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 on the rise across public sector institutions, and while the need for adopting Zero Trust is evident, the path to success is not as clear. This paper discusses the challenges that federal, state, and local government IT teams can face when rolling out a Zero Trust security model. It offers practical considerations to rapidly implement a Zero Trust architecture. This guidance also shows how end-to-end visibility and frictionless collaboration are vital success factors across all adoption phases.

TABLE OF CONTENTS

Introduction 3

Drivers for Zero Trust in the Public Sector 4

Risks and Challenges to Successfully Implement a Zero Trust Architecture 6

Visibility and Collaboration Considerations During a Zero Trust Rollout 7

Accelerating Zero Trust With Cloud-Ready Network Detection and Response 13

Conclusion 15

INTRODUCTION

Whether motivated by mandates or to improve the security posture of an organization, Zero Trust acknowledges that traditional network security controls—perimeter firewalls, intrusion detection systems, and VPNs—are no longer effective against sophisticated advanced threats or data breaches.

> **"Zero [T]rust 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)**

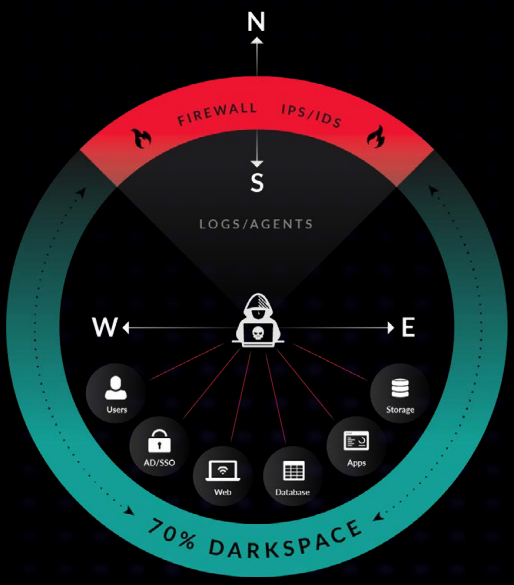
Unprecedented growth in remote and hybrid workers with the stark reality that adversaries can operate undetected for months—as shown with recent supply chain compromises and the thousands of public sector institutions impacted by ransomware in 2021[1]—have only bolstered the need for a Zero Trust approach.

Fallout from a rash of successful ransomware attacks in 2021—which impacted access to vital services and public welfare—has created further urgency. On May 12, 2021, President Biden signed Executive Order (EO) 14028 requiring all U.S. Federal departments and agencies to "advance toward Zero Trust Architecture."

> **"Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life."**
>
> **President Biden's Executive Order on "Improving the Nation's Cybersecurity" (May 2021)**

However, implementing an effective Zero Trust solution is a complex and complicated endeavor. It is not achieved by deploying a single product or by merely enacting new policies or procedures. Additionally, institutions cannot simply toss out all their existing infrastructure investments to roll out a new Zero Trust approach. This creates a challenge, however: maintaining multiple-access models, combined with a sprawling mix of on-premises systems and cloud-based solutions, leads to visibility gaps.

Traditional network and security monitoring tools based on logs or agents are ill-equipped to scale. These perimeter-based defenses prioritize north-south network traffic, leaving a real-time coverage gap of up to 70% of dynamic, hybrid environments:



The lack of proper visibility impedes the situational awareness and administrative oversight public institutions need to stay productive and secure.

A Zero Trust architecture also involves every facet of an institution's IT operations, requiring tight coordination and collaboration between often siloed IT teams—NetOps, SecOps, CloudOps, and others—to mitigate the risk of disruption.

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.

DRIVERS FOR ZERO TRUST IN THE PUBLIC SECTOR

Zero Trust is not a new concept: it was popularized in 2010 by then Forrester Research analyst John Kindervag[2], but 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.

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

Growing reliance on our "always connected" reality and the sudden shift to remote work in the early stages of the global COVID-19 pandemic, created fertile ground for threat-actors to unleash wave-after-wave of cyberattacks. In May 2021, President Biden signed Executive Order 14028 to make a *"significant contribution toward modernizing cybersecurity defenses[4]"* after a number of cybersecurity incidents gravely impacted both public and private sector entities.

> *"It is the policy of my Administration that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security. The Federal Government must lead by example."*
> *-President Biden's Executive Order 14028 (May 2021)*

Adopting a Zero Trust Architecture is a top priority in this order. While Biden's Executive Order and the detailed Zero Trust strategy provided in Office of Management and Budget (OMB) memorandum M-22-09 may be directed to executive branch departments and agencies, its example will set a new standard across the entire public sector.

