ForgeRock

WHITEPAPER

Digital Identity: The Foundation of Your Zero Trust Strategy

Table of Contents

Executive Summary

Your organization has likely invested heavily in cybersecurity. You've got a host of tools to protect your resources. Meanwhile, the world has changed. Businesses are undergoing digital transformation and making services available online. You can sign up for software as a service (SaaS) applications with just a username and password. Businesses now accommodate remote work on a massive scale, due to a global pandemic.

In this shifting environment, perimeter-based security is losing effectiveness. For example, you can't assume all access requests from within your organization's network are "trusted."

Industry experts from analysts to the U.S. Defense Information Systems Agency are working to define a security model suitable for the current environment. The leading models are **Zero Trust** and Continuous Adaptive Risk and Trust Assessment (**CARTA**).

This whitepaper covers some of the concepts around Zero Trust and CARTA, and how digital identity, managed through ForgeRock's comprehensive identity and access management (IAM) solution, can help you build a strong foundation for your organization's Zero Trust strategy.

NIST Seven Tenets of Zero Trust

1. Consider all data sources and computing services to be resources requiring protection.
2. Secure all communications regardless of network location.
3. Grant access to individual enterprise resources on a per-session basis.
4. Determine access to resources by dynamic policy – including the observable state of client identity, application/service, and the requesting asset – which may include other behavioral and environmental attributes.
5. Monitor and measure the integrity and security posture of all owned and associated assets.
6. Strictly and dynamically enforce all resource authentications and authorizations before allowing access.
7. Collect as much information as possible about the current state of assets, network infrastructure, and communications and use it to improve your security posture.[3]

What is Zero Trust?

Zero Trust is a security model that removes implied trust based on network location, focusing instead on evaluating each transaction or activity. In a Zero Trust architecture, information systems and services operate under the assumption that their networks are already compromised. Every user and every resource starts from a trust point of zero. The system grants access and authorization for resources based on the continuous evaluation of multiple signals over time.

The U.S. National Institute of Standards and Technology (NIST)[1] defines Zero Trust as practices that involve "moving defenses from static, network-based perimeters to focus on users, assets, and resources." The UK National Cyber Security Centre's Zero Trust Architecture principles are very similar to NIST.[2]

NIST's seven tenets, listed above, describe Zero Trust Architecture in a technology-agnostic way. Any technology solution can address these tenets based on their specific benefits.

What is CARTA?

Closely related to Zero Trust is Gartner's Continuous Adaptive Risk and Trust Assessment (CARTA) model. The CARTA model goes beyond verifying trust at login time, recommending continual and adaptive assessment of the end user and their activity. The two key dimensions of run-time decision making are authentication assurance and session duration. These dimensions degrade due to time, user action, or other causes. The platform must re-establish assurance of user identity by re-evaluating authentication and risk signals that are collected repeatedly. The CARTA model aims to reduce end-user friction by conducting small, unobtrusive, frequent checks.

1 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
2 https://www.ncsc.gov.uk/collection/zero-trust-architecture/introduction-to-zero-trust
3 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
4 https://www.forbes.com/sites/johnkoetsier/2020/09/26/global-online-content-consumption-doubled-in-2020/

CARTA also recommends adding friction for higher-stakes transactions. For example, if a logged-in banking customer wants to initiate a wire transfer, they are subject to transactional authorization, and the system prompts them to re-authenticate.

Why Do You Need a Zero Trust / CARTA Architecture?

The risk of man-in-the-middle attacks, credential theft, and sensitive data loss is at an all-time high: in 2020, global consumption of online content doubled,[4] and breaches caused by compromised usernames and passwords increased by 450%.[5]

In today's security environment, perimeter-based security based on IP address is no longer effective. An access request originating from the local coffee shop might be legitimate, while access seemingly from inside your organization might be an attempted breach. Before trusting a user, device, or system, you need to understand who they are, what they are doing, and whether they have permission to do it.

Zero Trust, including CARTA, is a fine-grained approach to preventing unauthorized access to data and services. When a user attempts to access a resource, the system may require more information before deciding whether to allow or deny access.

In the event of a breach, Zero Trust aims to limit the attacker's ability to move laterally in the network. This requires enforcing fine-grained access rules and making continuous authentication and authorization decisions for each access request.

The Zero Trust model is a priority for most IT services organizations. In 2021, 72% of organizations have either adopted Zero Trust, or are planning to adopt it.[6] 96% of security decision-makers have made Zero Trust their top priority to improve security and compliance and enable their organizations to detect and remediate threats easier and faster.[7] The global shift towards a hybrid workplace, where some folks work in-office and many others work remotely – has become another reason to adopt Zero Trust.

96%

of security decision-makers have made Zero Trust their top priority to improve security and compliance and enable their organizations to detect and remediate threats easier and faster.[7]

Why Legacy Security Solutions are Not Enough

Your security infrastructure probably includes things like firewalls and intrusion detection systems, network monitoring, Security Information and Event Management (SIEM), IAM and Role-based Access Control (RBAC). But in today's hyper-connected environment, legacy measures are losing effectiveness.

- Classic perimeter-based security solutions enforce policy on endpoints and payloads, assigning trust based on network location (IP address); but when anything can be remote, there is no more perimeter.
- Legacy IAM solutions cannot keep pace with today's demands to elevate both user experience and security – and many cloud IAM solutions can't fully support legacy applications. Furthermore, most IAM solutions have limited ability to integrate with identity governance solutions and incorporate RBAC intelligence into access decisions.
- Entitlement creep can become your organization's biggest vulnerability. Entitlement creep arises when user roles change: for instance, a staff software engineer might become a product manager. If managed improperly, roles and entitlements can follow their digital identities long after they are needed. A longtime employee with unnecessary entitlements is an enticing target. If an attacker targets the employee with a spear-phishing campaign and gets them to unwittingly enter their credentials into a fake website, the attacker can infiltrate the organization with the stolen credentials. If they succeed in moving laterally system to system in the network, they can

5 https://www.forgerock.com/resources/2021-consumer-identity-breach-report
6 https://www.statista.com/statistics/1228254/zero-trust-it-model-adoption/
7 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWGWha

exfiltrate valuable information, like company financials, Personally Identifiable Information (PII), and merger and acquisition (M&A) targets.

- Traditional RBAC solutions require manual, time-consuming data input and analysis to identify roles

> Entitlement creep can become your organization's biggest vulnerability.

across the organization – which can take months. In today's fluid business environments, where workforce users join, leave, or change job roles, by the time the RBAC role mining and modeling project finishes, it is already out of date. Manually-managed Role-based Access Control (RBAC) assigns each job role different levels of access to software licenses, SaaS applications, servers, and databases. Global organizations use traditional RBAC to simplify management of user identities and workforce access permissions. RBAC employs the principle of least privilege to provide privacy, security, and compliance benefits by restricting an employee's or contractor's access strictly to the resources they need to do their job. It is extremely difficult to achieve Zero Trust using manual RBAC processes and static data. Few IAM solutions can fully integrate RBAC intelligence into access decisions.

- Data-hungry apps and services like news feeds, stock feeds, and bank transactions rely on real-time streaming data. Typically, organizations that want to secure access to streaming data must install a third-party gateway and then integrate that product with their existing IAM platform.

It is extremely difficult to achieve Zero Trust using manual RBAC processes and static data.

Elements of a Zero Trust Architecture

Every cybersecurity vendor in the market today has a story to tell about Zero Trust; but no single product or solution can promise you an end-to-end Zero Trust architecture.

To implement Zero Trust, your organization might be looking at solutions to secure network infrastructure and data with next-generation firewalls and micro-segmentation, Continuous Diagnostics and Mitigation (CDM), threat intelligence, VPNs, and activity logs (see Figure 1). But you also need IAM.

Integrating IAM with Identity Governance and Administration (IGA) is also crucial for increasing your organization's security posture, by making sure your users have the level of access they need – and no more.

