A **GOVERNMENT TECHNOLOGY** THOUGHT LEADERSHIP PAPER

Cyber Defense Built for Government

Fighting Ransomware with Managed Detection and Response Partnerships

SPONSORED BY

SOPHOS

CIS Center for Internet Security

Introduction

State and local governments face a mounting cybersecurity challenge as ransomware and AI-driven threats grow more sophisticated while staffing shortages and aging infrastructure limit agencies' ability to respond. For many organizations, 24x7x365 threat monitoring remains out of reach, making trusted cybersecurity partnerships increasingly essential.

"A significant number of ransomware attacks now have a component of data exfiltration," says Paul Zindell, director of sales engineering for the public sector at Sophos. "You want to have that service looking through your environment, picking up on those detections and getting ahead of the problem before the ransomware payload is executed."

Government agencies manage highly sensitive data, from police records and tax information to unemployment and health services systems. At the same time, they must navigate strict compliance requirements, procurement cycles, grant funding limitations and aging technology environments. Not every cybersecurity provider is designed for those realities. Public sector organizations need trusted operational partners, not simply additional security tools.

Proven Expertise Backed by Trusted Technology

The nonprofit Center for Internet Security® (CIS®) helps public sector organizations access enterprise-grade cybersecurity capabilities through a shared-services model designed specifically for state, local, tribal and territorial (SLTT) governments. CIS supports a range of organizations, including election offices, K–12 school districts, public utilities and small municipalities that often operate with constrained resources.

The center provides CIS Managed Detection and Response™ (CIS MDR™) through deployment models that align with varying compliance and operational requirements, including GovCloud-compatible environments and commercial cloud options powered by Sophos endpoint protection technology.

CIS MDR combines detection technology with nationally coordinated threat intelligence from the Multi-State Information Sharing and Analysis Center (MS-ISAC), which CIS operates. This allows analysts to identify emerging attack patterns across thousands of SLTT organizations and rapidly provide defensive guidance during large-scale threat campaigns.

Pairing MDR services with endpoint protection helps agencies strengthen cybersecurity coverage without expanding internal headcount. The 24x7x365 U.S.-based CIS Security Operations Center (SOC) continuously monitors threats, manages response and supports agencies during off-hours and holidays. The CIS Cyber Incident Response Team (CIRT) provides forensic analysis and additional support when needed.

"We have this process down. We know what to do if something comes up," says Nathaniel Ludke, security operations center analyst for CIS. "Even when a government agency may not be in the office, we're still there."

The agencies best positioned to withstand cyberattacks are those that invest in trusted partnerships and coordinated defense before a crisis occurs — not during one.

Alliances Offer Stronger Prevention and Faster Resolution

Partnerships between CIS, Sophos and SLTT organizations help agencies simplify threat response and reduce the time between detection and containment.

If a device shows signs of ransomware activity, CIS analysts can correlate that behavior against MS-ISAC intelligence and active campaigns targeting other governments. Analysts can then isolate affected endpoints before encryption spreads laterally across systems.

Similarly, if credentials are compromised through phishing, CIS MDR can isolate affected endpoints, run scans, provide remediation guidance and escalate the issue to CIRT if needed.

CIS selected Sophos as a partner because its MDR, endpoint detection and telemetry capabilities align with the operational realities facing many SLTT organizations. Sophos provides scalable cloud infrastructure and integration support, while CIS maintains operational oversight and contextualizes telemetry using government-specific threat intelligence and SLTT-focused workflows.

Those workflows include support considerations for elections infrastructure, K-12 school systems, public utilities and rural municipalities, each of which faces distinct operational and regulatory challenges. The relationship also reflects CIS's public-good mission and vendor-neutral approach focused on improving government cyber resilience rather than promoting a single technology ecosystem.

The collaboration between CIS and Sophos extends beyond deploying existing technology. The organizations work together to evaluate emerging threats and introduce capabilities that better support government agencies and the communities they serve.

Conclusion

Solutions built around government-specific operational and compliance requirements give SLTT agencies a meaningful cybersecurity advantage. With the right MDR partnership, organizations can extend limited resources, improve ransomware readiness, and strengthen resilience with around-the-clock monitoring and response support.

Through its role operating the MS-ISAC, CIS combines nationally coordinated threat intelligence, SLTT-focused expertise and 24x7 MDR operations designed specifically for government environments. Combined with Sophos detection and response technologies, this approach helps agencies respond more effectively to evolving cyber threats.

As ransomware operations become more coordinated and AI accelerates threat activity, SLTT organizations need more than standalone security tools. They need trusted operational partners with national-scale visibility, government-specific expertise and a mission aligned with protecting public services and critical community infrastructure.

The agencies best positioned to withstand cyberattacks are those that invest in trusted partnerships and coordinated defense before a crisis occurs — not during one.

"The good news is in the cybersecurity world, a lot of the big groups responsible for these attacks have been taken down. But when they get taken down, there are a lot more smaller groups that come out of the woodwork," Zindell says. "It's important to be resilient and partner with an organization that actually knows your business."[1]

1. https://webinars.govtech.com/Cyber-Defense-Built-for-Government%3A-Why-Trusted-MDR-Partnerships-Matter-for-State-and-Local-Agencies--144529.html?

This piece was written and produced by the Government Technology Content Studio, with information and input from Sophos and Center for Internet Security.

Produced by Government Technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education.

www.govtech.com

Sponsored by Sophos

Sophos delivers superior cybersecurity outcomes by providing cybersecurity as a service to protect companies of all sizes from the most advanced cyberthreats. Our cybersecurity products and services include managed detection and response (MDR), firewall, email, endpoint (XDR), and cloud native security protection. Sophos products and services defend against ransomware, phishing, malware, and more. They connect through the cloud-based Sophos Central management console and are powered by Sophos X-Ops, our cross-domain threat intelligence unit. We provide fully managed security solutions so you can manage your cybersecurity directly with our security operations platform. Or, you can supplement your in-house team with Sophos' products and services.

www.sophos.com

Sponsored by CIS

The Center for Internet Security, Inc. (CIS) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Critical Security Controls® and CIS Benchmarks® guidelines, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®) organization, the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®) organization, which supports the rapidly changing cybersecurity needs of U.S. election offices.

To learn more, visit **cisecurity.org** or follow us on X: **@CISecurity**.

ADOBESTOCK/AI GENERATED