SSH

A Guide to Federal Zero Trust Access Management

Index

How to Use this Guide

Zero Trust is emerging as a critical cybersecurity principle across all industries, encouraging enterprises to “never trust, always verify.” A key component of Zero Trust requires credentials — such as usernames, passwords, and SSH keys — to be comprehensively managed and authenticated to mitigate threats that can snowball into devastating breaches.

Recently, federal regulations have been established to provide benchmark guidelines for implementing Zero Trust infrastructures to keep data safe from lingering eyes. In this guide, we unpack what this means for federal agencies and organizations moving forward.

Introduction to Zero Trust for Federal Agencies

Many organizations have already established basic internal policies for integrating Zero Trust architecture into their existing IT and OT frameworks, but the White House's recent executive order signals a widespread shift towards more concrete and universally accepted practices.

While the National Institute of Standards and Technology (NIST) offers general guidelines for transitioning into a Zero Trust environment, the executive order makes it mandatory that federal agencies adopt strategies to enforce this principle.

Key policies defined in the order require federal organizations to:

- **Remove contractual restrictions from cloud service providers that inhibit them from sharing threat information with federal departments responsible for cybersecurity**
- **Upgrade legacy machinery to facilitate new technologies and interoperable software**
- **Develop concrete security strategies involving Zero Trust authentication measures**
- **Facilitate cross-agency collaboration and reporting to strengthen supply chain security**
- **Establish a review board focused on reviewing, assessing, and overseeing Zero Trust implementations for vulnerability mitigation and adequate cyber safety enforcement**
- **Increase federal visibility into all devices used for activity on government servers and networks**

A key element here is Zero Trust authentication measures, since they are linked to:

- **Supply chain security (who has access to your sensitive information from outside your organization?)**
- **Identifying, tracking and auditing in-house access (how many doors are there to your classified data and who goes through which door?)**
- **Managing the credentials that allow access (how many keys to your kingdom are there and who has them?)**
- **Understanding where your critical data is (in-house data center, private cloud, public cloud, third-party servers, etc.)**
- **How your organization collaborates on sensitive data when emailing, sharing, and collecting data, or signing contracts**

With unmanaged and unsecured privileged access posing a major risk in federal environments, with potentially national and cataclysmic consequences, adopting Zero Trust architecture is of critical importance.

What is Zero Trust?

Forrester Research analyst John Kindervag first introduced Zero Trust architecture in 2010, advocating for the importance of denying privileged access by default. Zero Trust is an approach grounded in caution and skepticism — it's a security model in which all user identities and endpoint connections are always authenticated and never automatically trusted.

Whether embedded in software applications, hardware systems, or cloud servers, Zero Trust models require organizations to employ:

- **Multi-Factor Authentication (MFA)**, which prompts users and autonomous devices to provide additional authentication credentials upon sign-in
- **Just-in-Time (JIT) access**, which relies on single-use ephemeral certificates for temporary entry into privileged areas
- **Least privilege access**, which grants users just enough access to perform their expected tasks and nothing more
- **Segmentation of Duties (SoD)**, which refers to the concept of heavily restricting complete IT access for all individuals and machines, no matter the degree of access their privileged accounts allow
- **Microsegmentation**, which calls for IT environments to split into separate security zones to prevent organization-wide access to critical resources

There is not a single vendor that can deliver a full-blown Zero Trust architecture to a customer. In fact, a fully Zero Trust proof environment might be completely unattainable. However, it's a goal you should aspire towards to improve your security posture.

It is best to handle IT transactions as if assuming that an adversary has already breached an agency's walls, to ensure constant scrutiny and adherence to cybersecurity standards. And this is exactly why access management should be a key focus when adopting Zero Trust processes.

Why is Zero Trust Access Management Important Now?

Hybrid environments embracing remote and on-premises connectivity have gained popularity in the past several years as IoT devices and cloud servers provide game-changing interoperability to organizations. With the COVID-19 pandemic cementing hybrid IT/OT infrastructures in many organizations, entities now have the power to function beyond physical bounds with more ease than ever before.

