CROWDSTRIKE

White Paper

Whole-of-State Cybersecurity with CrowdStrike

Driving better security and operational outcomes

As state and local governments and educational institutions continue to be in the crosshairs of cyberattacks, cybersecurity remains a critical concern. The job of defending today's dynamic perimeter is increasingly complex, and teams are facing sophisticated cyber threats that can disrupt critical services and compromise sensitive data. Many of these entities find themselves without the budget, expertise and skills to thwart their attackers. To effectively safeguard operations and constituents' information, state governments need a comprehensive approach to cybersecurity. Whole-of-state cybersecurity is a collaborative effort across state government, local government and education to protect citizens, data and digital infrastructure.

Managing through the complexities

Understanding and addressing the common challenges state and local governments face are crucial for effectively deploying a comprehensive cybersecurity solution across the state. When embarking on a whole-of-state strategy, state government cybersecurity leaders need to consider the following.

Fragmented cybersecurity: State and local governments comprise numerous agencies, departments, counties, municipalities, cities and school districts, each with its own unique cybersecurity needs and infrastructure. Aligning these diverse entities under a single cybersecurity solution requires a comprehensive understanding of their varying requirements, technologies and operational structures — and a platform that is flexible enough to meet these individual needs. Distributed agencies and local teams need a platform that can allow them to build unique policies, address specific threats and respond to incidents and prioritize vulnerabilities that impact only them.

Budget constraints: State and local governments often face budget limitations and must carefully allocate resources across multiple initiatives. Balancing cybersecurity needs with the available budget can be a challenging task for cybersecurity leaders. Platform consolidation helps save cost, increase speed of incident response, and improve security outcomes, leading to better use of existing budgets and better return on future investments and funding.

Interagency coordination: Achieving effective collaboration and coordination among different agencies and entities within a state government is essential for a successful whole-of-state cybersecurity initiative. However, interagency cooperation may face organizational and cultural barriers as well as potential resistance to change. Establishing clear communication channels, shared goals and governance structures can help overcome these challenges.

Adversaries are targeting state and local governments:

58%

of state and local organizations experienced a ransomware attack in 2021

Source: Sophos, The State of Ransomware in State and Local Government 2022

Legacy systems and infrastructure: State and local governments often operate with legacy systems and diverse technology landscapes that have accumulated over time. Legacy systems may lack the necessary security features, making them vulnerable to cyber threats and requiring additional measures to ensure protection.

Compliance and regulatory requirements: State and local governments must adhere to various compliance and regulatory frameworks, such as data privacy laws and industry-specific regulations. Cybersecurity leaders need to carefully evaluate the solution's capabilities for addressing specific compliance needs and facilitating audits and reporting.

Skills and workforce challenges: State and local governments often face a shortage of cybersecurity professionals, making it challenging to effectively implement and manage an effective cybersecurity strategy. Upskilling existing staff, recruiting specialized talent and establishing training programs are important, as is choosing a cybersecurity partner that can augment your team's efforts by supporting crucial incident response and helping prioritize threats and vulnerabilities.

Evolving threat landscape: Cyber threats continuously evolve and become more sophisticated. The chosen solution must have the agility to adapt to emerging threats and provide timely updates and patches. Proactive threat intelligence capabilities are essential to stay ahead of threats and ensure a resilient cybersecurity posture.

Addressing these challenges requires a well-planned strategy that includes stakeholder engagement, thorough assessment of requirements, careful selection of the cybersecurity solution, robust project management, and ongoing monitoring and evaluation. By proactively identifying and mitigating these challenges, government cybersecurity leaders can pave the way for successful implementation of a whole-of-state cybersecurity strategy that effectively safeguards critical infrastructure, services and citizen data.

Adversaries are targeting state and local governments:

72%

of state and local governments attacked had their data encrypted

Source: Sophos, The State of Ransomware in State and Local Government 2022

Business value of a whole-of-state approach

Strengthened security posture: A whole-of-state cybersecurity approach enables consistent and unified security measures across all entities. By implementing standardized policies, procedures and controls, state governments can establish a strong security posture that minimizes vulnerabilities and ensures a higher level of protection against cyber threats. This approach promotes a proactive security mindset and reduces the risk of successful cyberattacks.

Improved collaboration and information sharing: State governments can foster collaboration and information sharing between various entities. By breaking down silos and establishing communication channels, cybersecurity leaders can share threat intelligence, best practices and lessons learned. This collaborative environment enables a more coordinated response to cyber incidents and facilitates the identification and mitigation of emerging threats.

