ExtraHop

Accelerate Zero Trust Adoption Through End-to-End Visibility and Frictionless Collaboration

Key considerations for planning, implementing, operating, and securing a Zero Trust deployment in Public Sector Institutions

EXECUTIVE SUMMARY

Zero Trust initiatives are increasing in importance across public sector institutions. While the need for adopting Zero Trust is evident, the path to success is not.

This paper discusses the challenges federal, state, and local government IT teams can face when rolling out a Zero Trust security model. It offers practical considerations to more rapidly achieve a Zero Trust mandate. This guidance also shows how end-to-end visibility and frictionless collaboration are vital success factors across all deployment phases.

TABLE OF CONTENTS

INTRODUCTION

Growing numbers of public sector agencies and organizations have started to evaluate and implement a Zero Trust security model. Embracing Zero Trust is an acknowledgment that traditional network security controls—perimeter firewalls, intrusion detection systems, and VPNs—are no longer effective in mitigating the risks of cyberattacks or data breaches.

> **"Zero Trust is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud-based assets that are not located within an enterprise-owned network boundary."**
>
> - NIST Special Publication 800-207 - "Zero Trust Architecture" (August 2020)

The widespread growth and adoption of cloud computing within the public sector have resulted in increasingly hybrid IT infrastructure. Trust can no longer be determined solely based on a user's or device's location within the network, shattering the efficacy of decades-old, defense-in-depth cybersecurity frameworks.

Instead, Zero Trust principles determine trust (and trustworthiness) dynamically, regardless of user location. Access privileges are not just granted once the user and device identities are authenticated but are continuously verified. Authorization to applications and resources is granular, lasting only for specific transactions on an as-needed basis. No asset or network segment is implicitly trusted.

> **"Trust is a vulnerability, and security must be designed with the strategy, 'Never trust, always verify.'"**
>
> -Forrester Blog - "A Look Back at Zero Trust: Never Trust, Always Verify" (August 2020)

Unprecedented growth in remote workers due to the global COVID-19 pandemic and the stark realities that adversaries can operate undetected for months—as shown with supply chain risks like the 2020 SUNBURST attack[1]—have only bolstered the need for a Zero Trust approach across the public sector.

However, implementing an effective Zero Trust solution is a complex and complicated endeavor. It is not achieved by deploying a single product nor merely enacting a new policy or set of procedures. Since institutions cannot simply toss out all their existing infrastructure investments to roll out a new Zero Trust approach, tight coordination and collaboration between often siloed IT teams—NetOps, SecOps, CloudOps, and others—is crucial.

As a result, all public sector entities will end up with an evolving hybrid Zero Trust architecture deployment for the foreseeable future—only specific user populations or groups of resources operate under a Zero Trust approach. Maintaining these multiple-access models combined with a sprawling mix of on-premises systems and cloud-based solutions leads to visibility gaps. This lack of proper visibility impedes the situational awareness and administrative oversight public institutions need to stay productive and secure.

In light of these challenges and risks, successfully meeting Zero Trust mission objectives requires more than just a shift in mindset. Without comprehensive visibility into your Zero Trust architecture and increased collaboration across IT operations, your Zero Trust security model can result in a false sense of protection—or worse, lead to productivity-impacting disruptions without any of the desired safeguards.

Public sector institutions can achieve their Zero Trust mandate more rapidly and with lower risk if these vital success factors—end-to-end visibility and frictionless collaboration—are considered across all phases of adoption.

DRIVERS FOR ZERO TRUST IN THE PUBLIC SECTOR

> De-perimeterization has happened, is happening, and is inevitable; central protection is decreasing in effectiveness.
>
> **JERICHO FORUM COMMANDMENTS**

Zero Trust, a term popularized in 2010 by then Forrester Research analyst John Kindervag[2], is not a new concept. Its origins can be traced back decades to forward-thinking IT organizations that recognized that pervasive internet connectivity would ultimately result in the "de-perimeterization" of enterprise networks. Trust—and access to trusted computing resources—would no longer be defined by being connected to an IP network behind the corporate firewall.

In the nearly two decades since groups like the Jericho Forum[3] introduced these concepts, the world has indeed changed. There is near-ubiquitous availability of high-speed internet access, leading to the exponential growth of connected devices and cloud computing adoption. It is not only possible, but it is an expectation that anyone can work from anywhere, at any time, without friction.

