dynatrace

TD SYNNEX
Public Sector

Implementing zero trust for federal agencies

Because the traditional perimeter no longer exists, **zero trust has emerged as an essential, leading component of today's cybersecurity strategies.** The White House Executive Order on Improving the Nation's Cybersecurity calls for agencies to advance toward a zero-trust architecture. The order "eliminates implicit trust in any one element, node or service, and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses."

Why zero trust?

When we all went to an office and sat in a designated workspace with an assigned desktop computer, security teams never had to consider something like zero trust. They only had to safeguard what was tucked inside a traditional perimeter.

Today, however, they struggle to defend a perimeter-less enterprise, with widespread satellite offices, cloud services and remote work arrangements. The current organizational culture is all about Bring Your Own ... Everything — especially devices and applications. This is blurring the line between the personal and professional usage of these tools, with a large number of employees treating their company laptop as a personal device, even allowing their children and friends to use it.

A modern imperative

That is why government leaders are increasingly concluding that zero trust is an imperative rather than a consideration. At its core, zero trust is about following the principle of "never trust, always verify." Applying the tenets of a least privilege environment, it "allows users full access, but only to the bare minimum they need to perform their jobs," according to the White House Executive Order. If a device is compromised, zero trust can ensure that the damage is contained.

As such, a comprehensive and successful zero trust program requires that organizations adopt the following five tenets:

- Security teams assume the network is hostile.
- Teams operate as if threats are either already inside the virtual gate or are plotting to gain entry — at all times.
- They authenticate and authorize every device, user and network flow.
- They recognize that the establishment of network locality should never suffice as an establishment of trust.
- They enforce dynamic policies that leverage as many sources of data as possible.

Four of five federal IT leaders say they are **including or defining zero trust within their cybersecurity strategy.**

Observability ensures enforcement

At Dynatrace, we work closely with government customers to help them achieve these goals. We empower them with automatic and intelligent observability so they can:

- continuously monitor and capture all data from logs, metrics and end-to-end transactions;
- apply artificial intelligence (AI) to set baselines; and
- automatically identify anomalous and potentially threatening activity to enforce least privilege.

Here's how observability extends to every device, browser and application supporting every user:

Dynatrace SmartScape maps in real-time all the components and dependencies in an agency's ecosystem, including what is expected — hosts, networks and other infrastructure — and unpredictable website, application, services and process activity.

Dynatrace's **Apdex** rating system is calculated for each discrete user action and application.

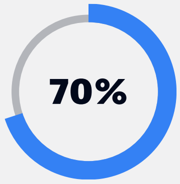
Dynatrace OneAgent automatically and continuously tracks all dependencies associated with an individual host.

Our AI engine, **Davis,** scours for risk vulnerabilities within applications running in the cloud, containers, virtual machines and traditional servers, while analyzing logs, metrics and traces for additional context to immediately pinpoint the root cause of issues.

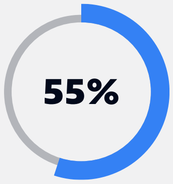
Dynatrace integrates with tools like **ServiceNow** and **Ansible** so agencies can rapidly resolve problems through auto-remediation, ensuring that applications are always on and fully optimized.

By the numbers

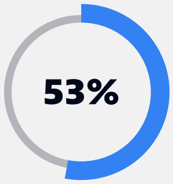
Government implementation of zero trust



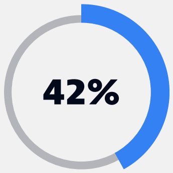
of federal IT leaders say that **zero trust has emerged as a greater priority** as more applications and devices access agency resources.



only 55 percent of federal IT leaders are **"very" confident in their agency's ability to deliver on a zero-trust framework.**



of federal IT leaders say that they are **"average" at best at limiting access to individual enterprise resources** on a per-connection basis.



of federal IT leaders admit they are **average at best at enforcing dynamic and strict user authentication** before access is allowed.

A clarion call for implementation

Top leaders from a wide range of government circles have voiced a sense of urgency for zero trust:

"We are being attacked in the cyber domain constantly, with state and non-state actors generating more than a billion cyber events a month on our networks across every DoD component around the world…We are moving towards more micro-segmentation in this cybersecurity model with zero trust. It will apply to our data and critical resources from our data centers to our mobile devices."

— **Vice Adm. Nancy A. Norton,** then Director of the Defense Information Systems Agency (DISA)

"Real-time authentication tests users, blocks suspicious activity and prevents adversaries from the kind of privilege escalation that was demonstrated in the SolarWinds incident. Many of the tools we need to implement (zero trust) already exist within industry and agency environments. But successful implementation will require a shift in mindset and focus at all levels within federal agencies."

— **Chris DeRusha,** Federal Chief Information Security Officer

"If (attackers) can get a foothold inside the organization, and then get a hold of our own bots and turn them against us, that would be catastrophic…Most of the folks who are a little more forward-thinking in this space are basically treating every bot or every virtual worker, as it were, almost as its own authorization case."

— **Steven Hernandez,** Department of Education Chief Information Security Officer

"(Today's) challenges affect the Army's ability to keep pace with our adversary's sophisticated cyberattack vectors, and a perimeter-defense approach cannot always counter these threats. If we cannot take a perimeter-defense approach, we have to rely on zero trust to keep us safe."

— **Raj Iyer,** Army Chief Information Officer

To take advantage of the Dynatrace Software Intelligence Platform, powered by AI:

☎ Call us at +1 888 833-3652

✉ Email us at USFederal@dynatrace.com

Chat with us

About Dynatrace

Dynatrace provides software intelligence to simplify cloud complexity and accelerate digital transformation. With automatic and intelligent observability at scale, our all-in-one platform delivers precise answers about the performance and security of applications, the underlying infrastructure, and the experience of all users to enable organizations to innovate faster, collaborate more efficiently, and deliver more value with dramatically less effort. That's why many of the world's largest enterprises trust Dynatrace® to modernize and automate cloud operations, release better software faster, and deliver unrivaled digital experiences.

dynatrace.com blog @dynatrace

dynatrace

TD SYNNEX
Public Sector