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

Government 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. Memorandums from authorities, such as the Office of Management and Budget, as well as findings from agency oversight scorecards are leading to the retirement of legacy, homegrown on-premises systems, and the move 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 2021 Future Workforce Report, over 40 million Americans will work fully remote in the next five years, a 23% increase from the prior year[5]. 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[6]—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 consolidating infrastructure, public sector institutions are increasingly compelled to share and collaborate in order to more effectively deliver services to benefit the citizens they represent. Data portability and access are vital ingredients in enabling these efforts. Much like electronic health records (EHR) speed up and improve patient experiences, widespread data sharing between institutions can vastly improve public policy. However, while there is little doubt of the transformative power of sharing data across sectors[7], there are significant privacy risks if access is left unchecked.

> “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”**

Increasing Reliance on Contractors and Partners - Scaling operations to deliver services to the communities public sector institutions serve have made government agencies more dependent on third parties. Be it the addition of short-term personnel or specialized service providers, each year millions of contract workers support federal, state, and local agencies in their respective missions[8]. 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 from insiders only increases. Weak links can be exploited and, if undetected, can lead to potentially life-threatening results. And while the continued evolution of Cybersecurity Maturity Model Certification (CMMC) requirements[9]—recently streamlined in a new 2.0 version[10]—demonstrate the importance of mitigating these risks across the Department of Defense (DoD), all public institutions at federal, state, and local levels face the same challenge.

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[11]. Gartner predicted over $17 billion of this would be spent in 2021 on solutions to improve public safety alone[12]. 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 cyberattackers. Once exploited, they become entry points for lateral movement across a public institution’s trusted network.

The conditions 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.

RISKS AND CHALLENGES TO SUCCESSFULLY IMPLEMENT A ZERO TRUST ARCHICTECTURE

> “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”**

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

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. 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 what data is at-rest and flowing through the network difficult at best. Every organization has vast workflows consisting of hardware, applications, and data, all of which are 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, and often 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, and mistakes or misconfigurations can cut off access or inadvertently expose sensitive resources. The impact is significant if it takes disjointed 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 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 rely solely on microsegmentation. Software-defined networking and microsegmentation can be a pragmatic 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) endpoints, bots, cloud services, and SaaS apps running in environments not owned by the institution. Accommodations must be made without diminishing safeguards for Zero Trust to work.

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 cooperate and proactively improve the likelihood of success. The sections that follow offer guidance at each phase where complete visibility and collaboration are vital.

Plan

The planning milestone of any wide-scale effort is crucial. Research by the Project Management Institute (PMI) revealed that 11.4% of each dollar invested on projects is wasted due to poor performance[13], and 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 they are communicating
- What your assets are, and where they are located
- How assets should be classified
- Whether or not assets are ready to participate in a Zero Trust environment

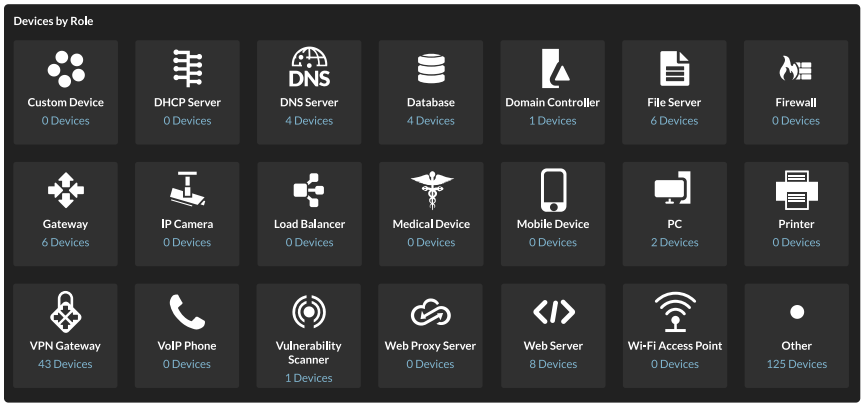
To find answers to these questions, you need to do a few things.

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 just traffic flows at Layers 2-4) by using the full fluency of enterprise application protocols to understand the nature of the communications between assets.

> "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**



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. Due to the number of IT teams involved in the delivery of any user experience, a shared single source of ground truth is required. Once more, 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.

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 when 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 ground truth to confirm that remediation is fully completed.

> “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.)**

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

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.

