Department of Veterans Affairs

Zero Trust First

Cybersecurity Strategy

September 2022

VA | U.S. Department of Veterans Affairs
Office of Information and Technology

Table of Contents

Overview

Over 19.5 million Veterans, their families, and their caregivers depend on Department of Veterans Affairs (VA) services for access to healthcare, benefits, and memorial services. Veterans not only expect but deserve VA services to be reliable, secure, and private. VA's Digital Transformation efforts have elevated the quality of Veteran services by introducing new technologies throughout the organization.

However, VA's Digital Transformation also introduces new cybersecurity challenges. Traditional cybersecurity strategies assume that a secure perimeter and trusted users are sufficient to defend an organization's IT assets. This is no longer good enough for VA. Digital Transformation and modern healthcare technologies create new and unpredictable pathways that bad actors can use to access VA's IT systems and data. To defend the new healthcare and benefit technologies our Veterans deserve, VA must develop a bold, modern cybersecurity strategy based on a Zero Trust architecture.

VA's Zero Trust First Solution

Our vision of a Zero Trust environment is a modernized cybersecurity environment at VA that makes it impossible for bad actors to access VA resources. VA's Zero Trust First Strategy starts with a simple premise: there are so many ways that a bad actor can compromise a network that we must assume our network will be breached. If we assume this, then the next line of defense is to assure that the bad actor cannot profit from breaching our network since no vital information or resources will be available to them if they do. Traditionally, users are implicitly trusted once they log in or devices are trusted when they are first connected to the network. Zero Trust First changes the rules and requires all users, devices, and transactions to continually prove they belong in the network. If a bad actor successfully breaches VA's network boundary, they still have "zero trust" once inside, and because of this, they cannot access the resources they had hoped to steal. Zero Trust, by definition, must:

- Assume the network is always hostile
- Accept that external and internal threats are always on the network
- Know that the environment of a network locality is not enough to decide to trust a network
- Authenticate and authorize every device, user, and network flow
- Implement policies that are dynamic and calculated from as many data sources as possible

Our goal is to secure Veterans' data – wherever it might live – while allowing legitimate access to Veteran and VA data. We recognize that Zero Trust is a security methodology requiring a shift in our organizational mindset, not a set of technologies or quick solutions. Our responsibility assumes four guiding principles:

1. Every asset, user, and transaction must be explicitly verified
2. Resource access and data protection must be based on the least privileges necessary for users to perform their tasks
3. VA must continuously and pervasively monitor everything on our network
4. Breaches are inevitable and must be quickly contained, thwarted, and eliminated

Zero Trust First Goals and Objectives

Zero Trust is a powerful and modern approach to frame the broad set of investments needed to secure our organization. VA's Zero Trust First cybersecurity strategy prioritizes seven goals to prevent bad actors from accessing, stealing, disrupting, or degrading VA's IT resources.

Goal 1

Enforce strong identity verification

The organization must be able to verify the person asking for access to corporate resources are, in fact, who they say they are, rather than an impersonation of someone who should have rights. VA will implement ongoing authentication of trusted users and continuously monitor and validate a user's trustworthiness to govern their access and privileges.

OBJECTIVES

- Enforce strong multifactor authentication for all end users
- Deliver internet-facing applications with strong authentication hardened against phishing attacks
- Explicitly authenticate and authorize all subjects, assets, and workflows across the enterprise
- Implement role-based or attribute-based access to all resources and data
- Implement a single user identity for authentication that enables a unified end user experience

Goal 2

Ensure all connecting devices are healthy

End users most often access VA information on computing devices such as PCs and smartphones. While you may have verified that the person is in fact the person you think it is via strong identity verification, they could be accessing VA resources on a device compromised by malware that will use the person's access to launch an attack. To guard against this, in addition to verifying the person's identity, we must also confirm that the device is healthy.

OBJECTIVES

- Enforce a consistent, secure configuration standard for all devices and systems connecting to VA's network or providing third-party services
- Enable continuous monitoring and scanning of all devices for good cyber hygiene
- Automate asset inventories and provide integrated health checks for all devices

Goal 3

Use rich telemetry and advanced algorithms to detect attacks and isolate affected systems

As attacks become more sophisticated and the attack surface becomes larger, it's vital to develop monitoring and alerting that rapidly identifies new attack methods. Once an attack has been identified, the impacted resources must be isolated to restrict further damage, and the resource must be remediated to save vital information and return the resource to productive use.

OBJECTIVES

- Enable a "monitor everything" approach using a blend of logging, advanced analytics, and automation to reduce uncertainty about our environment and identify significant events
- Strictly control access to VA resources from "non-human" end points (e.g., machine-to-machine communication)
- Ensure comprehensive deployment of analytics to drive threat detection and response capabilities

Goal 4

Enforce least privileged access

Once an attacker has found a way in, we must ensure that they cannot access vital information. One important way to do this is by limiting all users' information access to only those applications and data they need to accomplish their role in the organization.

OBJECTIVES

- Operating with administrator privileges on end user computing devices are normally prohibited so that unsafe software cannot be installed
- Consistently implement role-based or attribute-based access control management for all VA resources
- Strict policies on elevated privilege accounts are automated and continuously enforced
- Ensure all phases of the software development lifecycle enforce least privilege access

Goal 5

Protect sensitive VA information as an additional line of defense

A breach can happen despite our best efforts. VA must apply additional layers of protection using encryption and granular access rights to Veteran information to protect against data theft, even if the computing end point is compromised.

OBJECTIVES

- All data is encrypted at rest and in transit, and data access is restricted to only authorized users
- Sharing of sensitive information is restricted and continuously monitored through automated policy enforcement
- Access to all services and applications is conditional based on device, user attributes, and identified risk score
- Integrate automated security into VA's standard development pipeline and operations processes

Goal 6

Assure the health of our IT supply chain by enforcing strict security requirements on third-party IT providers

Bad actors can use compromised third-party software, hardware, and services to launch attacks against VA. Also, third-party service providers can inadvertently create new avenues for attacks through shadow IT. Verifying the cybersecurity hygiene of our supply chain and having visibility across the entire lifecycle of products at VA helps mitigate risks to VA systems and Veteran data.

OBJECTIVES

- Proactively monitor all third-party IT solution providers, including desktop, cloud services, and outsourced software developers to ensure alignment with VA's Zero Trust First Strategy
- Accelerate remediation or removal of third-party IT solutions that do not meet the standards of VA's Zero Trust First Strategy
- Regularly ensure that VA's IT acquisition processes are informed by and synchronized with Zero Trust First policies and requirements to secure the supply chain further

Goal 7

Assume and plan for VA network breaches

People are our best defense, and we must adopt a culture that continually trains and prepares VA employees to contain, recover, and protect suspicious activity. Ransomware and spear-phishing remain primary tactics used by bad actors to gain unauthorized access and attack organizations.

OBJECTIVES

- Develop a well-trained cybersecurity workforce and user base
- Regularly assess the resilience of our IT systems and business operations in the face of security incidents
- Establish a robust Information Security Contingency Program

U.S. Department of Veterans Affairs

Office of Information and Technology

www.oit.va.gov