In July 2019, a report published by the Defense Innovation Board (DIB)[4] made the case for moving to Zero Trust as an imperative for ensuring the "effectiveness of security and data sharing" across U.S. Department of Defense (DoD) networks:

> *"DoD cybersecurity is at a critical juncture. Its networks are growing in size and complexity...This expansion is stretching existing cybersecurity apparatuses to their breaking point, as an ever-growing number of users and endpoints increases the attack surface areas of the network...Blind trust in users and devices inside the perimeter of the network is not sustainable."*
>
> - "The Road to Zero Trust (Security)" by Kurt DelBene, Milo Medin, Richard Murray (July 2019)

These new realities are not unique to America's warfighters. All public institutions—at federal, state, and local levels—face the challenge of balancing demands for increased access to improve user productivity with the mandate to safeguard data privacy and integrity.

Additional factors driving adoption of Zero Trust principles within the public sector include:

- **Mandated IT modernization efforts.** With the objectives of cost savings, greater agility, and improved cybersecurity posture, public sector CIOs face increasing pressure to consolidate and optimize their IT infrastructure. Programs like the Data Center Optimization Initiative (DCOI)[5] and the Trusted Internet Connection policy (TIC 3.0)[6] are examples of these federally mandated requirements. Meeting mandates lead to retiring legacy, homegrown on-premises systems, and migrating to public cloud and SaaS alternatives. Modernization has many upsides, but it also rapidly expands an institution's attack surface area.

- **Growing Remote and Distributed Workforces.** Remote work was already expanding before the impact of COVID-19 accelerated the trend. According to Upwork's 2020 Future Workforce Pulse Report, over 36 million Americans will work remotely by 2025, an 87% increase from pre-pandemic levels[7]. Supporting these widely dispersed workers has led to faster-than-anticipated adoption of cloud services, significantly hampering the effectiveness of perimeter-based monitoring. 5G network build-outs are forecasted to add 1.9 billion 5G mobile

subscribers in the same period[8]—further fueling the ability and expectation to support a widely distributed workforce. Traditional VPNs and network boundary-based security controls are no longer capable of keeping up with these traffic volumes. Backhauling internet-destined traffic from remote devices for inspection becomes impractical if not wholly impossible.

- **Institutional Interdependencies and Data Sharing.** Similar to mandates to consolidate infrastructure, public sector institutions are compelled to share and collaborate to more effectively deliver services to benefit the citizens they represent. Data portability and access are vital ingredients to enabling these efforts. Much like electronic health records (EHR) speed up and improve patient experiences, analogous activities intend to improve public policy. While there is little doubt of the transformative power of sharing data across sectors[9], there are significant privacy risks if access is left unchecked.

- **Increasing Reliance on Contractors and Partners.** Scaling operations to deliver services to the communities' public sector institutions have made them more dependent on third parties. Be it the addition of short-term personnel or specialized service providers, each year millions of contract workers[10] support federal, state, and local agencies in their respective missions. As rising numbers of contractors gain temporary access to sensitive data and remotely connect to institutional networks to complete their work, the risk of compromise only increases. Weak links can be exploited, and if not detected, they lead to potentially life threatening results. The rapidly approaching deadlines for government contractors to comply with Cybersecurity Maturity Model Certification (CMMC)[11] requirements highlights the significance of this risk.

- **Accelerated Adoption of Internet of Things (IoT) and Automation.** Demand for IoT applications is expected to grow significantly in the coming years. The global market for IoT solutions is forecasted to reach around $1.6 trillion by 2025[12]. Gartner predicts over $17 billion of this will be spent in 2021 on solutions to improve public safety alone[13]. What results are millions of smart sensors sharing sensitive data over the network. Public sector entities must employ machine-driven data analysis and automation to maximize the value of this real-time data and quickly react. Rising numbers of "non-human users"—like machine-learning algorithms and robotic process automation (RPA) bots—now require access to sensitive data and applications. Unfortunately, many of these IoT devices and automations are unmanaged, making them prime targets for compromise by cyberattackers. Once exploited, they become an entry point for lateral movement across a public institution's trusted network.

The realities described above demonstrate the urgency for embracing Zero Trust. Perimeter-based security models offer little-to-no safeguards against unauthorized lateral movement within an organization once the network boundary is breached.