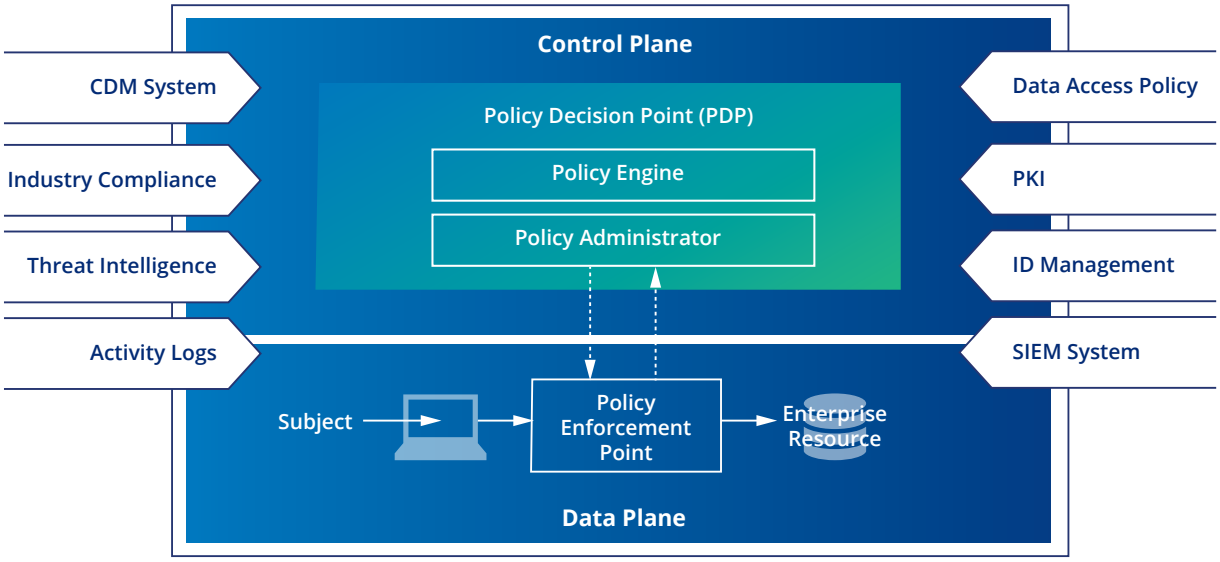


Figure 1: NIST Zero Trust Architecture

IAM and Digital Identity as Your Zero Trust Foundation

It's no secret that stolen credentials are still one of the leading causes of data breaches.[8] It makes sense that strong authentication, dynamic access management policy, authentication, and authorization are fundamental to the NIST Zero Trust model.

IAM implements fundamental features needed for Zero Trust: digital identity, session management, dynamic policy, strong authentication, and authorization. Integrating IAM with Identity Governance and Administration (IGA) is also crucial for increasing your organization's security posture, by making sure your users have the level of access they need – and no more.

8 Verizon Data Breach Investigation Report 2021

Choosing the Right IAM Solution for Your Hybrid Enterprise

Your IAM solution should provide full visibility and modern identity capabilities across legacy and modern systems. Legacy IAM solutions cannot support Zero Trust effectively. Meanwhile, organizations of all sizes and industries are already "in the cloud" or working to migrate at least partially to the cloud. To achieve Zero Trust, you need to support IAM during cloud migration, or to continue indefinite support for legacy applications.

The ForgeRock Identity Platform (hereafter referred to as "ForgeRock") is the industry's only comprehensive Identity Platform as a Service. ForgeRock provides the flexibility, ease, and security of an enterprise-grade identity solution, enabling you to support any identity type (consumers, workforce, things), any use case, and any environment (on premises, any cloud, as-a-service, hybrid IT).

ForgeRock enables continuous runtime prediction, prevention, detection, and response that helps validate user identity while providing continuous protection against fraudulent sign-ups or account hijacking, consistent with Zero Trust and CARTA.

- **Identity Cloud** enables you to comply with the EU's General Data Protection Regulation (GDPR) or other regulatory data residency requirements with ForgeRock's patented full tenant isolation. Your organization's data is never commingled with that of other organizations. Identities from one environment are never valid in another; accidental or malicious access in another customer environment can never impact yours.
- **ForgeRock Access Management** provides single sign-on (SSO) tokens, OAuth 2.0 and Open ID Connect providers, and an authorization engine. These features provide intelligence to access decisions, and store information about user sessions to send to downstream risk engines, threat analytics, and behavioral analytics applications for further analysis.
- **ForgeRock Intelligent Access** is a low-code/no-code dynamic orchestration and intelligence engine that pre-identifies and strongly authenticates users. It continuously validates user identity even after they authenticate, consistent with Zero Trust and CARTA.
- **ForgeRock Identity Management** fully automates the entire identity lifecycle management process so you can quickly create and provision new user accounts, seamlessly manage user access to target applications and resources, and quickly deprovision user accounts.
- **ForgeRock Identity Governance and Administration** (IGA) is a modern, artificial intelligence (AI)-driven identity lifecycle management solution that simplifies access requests, approvals, certifications, and role-mining/modeling processes. By leveraging an AI/machine learning (ML) analytics engine, the ForgeRock Identity Governance solution can identify and apply appropriate user access, automate high-confidence access approvals, recommend certification for low risk accounts, and automate the removal of unnecessary roles.
- **ForgeRock Autonomous Identity** is an AI-powered solution that ingests rich data representing all aspects of identity across the enterprise. Autonomous Identity proactively identifies access risks – rather than manually correlating masses of identity data to make access decisions. It uses machine learning techniques to dynamically identify roles and entitlements to be approved or revoked.
- **ForgeRock Identity Gateway** is an intelligent, identity-aware reverse proxy that can be deployed anywhere. It acts as the policy enforcement point (PEP) that communicates with ForgeRock Access Management for policy decisions.
- **Modernization Accelerators** are open-source accelerators that help your organization maintain any needed legacy systems while migrating to modern IAM technologies.
- **Software development kits (SDKs)**, agents, REST application programming interfaces (APIs), and an OAuth 2.0 resource server support policy enforcement at the edge, including Zero Trust to iOS and Android mobile endpoints.

The Path to Zero Trust

Zero Trust is not a "one and done" project. It is a gradual process that starts with setting up the program, getting budgetary approval, and identifying the top priorities for protection. Begin by collecting information about your environment. What are the resources in your organization? Do you depend on a mixture of legacy and modern applications and systems? Where are they located? Who has access to what systems, and is the access level appropriate for what they need to do?

Hybrid IT environments – with a mixture of on-premises and cloud resources – are common in larger enterprises. If your organization is shifting more and more resources to the cloud, how connected and protected are your legacy systems? If you need to maintain legacy systems,

how can you secure them from data breaches using modern technologies?

Your Zero Trust journey requires you to define risk levels and levels of assurance, and classify assets and access. You also need to apply a standard taxonomy across the organization for managing assets, identities, roles, and policies. If you're implementing a cloud architecture, you need to plan to protect services, APIs, and everything else consumed "-as-a-Service."

Forrester[9] recommends a staged approach to Zero Trust: after initial planning, you should protect users from identity and credential theft with multi-factor authentication (MFA) and risk-based authorization. Next, protect devices, workloads, and networks.

The journey continues with expanding your Zero Trust model across more resources, continuously improving your implementation and refining your methods. As your Zero Trust practice advances, consider incorporating automation, orchestration, and advanced detection techniques like AI and ML to make your processes more efficient.

Supporting Zero Trust with ForgeRock

When choosing an IAM solution, look for one that is flexible enough to support as many as possible of the seven NIST Zero Trust tenets in your organization's environment.

ForgeRock can help you use IAM as your foundation for implementing the NIST tenets of Zero Trust.

Protect All Resources

> **Tenet One**
> Consider all data sources and computing services to be resources requiring protection.

You can't protect resources you don't know about. Your IAM system should be able to identify and assign a digital identity to any:

- Human identity (person) – e.g. employee, business partner, contractor, consumer
- Non-human identity – Internet of things (IoT) device, service, or microservice

Your IAM should help you establish relationships between human and device identities. Every application or service – whether legacy or modern – should be protected through secure registration, authentication, and authorization policies.

