Identity Security for State and Local Government

Thank you for downloading this CyberArk Solution Brief. Carahsoft is the distributor for CyberArk cybersecurity solutions available via GSA, CMAS, MHEC, and other contract vehicles.

To learn how to take the next step toward acquiring CyberArk's solutions, please check out the following resources and information:

For additional resources:
carah.io/CyberArkResources

For upcoming events:
carah.io/CyberArkEvents

For additional CyberArk solutions:
carah.io/CyberArkSolutions

For additional cybersecurity solutions:
carah.io/cybersolutions

To set up a meeting:
Cyber-Ark@carahsoft.com
703-871-8548

To purchase, check out the contract vehicles available for procurement:
carah.io/CyberArkContracts

CYBERARK

SOLUTION BRIEF

IDENTITY SECURITY FOR STATE AND LOCAL GOVERNMENT

SECURE ALL IDENTITIES WITH THE CYBERARK IDENTITY SECURITY PLATFORM:

- Administrators: IT admins, cloud admins, sys admins, app or DB Admins
- Third Parties: external vendors and consultants
- Business users
- Standard end users
- Machine identities
- Applications

"Identity is everything now."

Jay Gazlay, Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA)

ESTABLISHING A NEW PERIMETER

The rise in ransomware resulting in data breaches of the IT infrastructure is becoming a daily occurrence. The unauthorized access of traditional network security perimeters of state and local governments, law enforcement agencies, and transportation target the core of the citizen's daily life. These breaks in security have one thing in common – they're low-hanging fruit for hackers. In fact, state and local governments have become one of the most targeted public sectors for data breaches yet they have the least amount of funding and resources to protect themselves from cyberattacks.

Phishing, ransomware, malware, insider threats and more challenge state and local governments more and more every day. At the same time, municipalities face a lack of qualified cybersecurity staffing and budget constraints, legacy IT infrastructure and workforce changes wrought by the pandemic in addition to modernizing their environment with digital transformation. Each endpoint and application connection creates a potentially harmful entry point into the municipalities' most sensitive data. As the perimeter expands, risks increase and traditional security methods are no longer enough.

IDENTITY IS THE NEW BOUNDARY

To protect valuable state, county or city data, CISOs must strengthen their cybersecurity posture and work closely with all stakeholders to protect its citizens, crucial data, taxpayers' money and reputation in the community. CISOs and IT admins need to ensure municipalities adopt an "assume breach" mindset and embrace a Zero Trust model to protect the employees' and citizens' identities. Identity is now the new security perimeter and least privilege is the way to implement a Zero Trust philosophy.

Securing the expanding number and types of identities – within business applications, from hybrid to multicloud workloads and throughout the DevOps pipeline – requires a new approach rooted in privileged access. Security leaders recognize that nearly every recent major cyberattack has involved compromised identities and subsequent manipulation of privileged access. Management of privileges, trust, and identities in these dynamic environments is the key to successfully enabling innovation, supporting a mobile workforce, and ensuring the protection that state and local government employees, as well as the citizens, expect.

CYBERARK'S IDENTITY SECURITY PLATFORM

CyberArk's Identity Security Platform is built on the pillars of management for Access, Privilege, and DevSecOps to deliver authentication, authorization, access, and audit in an integrated, seamless manner—enabling security at every step in the Identity Security lifecycle. Our intelligent approach balances the need for better security with end user productivity. CyberArk solutions leverage real-time intelligence and analytics to create a context-based, adaptive approach to the Identity Security lifecycle – for all identities, across all systems and apps, using any device. To mitigate the risk of a security breach, state and local governments need to adopt a security solution with consistent controls that specifically address their privileged access management (PAM) exposure.

Moreover, Executive Order 14028 requires federal agencies to adopt Zero Trust as a measure "to prevent, detect, assess, and remediate cyber incidents" as a key part of modernizing cybersecurity programs, services, and capabilities. CyberArk solutions bring this same critical capability to state, local, and municipal infrastructures.

CUSTOMER EXAMPLE

A large city struggled with on-premises privilege management and had experienced turnover in the Information Security team. The CTO decided that the best solution was to move the project to the cloud and implement CyberArk Privilege Cloud.

Moving the project to the cloud brought the city the latest technical and security advantages, with minimal impact on its limited resources.

ESTABLISH PAM SUCCESS WITH THE CYBERARK BLUEPRINT

CyberArk has developed a prescriptive blueprint to help state and local governments establish and evolve an effective PAM program. The CyberArk Identity Security Blueprint is designed to defend against three common attack chain stages used to steal data and wreak havoc. Simple, yet comprehensive, the CyberArk Blueprint provides a prioritized, phased security framework that closely aligns PAM initiatives with potential risk reduction, helping state and local governments address their greatest liabilities as quickly as possible. As a leader in Identity Security, CyberArk is uniquely positioned to deliver a thorough and effective PAM blueprint designed to:

- **Prevent Credential Theft through session isolation, removal of hardcoded privileges and access.**
- **Stop Lateral and Vertical Movement** with credential boundaries, ephemeral (non-persistent) access and credential randomization.
- **Limit Privilege Escalation and Abuse** by providing least privilege, adaptive response and delivering user behavior analytics to you and your team.

THE NEXT NORMAL

The world has changed, and no municipality is exempt. Stakeholder expectations and demands have changed to meet the expanding threat landscape. Your ability to reduce risk and protect your networks, assets, intellectual property, users, and citizens is dependent on how you protect your new perimeter: Identity.

About CyberArk

CyberArk (NASDAQ: CYBR) is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security solutions for any identity – human or machine – across business applications, distributed workforces, hybrid cloud workloads, and throughout DevOps pipelines. The world's leading organizations trust Cyberark to help secure their most critical assets. To learn more about CyberArk, visit www.cyberark.com.

©Copyright 2021 CyberArk Software. All rights reserved. No portion of this publication may be reproduced in any form or by any means without the express written consent of CyberArk Software. CyberArk®, the CyberArk logo and other trade or service names appearing above are registered trademarks (or trademarks) of CyberArk Software in the U.S. and other jurisdictions. Any other trade and service names are the property of their respective owners. U.S., 06.21. Doc. 265206

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice.