tenable

Solution Brief

Tenable for State & Local Government and Education (SLED)

Protect Critical Infrastructure and Citizen Data

State and local government and the education (SLED) sector collect and process significant amounts of personal data and therefore are prime targets for today's frequent and increasingly complex malware and ransomware cyberattacks. While hacks at the SLED level may receive less media attention than federal infrastructure breaches, they can be equally devastating. Americans rely on and frequently interact with SLED systems like Medicaid and the Department of Motor Vehicles (DMV)—both of which handle reams of sensitive personal information.

Financially motivated adversaries infiltrate SLED networks to steal and subsequently sell or otherwise exploit lucrative data, including Social Security numbers, credit card information, and tax and health records that yield profitable payouts on the black market.

> **"SLED governments protect vital aspects of everyday life for U.S. citizens, including schools, roads and medical care. Ensuring that these increasingly Web-based systems are protected from cyberattacks is vital to protecting the nation's critical infrastructure."**
>
> -Examining the State, Local IT Connection to National Infrastructure

SLED agencies and institutions are under mounting pressure to protect citizen data, critical infrastructure, and the delivery of public services. The proliferation of sophisticated attacks by organized crime and nation-states against commercial entities has raised awareness in the SLED arena and driven a heightened sense of urgency to prevent breaches. Establishing a more resilient cybersecurity defense is essential to maintaining our way of life.

Solutions

- *Tenable.io*
- *SecurityCenter Continuous View*
- *Nessus Network Monitor*

Key Benefits

- Infrastructure and Data Security
- *Continuous Compliance*
- *Resource Optimization*
- *Reduced Risk*

The City *of*
SAN DIEGO

> ***"Tenable has helped us build a flexible, streamlined security program that reduces our attack surface."***
>
> *-Gary Hayslip, CISO, City of San Diego*

Key Challenges

According to the Center for Internet Security, state and local governments are still playing catch up in cybersecurity and fall well below minimum maturity level benchmark recommendations. SLED organizations often lack the visibility and actionable intelligence to assess current security posture, and the proper controls and protections to block malware from infecting systems.

Infrastructure and Data Security
Protecting critical infrastructure and citizen data is of paramount importance to national security, individual privacy and daily living, but many SLED agencies don't have the tools and technologies required to monitor networks, devices and applications across on-prem, cloud and mobile environments. Insider and outsider threats and vulnerable third-party vendor and business partner systems continue to jeopardize cybersecurity posture.

Continuous Compliance
SLED organizations face increased scrutiny and stricter policy enforcement from regulators that are demanding higher levels of protection for citizen data and greater transparency with regard to breach incidents. Ensuring adherence to standards and frameworks is especially difficult for smaller agencies with fewer resources.

Resources and Expertise
Budget-constrained SLED entities struggle to compete with private sector organizations for premium cybersecurity talent with the skills and expertise required to manage modern risk. A shortage of staff resources coupled with financial constraints on essential investments in best-of-breed emerging security technologies leave SLED networks vulnerable to compromise and hinder ability to improve security posture. Integrating and managing complex security products and standalone point solutions is an overwhelming and time-consuming task for many SLED organizations.

Legacy Systems
Many states rely on IT systems that are decades old. Agencies struggle to secure outdated technology and unsupported shadow IT infrastructure. Critical updates are not available, vulnerabilities go unpatched, and older systems do not interoperate with modern platforms.

SLED organizations need simple, flexible, scalable and integrated tools and technologies that enable a comprehensive and dynamic defense against cyber threats.

Solutions Overview

Tenable cybersecurity solutions empower governments and schools to rigorously protect citizen data and critical infrastructure. Our vulnerability management and analytics tools and technologies enable agencies to gain full visibility and continuously monitor security and compliance posture; evaluate vulnerabilities across the ecosystem; measure and analyze effectiveness of security mechanisms; and understand, prioritize and mitigate risk.