> "Zero Trust is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud-based assets that are not located within an enterprise-owned network boundary.
>
> **NIST SPECIAL PUBLICATION 800-207 - "ZERO TRUST ARCHITECTURE"**

RISKS AND CHALLENGES TO SUCCESSSFULLY IMPLEMENT A ZERO TRUST ARCHITECTURE

The need for adopting Zero Trust is evident across public sector institutions, but the path to success is not.

Getting started means more than just purchasing a new tool, completing checklist steps, or demonstrating compliance to a new risk-management framework. It necessitates a wholesale reexamination of the organization's current security controls and culture. A comprehensive identification and classification of all institutional resources is also required. This is a tall order in its own right when supporting mission objectives is paramount for IT. Several factors complicate success:

- **You can't protect what you don't know about.** The complexity and dynamic nature of today's enterprise infrastructure makes knowing the data on the network and going through that network difficult at best. Every organization has vast workflows consisting of hardware, applications, and data spread across the edge, core, remote sites, cloud deployments, physical facilities, and mobilized workforces. Methods for conducting the requisite inventory are often manual, time-consuming, or incomplete. Point-in-time scans and Excel spreadsheets present a dated and inadequate view, leading to network-security blind spots.

- **You have to build the plane while you're flying it.** Practically every Zero Trust implementation will be rolled out over an existing enterprise environment. The risk of lost productivity during implementation has real consequences. Users rely on uninterrupted access to the apps and data they need to get their jobs done. Mistakes or misconfigurations can cut off access or inadvertently expose sensitive resources. The impact is significant if it takes IT operations too long to detect broken user experiences, breaches, or malicious activities.

- **You need to account for cultural boundaries, not just network ones.** Zero Trust requires an organization-wide commitment and a change management program that breaks down barriers between all facets of the institutional mission. A lack of alignment between mission stakeholders and IT prevents the mindset changes that Zero Trust needs to be viewed as a mission-critical mandate. Shared acceptance that the network is likely already breached by bad actors and malicious software is crucial. So is the understanding that implementation and operation of Zero Trust cannot be slowed by long-standing functional silos and limited coordination between IT groups.

- **You can't just rely on microsegmentation.** Software-defined networking and microsegmentation can be a practical network-based approach to Zero Trust. However, many microsegmentation solutions require agents to be installed on endpoints to participate. This limits users, processes, devices, and resources that cannot be instrumented with an agent: IoT devices, bring your own device (BYOD) assets, bots, cloud services, and SaaS apps running in environments not owned by the institution. For Zero Trust to work, accommodations must be made without diminishing safeguards.

> "Zero Trust is not a thing you buy, it is a security concept, strategy, and architectural design approach.
>
> **ACT-IAC WHITE PAPER: "ZERO TRUST CYBERSECURITY CURRENT TRENDS"**

These challenges to adoption can be mitigated by two fundamentals: **complete visibility** and **increased collaboration**.

VISIBILITY AND COLLABORATION CONSIDERATIONS DURING A ZERO TRUST ROLLOUT

Zero Trust implementations generally follow four phases: plan, implement, operate, and secure. At each stage, IT and security have an opportunity to proactively improve the likelihood of success. The following offers considerations for each phase where complete visibility and collaboration are vital.

Plan

The planning milestone of any wide-scale effort is crucial. Recent research by the Project Management Institute (PMI) revealed that 11.4% of each dollar invested on projects is wasted due to poor performance[14]. Poor planning is often the root cause. As if the stakes weren't high enough, poor planning of a Zero Trust architecture implementation can lead to more than budget waste. It can fatally hamper a public institution's ability to achieve its mission objectives.

Before you can effectively define policies and choose the right security controls, you need visibility into:

- Who and what is communicating on your network?
- How are they communicating?
- What and where are the assets?
- How should they be classified?
- Are they ready to participate in a Zero Trust environment?

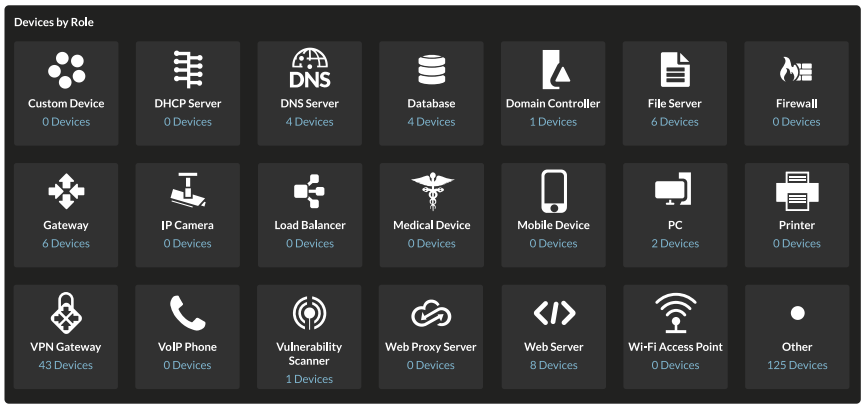
To find answers to these questions, you need to:

