MFGS INC
Plan. Build. Deliver. Run.

BEST PRACTICES FOR A MODERN IDENTITY AND ACCESS MANAGEMENT PROGRAM

Why successful Zero Trust architecture requires a software solution that trusts no one!

Why Successful Zero Trust Architecture Requires a Software Solution that Trusts No One!

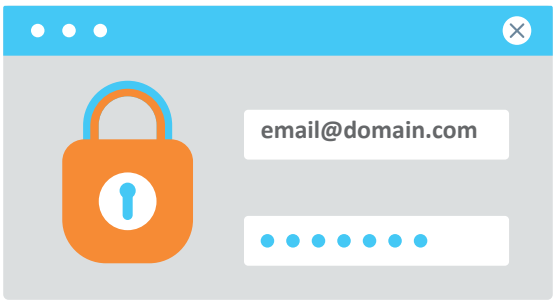
Traditional security practices and methodologies around enterprise authentication are outdated and easily bypassed. Countless enterprises have accounts with unrestricted permissions or users who obtain 'god-level' or over privileged accounts (over privileged accounts)' which are prime targets for actors with malicious intent. Once accessed, these accounts allow a bad actor to easily traverse the enterprise network with little to no detection or restriction while they corrupt systems, steal data, maintain persistence, laterally move, and more. On average, the impact of data breach to an agency or company within the United States is $4.45 million, a 15% increase over the last 3 years.[1]

$4.45 ***million / avg. cost of data breach***

15% increase over the last 3 years!

Why Traditional Methods No Longer Work

Traditional authentication methods can present several challenges to agencies that may lead to active exploitation of privileged accounts and lateral movement throughout an enterprise. Here are some common issues:



1. Vulnerabilities to Password-Based Attacks: Passwords are the most common form of authentication, but they can be susceptible to various attacks including brute-force attacks, dictionary attacks, and social engineering. Usual password policies designed to strengthen against password-based attacks are self-damaging as they limit the possibility of creativity within passwords. Users are creatures of habit when it comes to password complexity requirements as they tend to utilize easily recallable, pneumonic passwords that are typically found in most lexicons.

2. Lack of Strong Authentication Factors: Traditional authentication methods often rely solely on passwords i.e., single-factor authentication. Single-factor authentication is less secure compared to multi-factor authentication (MFA), which combines two or more authentication factors e.g., passwords, smart cards, biometrics, etc. The lack of strong authentication factors increases the risk of unauthorized access. An independent study conducted by Microsoft shows just 11% of organizations utilize multi-factor authentication and that it can prevent up to 99.9% of automated attacks and on average 80% of sophisticated cyber-attacks such as insider threats.[2]

3. Credential Sharing and Reuse: In certain situations, users may share credentials or reuse passwords across different systems due to convenience. Reports have shown that 53% of people use the

[1] https://www.ibm.com/reports/data-breach
[2] https://webinarcare.com/best-multi-factor-authentication-software/multi-factor-authentication-statistics/

the same password across multiple systems and accounts.[3] This practice can significantly undermines security, as it becomes easier for attackers to gain unauthorized access to multiple systems by compromising a single set of credentials.

of people use the same password across multiple systems and accounts.

4. Difficulty in Managing Access: Traditional authentication methods often require administrators to manage user accounts and passwords manually. This process can be time consuming, error-prone, and challenging to scale, particularly in large organizations with numerous users and systems. It can lead to inconsistencies, delays in granting or revoking access, and difficulties in maintaining a centralized view of user privileges. Given the complexity of permissions required for a specific role to function, over-privileged accounts are created to ensure operations flow smoothly and minimize downtime. Over-privileged accounts are typically created due to convenience or lack of knowledge of required permissions to effectively perform daily functions. Most account administrators generally err on the side of over-privileged accounts versus under privileged, giving way for actors to seize the opportunity to utilize these accounts for malicious intent.