Enhanced situational awareness: A comprehensive cybersecurity solution implemented at the state level provides a centralized view of the entire government network. This visibility allows cybersecurity leaders to gain real-time situational awareness of potential threats, vulnerabilities and ongoing attacks. With this information, they can make informed decisions, prioritize response efforts and effectively allocate resources to mitigate risks and protect critical assets.

Cost efficiency and resource optimization: Adopting a whole-of-state approach to cybersecurity enables economies of scale. By consolidating security efforts, leveraging shared resources and avoiding redundant solutions, both state and local governments can achieve cost savings. Centralized management and standardized security measures also streamline security operations, reducing administrative overhead and optimizing the allocation of cybersecurity resources.

Streamlined compliance and governance: A comprehensive cybersecurity solution aligned with regulatory requirements simplifies compliance efforts for state and local governments. By implementing consistent security controls and mechanisms, these entities can ensure compliance with relevant laws, regulations and industry standards. A whole-of-state approach facilitates audits, reporting and regulatory assessments, reducing the compliance burden on individual entities.

Adversaries are targeting state and local governments:

59%

increase in the frequency and complexity of state and local government attacks from 2020 to 2021

Source: Sophos, The State of Ransomware in State and Local Government 2022

Resilience against advanced threats: Whole-of-state cybersecurity solutions from CrowdStrike incorporate advanced technologies such as artificial intelligence (AI), machine learning (ML) and behavioral analytics. These technologies enable proactive threat detection, rapid response and adaptive defense. By leveraging these capabilities, state and local governments can effectively detect and mitigate sophisticated cyber threats, such as ransomware attacks, advanced persistent threats (APTs) and zero-day attacks that exploit vulnerabilities in the software supply chain or in your IT infrastructure.

Comprehensive incident response: A whole-of-state approach enables a coordinated and efficient incident response process. With centralized incident management capabilities, cybersecurity leaders can orchestrate incident response efforts, ensuring timely and effective remediation. Coordinated incident response minimizes the impact of cyber incidents, reduces downtime and helps restore services quickly, thus minimizing disruptions to government operations.

Funding whole-of-state strategies with grants

There are various ways to fund whole-of-state strategies, and many states are opting to leverage funding provided by federal grants. Through the Infrastructure Investment and Jobs Act (IIJA) of 2021, Congress created the State and Local Cybersecurity Improvement Act, which established the State and Local Cybersecurity Grant Program, appropriating $1 billion to be awarded over four years.

The State and Local Cybersecurity Grant Program requires states to apply for funding and pass 80% of this funding to state and local governments.

There are three possible methods that states can use to pass down the funds:

1. States subgrant funds directly to eligible local entities to purchase necessary cybersecurity solutions and cover other eligible expenses.
2. States purchase cybersecurity solutions and cover other eligible expenses on behalf of all local governments.
3. States combine the two methods above, purchasing cybersecurity solutions and covering other eligible expenses on behalf of ***some*** local governments while allocating funds to others.

It is up to individual states to decide which method to use.

Adversaries are getting more sophisticated, moving beyond malware and abusing valid credentials:

71%

of attacks in 2022 were malware-free, increasing from 39% in 2018

Source: CrowdStrike 2023 Global Threat Report

In addition, in early 2023, the U.S. Department of Homeland Security (DHS) announced more than $2 billion in funding for eight preparedness grant programs. These programs address six national policy priority areas that reflect the current complex threat environment. Cybersecurity is a key priority area, and funding from both the State Homeland Security Program (SHSP) and the Urban Area Security Initiative (UASI) can be used to invest in cybersecurity efforts. The grant application process varies from state to state, and some state application windows may be open for a limited time or have additional requirements.

Finding grant opportunities

Through 2024, these state and federal grants will be available to support cybersecurity projects across the United States. CrowdStrike's Grant Support Program experts can provide information to help you capitalize on these opportunities. The program provides state, county and city agencies, state administrative agencies, educational institutions, healthcare organizations and utility providers with valuable grant information, customized funder prospecting research and program consultation to help develop project ideas, draft submissions to get technology-rich projects funded and expand initiatives that are already in the works.

DHS preparedness grant programs

The preparedness grant programs provide critical funding to help state, local, tribal and territorial officials prepare for, prevent, protect against and respond to acts of terrorism. Further information is available at *www.dhs.gov* and *www.fema.gov/grants.*

Ransomware attacks impacted the organizational ability to operate for

82%

of state and local governments

Source: Sophos, The State of Ransomware in State and Local Government 2022

The power of CrowdStrike

By leveraging CrowdStrike's advanced technology and expertise, state governments can achieve the following benefits.