If your current IAM solution fails to meet these criteria, some of your resources will remain unprotected, making the achievement of Zero Trust difficult. ForgeRock can help you protect all your resources, as described in the following sections.

Secure All Communications

> **Tenet Two**
> Secure all communications regardless of network location.

Your IAM system should enable you to assign identities to all data sources and computing services – no matter the location. Your IAM solution should help you design dynamic, identity-centric policies to secure your communications. However, this can be a challenge if your organization relies on legacy applications and IAM that do not support modern identity standards.

ForgeRock Identity Gateway enables you to secure communication everywhere. Identity Gateway bridges the gap between legacy business applications and modern identity management. You can deploy Identity Gateway anywhere to enforce authentication and authorization of legacy and modern applications, APIs, and microservices.

> Your IAM solution should verify and authenticate human and non-human identities for the services they are requesting access to, for a specific purpose or period of time.

9 https://www.forrester.com/report/a-practical-guide-to-a-zero-trust-implementation/res157736?objectid=res15773

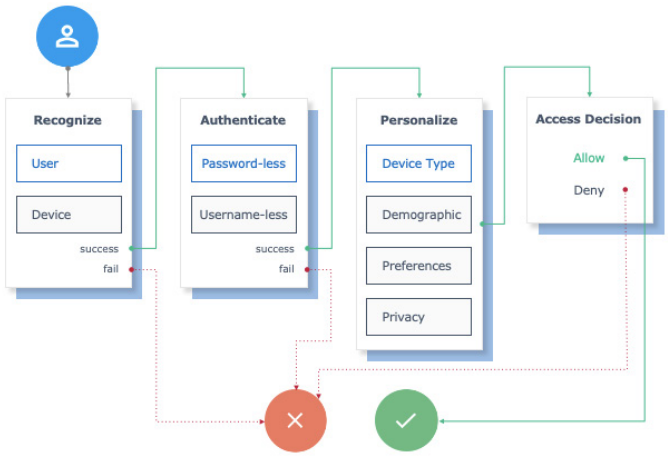


Figure 2: Designing Dynamic User Journeys with ForgeRock Intelligent Access

Grant Access on a Per-Session Basis

> **Tenet Three**
> Grant access to individual enterprise resources on a per-session basis.

Authentication protects users and your resources by verifying users are who they claim to be. Users are authenticated against a reliable identity store, typically using a combination of "Something you know, something you have, and something you are." But authentication should not be a one-time event. Your IAM solution should verify and authenticate human and non-human identities for the services they are requesting access to, for a specific purpose or period of time. It should enable you to make ongoing access decisions based on context-driven signals, and incorporate strong authentication technologies and multi-factor authentication in intelligent ways that avoid annoying your end-users.

With ForgeRock Intelligent Access, you can design authentication journeys from the simplest username and password-based authentication to complex yet transparent-to-the-user journeys. For example, you can combine registration, authentication, usernameless and passwordless authentication, and strong authentication that captures rich context based on the device and user.

Determine Access by Dynamic Policy

> **Tenet Four**
> Determine access to resources by dynamic policy – including the observable state of client identity, application/service, and the requesting asset – which may include other behavioral and environmental attributes.

You can protect your organization by understanding and validating client identity, and applying dynamic access policy to the application or service. Dynamic access can be based on criteria like behavior, time of day, device information, and deviations from "normal" conditions.

Make Intelligent and Dynamic Access Decisions

ForgeRock Intelligent Access enables you to design user journeys that can detect environmental attributes even before a user authenticates. Instead of simply trusting a successful authentication on its own, ForgeRock incorporates other attributes such as device ID, impossible travel between initial and step-up authentication attempts, and behavioral characteristics. You incorporate multiple pre-built and tested integrations with ForgeRock's Trust Network partners offering behavioral biometrics, identity proofing, and fraud detection solutions. You can assign dynamic and fine-grained authorization policies to allow, require step-up authentication, redirect to a honeypot for monitoring, throttle their traffic, or force logout for authenticated users who do not meet your organization's Zero Trust policies.