> “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**

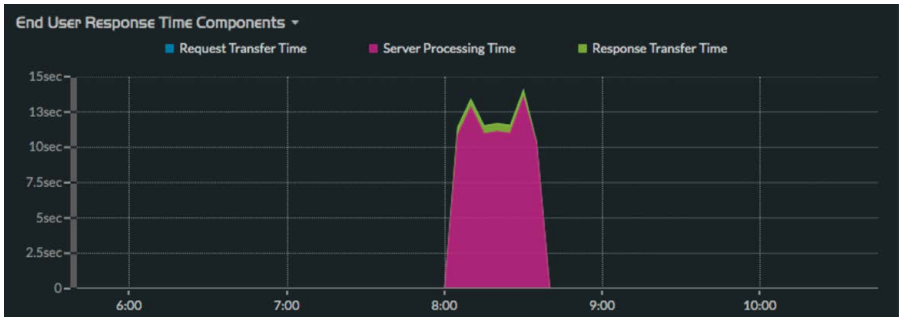
A better way requires complete coverage of all these moving parts from a single pane of glass, accessible by all the IT operations teams involved. This can only be accomplished by transforming raw network traffic into the most complete record of everything happening within the Zero Trust environment.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

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 many Zero Trust implementations remain stuck in pilot phases or are 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 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 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 small task. It is vital that teams look for more than a handful of vanity metrics as a *good enough* way to complete this effort.



Fast Resolution of Broken User Experiences

Slow or buggy user experiences risk impacting productivity and the institution's ability to meet its mission. 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. Therefore, 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

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 infrastructures already makes it hard enough to monitor and diagnose performance issues and identify security risks. Once a Zero Trust model is layered onto the network, existing tooling and processes can be stressed to the 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.

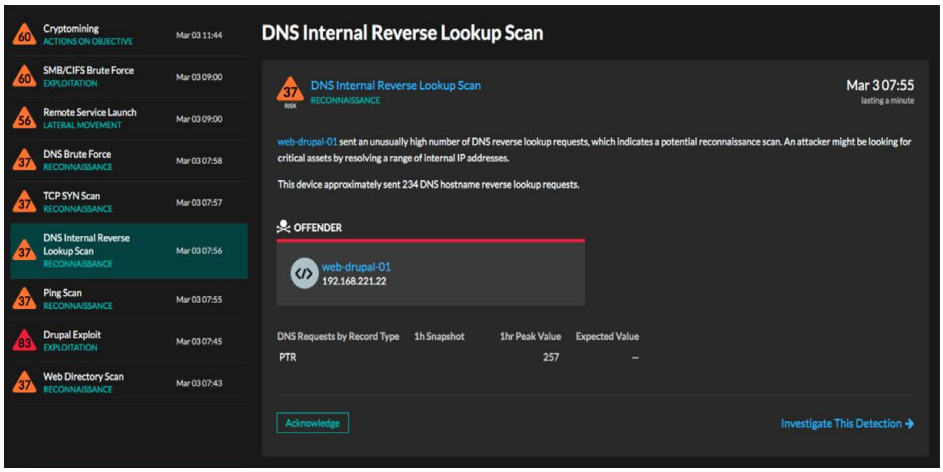
Additionally, a network-based approach makes it possible to identify and monitor "uninstrumentable" and unmanaged assets. IoT devices, VoIP phones, printers, BYOD endpoints, and even remote users can be discovered and monitored since the network sees everything.

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. Add to that resource-strapped and overburdened IT operations teams trying to keep up, and it's easy 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 their 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.



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 user experience issues, public sector IT teams can accelerate and ensure the success of their Zero Trust efforts. Adopting a 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. This collaboration can best be achieved through a single trusted source of ground-truth visibility. That visibility needs to completely cover the entire hybrid infrastructure—east-west traffic as well as north-south—without 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 management frameworks, operational modernization mandates—like those outlined in Office of Management and Budget (OMB) memorandum M-21-31—and other IT governance requirements. The dynamic segmentation of networked resources and other side effects of Zero Trust make auditing and reporting 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 event log management modernization requirements demands comprehensive visibility[14]. Privacy regulations have disclosure requirements that put pressure on incident response teams to conduct their investigations quickly and accurately, requirements that are often becoming more strict as time goes on. 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 both logs and humans combined.

Responding to Alerts That Matter

Security threats are not only growing in sophistication, but once attackers are inside, it is becoming increasingly difficult to detect them. Zero Trust goes a long way towards mitigating these risks, but the dynamic nature of microsegmentation and potential compromises of trusted user credentials elevates the urgency of knowing which alerts require immediate attention.