At the same time, this progress leaves a wider attack surface for hackers to exploit. The use of passwords or SSH keys (that typically outnumber passwords by the ratio of 10 to 1) and other credentials alone is no longer enough to prevent the wrong user from accessing confidential data without detection. That's why Zero Trust initiatives are essential — they add security checkpoints throughout the authentication process to further validate the identity of the user or machine, keeping suspicious users out.

Zero Trust regulations are pouring in from the Cybersecurity and Infrastructure Security Agency (CISA), Defense Information Systems Agency (DISA), National Security Agency (NSA), NIST, and other federal organizations. Some notable mandates include:

- **Sarbanes-Oxley (SOX):** Requires public companies to prove the legitimacy and accuracy of financial statements and management credentials used for financial reporting. Also known as 15 U.S. Code Chapter 98. Penalties for falsehood and fraud include fines between $1 million and $5 million and between 10 to 20 years of prison time.
- **SEC Rule 30:** Created by the U.S. Securities & Exchange Commission, SEC Rule 30 is outlined in 17 CFR Part 248 Regulation S-P. It requires U.S. and international financial institutions registered with SEC to develop and implement written internal policies for safely managing and storing consumer financial and personal information. Violations include civil fines of up to $1 million.

  Just recently, SEC fined Wall Street companies over 1.8 billion dollars for using unencrypted and untrackable communications.
- **Gramm-Leach-Bliley Act (GLBA):** GLBA is comprised of a Security Rule and a Privacy Rule (16 CFR Part 314) that extend to all entities within the financial sector — the GLBA requires all companies and their respective employees to establish a baseline security framework and behavioral guidelines to properly safeguard consumer information. This act urges companies to provide consumers with written disclosures thoroughly outlining the use, handling, and sharing of their private data. Violations typically result in fines of over $1 million, with the possibility of a business' FDIC insurance being revoked.
- **Defense Federal Acquisition Regulation (DFAR):** Applicable to individual contractors and subcontractors affiliated with the U.S. Department of Defense, this regulation requires employees to sufficiently protect, transmit, and store unclassified government information at all times — especially within internal applications and systems. DFAR is outlined in 48 CFR § 252.204-7012. Penalties include revoked privileges and termination from the Department of Defense.
- **Food and Drug Administration (FDA) Regulations:** The Use of Electronic Records in Clinical Investigation specifically orders all organizations associated with the clinical testing and review of medical products to maintain and monitor their IT infrastructures as they interact with data stemming from these investigations. In addition to breach and data leak prevention, these regulations (21 CFR Part 11) preserve the integrity of all recorded information. Violations result in audits conducted by the FDA.

- **Health Insurance Portability and Accountability Act (HIPAA):** HIPAA, one of the most widely known cybersecurity policies, details and enforces strict rules over the handling of medical information across the healthcare field, prioritizing patient consent. Penalties for violations vary, but recent fines have reached upwards of $20 million.
- **PCI-DSS:** The Payment Card Industry (PCI) Security Standards Council (SSC) was founded by major credit card companies (such as American Express, Visa, MasterCard, and Discover) with the following two priorities:
    - Helping merchants and financial institutions understand and implement standards for security policies, technologies, and ongoing processes that protect their payment systems from breaches and theft of cardholder data.
    - Helping vendors understand and implement standards for creating secure payment solutions.

Because of the increasing number of these mandates, Zero Trust will become a leading priority for many entities looking to protect themselves to a federal standard.

Zero Trust and the Quantum Threat

Public key cryptography (PKC) offers security in the length of its keys as well as the algorithms used to generate these keys. For example, the Rivest-Shamir-Adleman (RSA) algorithm leverages two prime numbers to generate a private and public key. Users or devices would have to perform the nearly impossible task of factoring the 2048-bit value to extract the two prime numbers to decrypt the public key.

Unfortunately, quantum computing can solve incredibly complex computations, such as the RSA algorithm, in a short amount of time, rendering classical encryption algorithms obsolete. As a result, the U.S. government announced legislation designed to fortify existing infrastructures with quantum-proof solutions and heightened security policies.