Enforce Policy at the Edge

To enforce policy at your network edge, ForgeRock includes Identity Gateway and support for Zero Trust to iOS and Android mobile endpoints. ForgeRock exposes all services and capabilities via a developer-friendly REST API. If you wish to expose the API externally, you can leverage ForgeRock Identity Gateway for more advanced protection. ForgeRock supports easy integration through standards including WS-Federation, SAML2, OAuth 2.0, OpenID Connect, and User Managed Access (UMA).

Monitor the Integrity and Security of All Assets

> **Tenet Five**
> Monitor and measure the integrity and security posture of all owned and associated assets.

This tenet recommends that you apply continuous diagnostics and mitigation (CDM) or similar systems to monitor your devices and applications, and take remedial action when needed.

Monitoring and remediation also applies to digital identities, job roles, and access privileges.

Incorporate Role-based Access Control into Zero Trust Access Decisions

Your IAM solution, working in conjunction with ForgeRock IGA, can play a huge role in maintaining or improving the security posture of your organization's assets – whether they be hardware, software, or cloud services.

This requires a clear and current picture of user roles and entitlements, something traditionally done by RBAC. Your IAM solution should be able to incorporate RBAC data from your identity governance solution to eliminate excessive, duplicate roles and entitlements that put your organization at risk of both internal and external breaches.

Automate RBAC and Least Privilege Access

AI-based RBAC forms the ideal foundation for automating and achieving a Zero Trust architecture.

Automation, artificial intelligence, and machine learning can help you identify user attributes and roles, and learn how they are used, with confidence scores for each user access. This information enables you to make access decisions with higher confidence in less time, and to automate user access for low-risk users.

ForgeRock Autonomous Identity proactively identifies access risks with AI, and uses machine learning techniques to dynamically find roles and entitlements to approve or revoke.

AI and ML reduce your risk by discovering role-based access patterns and recommending optimized role structures. These recommendations help you establish least privilege access and improve your organization's security posture. You can customize your risk criteria without having to hire a data scientist or pay for expensive professional services to do the laborious data analysis.

With Autonomous Identity, you can effectively enforce least privilege access. If a different access level is needed, Autonomous Identity can easily request, grant, or remove permissions. This AI-driven dynamic approach to RBAC successfully implements the "trust nothing, verify everything" philosophy behind Zero Trust.

Strictly Enforce All Authorizations Before Allowing Access

> **Tenet Six**
> Strictly and dynamically enforce all resource authentications and authorizations before allowing access.

ForgeRock Identity Gateway's throttling capability prevents unwanted traffic from impacting the operations of protected Web APIs and applications.

If your enterprise manages software and services in a hybrid IT environment, you need an IAM solution that can enforce authentication and authorization for all of your resources – no matter where they reside. This is a challenge if you rely on legacy business systems that are not compatible with cloud-based IAM.

Authenticate and Authorize Legacy Applications

Many legacy applications have little or no built-in capability for modern IAM functions like user registration, authentication, authorization, or federation. ForgeRock Identity Gateway supports these critical capabilities. For applications that support header-based authentication, Identity Gateway uses HTTP header injection. For applications that support federation standards, Identity Gateway uses protocol translation.

Where a legacy application cannot be modified directly, ForgeRock Identity Gateway can control access using an approach similar to a reverse proxy. Communication with the legacy application goes through Identity Gateway, which inspects the traffic and modifies it if necessary. This ensures that the user possesses proper authentication and authorization to access the resource. Identity Gateway can pass user credentials or profile data needed by the application using functions like credential replay, form-fill, header injection, and cookie injection.

Protect Against DDoS Attacks

ForgeRock Identity Gateway provides security above and beyond simple access management. Most organizations encounter situations where they must slow down traffic to improve security. For example, a distributed denial-of-service (DDoS) attack can send massive floods of messages to web servers, slowing down performance or completely overwhelming servers. Bots can set up automated actions within the application, such as downloading a large number of bank statements at once, to overwhelm servers.

