Making Zero Trust Actionable: Key Ways to Accelerate Your Journey

MARKET TRENDS REPORT

govloop paloalto NETWORKS carahsoft

Executive Summary

Federal agencies are under pressure to adopt zero trust in order to build cybersecurity resilience into their IT networks and environments.

Both President Biden's **Executive Order on Improving the Nation's Cybersecurity** and the **federal Zero Trust architecture strategy** from the U.S. Office of Management and Budget (OMB) make this an explicit priority. Under these guidelines, federal departments and agencies are tasked with implementing zero trust to strengthen their cyber defenses by the end of fiscal year 2024.

The stakes are high: The Executive Order and OMB strategy came out in response to a number of high-profile breaches targeting federal government resources. State and local governments and educational institutions are also seeing a record number of cyber attacks, and thus have an urgent need to move toward zero trust as well.

In addition to the zero trust mandates, agencies are struggling to implement cyber controls in a changing technology environment. With the shift to cloud, new architectures and new delivery models, the IT environment is increasingly interconnected, making it all the more urgent to eliminate implicit trust.

Zero trust is not one specific product or technology. It's a methodology coupled with a change in mindset. Rather than viewing zero trust through a narrow lens, as a specific product or technology, agencies and institutions need to take a more holistic and comprehensive approach.

To learn more about what zero trust means, GovLoop collaborated with cybersecurity firm Palo Alto Networks on this report. We'll look at how to develop a zero trust plan that is capable of supporting and protecting the business of government.

By The Numbers

94%

of IT leaders report challenges with implementing zero trust, including lack of clarity, other priorities and lack of resources.

72%

of IT leaders have plans for adopting zero trust or have already adopted it.

More than **70%** of federal agencies are aggressively adopting zero trust principles.

67%

of state and local IT leaders are introducing or expanding a zero trust framework.

83%

of cybersecurity professionals say zero trust is strategically necessary for their ongoing business.

How to Take a Holistic Zero Trust Approach

Zero trust promises to reduce complexity around public sector cyber efforts while driving greater operational efficiency. A holistic approach to zero trust would be:

- **Comprehensive:** As mentioned above, zero trust is a methodology and should never focus on a narrow technology. Instead, it should consider the full ecosystem of controls that many agencies rely on for protection.
- **Actionable:** Comprehensive zero trust isn't easy, but getting started shouldn't be hard. For example, begin with what you have. Think about what current set of controls can be implemented using the security tools you have in place today.
- **Intelligible:** Your zero trust approach should be easy to convey to both nontechnical and technical leaders in a concise, easy-to-understand summary.
- **Ecosystem-friendly:** The vendor you choose to help you on your zero trust journey should have a comprehensive portfolio with a broad ecosystem of security partners, and an unparalleled ability to make your zero trust journey a reality.

At its core, zero trust is about eliminating implicit trust across the organization. This means eliminating implicit trust related to users, applications and infrastructure.

- **Users:** "Zero trust for users starts with establishing strong identity controls that must be continually validated for every user," said Drew Epperson, Senior Director of Systems Engineering in Public Sector at Palo Alto Networks. "This includes using best practices such as multifactor authentication and just-in-time access, which is granting users access to applications or systems for a predetermined period of time, on an as-needed basis."
- **Applications:** The shift to cloud is driving new application development practices and faster application rollout. "Design with zero trust principles from the start when it comes to application modernization and cloud adoption," Epperson said. "For cloud native environments, a zero trust architecture continuously runs cybersecurity checks at every stage of the software development lifecycle. From a development and DevOps perspective, this results in safe and frictionless application development."
- **Infrastructure:** Because the average organization runs 45 cybersecurity-related tools on its network, IT teams often have poor visibility and control over unmanaged resources such as IoT devices and supply chain infrastructure. "That means for everything infrastructure-related, including routers, switches, cloud and especially IoT, eliminating implicit trust is even more critical and must be addressed in the zero trust strategy," Epperson said.