The government's security memorandum highlights current weaknesses in public-key cryptography and prompts federal agencies to move toward Zero Trust models through research, staff proficiency, and cross-department collaboration. Key policies urge agencies to:

- Move away from perimeter-based security in this era of cloud computing
- Encrypt all data in transit
- Categorize data based on protection needs and privileged access
- Leverage identity and privileged access management platforms for automated authentication, security, and surveillance

- Retire credentials and move into a passwordless future
- Eradicate reliance on basic security implementations, like VPNs and firewalls
- Employ immutable environments that can't be easily configured

This means federal agencies will have to develop Zero Trust solutions that work in tandem with these mandates to stay fully protected against quantum brute force attacks.

The 7 Pillars of a Zero Trust Access Security Model

Reinforcing the security of every IT/OT touchpoint takes careful consideration, coordination, and cooperation to ensure proper alignment with all moving parts. The Zero Trust security model is often broken down into six pillars to help entities account for all assets and resources within their extensive data framework. Federal agencies and organizations are encouraged to use these pillars as guidance for fully incorporating Zero Trust features into their environment.

Users

The primary tenet of the Zero Trust model, user identity authentication and management involves using tools like MFA, Identity and Access Management (IAM), and Privileged Access Management (PAM) to heavily monitor and limit user access to an organization's confidential material.

Federal agencies are required to continuously authenticate human and non-human user touchpoints, and appropriately issue and revoke privileged permissions to reduce the risk of internal breaches.

Devices

The apparatuses used to access networks and servers must also be monitored for any bugs or vulnerabilities that may inhibit the efficacy of identity and privileged access security solutions. The Department of Defense, in its Zero Trust Reference Architecture handbook, recommends implementing Mobile Device Managers and Trusted Platform Modules that offer visibility into the performance of devices as access requests are performed.

These measures help to prevent connections from being intercepted by threats like man-in-the-middle attacks, should a device be compromised. Frequent, real-time assessments are also recommended to investigate anomalies in activity and access.

Networks

When used in hybrid environments, firewalls and other perimeter-based security applications provide insufficient coverage against intrusion. Microsegmentation is a stronger alternative that supplements remote environments and hybrid integration points with additional authentication checkpoints.

awareness and control over network-based connections. This helps organizations detect breaches before they can inflict widespread damage.

Federal agencies are required to narrow their focus on privileged network access and dynamic traffic flows through heightened awareness and control over network-based connections. This helps organizations detect breaches before they can inflict widespread damage.

Applications

Secrets and workload tasks should also be under strict surveillance. Analyzing who is accessing particular data and how they're retrieving it helps executive decision-makers better understand the level of permission they should grant each user and device. MFA can also be applied to applications to prevent unauthorized entities from entering zones housing valuable data.

The management of containers and virtual machines through proxy authentication tools keeps federal agencies secure at each and every touchpoint in an application stack.

Analytics

Without performance metrics, there's no surefire way to assess how effective Zero Trust implementations are within an enterprise. Auditing and logging programs give administrators transparency into the overall security picture of an environment, enabling agencies to keep all security solutions working seamlessly with one another.

Dedicating a workforce to analytics and traffic supervision will help federal agencies extinguish small fires before they escalate into a catastrophe.

Automation

Orchestration through automation ensures that all security solutions are managed regularly for complete oversight and timely resolution. Tools like Security Information and Event Management (SIEM) solutions are helpful provided that well-defined policies and configuration settings are established.

With automation, federal agencies can better monitor entire networks, assured that various security implementations are reliably keeping all users, devices, applications, and networks safe.

Data Classification

Implementing policies that restrict the sharing of and access to sensitive data is vital for achieving Zero Trust. In IT/OT environments, this is called following the principle of least privilege, where a person is granted the minimum level of access necessary to get the job done.

In business contexts, examples of this include sending personally identifiable information (PII) over email, collaborating on contract details in a shared workspace, signing contracts, and capturing information in web forms.

All this data needs to be classified according to the sensitivity level of the data — for example, confidential, restricted, or secret. Moreover, you should always ensure that data is shared using end-to-end encryption not available in regular collaboration tools like Outlook, Slack, or Adobe Sign.

