

# TENABLE FOR STATE AND LOCAL GOVERNMENTS

State and local governments are on the front lines of cybersecurity. They hold access to sensitive databases and PII, and often manage critical infrastructure. To meet citizens' needs, State and Local Government (SLG) institutions are embracing digital technologies from mobile to IoT to cloud. With the increased amount of sensitive data to protect, an expanded attack surface and increasingly sophisticated attacks, cybersecurity has become a top concern for state and local governments.

## PROTECT YOUR AGENCY WITH TENABLE SOLUTIONS

Tenable's portfolio of solutions enable U.S. state and local governments to protect citizen data and to wisely manage risk to critical infrastructure by identifying, monitoring, and prioritizing vulnerabilities across the entire network – including on-premises, cloud, OT, mobile and virtual environments.

### Protect Critical Infrastructure

Protecting critical infrastructure and citizen data is of paramount importance to national security, individual privacy and daily living. Recent attacks on energy providers, water systems and natural gas pipelines demonstrate how attackers take advantage of blind spots on agency networks to gain access to data and sensitive information. Tenable Vulnerability Management solutions work with Tenable.ot to unify cybersecurity for IT and OT and harden defenses to eliminate traditional blind spots and security risks. Built to protect industrial and critical infrastructure, Tenable.ot delivers deep situational awareness across all sites and their respective IT and OT environments. You get complete visibility into your converged environment with the ability to discover and assess all assets and their vulnerabilities. From inventory management and asset tracking to threat detection at the device and network level, vulnerability management and prioritization, and configuration control, Tenable's OT security capabilities maximize your visibility, security, and control across your entire operations.

## KEY BENEFITS

- Safeguard critical infrastructure and citizen data
- Quickly demonstrate compliance with regulatory standards and operational frameworks
- Get visibility into all the assets, and vulnerabilities, on your extended network
- Easily prioritize vulnerabilities before they become a breach
- Harden defenses to stop ransomware
- Accelerate Zero Trust with full visibility into the assets and users on your network
- FedRAMP authorized

## TECHNOLOGY COMPONENTS

- Tenable.io
- Tenable.sc
- Tenable.ot
- Tenable.ad
- Tenable.cs
- Tenable Lumin

## Stop Ransomware

More and more ransomware strains use software vulnerabilities as an initial attack vector. These flaws can be older and well known or new vulnerabilities such as Log4j, so it's essential to continuously assess your entire attack surface as your environment changes and new threats emerge. Tenable solutions provide proactive protection against ransomware, hardening your defenses and ensuring you know what vulnerabilities to fix first. Your attack surface is continuously assessed to find flaws before they become business impacting issues. Using real-time threat intelligence and easy to understand risk scores you can prioritize vulnerabilities and understand the latest attack paths ransomware groups use to guide remediation.

## Discover More Vulnerabilities On More Attack Surfaces

Agency attack surfaces are growing in complexity and cyber criminals are deploying more advanced methods to target user and agency infrastructure weaknesses. Today's modern network environment goes beyond the scope of traditional IT- to include cloud, OT, mobile and web apps. Different types of assets constantly enter and exit the enterprise. Tenable industry leading VM solutions ensure you have a complete picture of all the assets, connected devices and users on your network, as well as their corresponding vulnerabilities. Going beyond traditional IT assets, Tenable technologies continuously discover and assess new technologies, platforms and devices including cloud services, operational technology (OT), modern web apps and Active Directory (AD) domains. With full visibility into your network assets, vulnerabilities and blind spots, you can predict the vulnerabilities attackers are most likely to exploit in the near future so you can quickly begin remediation.

## Prioritize Vulnerabilities

Tenable solutions provide built-in prioritization capabilities to identify high risk vulnerabilities so you can proactively stop attacks. Vulnerability data, threat intelligence and data science are combined to give you easy to understand risk scores to quickly assess risk. Through measurement and comparative benchmarking of program effectiveness, [Tenable Lumin](#) elevates cyber risk management even further with additional prioritization metrics and capabilities, such as cyber exposure visualizations, asset criticality ratings, cyber exposure risk scoring, remediation and assessment maturity measurements and peer benchmarking, as well as providing the ability to track risk reduction over time.

## Accelerate Zero Trust

Visibility is a foundational component of a Zero Trust Architecture. Tenable helps accelerate your journey to Zero Trust by providing critical visibility and insight into

assets and users on your network from IT to OT, code to cloud and AD to Azure. Agencies can identify and classify assets, inventory devices, map the flow of sensitive assets and data, and understand vulnerabilities on all connected devices. Risk scores and asset criticality metrics can be used to inform policy decision points to make a trust/no trust decision.

## Maintain Compliance

Tenable helps your agency stay secure and compliant. Tenable FedRAMP authorized solutions bring framework investments to scale and maturity and consistently demonstrate compliance with regulatory standards and operational frameworks, including NIST 800-53, CIS Controls, Criminal Justice Information Service (CJIS), FedRAMP and IRS 1075 (FTI). As a long time partner of the Federal Government, Tenable understands the importance of supporting mission critical federal initiatives including ACAS, CDM, Zero Trust and more.

## About Tenable

Tenable® is the Cyber Exposure company. Approximately 40,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies.

**For More Information:** Please visit [tenable.com](https://tenable.com)  
Please email us at [sales@tenable.com](mailto:sales@tenable.com)  
or visit [tenable.com/contact](https://tenable.com/contact)