5. Lack of Flexibility and Interoperability: Traditional authentication methods may not seamlessly integrate with modern technologies, cloud-based systems, or other agencies' authentication mechanisms. This lack of flexibility and interoperability can impede collaboration, hinder system integrations, and limit the ability to adopt emerging security standards and technologies. These legacy methods and security implementations leave open attack vectors as newer systems and capabilities are not integrated with the correct accesses.

The Latest Best Practices

To combat this, federal agencies, specifically the Department of Defense (DOD) (per Executive Order 14028 “Improving the Nation’s Cyber Security”) have pushed to move from traditional security practices and authentication protocols to a Zero Trust methodology. The ideology has shifted from “trust, but verify” to “never trust, always verify.”

> ***“Never trust, always verify.”***

Zero Trust is a progressive security concept and framework that challenges the dated approach of trusting entities within a network by default. In a traditional network model, once a user or device gains access to the network, they are typically granted a certain level of trust and are able to move laterally within the network with relative freedom.

The fundamental principle of Zero Trust is that trust should not be automatically granted to any user, device, or application, regardless of their location or status within the network. Instead, it advocates for verifying and validating each entity's identity and security posture continuously and dynamically. This approach works under the assumption that the network is already compromised, and it focuses on minimizing the potential damage that could result from a breach.

In a Zero Trust model, access control decisions are based on multiple factors, including user identity, device health, location, and other contextual information. Rather than relying solely on a username and password, Zero Trust utilizes multifactor authentication (MFA) and other robust identity

[3] https://www.securitymagazine.com/articles/92331-of-people-admit-they-reuse-the-same-password-for-multiple-accounts

verification methods to ensure the legitimacy of the user or device. Continuous monitoring and assessment of user behavior, network traffic, and application interactions are also integral to the Zero Trust approach.

Here are some ways Zero Trust methodologies can enhance the security of U.S. federal government agency enterprise networks:

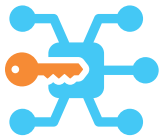
1. Segmentation: Zero Trust advocates for dividing the network into smaller, isolated segments. Each segment has its own security controls and access policies, limiting lateral movement in case of a breach. By segmenting the network, the impact of a compromise is limited, preventing unauthorized access to sensitive information and systems.

2. Identity and Access Management (IAM): Zero Trust emphasizes strong authentication and restricts access controls. It incorporates multi-factor authentication (MFA), which requires users to provide multiple credentials to verify their identity. Additionally, access is granted on a "need-to-know" basis, with granular access controls, reducing the attack surface and minimizing the risk of unauthorized access.

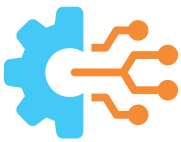
3. Continuous Monitoring: Zero Trust employs continuous monitoring to assess the security posture of the network and its components. By continuously monitoring network traffic, user behavior, and device health, potential threats can be detected in real-time, allowing for immediate response and remediation. This proactive approach enhances the overall security posture of the DOD enterprise security networks.

4. Micro-Segmentation and Application Controls: Zero Trust incorporates micro-segmentation at the application level, ensuring that only authorized users or devices can access specific applications and services. This approach limits the lateral movement of threats, as each application or service is protected by its own set of controls and policies. It also enables fine-grained access controls based on the principle of least privilege, providing utmost minimal access for a user or service to execute their role.

5. Encryption and Data Protection: Zero Trust methodologies emphasize the use of encryption and data protection techniques. By encrypting sensitive data both at rest and in transit, the data remains unintelligible and unusable to unauthorized individuals, even if a breach occurs. Data protection measures - such as data loss prevention (DLP) and data classification - are also implemented to safeguard sensitive information.



6. Behavioral Analytics and Artificial Intelligence (AI): Zero Trust leverages behavioral analytics and AI to detect anomalous behavior and potential threats. By monitoring user and device behavior, AI algorithms can identify activities that deviate from normal patterns, flagging suspicious activities and potential security breaches. This enables proactive threat hunting and helps to mitigate risks before they cause significant damage.