> "Only 15% expressed a very high level of confidence that all the devices on their network are discoverable.
>
> **SANS NETWORK VISIBILITY AND THREAT DETECTION SURVEY**

Conduct a comprehensive inventory and classify all assets.

The first step in planning is discovering everything *that is*, *should*, and *should not* be communicating across the network. There are many techniques to achieve this objective, however these are often manual and cannot account for the hybrid and dynamic nature of today's public sector IT infrastructure.

Instead, continuous and real-time discovery is imperative. Additionally, mechanisms need to be in place to automatically classify discovered assets based on observed behavior, not only its scanned profile. The best way to accomplish this is through real-time, full-content analysis of all network traffic. Not only traffic flows at layer 2-4 but using full fluency of enterprise application protocols to understand the nature of the communications between assets.



Map all workflows and understand dependencies.

To avoid painful disruptions or the unintended exposure of sensitive resources, it is incumbent to gain visibility into all application activity across the network. Again, there are several techniques to map these relationships. The most effective approach achieves end-to-end visibility that spans the entire application delivery chain from on-premises to the cloud.

Network-based traffic analysis is the best method to obtain a real-time, objective, and complete view into every transaction. When combined with advanced machine learning algorithms and contextual analysis, previously opaque relationships become crystal-clear maps of dependencies that must be considered before enacting any Zero Trust changes. Importantly, any method that does not account for the increasing amount of encrypted traffic—like TLS 1.3 encrypted transactions—will result in an incomplete picture.

> “In order to get the benefits from Zero Trust you need to know about each component of your architecture through to the services and data they are accessing.
>
> **THE NATIONAL CYBER SECURITY CENTRE (U.K.)**

Assess and remediate readiness for Zero Trust.

When preparing to deploy a Zero Trust architecture, success is predicated on a number of essential components working effectively: identity management, policy management, device health monitoring, and network segmentation, among others. Ensuring any participating device with weak cipher suites or out-of-date certificates are identified and addressed is vital in eliminating disruptions or vulnerabilities. Similarly, uncovering any pre-existing issues with authentication mechanisms, DNS resolution, or other common error states easily lost in the noise of day-to-day network usage goes a long way to ready the infrastructure for Zero Trust.

As these hygiene and compliance activities impact the full-stack, it is essential that all IT groups collaborate closely and work from a dependable, single source of truth to confirm that remediation is fully completed.

Implement

As previously mentioned, Zero Trust is not achieved by using one product, policy, or procedure. When it comes time to implement a Zero Trust architecture, having complete visibility into all facets makes the difference between success and failure. With all hands on deck across IT and security operations, implementation calls for breaking down long-standing silos between groups, including the separate and disconnected tools used by each team to troubleshoot any issues that arise.

Confirmation of policies and microsegmentation.

In the most simplest terms, Zero Trust is about affecting in real time the right policies on the right assets to facilitate the right communications between subjects (users and non-human processes) and resources (data, applications, and services). While simple sounding, it is challenging to piece together all the evidence necessary to confirm that these expected outcomes are happening according to design. Trying to parse individual logs from servers, containers, network switches, and authentication services turns this into a Herculean task.

A better way requires complete coverage of all these moving parts from a single pane of glass. This can only be accomplished by transforming raw network traffic into the most complete record of everything happening within the Zero Trust environment. This eliminates any visibility gaps and provides the necessary inputs for real-time analysis and actionable insight into the end-to-end user experience.

