now, we have to be ready to defend users, apps and data wherever it's at."

READ MORE: Identity is the new perimeter for government cybersecurity.

Utah CIO Gains Efficiencies Through Automation

Utah's Division of Technology Services uses Google's Chronicle Security Operations platform, which it implemented roughly five years ago, in addition to a SentinelOne endpoint protection solution with AI capabilities.

Other tools the state tried couldn't handle the scope of its information; funneling 10 terabytes of data daily into Google's platform isn't uncommon, says Utah CISO Phil Bates.

"If a new exploit comes out, you'll see a wave of scanning traffic from various sources trying to identify if you have those elements, and they can go after them," Bates says. "You can get denial of service attacks that will really flood your logs."

With Chronicle SecOps — renamed Google Security Operations in 2024 — organizations can retain and analyze unfiltered data and pivot between alerts, investigations and playbooks using one console.

40%

The percentage of public sector agencies that report threat detection and response is their most resource-constrained cybersecurity function

Source: SANS Institute, "Only 1 in 3 Government Cybersecurity Programs Are Fully Funded, the 2026 Cybersecurity Readiness in Government Survey Reveals, May 27, 2026

"Artificial intelligence tools go zipping through that massive amount of information, scanning for snippets of malicious code that might be there, and upon finding those, can generate a ticket that goes to one of our cybersecurity engineers to evaluate the risk," says CIO Alan Fuller. "That added a lot of value for us."

The platform's ability to handle large amounts of data, Bates says, proved beneficial when the state began shifting some applications from an on-premises data center to a Google- and Amazon-based cloud infrastructure in 2022.

"For a period of time, we doubled the volume we had in our logs," he says. "Chronicle handled it with no problems. If we had an on-premises solution with a limited amount of storage, we would have been in real trouble."

Rolling out Google's cloud-based security operations platform took less than 30 days, according to Bates, and it's consistently provided more timely results than previous solutions.

"If we got some information and I ran it in the other system, it would take probably eight hours to go back a day and search through all the data," he says. "I get that same return out of Chronicle in 30 seconds."

BRIAN STAIFFER/THESPOT

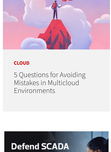
Latest Articles

When Government Gets Spatial: A Practical Path to Spatial AI for State and Local Agencies


5 Questions for Avoiding Mistakes in Multicloud Environments


Starlink Low-Earth Orbit Satellite Connectivity And How State Agencies Can Write Smarter RFPs


Closing The Whole-Of-State Cybersecurity Gap


DIGITAL WORKSPACE

When Government Gets Spatial: A Practical Path to Spatial AI for State and Local Agencies


CLOUD

5 Questions for Avoiding Mistakes in Multicloud Environments

Trending Now

Interoperability in Action: How Indiana And FirstNet Supported Texas Flood Search And Rescue Efforts

Q&A: New Jersey's Chief Innovation Officer Lifts The Curtain On Launching AI Projects

More On

ARTIFICIAL INTELLIGENCE | NETWORK MONITORING | NETWORK MANAGEMENT SOFTWARE | ENDPOINT SECURITY | FIREWALLS | IDENTITY MANAGEMENT | INTRUSION DETECTION | RISK ASSESSMENT | THREAT PREVENTION | MACHINE LEARNING | SECURITY SOFTWARE

Related Articles

SECURITY

Closing the Whole-of-State Cybersecurity Gap

ARTIFICIAL INTELLIGENCE

AI in State Government: Moving From Pilots to Operational Impact

SECURITY

How State and Local Governments Should Approach Data Exfiltration Prevention

Research Everything IT


Tap into practical IT advice from CDW experts.

Visit the Research Hub

Get StateTech in your Inbox

Browse Email Archives

Subscribe to StateTech Magazine

Browse Magazine Archives

Copyright © 2026 CDW LLC 200 N. Milwaukee Avenue, Vernon Hills, IL 60061

Do Not Sell My Personal Information