Incident response teams—especially those facing skills shortages—need a better way to detect and prioritize investigations. Surfacing incident-specific transaction records and relevant packets reduces friction and accelerates response. Obtaining 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, technologies, and teams. Nothing can operate in isolation (nor should it), especially when security incidents require a fast response. This means doing more with less, which in turn means relying on automation.

At the core of a successful approach is a threat response that can be triggered rapidly 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 integration options for firewalls, identity stores, policy enforcement points, endpoint detection and response, SIEM systems, and more.

ACCELERATING ZERO TRUST WITH CLOUD-READY NETWORK DETECTION AND RESPONSE

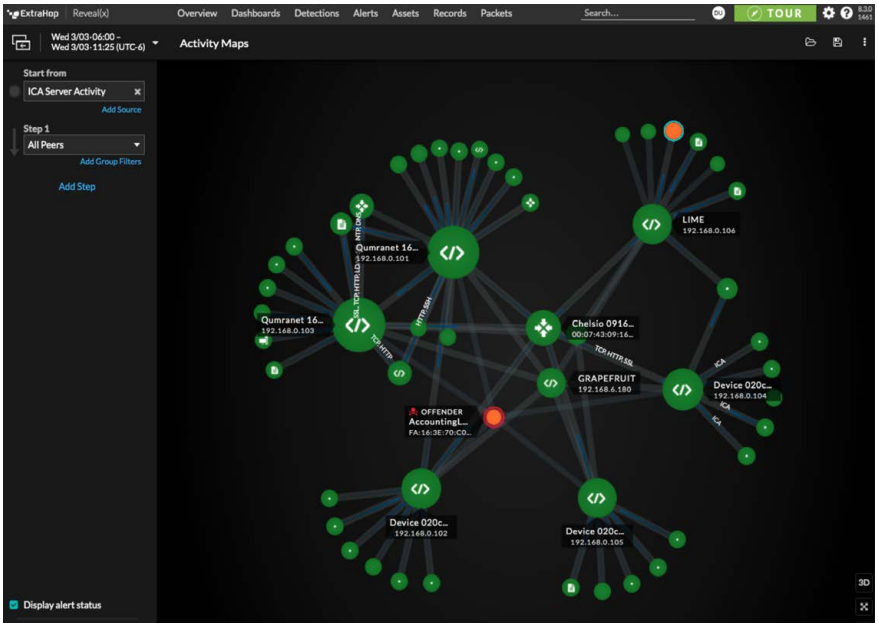
ExtraHop Reveal(x) is the only cloud-ready network detection and response (NDR) product that provides the scale, speed, and visibility required by public sector organizations to detect and respond to advanced threats in hybrid network architectures, containerized applications, and the cloud.

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

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**



Stop Breaches 84% Faster

Investigate a live attack in the full product demo of ExtraHop Reveal(x), network detection and response, to see how it accelerates workflows.

START DEMO

Real-time Detection of 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 Across Your Zero Trust Environment

- Accelerate investigation workflows with customizable dashboards 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 Emisoft "The State of Ransomware in the US: Report and Statistics 2021" (January 2022)

2 Dark Reading: Forrester Pushes 'Zero Trust' Model for Security (September 2010)

3 Visioning White Paper - What is the Jericho Forum? (February 2005)

4 FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks (May 2021)

5 Future Workforce Report Business Use of Freelancers Accelerates Amidst the Pandemic (September 2021)

6 Statista Forecast number of mobile 5G subscriptions worldwide from 2019 to 2024 (May 2020)

7 Accelerating the Sharing of Data Across Sectors to Advance the Common Good (July 2019)

8 Marketplace - The U.S. Government is becoming more dependent on contract works (January 2019)

9 Office of the Under Secretary of Defense for Acquisition & Sustainment

10 Strategic Direction for Cybersecurity Maturity Model Certification (CMMC) Program (November 2021)

11 Statista Forecast end-user spending on IoT solutions world from 2017-2025 (January 2021)

12 Gartner Press Release (October 2020)

13 Project Management Institute: Pulse of the Profession 2020 (February 2020)

14 OMB M-21-31 "Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents" (August 2021)

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.

ABOUT EXTRAHOP NETWORKS

ExtraHop is on a mission to stop advanced threats with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform, Reveal(x) 360, helps organizations detect and respond to advanced threats—before they compromise your business. We apply cloud-scale AI to petabytes of traffic per day, performing line-rate decryption and behavioral analysis across all infrastructure, workloads, and data-in-flight. With complete visibility from ExtraHop, organizations can detect malicious behavior, hunt advanced threats, and forensically investigate incidents with confidence. When you don't have to choose between protecting your business and moving it forward, that's security uncompromised.

info@extrahop.com
www.extrahop.com