7. Incident Response and Remediation: Zero Trust methodologies emphasize incident response and remediation capabilities. In the event of a security incident, having well-defined incident response plans and processes ensures swift and effective threat containment, eradication, and data

recovery. Zero Trust networks are designed with resiliency in mind, allowing for quick isolation of affected segments and minimizing the impact on the overall network.

By implementing these Zero Trust methodologies, the U.S. federal government agencies, including the Department of Defense, can greatly enhance the security structure of their enterprise security networks. It enables a more granular and proactive approach to security, reducing the attack surface, limiting lateral movement, and improving incident response capabilities.

Without advanced authentication methodologies in place such as Zero Trust, the Department of Defense and other agencies could potentially face many challenges, such as: security breaches, insider threats, data loss and leakage, compromised identities, weakened auditing and compliance, lack of accountability, and reduced operational capabilities – all of which can be fatal to an agency's overall mission.

The Department of Defense places a high priority on security and is attempting to deploy robust authentication measures to protect its networks and sensitive information such as:

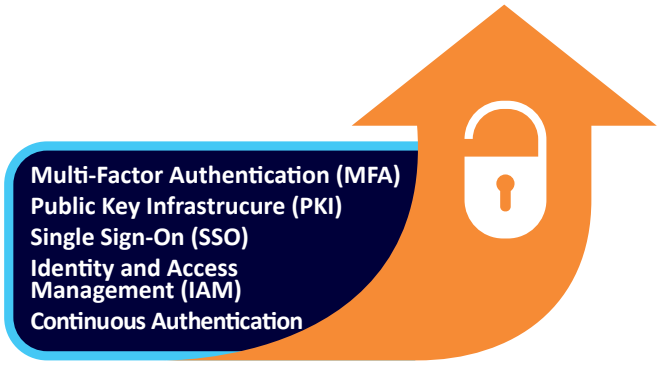
1. Multi-Factor Authentication (MFA): As previously mentioned, MFA combines two or more authentication factors to verify a user's identity. Typically, these factors include something the user knows (password), something the user has (hardware token or mobile authentication), or something the user is (biometrics like fingerprints or facial recognition). Implementing MFA significantly strengthens security by requiring additional verification beyond a weak single-factor password.

2. Public Key Infrastructure (PKI): PKI is a cryptographic system that uses public and private key pairs to authenticate users and ensure secure communication. It involves issuing digital certificates that link a user's identity to their public key. PKI can be used to authenticate users during network login processes, secure email communications, and verify the integrity of digital documents.

3. Single Sign-On (SSO): SSO allows users to log in once with a single set of credentials and gain access to multiple applications or systems without re-authentication. SSO can be integrated with other authentication mechanisms, such as MFA or PKI, to provide a streamlined and secure authentication experience while reducing the risk that comes with weak passwords or repeated login attempts.

4. Identity and Access Management (IAM): IAM solutions help manage user identities, access privileges, and permissions. They provide centralized control over user accounts, authentication mechanisms, and authorization policies. IAM systems can enforce strong password policies, monitor user activity, and ensure that appropriate access levels are assigned based on job roles and responsibilities.

5. Continuous Authentication: Rather than relying solely on a one-time authentication event, continuous authentication analyzes ongoing user behavior, device characteristics, and other contextual factors to constantly verify the user's identity. This approach helps detect anomalies and potential security threats, such as unauthorized access or account takeover attempts.



MFGS, Inc.'s Software Solution for Modern Identity and Access Management

NetIQ, available through MFGS, Inc., is an identity and access management (IAM) tool that provides an overlay to traditional authentication protocols and implementations that enhances user provisioning functionality, least permission methodologies, and implements Zero Trust policies. While NetIQ alone does not entirely satisfy the DOD Zero Trust Strategy released in October of 2022, it offers features and integrations that when combined with other MFGS, Inc. products, can fully satisfy a Zero Trust architecture.

Let's explore how NetIQ components can align with these objectives:

1. Identity Governance and Administration (IGA): NetIQ's IGA component helps establish strong identity management practices by providing centralized user provisioning, deprovisioning, and access request workflows. This helps organizations enforce least privilege access, a fundamental principle of Zero Trust, by granting access based on defined policies and ongoing need. By managing user identities effectively, IGA enhances overall security posture.