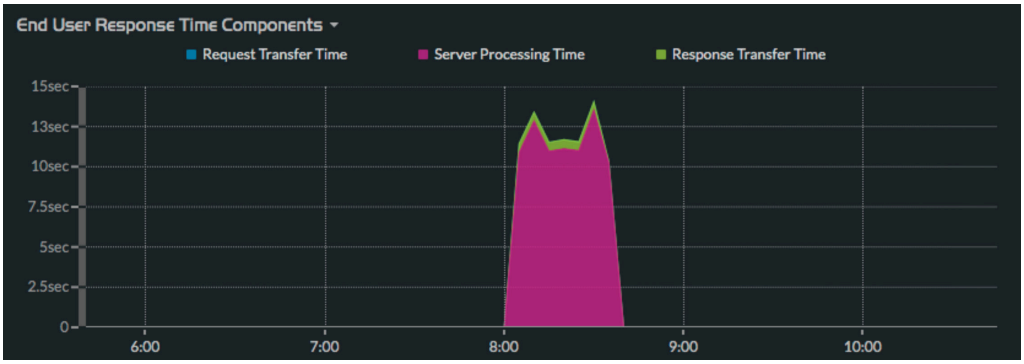
> “Maintain a consistent user experience. We wanted the transition to Zero Trust networking to be as noninvasive to the user as possible.
>
> **MICROSOFT IT SHOWCASE**

But, it shouldn't stop there since practically all network traffic will be encrypted as an essential security control to implement Zero Trust. Confirmation of expected policy enforcement is only possible with the ability to securely decrypt payloads and deeply analyze the encapsulated layer 7 protocols without risking the integrity or privacy of these communications.

Detailed measures of the user experience before, during and after.

One of the many reasons why most Zero Trust implementations are in pilot phases or limited to subsets of users is the lack of clarity on what impact it will have on the user experience. Gaining confidence in a Zero Trust deployment involves having a reliable way to baseline these experiences before Zero Trust was enacted. Once underway, having detailed measures during the rollout phase and afterward gives public sector IT teams the empirical evidence that productivity has not been degraded.

For all the factors previously cited, achieving this can be difficult, if not impossible, when traditional tools and methods are used by individual monitoring teams. Capturing, analyzing, and retaining performance metrics of the entire user experience (both across the infrastructure and along the entire application stack) is only possible through comprehensive and real-time visibility of all network transactions. Collecting and storing a dataset that can support all operations teams—with enough forensic lookback—is no easy task. It is vital that teams look for more than a handful of vanity metrics as a good enough way to complete this effort.



Measure response at each phase to reduce the impact on user experience.

Fast resolution of broken user experiences.

Slow or buggy user experiences risk impacting productivity and the institution's ability to meet its mandates. During the implementation of Zero Trust, any time spent finger pointing between IT ops teams delays resolution. Root-cause determination means piecing together disparate signals from different parts of the application stack across a dynamically segmented network.

Traditional monitoring tools that are based on logs or agents can only offer limited visibility, leading to blind spots that slow triage and troubleshooting. The added complexity of applied Zero Trust access policies exacerbates this situation.

Having the means to proactively detect, investigate, and address any application or network performance issues during an implementation directly increases organizational confidence in Zero Trust.

Operate

Reaching the operational state is no small feat. It is also just the beginning of the process of successfully embracing a Zero Trust security model. Operating a Zero Trust environment means ensuring both the ongoing effectiveness of these new dynamic access policies and the operational health of the infrastructure that executes enforcement. The user experience and all cyber defenses must be continuously monitored and proactively addressed whether it is an outage or breach.

> “Establish full visibility of all activity across all layers from endpoints and the network to enable analytics that can detect suspicious activity.
>
> **NSA CYBERSECURITY GUIDANCE ON ZERO TRUST SECURITY MODEL**

Complete coverage and real-time visibility.

The hybrid nature of public sector IT infrastructure already makes it hard enough to monitor and diagnose performance issues or identify security risks. Once a Zero Trust model is layered onto the network, existing tooling and processes can be stressed to a point of being ineffective. Yet, end-to-end visibility is most vital to the Zero Trust model.