Adapt to the Cloud Mindset

While a shift to the cloud has enabled significant advances, especially for development teams, these new architectures—along with new delivery and consumption models—also pose a challenge.

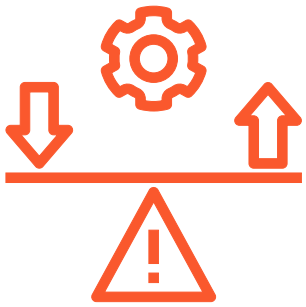
- **Attack surface:** An expanding catalog of apps creates a broader attack surface while implied trust granted to microservices yields new opportunities for attackers to move laterally.
- **Remote work:** The work-from-home environment further complicates the picture. A hybrid workforce is the new reality. Governments and educational institutions must provide least-privilege access from anywhere to all applications while delivering an optimal user experience. The days of treating private applications differently from cloud-based applications are gone. Hybrid users need consistent access to all their applications—whether on premises, in cloud-based data centers, internet-based or SaaS—anywhere they now work.
- **A narrow security view:** Even as they migrate to cloud, many in government still view network access as the sole goal of their cyber controls. To comply with the Executive Order and OMB strategy, zero trust needs to be thought of more broadly and holistically. IT leaders need to understand that zero trust is a methodology and move beyond the tendency to view it as a collection of specific products and narrow technologies.

Best Practices in Zero Trust

Think in Terms of the Ecosystem

Zero trust is more than the sum of the various products and technologies you might deploy. “In developing their strategies, agencies need to consider the entire ecosystem of controls—network, endpoints, cloud, applications, Internet of Things devices, identity and more—that they rely on for protection,” Epperson said.

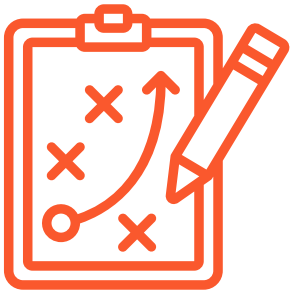
While many vendors label anything they sell as “zero trust” these days, it’s important to understand zero trust as a methodology that enables policy-driven protection and enforcement for all users, applications and infrastructure. This approach will also safeguard the data communications between these elements, regardless of location.



Identify Solutions Already in Place and Assess Risk

In order to move effectively toward a comprehensive zero trust strategy, it’s helpful to take stock of existing resources and identify potential liabilities. “Do an audit of what you have in place today and optimize those products and solutions. In other words, if you have technology in place that is working for you, start there.” Epperson said.

Working either on its own or with support from an outside vendor, an agency can determine its current security posture in order to maximize the return on both new and existing security investments. “Look at what security capabilities you have today and whether you’re using them as effectively as possible,” Epperson said. “Consider what current set of controls can be immediately leveraged and start applying zero trust best practices across your organization.”



Create a Zero Trust Plan

Zero trust is best viewed as a journey, and like every journey, it requires a map. It’s important to create a plan of action in order to move forward effectively, and to have executive support for that plan.

“A zero trust plan often requires a mindset shift among top leadership around this point of view,” Epperson said. “Proactive, substantive conversations on this topic must occur, and the CISO must be invited to the head table to engage in discussions and planning. This dialogue can help move the cybersecurity budget from insufficient to appropriate. It also prevents common misconceptions that can create doubt within the organization.”

Having a zero trust plan in place ensures a more seamless and coordinated approach. A solid plan can help to create a zero trust culture in an organization, and can help ensure IT doesn’t get overburdened by the complexity of too many security controls. With a plan in place, an organization is empowered to implement fewer tools, leveraging automation for maximum efficiency.

Case Study: How Palo Alto Networks Put Zero Trust to Work

When Palo Alto Networks began its own zero trust approach, the team realized it needed to first map out a strategy.

"Zero trust is a journey," said Niall Browne, Chief Information Security Officer for Palo Alto Networks. "And with a journey, the first question is, 'Where do you start?'"

