ExtraHop

ExtraHop Reveal(x) for State and Local Government

Stop advanced threats with cloud-native visibility, detection, and response

State and local government IT teams safeguard every digital interaction and protect the delivery of public services from advanced threats and performance issues. The distributed nature of their facilities and their constituents make this a demanding endeavor for already stretched thin resources.

One missed network intruder, one undetected ransomware attack, or one broken citizen experience risk the ability to provide vital services, bolstering economic opportunity, and improving the overall welfare of businesses and residents.

> “
>
> Ransomware attacks cost state and local governments over $18B in 2020.[1]

Despite what’s at stake, IT and security teams face constant headwinds:

Advanced persistent threats and zero-day exploits put every networked asset at risk for compromise. A 700% increase in ransomware attacks and game-changing events, like the 2020 SUNBURST hack, are constant reminders of the razor-thin margin for error.

Unprecedented levels of remote working in response to the global COVID-19 pandemic expanded the attack surface introducing new risks to the confidentiality and integrity of sensitive citizen data.

Data sharing and open government initiatives promise innovation and new levels of collaboration while also adding new stresses on IT to enforce data privacy policies properly.

Compliance with regulatory requirements, including the NIST Cybersecurity Framework (CSF), HIPAA, the FBI’s Criminal Justice Information Services (CJIS) policies, and others add time-consuming overhead and reporting obligations.

The Challenge: Municipalities Face A Difficult Balancing Act

Each year, state and local governments spend trillions of dollars on programs and services for its constituents. From education to infrastructure to public safety, the impact of IT issues or data breaches have real implications on lives and livelihoods. Even with this crucial charter, cities, counties, and states have to navigate these challenges on lean budgets and a competitive market for IT talent

As targeted attacks on state and local governments have risen more than 50% over the past several years, it is evident that the reliance on prevention alone is no longer sufficient to stave off sophisticated attacks or determined adversaries. Once breached, intruders move laterally to accomplish their objectives: hold municipalities hostage with ransomware, exfiltrate valuable data, or worse.

The Opportunity: Gain Visibility, Reduce Risk, and Respond Quickly

Improving an overall security posture starts with stopping advanced threats before they result in a breach. To beat back intruders already inside a network, state and local governments need complete visibility, real-time situational awareness, and high-fidelity contextual data. You can boost your IT team's ability to protect sensitive municipal data and deliver a secure citizen experience with this insight.

UNIFY VISIBILITY AND IMPROVED CYBER HYGIENE

Network visibility is the cornerstone of risk management frameworks, such as NIST, CIS Controls, and MITRE ATT&CK, and regulations, such as CCPA, HIPAA, and PCI DSS. Comprehensive real-time visibility is critical to stop cyber threats, demonstrate compliance, and maintain service levels.

- Without east-west traffic visibility, 70% of your hybrid network is in the dark and risks missing intruders who find ways past even the most world-class defenses.
- Encrypted traffic leads to dark spaces, which attackers can exploit to mask malicious activities, or application performance issues go undetected
- Up-to-date and complete asset inventory and classification (including IoT devices) are essential to improve network security and health

State and local government IT functions that closely collaborate to identify gaps, blind spots, troubleshoot degraded performance, and uncover threats increase the speed and scale of public service delivery and overall citizen experience.

ACCELERATE ZERO TRUST ADOPTION

With advanced persistent threats, supply chain attacks, and zero-day exploits, trust can no longer be determined by a user's or device's location on the network. This has made embracing a Zero Trust security model imperative. However, without complete visibility, a Zero Trust security model can result in a false sense of protection

- Mapping all workflows and understanding dependencies is crucial to avoid painful services disruptions or an unintended exposure of sensitive data resources
- Confirmation of microsegmentation outcomes—especially when traffic is encrypted—depends on harnessing the ground truth of the network without requiring agents or parsing individual logs
- Incident response teams need to know which events and alerts require immediate attention based on the local context and observed behaviors

State and local government IT teams that combine real-time insights into the network with advanced machine learning to detect unusual behavior can achieve their Zero Trust objectives more rapidly and with lower risk.

ENABLE FRICTION-LESS COLLABORATION ACROSS IT FUNCTIONS

The pervasiveness, velocity, and scope of today's sophisticated threats demand an integrated approach.

- War rooms and the IT blame game slow response times and distract from resolving incidents and delivering major initiatives
- Operational and cost efficiency gains are possible by minimizing tool sprawl and technologies with overlapping functionality
- Streamlining threat response workloads and troubleshooting across NetOps, SecOps, and CloudOps is possible if each team has access to the same deep visibility data across the entire hybrid environment

State and local government IT teams that break down silos by standardizing on a single source of truth eliminate operational friction and boost productivity.

The Solution: Reveal(x) Cloud-native NDR for State and Local Governments

ExtraHop Reveal(x) cloud-native network detection and response (NDR) provides the scale and the intelligence needed to analyze hybrid environments from the inside out to detect and respond to threats before they cause damage.

Reveal(x) passively monitors your network and analyzes all network interactions to deliver complete visibility, real-time detection, and intelligent response to improve your organization's ability to stop advanced threats, troubleshoot downtime and slow applications and improve your network and security hygiene.

Reveal(x) is backed by the ExtraHop Threat Research team. As soon as new threats and attack tactics are discovered, new detectors can be quickly deployed to immediately improve the expertise and effectiveness of SecOps teams

Achieve 360-degree visibility to quickly detect, investigate, and respond to threats with an integrated workflow for unparalleled insight across the hybrid network, cloud workflows, and IoT devices. Even network traffic is encrypted with TLS 1.3.

Stop advanced threats that other solutions won't see, streamline your operations, and accelerate investigations into any incident with a click. No war rooms. No waiting on other teams.

Detect suspicious activity with cloud-based machine learnings and advanced behavioral analysis to uncover indicators of compromise, such as command and control, brute force, lateral movement, privilege escalation, unusual protocol communication, and data staging and exfiltration. Decrypt traffic to identify threats and anomalies within SSL/TLS encrypted traffic.

Complete Visibility

Discover and classify all assets communicating on the hybrid network

Identify and profile every managed, unmanaged, or rouge device—including enterprise IoT.

Eliminate friction between NetOps, SecOps, and CloudOps teams

Real-Time Detection

Monitor and safeguard network traffic in real-time a line rate up to 100 Gbps

Improve analyst efficiency with a single integrated workflow with real-time threat detection

Enable faster answers through cloud-based machine learning

Intelligent Response

Troubleshoot incidents and investigate root cause in less time

Use historical data to hunt threats and discover if you have been previously impacted

Automate and orchestrate responses through integrations with like CrowdStrike, Phantom, Demisto, and Palo Alto Networks

[1] A Comparitech research report (March 2021)

ABOUT EXTRAHOP NETWORKS

ExtraHop delivers cloud-native network detection and response to secure the hybrid enterprise. Our breakthrough approach applies advanced machine learning to all cloud and network traffic to provide complete visibility, real-time threat detection, and intelligent response. With this approach, we give the world's leading enterprises including The Home Depot, Credit Suisse, Liberty Global and Caesars Entertainment the perspective they need to rise above the noise to detect threats, ensure the availability of critical applications, and secure their investment in cloud. To experience the power of ExtraHop, explore our interactive online demo or connect with us on LinkedIn and Twitter.

ExtraHop

520 Pike Street, Suite 1600
Seattle, WA 98101
877-333-9872 (voice)
206-274-6393 (fax)
info@extrahop.com
www.extrahop.com