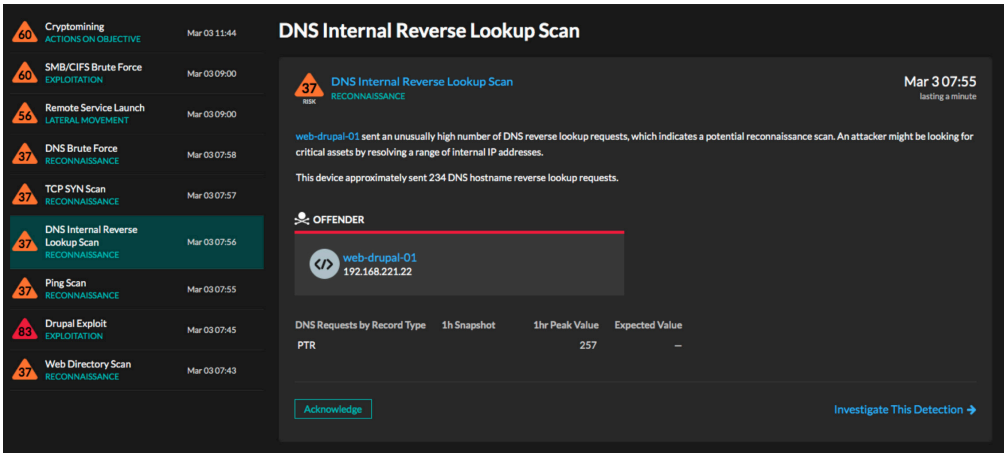
No matter what stage of a Zero Trust adoption journey or IT modernization effort, there is no better substitute than the network itself as the first and most reliable source of real-time insight. The best approach is to passively monitor and analyze unstructured packets at line-rate, even when they are encrypted, all the way through layer 7.

Additionally, a network-based approach makes it possible to identify and monitor uninstrumentable and unmanaged assets. IoT devices, VoIP phones, printers, BYOD endpoints, and even remote users can be discovered and monitored since the network sees everything.

Use of advanced machine learning and behavioral analysis.

The volumes of data, the speed of workflow transactions, and the sophistication of risks to public institution networks makes identifying, investigating, and responding to incidents challenging enough. Add to that resource-strapped and overburdened IT operations teams trying to keep up, and it’s not hard to understand how it is nearly impossible to focus on what really matters at any given moment. Issues can go undetected for weeks or months, and once discovered, it can be a struggle to assess its impact and full scope.

A better way applies advanced analysis and machine learning to automatically correlate seemingly disparate events into proactive notifications. Once alerted, immediate access to the full context of the incident accelerates investigation and response. This boosts situational awareness and analyst productivity. More importantly, this restores confidence and trust without reducing the effectiveness of the Zero Trust architecture.



Advanced analysis automatically correlates disparate events into actionable notifications.

Increased collaboration between IT operations and security.

Zero Trust touches every aspect of a public institution's environment. In turn, this tightly coupled relationship necessitates a similar operating model between traditional IT and security organizational silos.

> "Network operations and security operations teams must be partners, not adversaries.
>
> **SHAMUS McGILLICUDDY, EMA**

By streamlining threat response workflows and troubleshooting of user experience issues, public sector IT teams can both accelerate and assure the success of their Zero Trust efforts. Adopting a more collaborative approach that centers on using the same visibility and investigation tooling reduces operational expenses by eliminating unnecessary tool sprawl. It also eliminates the barriers that can stand between mission outcomes and delivering a great user experience.

To support increased collaboration between operational teams supporting the Zero Trust environment, a single trusted source of visibility needs to completely cover the entire hybrid infrastructure, east-west traffic as well as north-south without any gaps or blindspots.

Secure

Securing a Zero Trust architecture is equally critical to the safeguards Zero Trust aims to deliver. The availability and integrity of the numerous components required to operate Zero Trust need to be maintained. Ensuring identity stores are not compromised and policy enforcement points are operating in a healthy state are just two examples where IT operations teams need to cooperate and remain vigilant to keep the Zero Trust environment functioning.

Public sector entities are also expected to demonstrate compliance with a number of risk manage-ment frameworks and other IT governance requirements. The dynamic segmentation of networked resources and other side effects of Zero Trust make auditing and reporting of compliance a challenge.

Again, complete visibility and collaboration are crucial for safeguarding the safeguards.

Continuous monitoring and automated compliance.

Real-time situational awareness and continuous diagnostics and mitigation (CDM) are table stakes for any public-sector institution to meet stringent compliance requirements. Adherence to risk management framework (RMF) reporting obligations and NIST guidelines need fast answers. Privacy regulations increasingly have strict disclosure requirements that put pressure on incident response teams to conduct their investigations quickly and accurately. Having to scour multiple logs or follow manual processes adds more stress on already stretched IT teams.

Perimeter and endpoint monitoring and asset management can only answer so much. Neither will help continually monitor and maintain compliance for devices not already under management. Instead, an agentless, network-based traffic analysis approach can deliver immediate answers to complex questions with zero negative impacts to performance and with far higher fidelity than logs or humans combined.