It is also important that you:

- Verify the person who gains access to the data
- Have a solid audit trail of all access and changes,
- Give read/write access as needed
- Implement additional security controls such as multi-factor authentication (MFA)

Benefits of Zero Trust Access Management for Federal Agencies

Federal agencies are responsible for overseeing societal matters, and often depend on a bustling IT/OT ecosystem to navigate a hectic schedule. While security is a priority for agencies possessing libraries of highly classified government assets, it's time to usher in a new era of cybersecurity that's armored with future-proof solutions.

Besides protecting national data and resources, Zero Trust enables federal agencies to:

- **Eliminate the need for password-based authentication** and provide support for passwordless, ephemeral certificates. This greatly reduces the number of keys and credentials for hackers to exploit while minimizing credential management workloads.
- **Accelerate operations by freeing up compliance-related tasks.** Automated Zero Trust solutions relieve human resources that could be funneled toward priority tasks, helping agencies better serve their respective communities. Zero Trust also gives agencies more time to continuously improve existing security measures to stay ahead of growing threats.
- **Centralize security zone management** and overall infrastructure traffic flows. Leveraging a single system that controls access mitigates the risk of human error and quickly directs administrators toward failing security points.
- **Invest in technology to align with modern cybersecurity goals.** The Zero Trust model accounts for hybridity, enhancing automated interoperability across cloud and on-premises servers, networks, wireless devices, and disparate security applications — crucial for federal agencies requiring cross-department communications.

How to Transition to a Zero Trust Model

As the White House urges federal agencies to swiftly transition to Zero Trust, it's important not to conduct a complete overhaul of existing solutions. This could cause unintended leaks through unprotected endpoints becoming exposed as legacy systems are deactivated.

Instead, follow a gradual implementation plan that shields transition points as Zero Trust features are introduced. The best way to do this is to take inventory of all the assets, resources, credentials, applications, and devices your organization depends on to perform daily tasks. Map out points of contact, connectivity, and traffic channels to better understand data movement across your IT and OT environments.

Then, pinpoint areas that need the most improvement in security and upgrade them with Zero Trust solutions. You can start by switching to JIT certificate models that limit re-entry into certain security zones without authentication. This model effectively limits the use of always-on credentials in favor of temporary access verified every time a connection is made and allows organizations to migrate to passwordless and keyless authentication methods. You can do this gradually with a hybrid model that allows you to modernize your environment at a pace you can manage and control. The ultimate goal is to retire as many legacy applications as possible, without compromising data integrity.

Trust SSH for Reliable Zero Trust Solutions

Integrating Zero Trust solutions into any IT and OT environment can be an overwhelming feat, but SSH makes it simple with frictionless management tools that organize, audit, rotate, and flag assets as they're used within the cloud or in-office.

From key and password management and secure business collaboration to remote privileged access management, our solutions are designed with the future in mind, offering quantum-safe cryptography, role-based access control, and up-to-date regulatory compliance. SSH's Zero Trust solutions even allow you to migrate to a fully passwordless and keyless environment at a pace that suits you, all while managing your existing credentials.

Keep your security framework several steps ahead of today's threats and tomorrow's worries — get in touch with us today to learn how you can better protect your data with Zero Trust architecture.

We’d love to hear from you

Get in touch
with our experts
around the world.

GLOBAL HEADQUARTERS

Helsinki

SSH COMMUNICATIONS
SECURITY CORPORATION

Karvaamokuja 2b, Suite 600
FI-00380 Helsinki
Finland
+358 20 500 7000
info.fi@ssh.com

US HEADQUARTERS

New York City

SSH COMMUNICATIONS
SECURITY, INC.

434 W 33rd Street, Suite 842
New York, NY, 10001
USA
Tel: +1 212 319 3191
info.us@ssh.com

APAC HEADQUARTERS

Hong Kong

SSH COMMUNICATIONS
SECURITY LTD.

35/F Central Plaza
18 Harbour Road
Wan Chai
Hong Kong
+852 2593 1182
info.hk@ssh.com

Let's get to know each other

Want to find out more about how we safeguard mission-critical data in transit, in use, and at rest for leading organizations around the world? We'd love to hear from you.

Request a Demo