Centralized threat detection and response: The cloud-native CrowdStrike Falcon® platform provides real-time visibility into potential threats across the entire state government network. With continuous monitoring and rapid response capabilities, it enables proactive threat detection and minimizes response times, which can prevent potential damage and reduce the impact of cyber incidents.

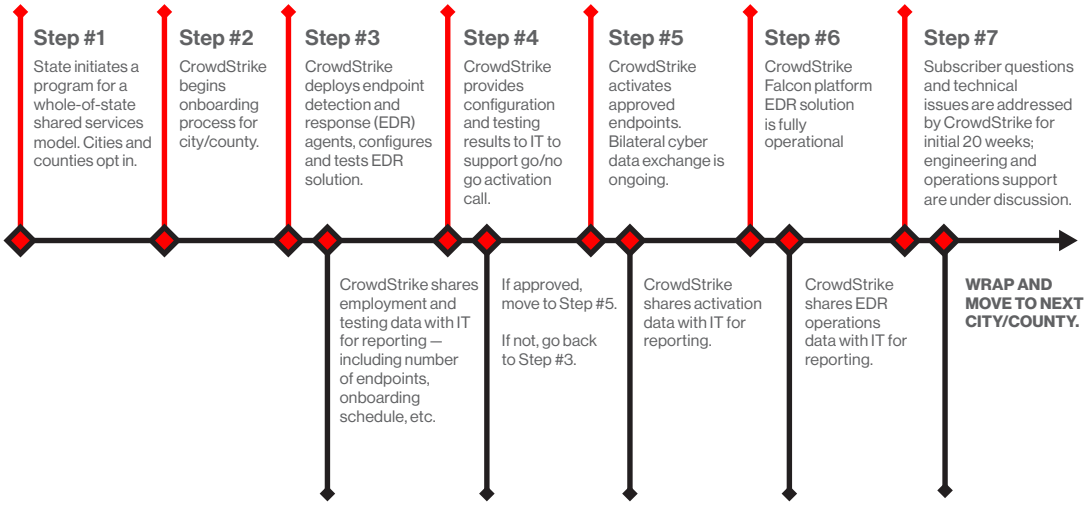
Unified security management: CrowdStrike enables state governments to consolidate their cybersecurity operations, streamlining security management processes and enhancing coordination between agencies, counties, municipalities, cities and school districts. A unified security management approach helps ensure consistent application of security policies, facilitates information sharing and improves overall situational awareness.

Scalability and flexibility: The Falcon platform can be tailored to the specific needs of state governments, accommodating the unique requirements of diverse entities. Whether it's scaling to cover multiple agencies or adapting to different infrastructures and technologies, the Falcon platform offers flexibility without compromising the effectiveness of the cybersecurity measures.

Proactive threat intelligence: CrowdStrike's threat intelligence capabilities provide state governments with invaluable insights into emerging threats and attack trends. Leveraging ML and AI, the Falcon platform continuously analyzes vast amounts of data to identify potential risks and indicators of compromise, enabling proactive defense measures and reducing the likelihood of successful cyberattacks.

Advanced endpoint protection: CrowdStrike's endpoint protection technology safeguards state government devices, including desktops, laptops and servers. By utilizing next-generation antivirus, ML and behavioral analysis, it can detect and prevent malware, ransomware and other advanced threats, helping to ensure the security of critical systems and sensitive data.

Timeline of Activities for CrowdStrike's Whole-of-State Approach



Implementing a whole-of-state approach to cybersecurity with CrowdStrike empowers state governments, local governments and educational institutions to stay ahead of cyber threats, strengthen their defenses, and better protect essential services and citizen data. CrowdStrike can work with you every step of the way to help with implementation and onboarding for each separate agency, city and county, as well as adoption, testing, and technical and operational support. By centralizing security management, leveraging advanced threat intelligence and deploying robust endpoint protection, state governments can create a more secure environment for their operations while fostering collaboration and resilience across all entities within the state.

Visit our website to get started: www.crowdstrike.com/solutions/public-sector/whole-of-state-cybersecurity/.

Contact us today at grants@crowdstrike.com for funding information.

Follow us:

- **Blog ›**
- **Twitter ›**
- **LinkedIn ›**
- **Facebook ›**
- **Instagram ›**

CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.