Responding to alerts that matter.

Security threats are only growing in sophistication and once an attacker is inside, it can be extremely difficult to detect them. Zero Trust goes a long way to mitigating these risks, but the dynamic nature of microsegmentation and potential compromises of trusted user credentials elevates the criticality of knowing which alerts require immediate attention.

Incident response teams—especially those facing skills shortages—need a better way to detect and prioritize investigations. This means once alerted of suspicious activities, arm on-call analysts with rich local context and an intuitive investigation flow for every detection. Surfacing incident-specific transaction records and relevant packets reduces friction and accelerates response. Obtaining the real-time visibility and advanced behavioral analysis to automatically stitch together related events and understand context is key to achieving this goal.

Integrating existing investments and automating response.

Public sector security teams are expected to run lean operations while also minimizing the time to remediate incidents. At the same time, Zero Trust relies upon investments in a number of security toolsets and technologies. Nothing can, nor should be operating in isolation, especially when security incidents are detected and require a fast response. This means doing more with less and relying on automation.

At the core of a successful approach is a threat response that can be triggered immediately to enable both immediate, fully automated responses as well as augment manual investigation and remediation. Such a solution must play nice with every component of the Zero Trust architecture and security workflow, offering both out-of-the-box and custom integration options for firewalls, identity stores, policy enforcement points, endpoint detection and response (EDR), SIEM systems, and more.

ACCELERATING ZERO TRUST WITH CLOUD-READY NETWORK DETECTION AND RESPONSE

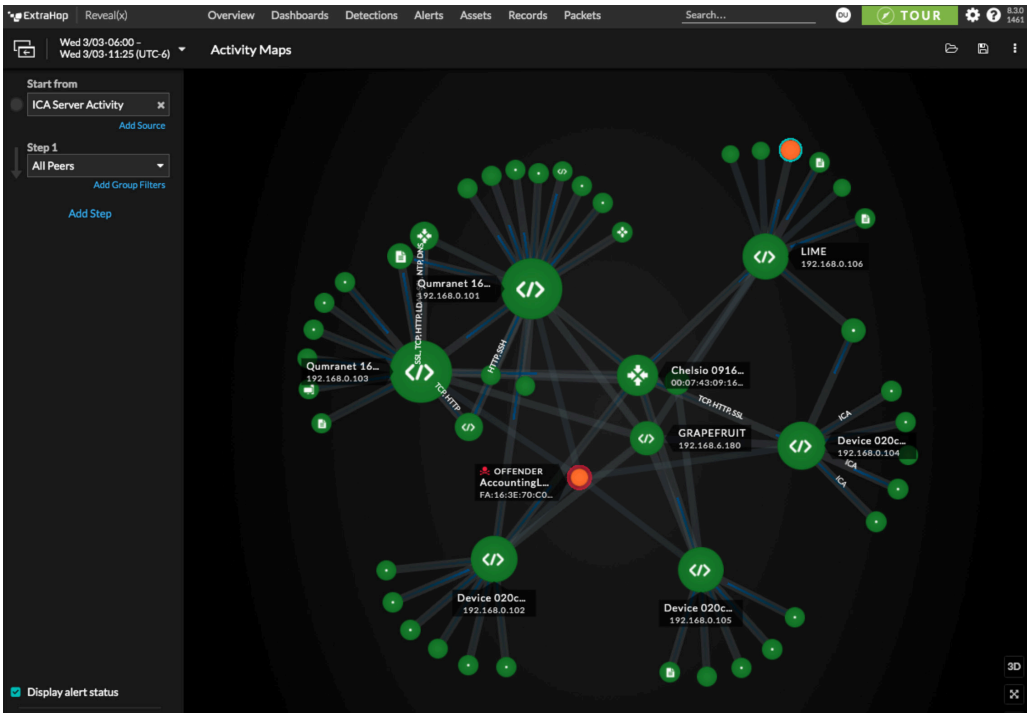
ExtraHop Reveal(x) is the only cloud-ready Network Detection and Response (NDR) product that provides the scale, speed, and visibility required by public sector organizations to detect and respond to threats and rise above the noise of increasingly complex hybrid network architectures, containerized applications, and the cloud.