The Tenable cybersecurity solutions portfolio for SLED includes cloud-based and on-prem vulnerability management platforms:

Tenable.io
The World's First Cyber Exposure Platform

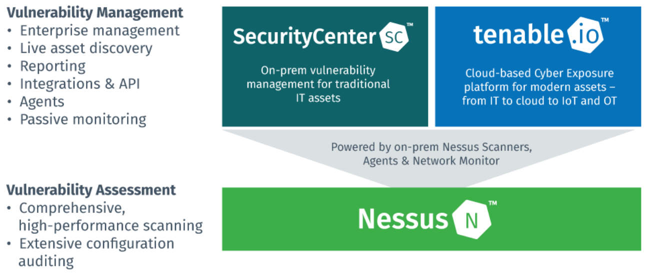
Manage risk on the modern attack surface. Tenable.io enables real-time discovery of every modern asset across all digital computing environments. Live discovery allows SLED organizations to accurately assess, analyze and prioritize constantly evolving vulnerabilities across the entire ecosystem. Bring clarity to security posture with an asset-based approach to security that provides maximum coverage in a dynamic landscape.

SecurityCenter Continuous View
The Market-Defining Continuous Network Monitoring Solution

Continuously discover, assess, improve and report on every aspect of network security and compliance, encompassing all on-prem, virtual, cloud and mobile devices, systems and technologies.

Nessus Network Monitor

Gain complete visibility of device security and overal network status with a combination of active scanning and passive monitoring. Deploy Nessus Network Monitor to non-intrusively detect assets and their vulnerabilities. Passive monitoring is safe for sensitive devices and avoids the need to take critical systems offline for assessment.


Vulnerability Management
• Enterprise management
• Live asset discovery
• Reporting
• Integrations & API
• Agents
• Passive monitoring
SecurityCenter SC™
On-prem vulnerability management for traditional IT assets
tenable.io™
Cloud-based Cyber Exposure platform for modern assets – from IT to cloud to IoT and OT
Powered by on-prem Nessus Scanners, Agents & Network Monitor
Vulnerability Assessment
• Comprehensive, high-performance scanning
• Extensive configuration auditing
Nessus N™

SLED Portfolio Features and Capabilities

- Continuously monitor on-prem, mobile and cloud-based SLED assets for vulnerabilities and threats to safeguard critical infrastructure and citizen data.
- Gain the visibility and actionable intelligence required to quickly contextualize, prioritize and remediate vulnerabilities in IT infrastructure.
- Discover and manage unknown assets and shadow IT, including legacy systems and applications connected to the network.
- Automate audit reporting and get a unified view of compliance status.
- Assess, demonstrate and maintain compliance with all SLED regulatory standards and guidance, including Criminal Justice Information Services (CJIS) and Federal Taxpayer Information (FTI).
- Rely on streamlined reporting tools to communicate cyber risk in business terms, providing meaningful context and actionable insight to government and education leaders.

Benefits

Through visionary technology and unrelenting innovation, Tenable is revolutionizing how government agencies and educational institutions understand, manage, measure and reduce cyber risk across the modern attack surface. Encouraging dialogue and collaboration between security teams and organizational leaders raises awareness of vulnerabilities and informs smarter business decisions.

Infrastructure and Data Security: Gain a real-time view of vulnerabilities and potential threats impacting digital assets across the SLED environment. Get the actionable intelligence required to proactively protect government systems and citizen data.

Continuous Compliance: Automatically assess security posture across SLED networks. Pinpoint nonconformance issues and maintain adherence to all regulatory requirements.

Resource Optimization: Facilitate prioritized allocation to maximize limited resources. Leverage easy-to-use reporting tools to demonstrate the impact of security investments.

Reduced Risk: Continuously identify, assess, monitor and rapidly remediate security weaknesses and potential attack vectors in SLED systems to close gaps and improve risk profiles.

About Tenable

Tenable™ transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats and reduces exposure and loss. With more than one million users and more than 21,000 customers worldwide, organizations trust Tenable for proven security innovation. Tenable customers range from Fortune Global 500 companies, to the global public sector, to mid-sized enterprises in all sectors, including finance, government, healthcare, higher education, retail and energy. Transform security with Tenable, the creators of Nessus® and leaders in continuous monitoring, by visiting tenable.com.

For More Information: Please visit tenable.com
Contact Us: Please email us at sales@tenable.com or visit tenable.com/contact