Palo Alto Networks began its journey to zero trust by identifying its "crown jewels"—that is, its most critical assets that needed to be protected. For Palo Alto Networks, that included source code, intellectual property and its supply chain.

With its crown jewels identified, the next step involved understanding where those crown jewels were found. In other words, stakeholders needed to identify in what applications the data lived and where it resided on the infrastructure. They also had to identify which users were accessing it. Once they answered those questions, they knew where to start with zero trust.

To make this more manageable, Palo Alto Networks consolidated its technology stacks. Instead of managing a software stack, a security stack and so on, all transactions run through a central network platform stack, providing end-to-end visibility of its environment.

"Consolidating those stacks also made it possible to bring in automation, which is essential to zero trust," Browne said.

In a typical day, the Palo Alto Networks security operations center (SOC) team processes more than 17 billion security events. Their **Cortex XDR** application reduces these events to an average of 467 alerts. Their automated **Cortex XSOAR** platform is able to take those 467 alerts and reduce them to just 67 incidents needing analysis. Fifty-eight of those are automatically remediated by XSOAR. That leaves nine incidents that the SOC must handle manually.

By going from 17 billion security events to nine, the net result is that the SOC is able to identify and respond to events more effectively and quickly. Today, the mean time to detect an event is 10 seconds, and the mean time to respond to high-priority alerts is one minute.

That accelerated response time is critical. Zero trust is built on the assumption that malicious actors will get inside your network perimeter, so the real task is to detect them, contain them and mitigate the damage. In other words, it's about improving your cyber resilience.

"If malicious actors are going to get in, you need to be a cyber-resilient organization," Browne said. "The best way to achieve resilience is by taking a zero trust approach to cybersecurity."

PALO ALTO NETWORKS: YOUR PARTNER FOR ZERO TRUST

Palo Alto Networks is a trusted public sector partner, having supported hundreds of states, localities, K–12 schools and universities. The public sector is managing data more broadly and rapidly than ever to enable its critical missions. More data in more places makes a zero trust strategy at all levels of government and education imperative. Palo Alto Networks enterprise and cloud offerings can protect agencies in critical operating environments while providing assistance on the journey toward zero trust.

Palo Alto Networks approach to zero trust addresses users, applications and infrastructure in order to deliver a comprehensive set of security capabilities. It introduces consistent controls across the entire organization and brings to life security-by-design across the entire security ecosystem.

In addition, the Palo Alto Networks Certified Professional Services Partner Program can help agencies accelerate implementation, minimize risk and gain confidence as they roll out their zero trust strategy.

Conclusion

At a time when the frequency and severity of cyberattacks is on the rise, the recent cybersecurity Executive Order and the related federal zero trust architecture strategy are driving federal agencies in the direction of heightened awareness. Those same requirements have put state, local and educational entities on notice: They too are thinking more seriously about cybersecurity. Faced with this imperative to implement significant improvements, the public sector needs to adopt a holistic approach to zero trust.

It's especially important that agencies take steps to eliminate implicit trust across users, applications and infrastructure, as cloud-based solutions bring to the fore new architectures and new delivery models. In an increasingly interconnected IT landscape, they can no longer afford to view zero trust through a product-specific lens. Rather, they need to take a holistic view.

Working from this base, they can implement scalable solutions that more effectively protect agency activities and citizen data in the face of mounting cyberthreats.

ABOUT PALO ALTO

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

ABOUT CARAHSOFT

Carahsoft is The Trusted Government IT Solutions Provider®. Our technology manufacturers and reseller partners are committed to providing IT products, services and training to support government agencies as well as healthcare and education organizations. As the Master Government Aggregator®, Carahsoft holds over 100 state contracts and cooperative purchasing vehicles, including NASPO ValuePoint, OMNIA Partners, PEPPM and GSA, to meet the technology needs of state and local governments across the U.S.

Visit www.carahsoft.com, follow @Carahsoft, or email sales @carahsoft.com for more information.

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop