Zero-Trust Security: The New Government Model

A GOVLOOP PLAYBOOK

govloop

Alcatel·Lucent Enterprise

Introduction

Recent cyberattacks have revealed an uncomfortable truth: **Public-sector data, networks and IT are less secure than agencies thought.** Now, doubts exist that traditional, perimeter-based security can protect governments. To guarantee mission wins, agencies at every level need a new gold standard for cybersecurity.

President Joe Biden's **executive order (EO) on cybersecurity** could not have come at a better time. Instead of relying on outdated tactics, Biden's EO directed America's cybersecurity toward a new future: zero-trust security.

This represents a big shift in how agencies think about security. In zero-trust security, all computing entities are deemed untrustworthy by default. Actively practicing zero-trust security also requires such unfamiliar concepts as continuous monitoring, network segmentation, identity and access management and the principle of least privilege. With such a steep learning curve, how can agencies quickly understand zero-trust security and align with the transformative details in Biden's EO?

Govloop and Alcatel-Lucent Enterprise, a telecommunications equipment provider, created this playbook to help answer that question.

In this playbook you'll find...

- What zero-trust security is, how it works and its similarities to and differences from traditional, perimeter-based security
- Definitions, facts, figures and timely news illustrating zero-trust security's growing importance
- The four elements that agencies need to effectively implement and practice zero-trust security
- Case studies demonstrating how zero-trust security is helping agencies score mission wins
- Best practices for embracing and maintaining healthy zero-trust security
- Insights from Brian Gattoni, Chief Technology Officer (CTO) at the Cybersecurity and Infrastructure Security Agency (CISA)
- Thought leadership from Steven Kleinpeter, Director of Federal Sales, and Patricio Martelo, Director of Network Architecture, for Alcatel-Lucent Enterprise

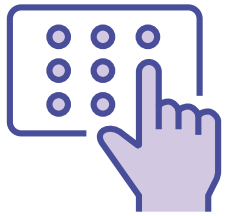
Need to Know

Understanding the following terms can aid agencies with navigating zero-trust security and its components.

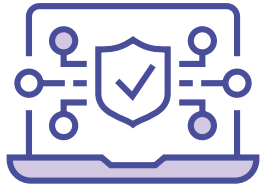
Zero-trust security is the philosophy that users and other computing entities should never be trusted. Instead, agencies should constantly verify the identity and access privileges these entities have. Zero-trust security also assumes that security incidents are inevitable, as threats can emerge from inside or outside any perimeter. Most importantly, zero-trust security is not a technology — it is an overarching approach that people, processes and tools undertake together.

Continuous monitoring uses automation to check systems for compliance issues or security risks in real time. This practice's insights can determine how agencies audit and govern computing entities to avoid interruptions and manage security risks.

Network segmentation splits IT networks into easier-to-manage segments. Besides improving an IT network's performance, this move can prevent breaches by malicious actors or malware from spreading.



Identity and access management refers to the framework of policies and technologies that control who has access to which network assets. For example, an identity and access management framework can verify users' identities, their roles and the permissions they have for engaging with resources.



The principle of least privilege is the idea that all users and systems should receive the minimum access privileges needed for their jobs. For instance, agencies' interns should not have the same data-handling abilities as their supervisors.

BY THE NUMBERS

In May 2021, the White House requested in its federal budget for fiscal 2022 **$750 million** in investments tailored to responding to lessons learned from the SolarWinds breach. In December 2020, a massive breach involving SolarWinds' network monitoring software was first publicly disclosed. The incident impacted scores of agencies and private sector companies nationwide.

The White House also announced in August 2021 that Google will invest **$10 billion** over the next five years to expand zero-trust security programs, help secure the software supply chain and enhance open-source security.

The House Oversight Committee revealed in November 2021 recent data showing that financial institutions reported **$590 million** in ransomware-related transactions during the first six months of 2021. Ransomware is a malicious software that blocks access to or threatens to publish victims' data unless a ransom is paid.

House Oversight Committee Chairwoman Carolyn Maloney noted in November 2021 that the Infrastructure Investment and Jobs Act includes **$1 billion** to help state and local governments shore up their cybersecurity and prevent ransomware attacks.

An October 2021 survey by the National Association of State Chief Information Officers (NASCIO) found that **67%** of state and territory chief information officers (CIOs) chose introducing or expanding a zero-trust security framework as the cybersecurity initiative that will receive the most attention over the next two to three years because of the COVID-19 pandemic's impact.

In the same NASCIO survey, **69%** of state and territory CIOs picked continuous enterprise cybersecurity assessments when answering which cybersecurity initiative would receive the most attention during the next two to three years due to the COVID-19 pandemic's influence.

In the News

A May 2021 cyberattack against the Colonial Pipeline sparked national concerns about cybersecurity by causing gas shortages in multiple states. Since then, the federal government has pushed for widespread zero-trust security nationwide.

FEBRUARY 2021

New York City Explores Zero-Trust Security

New York City Cyber Command (NYC3) coordinates the Big Apple's cyber defenses across more than 100 agencies by preventing, detecting, responding to and recovering from threats. Recently, NYC3 closed a **request for information** (RFI) about implementing zero-trust security citywide after more than two months seeking public comment. The RFI discussed NYC3's vision for transitioning New York City to a zero-trust security architecture that relies on risk-based access and continuously authenticating computing entities.

THE TAKEAWAY: **NYC3 issued the RFI to seek community input about how zero-trust security could address such common public-sector problems as protecting sensitive constituent data.**

MAY 2021

Biden Calls for Zero-Trust Security Federal Governmentwide

Biden's **EO on Improving the Nation's Cybersecurity** instructed federal agencies to advance toward zero-trust security architectures; the order also told agencies that zero-trust architectures must factor into their cloud computing migrations. Finally, the EO identified federal agencies like the Homeland Security Department (DHS) that will help their peers successfully reach zero-trust architectures.

THE TAKEAWAY: **Biden's EO established cloud computing, interagency collaboration and zero-trust security as cornerstones of the federal government's future modernization efforts.**

MAY 2021

Montana Seeks Zero-Trust Security Statewide

Chief Information Security Officer (CISO) Andy Hanks recently announced that Montana **plans on adopting zero-trust security statewide**. Montana's transition to zero-trust security may take three to four years, Hanks said. Hanks also noted that Montana's agencies are gradually adopting zero-trust security practices like continuously authenticating users' access requests. Additionally, Hanks said Montana would likely need more cybersecurity logging and continuous authentication mechanisms to deploy zero-trust security statewide.

THE TAKEAWAY: **Moves like Montana's can help governments of any size tackle growing security threats like ransomware.**

JUNE 2021

CISA Outlines Zero-Trust Security Maturity

After Biden's cybersecurity EO emerged, CISA released a draft of its **Zero Trust Maturity Model**. Per the EO's details, CISA's document assisted agencies with creating and implementing zero-trust security strategies agencywide. The model also listed identities, devices, networks and environments, application workloads and data as the five pillars that agencies' zero-trust security architectures must address. Lastly, CISA detailed what the traditional, advanced and optimal versions of zero-trust security architectures look like for agencies.

THE TAKEAWAY: **CISA's maturity model gave agencies benchmarks for implementing or improving their zero-trust security architectures.**

State of Montana Newsroom

Montana Focuses on Ransomware Defense, Shifting to Zero Trust

Montana CISO Andy Hanks details the state's key cybersecurity priorities for 2021 and beyond.

State Information Technology Services Division
May 25 2021

As the recent ransomware attack against a vital oil and gas pipeline operator, Colonial Pipeline, makes clear, such attacks are not going away and are becoming more persistent and targeting higher-profile entities. The FBI has attributed the attack to a criminal group, DarkSide.

AUGUST 2021

NIST Lists Steps for Zero-Trust Security Migrations

Following CISA's move, the National Institute of Standards and Technology (NIST) published a draft cybersecurity white paper called **Planning for a Zero Trust Architecture: A Starting Guide for Administrators.** This publication explained how the **NIST Risk Management Framework** (NIST RMF) can help agencies integrate zero-trust security into their risk analysis and management. The white paper also listed the seven steps that system administrators should follow — say, mapping potential attack surfaces to secure — when migrating to zero-trust security architectures at their agencies.

THE TAKEAWAY: **Zero-trust security can strengthen agencies' risk analysis and management, making it a mentality closely fitting the NIST RMF.**

SEPTEMBER 2021

OMB Publishes a Federal Zero-Trust Strategy

The latest zero-trust security development is the Office of Management and Budget (OMB) issuing a draft **Federal Zero Trust Strategy**. Initially, the strategy established a shared baseline for early zero-trust security maturity among federal agencies. From there, the memorandum requires agencies to meet various zero-trust security goals related to their identities, devices, networks, applications and data by fiscal 2024. For instance, all federal agencies must treat their applications as internet-connected by that deadline. Ultimately, the strategy specifies five criteria — like strengthening identity practices — all federal zero-trust security architectures should meet.

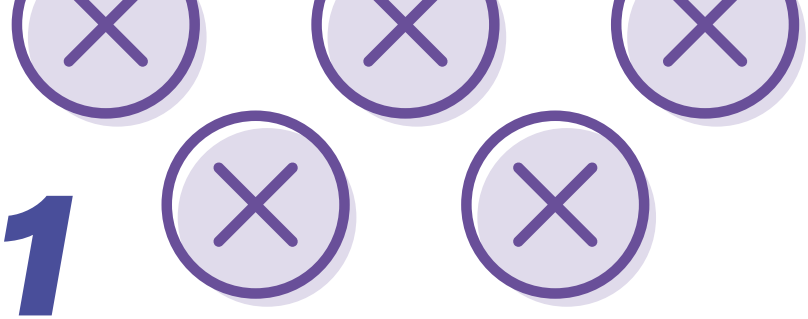
THE TAKEAWAY: **The Federal Zero Trust Strategy plots clear stops for agencies along the road to zero-trust security governmentwide.**

The Playbook:
Zero-Trust Security's 4 Components

Perimeter-based security has adequately defended agencies for a long time, but trends like the ubiquity of mobile devices suggest that its effectiveness is waning. Events like the Colonial Pipeline attack also hint that cybercriminals may be more dangerous than before. To cope, the public sector needs reinvented security.

Why would agencies hesitate to embrace zero-trust security? The reason is that zero-trust security is not a product or solution that agencies can buy. Instead, zero-trust security contains multiple components, each with its own challenges that agencies must address.

The good news is that any agency can leverage the four components anchoring zero-trust security. The four components are:



1

Never Trusting Anything

THE CHALLENGE: Trust is a positive quality that can build confidence between two parties in any government relationship.

But cybercriminals are ruthless, and they can exploit computing entities — including users, devices and systems — to erode that faith. From applications to data, bad actors have numerous ways to deceive agencies' unsuspecting employees.

To protect assets like sensitive constituent information, public-sector workers need zero-trust security's skepticism.

THE SOLUTION: Zero-trust security automatically distrusts all computing entities until their safety can be verified. While the concept seems simple, living it can be hard; picture denying access to familiar users whose identities cybercriminals may have compromised.

"Zero-trust security takes security controls to the paranoid level," said Patricio Martelo, Director of Network Architecture at Alcatel-Lucent Enterprise. "The presumption is that malicious attackers are already active on the network."

THE IMPORTANCE: When it comes to security, the stakes for agencies are high. Constituents not only rely on agencies for essential products and services like food stamps — they also trust agencies with private details like their Social Security numbers. Security incidents jeopardize both areas, potentially hurting the ties between agencies and their constituents.

"The cost of not moving forward with zero-trust security is so much greater than the cost of implementing it," said Steven Kleinpeter, Director of Federal Sales at Alcatel-Lucent Enterprise. "For every dollar that is spent, you are saving thousands of dollars."

2

Managing Identities and Access

THE CHALLENGE: All computing entities are a security risk for agencies because cybercriminals can use each one to trick employees into giving them access to sensitive items like data.

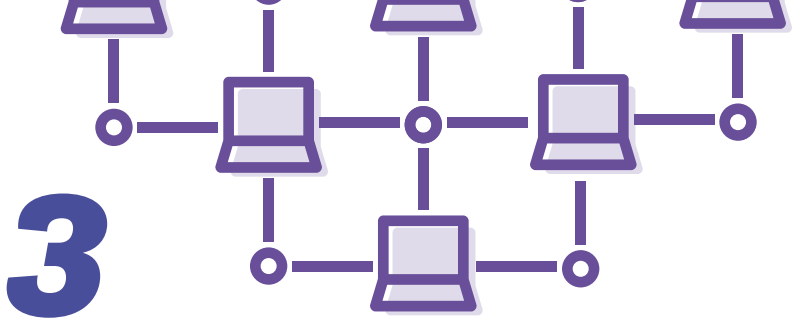
Hybrid workforces further complicate this situation by making traditional network perimeters more porous. With so many on-site and remote computing entities to infiltrate, cybercriminals never stop endangering agencies.

THE SOLUTION: Identity and access management guided by the principle of least privilege can elevate zero-trust security in two ways. First, this principle pushes agencies to determine the identity of all computing entities on their networks. After this, the principle presses agencies to give these entities the minimum access to resources that they need to fulfill their role's functions. Over time, governing identities and access in this way increases security and manages risk better.

"Identity and access management is absolutely key," Martelo said. "Networks are dynamic. Every verification that we do depends on identities."

THE IMPORTANCE: Some things are so vital that only the people who need them for their roles deserve access to them. When it comes to national security, for example, the president requires more top-secret information than a White House guard. In zero-trust security, the principle of least privilege applies this level of seriousness to identity and access management, halting potentially damaging access to valuables.

"We are moving into the same kind of environment that our federal government uses for classified documents," Kleinpeter said. "If you go into the Pentagon, you don't just go in and check out any document you want."



3 Segmenting Networks

THE CHALLENGE: Network security is not one-size-fits-all — different applications, systems and data require different security measures.

Take data. Agencies should not secure the classified data on their networks in the same way as unclassified data.

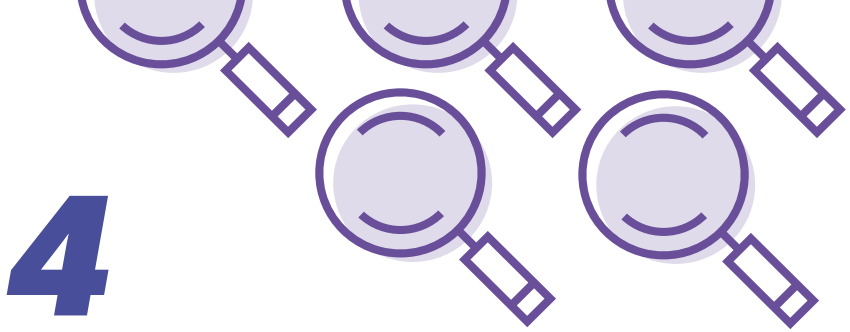
In perimeter-based cybersecurity, once a threat breaches a network, it has free reign to wreak havoc elsewhere. In today's world, agencies must have a way to respond to disruptions like these.

THE SOLUTION: Network segmentation provides agencies with flexibility before, during and after security headaches. Before complications, agencies can institute stricter or looser security controls over their network's various segments depending on the computing elements each contains. During mishaps, agencies can seal off their different network segments to keep security menaces from spreading. After security shortcomings, agencies can tighten the defense and performance capabilities of their network segments as needed.

"You can have segmentation for your remote, mobile users and everyone else on site," Martelo said as an example of network segmentation. "A hybrid environment is pretty much everywhere today."

THE IMPORTANCE: At the most basic level, segmentation can improve a network's performance. Beyond that, segmentation makes networks more manageable and secure as agencies can apply granular policies to them. While navigating security incidents, the advantages of network segmentation can be huge — agencies can halt intruders before they spread throughout entire networks.

"This is classic defense," Kleinpeter said. "Once you get past the perimeter, there have to be some controls to mitigate the damage."



4 Continuously Monitoring Computing Entities

THE CHALLENGE: Currently, agencies have more computing entities on their networks than ever to worry about. The volume of devices alone is exploding due to the internet of things (IoT), the web of devices that can connect to one another and exchange data.

Another challenge is that modern networks tend to be fluid — for instance, a reconfiguration can leave gaping vulnerabilities in a network that was once secure.

Consequently, agencies must watch their networks ceaselessly for potential security incidents.

THE SOLUTION: Continuous monitoring can give agencies the power to see every risk and compliance issue on their networks. Wielding context from continuous monitoring in real time, agencies are more capable of catching and fixing potential hazards.

"Continuous monitoring is essential for restricting and revoking access to devices and users that have been compromised," Martelo said. "It is about containing the damage."

THE IMPORTANCE: Continuous monitoring aims to inform agencies so that they obtain stronger vigilance. With so many computing entities in the world, knowing which entities matter and which ones do not can assist agencies with prioritizing their security efforts. Gradually, continuous monitoring improves agencies' decision-making about security so that their workers are not wasting their energy, funding and time on minor computing entities.

"If there is a problem user, they can be quarantined from the network and the situation can be remediated," Kleinpeter said. "Or it could be a laptop, a smartphone or a tablet."

How to Reach Zero-Trust Security Nirvana

While there is no denying technology's role in zero-trust security, it is not an outcome that agencies reach by flipping a switch.

Rather, zero-trust security extends beyond agencies' technology to their people and workflows. Collectively, agencies' people, processes and technology cultivate an active state of being constituting zero-trust security.

In June 2021, CISA released a draft Zero Trust Maturity Model intended to help nurture agencies' zero-trust security. GovLoop recently spoke with **CISA CTO Brian Gattoni** about this document, how it aligns with Biden's cybersecurity EO and the advantages zero-trust security offers agencies.

This interview has been lightly edited for clarity and length.

What shortcomings have incidents like the Colonial Pipeline cyberattack revealed about traditional, perimeter-based security?

Gattoni: As the federal government continues to expand into cloud and mobile environments, agencies' assets, data and components are now commonly located in areas beyond that traditional network boundary. This changes their risk and vulnerability posture to cyberattacks like ransomware. Incidents like the Colonial Pipeline serve as an important reminder that anyone can be hit by a cybersecurity breach. Those ransomware incidents can severely impact organizations and leave businesses unable to operate and deliver mission-critical services.

The best defenses for businesses of any size and any sector start with proper cybersecurity hygiene. That's a core building block toward establishing that organization's journey toward zero trust. It is the basic cybersecurity hygiene principles of keeping your software up to date, implementing multi-factor authentication, running up-to-date virus software and designing security from the inside out. This helps you consider leveraging your cloud-native applications, implementing strong identity credential and access management, least privilege and investing in strong email protections.

How does zero-trust security contribute toward the goal of improving America's cybersecurity that was outlined in Biden's recent EO?

The cybersecurity EO emphasizes the implementation of zero-trust and shifting that security closer to agencies' data. If data is the principal asset, we've got to move our trust establishment closer to it and put the security nearer to the thing we're securing.

In this new architecture, agencies will have better visibility into their networks. And CISA will have better visibility across the federal civilian executive branch to monitor and protect those assets more dynamically.

How does CISA's Zero Trust Maturity Model expand upon the recent cybersecurity EO's zero-trust security details?

We developed the Zero Trust Maturity Model here in 2021 to help agencies develop implementation plans as required by the executive order. The Maturity Model is designed to assist agencies with where they are now, where they may need to go and what services are available to them to help them get there in order to re-architect their networks in line with zero trust. The model represents a gradient of implementation, a spectrum across five distinct pillars where minor advancements can be made over time toward optimization and that final state of establishing that zero-trust nirvana everyone seeks.

The five pillars are identities, devices, networks, application workloads and data itself. Each pillar includes a cross-cutting detail on the visibility and analytics established between all the pillars, as well as the automation and orchestration elements across those pillars.

Each of these maturity levels is broken into three stages with increasing levels of protection, complexity and detail for adoption. There's traditional, advanced and then the optimal state.

Zero trust is not a snapped finger and achieved initiative. It is a journey over time where you must make explicit decisions about what you're going to transform. The Maturity Model helps people understand where they are now in that journey, local to their experience. Risk management and enterprise development are very localized issues. Where are they in their own individual journeys, how can they take steps forward and engage with CISA to advise them on that process?

What is the main takeaway people should have about zero-trust security?

Zero trust is a critical step in securing our nation's most valuable data. But implementing this concept is a long journey. An organization cannot buy zero trust off the shelf and implement it in a few months. Rather, those organizations can expect the implementation of zero trust to take multiple years on the order of five to 10 years as you move through that maturity model toward an optimal state.

Implementing zero trust is also a culture shift for the organization. It requires coordination between infrastructure, engineering, security and implementation teams who are establishing that continually secure enterprise and mission or business operators who understand their role in implementing that security.

Technology alone has rarely solved a problem. The intersection of technology, people and processes — which, in mature organizations can be surmised as a culture shift — is the successful way forward in any new paradigm.

Upcoming Federal Zero-Trust Security Projects

The Technology Modernization Fund (TMF) is a federal program that offers funding and operational, technological and transformational consulting to agencies' cybersecurity and IT modernization projects.

Highlighting zero-trust security's rising relevance, the TMF Board awarded support to three agencies undertaking projects related to the security posture in September 2021. The three initiatives are:

The Office of Personnel Management's (OPM) Zero Trust Networking project

Citing OPM's status as the federal government's human resources (HR) provider, the TMF Board awarded the agency $9.9 million. The funding will help OPM protect sensitive data from millions of current and retired federal employees by utilizing a zero-trust cybersecurity architecture strategy.

The strategy aims to apply zero-trust security solutions to five pillars at OPM: identities, devices and endpoints, networks and environments, application workloads and data. OPM's effort strives to reduce the agency's attack surface while adding cybersecurity protections, visibility and resilience to services agencywide. The project will additionally align OPM with Biden's cybersecurity EO while progressing toward an optimal level in CISA's Zero Trust Maturity Model.

The Education Department's (ED) Zero Trust Architecture

This plan establishes a two-year timeline for enacting a program encompassing ED's architecture, design, strategy and implementation roadmap for zero-trust security.

The TMF Board gave ED $20 million for the effort, which will also create an enterprisewide program management office for its zero-trust security work. The goal is a more secure — and less burdensome — user experience (UX) for ED's employees and the public. For its part, the project's roadmap will also lay out the adoption of an advanced architecture involving zero-trust security for ED's cloud environments. By 2023, ED's project will additionally catalog its security orchestration, automation and response (SOAR) and other modern cybersecurity technologies. SOAR software manages security threats and vulnerabilities, responds to incidents and automates operations.

The General Services Administration's (GSA) Advancing Zero Trust project

The TMF Board provided the GSA with $29.8 million to modernize its legacy network systems and implement an advanced zero-trust security architecture. This architecture will focus on three blocks: users and devices, networks and security operations.

The GSA wants continuous security verifications of its applications, devices, data and users alongside broad visibility into its ecosystem agencywide. The project also hopes to refine the GSA's UX while adhering to zero-trust security tenets for the global connections between the agency's applications and environments. Finally, the effort will include multiple modernization maneuvers. One focus area will be the GSA's telework operations, which will have their directory designs replaced to incorporate enhanced security principles.

INDUSTRY SPOTLIGHT

The Zero-Trust Security Evolution

An interview with Steven Kleinpeter, Director of Federal Sales, and Patricio Martelo, Director of Network Architecture for Alcatel-Lucent Enterprise

Change is hard, and few shifts can seem as daunting as overhauling agencywide security. Yet that is what zero-trust security asks of governments — abandoning conventional, perimeter-based defenses for a more fluid variety based on wariness.

Fortunately, zero-trust security can be a smooth journey rather than a faraway destination for agencies. From the top down, any agency can take straightforward steps to raise its zero-trust security competence.

"Zero-trust security turns the old legacy model on its head," Martelo said. **"This is an evolution, not a revolution."**

Martelo and Kleinpeter, his fellow expert at Alcatel-Lucent Enterprise, provided agencies with three methods for heightening their zero-trust security.

1. Catalog computing entities.

Agencies cannot secure all their computing entities if they do not realize that some of these entities exist. Think about contemporary mobile devices. No agency should forget tablet security if their laptops and smartphones are accounted for.

"IoT is the weakest link," Martelo said. "You need to know what is on the network."

Documenting their computing entities can aid agencies with continuously monitoring them. The resulting zero-trust security is more adaptive and effective agencywide.

"You should be able to bring up one pane of glass and see what is happening on your network," Kleinpeter said.

2. Carefully pick equipment.

People would not secure their houses with faulty locks, and the same spirit can apply to government technology. Robust zero-trust security may require agencies to examine their tools for even tiny flaws.

Imagine the typical network switch transferring data between computing devices. True zero-trust security suspects that even the software code supporting this hardware may be perilous.

"When you put a switch into your network, if you can't verify the code, you're starting off from the wrong point," Kleinpeter said. "The software running these switches and doing the work needs to be trustworthy."

Whether they are people, processes or technologies, zero-trust security assumes that everything has hidden hazards.

3. Exercise caution on vendors.

With zero-trust security, there is no such thing as above and beyond. When procuring products and services, agencies should pay attention to the vendors taking extra precautions.

One attribute to look for is independent third-party verification and validation. This process features a third party outside of the product's creation testing and affirming it meets its security and other standards.

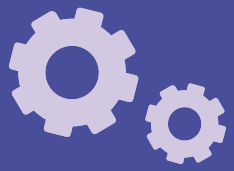
"They go through our code line by line to make sure there's no malicious code," Kleinpeter said of the procedures that Alcatel-Lucent Enterprise's operating software undergoes.

Alcatel-Lucent Enterprise can furnish agencies with software platforms that allow them to debut zero-trust security and then easily enforce it agencywide. Platforms like these assist agencies by keeping zero-trust security and mission wins in sight.

"Zero-trust security does not require a rip and replace to get there," Kleinpeter said. "It is a constant effort to make sure that you're securing what's happening."

Next Steps

After adopting zero-trust security, these three tactics can make agencies' defenses even tougher:

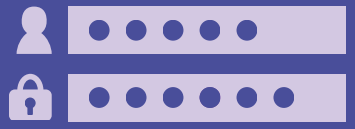


1. Automate basic security tasks like patching software.

Human error may be one of agencies' biggest security risks, but automation can alleviate this burden by performing tasks like resetting passwords without involving people. As agencies automate more things, their workforces have smaller daily checklists and more space for complex activities. Agencies can even automatically block unapproved devices from joining their networks, an easy configuration that can skip problems caused by suspect tools.

2. Encrypt both resting and in-transit data.

Whether data is flowing across agencies' networks or stored in their databases, it ranks among the biggest temptations for cybercriminals. Encryption renders data into a form that ideally can only be translated by authorized parties. Beyond making data harder for cybercriminals to decipher, encryption also prods agencies to validate every entity requesting this information. Biden's recent cybersecurity EO additionally mandates encryption for federal agencies, suggesting that the technique may eventually trickle throughout the public sector.



3. Make multi-factor authentication second nature.

Much like encryption, Biden's EO also requires federal agencies to institute multi-factor authentication. Multi-factor authentication forces users to present two or more pieces of evidence for verification when accessing someone's sensitive materials. Typically, these components include something only the user *knows* (a birthday), something the user *has* (a randomly generated token sent to their smartphone) or something the user *is* (the owner of unique fingerprints). Overall, multi-factor authentication empowers zero-trust security by making user identity verification stricter and more cautious.

With Biden's cybersecurity EO bringing extra attention to zero-trust security, there is no time like the present for agencies to own this methodology.

Alcatel·Lucent Enterprise

Thank you to Alcatel-Lucent Enterprise for their support of this valuable resource for public-sector professionals.

For more on ALE's zero trust architecture: download the eBook
For more information: https://www.al-enterprise.com/en/industries/government/defence-solutions

govloop

About GovLoop

GovLoop's mission is 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 the public sector.

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