Unlike perimeter-focused tools that rely on fixed agents or gateway devices, Reveal(x) agentless network traffic analysis passively monitors all network interactions. The result is the complete coverage and end-to-end visibility, real-time detection, and intelligent response IT and security teams need to achieve their Zero Trust objectives. Reveal(x) enables public sector IT to break down silos between operations teams and enable new levels of collaboration by standardizing on a single pane of glass and source truth.

Complete visibility of your Zero Trust architecture.

- Achieve 360-degree visibility—without agents—of hybrid networks, cloud transactions, and device types.
- Automate the discovery of every asset on the network.
- Identify and profile every managed, unmanaged, or rogue device—including enterprise IoT.

> “With ExtraHop, we can easily search and identify unsecured connections, which lets us mitigate that threat before it ever becomes a problem.
>
> **MARVIN CHRISTENSEN, CIO, NATIONAL IGNITION FACILITY**



Real-time detection of disruptive threats to Zero Trust safeguards

• Streamline operations with one integrated workflow for cyber, network operations, cloud, and DevSecOps teams.

• Detect suspicious activity using advanced machine learning and behavioral analysis to identify threats and performance anomalies with high fidelity.

• Monitor and safeguard network traffic in real time—including SSL/TLS encrypted traffic—up to 100 Gbps to validate segmentation outcomes.

Intelligent response that integrates across your Zero Trust environment

• Accelerate investigation workflows with customized dashboard and associated packets for any incident just a click away.

• Save analyst time and automatically uplevel operational staff to take on more significant investigative responsibilities.

• Integrate with solutions like CrowdStrike, Phantom, Demisto, and Palo Alto Networks and automate remediation.

With Reveal(x), public sector IT teams can more rapidly, confidently, and cost-effectively meet their Zero Trust goals without compromising their ability to support the institution's mission.

Sources

[1]Source: ExtraHop "SUNBURST: An Origin Story" (January 2021)
[2]Source: Dark Reading: Forrester Pushes 'Zero Trust' Model for Security (September 2010)
[3]Source: Visioning White Paper - What is the Jericho Forum? (February 2005)
[4]Source: DIB Zero Trust White Paper: The Road to Zero Trust (Security) (July 2019)
[5]Source: M-19-19: Memorandum for Chief Information Officers of Executive Departments and Agencies (June 2019)
[6]Source: CISA Trusted Internet Connections
[7]Source: Upwork Study Finds 22% of American Workforce Will Be Remote by 2025 (December 2020)
[8]Source: Statista Forecast number of mobile 5G subscriptions worldwide from 2019 to 2024 (May 2020)
[9]Source: Accelerating the Sharing of Data Across Sectors to Advance the Common Good (July 2019)
[10]Source: Marketplace - The U.S. Government is becoming more dependent on contract works (January 2019)
[11]Source: Office of the Under Secretary of Defense for Acquisition & Sustainment
[12]Source: Statista Forecast end-user spending on IoT solutions world from 2017-2025 (January 2021)
[13]Source: Gartner Press Release (October 2020)
[14]Source: Project Management Institute: Pulse of the Profession 2020 (February 2020)

Conclusion

The drivers for Zero Trust across federal, state, and local government institutions are clear. It was first catalyzed by the new realities of pervasive internet access, the growth of mobile devices, and the accelerated adoption of cloud computing. Now public sector institutions face new mandates to modernize to support widely distributed and diverse workforces. They are also benefiting from new models of interagency collaboration. When combined with an explosion in unmanaged devices, IoT applications, and automation, it is easy to see how traditional perimeter defenses are no longer enough. A network boundary can no longer determine trust.

While Zero Trust's criticality is evident, the journey to successful implementation is fraught with risks and challenges. Zero Trust is not achieved by buying a new tool or adopting a new risk management framework. It is a wholesale reexamination of security controls, access models, and organizational culture. Successfully achieving these goals requires new levels of visibility across the entirety of an institution's IT infrastructure and new levels of collaboration between all teams in IT operations.

Public sector institutions can achieve their Zero Trust mandate more rapidly—with lower risk—if these vital success factors of end-to-end visibility and frictionless collaboration are incorporated into all adoption phases.

ExtraHop Reveal(x) is the only cloud-ready network detection and response (NDR) product that provides the scale, speed, and visibility required by public sector organizations. Reveal(x) eliminates blind spots other tools miss and gives public sector IT teams the confidence to meet their Zero Trust goals without compromising their ability to support the institution's mission.

ExtraHop

info@extrahop.com
www.extrahop.com