2. Single Sign-On (SSO): NetIQ's SSO capability simplifies authentication for users by enabling them to log in once and access multiple applications seamlessly. This improves user experience and reduces the need for users to remember and manage multiple credentials. While SSO itself is not a Zero Trust concept, it can interface with other NetIQ components to enforce strong authentication methods, such as multi-factor authentication (MFA), for accessing sensitive resources.

3. Risk-based Authentication (RBA): NetIQ offers RBA features that enable adaptive authentication based on risk factors such as user location, device being used, and behavior patterns. This approach aligns with the principles of Zero Trust by dynamically evaluating the risk associated with each access attempt and enforcing stronger authentication measures when necessary. For example, if a user attempts to access a critical resource from an unfamiliar location, RBA may require additional authentication factors before allowing access.

4. Multi-Factor Authentication (MFA): NetIQ supports MFA, which adds an extra layer of security beyond traditional username and password authentication. MFA can come in three ways: something they know (password), something they have (smartphone or hardware token), or something they are (biometric data). By requiring users to provide multiple authentication factors, MFA strengthens the authentication process and mitigates the risk of credential theft or unauthorized access.

5. User Behavior Analytics (UBA): NetIQ's UBA component monitors and analyzes user behavior patterns, such as login times, locations, and resource access patterns. This allows organizations to detect anomalous activities and potential security breaches in real-time. By incorporating UBA into the authentication process, organizations

can enhance their ability to identify and respond to suspicious or malicious behavior before any major damage is done, aligning with Zero Trust principles.

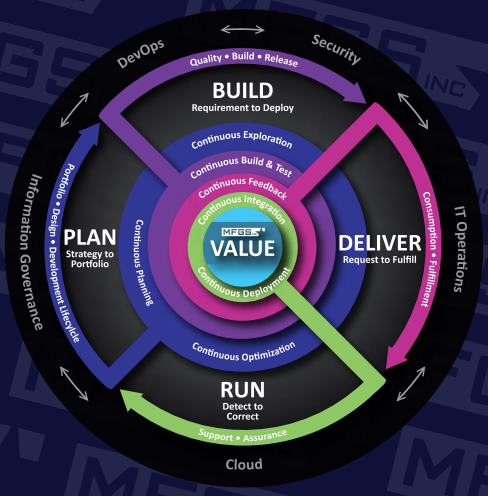
The successful implementation of NetIQ within an enterprise enables an efficient workforce reducing friction with adaptive access controls. It enables easily managing user identities for a more secure, seamless user experience. Finally, NetIQ provides a comprehensive identity and access management platform ensuring secure access and governance across platforms.

The successful implementation in a large DOD customer has been able to support nearly 800,000 users while reducing the number of global active directory admins from 800 to three thereby reducing the potential entry points by 99.6%.

NETIQ reduced the potential entry points by **99.6%!**

Reduced the number of global active directory admins from 800 to three.

To learn more about how NetIQ can transform your agency's identity and access management practices, complete the form via this QR code and a member of our team will be in touch.



About The Mission Dominance Model

MFGS, Inc.'s *Mission Dominance Model* aims to illustrate how each area of enterprise software architecture interconnects to support the software development lifecycle. The *Foundations* outer ring bolsters each of the phases of *Plan, Build, Deliver,* and *Run* in driving *Mission Dominance*.

MFGS INC
Plan. Build. Deliver. Run.

Mission Dominance in Whitepaper

NetIQ fits into the Build and Deliver phases of the MFGS, Inc. *Mission Dominance Model*. The model aims to illustrate how each area of enterprise software architecture interconnects to support an optimally efficient automated product development capability. The *Foundations* outer ring bolsters each of the phases of *Plan, Build, Deliver,* and *Run* in driving *Mission Dominance*.

Learn more:

mfgsinc.com
linkedin.com/company/mfgs-inc
@MFGSInc