ForgeRock Identity Gateway's throttling capability prevents unwanted traffic from impacting the operations of protected Web APIs and applications. Throttling limits the number of transactions allowed over a specific time period – per second, per minute, per hour, per day, per week, and so on. You can set throttling limits for each user, domain name, and IP address, or for classes of applications or users. Throttling slows down traffic when it reaches a specified limit to maintain a healthy load to the API backend, prevent DDoS attacks, and keep response times within service level agreements (SLAs).

Control Access for Microservices and Real-Time Streaming Data

Enterprises are adopting cloud-native capabilities like containers, dynamic orchestration, microservices, and serverless architectures. ForgeRock offers several options for supporting modern IAM capabilities for all communications between microservices.

Microservices communicate frequently with each other, increasing latency. ForgeRock Identity Gateway boosts performance by performing authentication close to each microservice and caching policies.

Data-hungry apps and services like news feeds, stock feeds, and bank transactions rely on real-time streaming data. Organizations that want to secure access to streaming data typically install a third-party gateway and then integrate that product with their existing IAM platform. ForgeRock Identity Gateway can control access to streaming data as easily as it secures traffic to traditional apps and APIs.

Collect as Much Actionable Information as Possible

> **Tenet Seven**
> Collect as much information as possible about the current state of assets, network infrastructure, and communications and use it to improve your security posture.

Your organization should be able to monitor, collect, and take action on the security posture of your assets, network traffic, and access requests. Consider whether your IAM solution can meet these requirements by integrating with identity governance and administration solutions.

Integrate IAM with Identity Governance and RBAC

Global organizations have leveraged traditional IGA and RBAC solutions to simplify management of user identities and workforce access permissions. While RBAC has helped reduce administrative work, maximize operational efficiency, and improve regulatory compliance, its effectiveness erodes over time due to its manual, labor-intensive approach.

Organizations that want to secure access to streaming data typically install a third-party gateway and then integrate that product with their existing IAM platform. ForgeRock Identity Gateway can control access to streaming data as easily as it secures traffic to traditional apps and APIs.

ForgeRock's AI-driven IGA is an integral part of ForgeRock's comprehensive Identity Platform. It allows you to establish policies for user access rights and continuously monitor their proper implementation from a centralized location.

Revoke Unnecessary Access with Closed Loop Remediation

During periodic access certification, your identity governance solution will likely identify users whose access privileges and permissions exceed what they need. Zero Trust principles require that you properly review and revoke these excess privileges immediately. This process is called closed loop remediation.

An IGA solution reaches out to the target system or end point (such as Office 365, SAP, Slack, Top Secret) via a direct connector to remove the specific accounts, roles, permissions, and privileges. When permissions and privileges are properly removed, the IGA reports this to the IGA administrator. This is an automated process. It can be difficult to demonstrate compliance with this requirement to auditors.

ForgeRock's IGA solution lets you schedule periodic access reviews that integrate with workflow engines to enact closed-loop remediation. You can strengthen your security posture and drive regulatory compliance, automatically.

Make Digital Identity Your Foundation for Zero Trust

In today's always-on, always Internet-connected world, cyber threats can come from anywhere, and unauthorized access is the number one attack vector. It is no longer enough to grant trust based on a device, network, browser, user, or token. This outdated approach increases the threat of a man-in-the-middle attack, token theft, or token misuse.

IAM provides many of the tools essential to achieving the goals of security, privacy, experience, and compliance defined by a Zero Trust or CARTA architecture. Integrating IAM with AI-powered identity governance can help you identify and fix access blind spots and provide wider and deeper insight into risks in the user access landscape.

As the only digital identity leader with more than 3 billion identities under management, ForgeRock helps people safely and simply access the connected world at scale. ForgeRock enables exceptional digital experiences with Zero Trust/CARTA-aligned security, privacy, and compliance, AI-driven identity governance, comprehensive functionality, and simple deployments.

About ForgeRock

ForgeRock, the leader in digital identity, delivers modern and comprehensive Identity and Access Management solutions for consumers, employees and things to simply and safely access the connected world. Using ForgeRock, more than a thousand global customer organizations orchestrate, manage, and secure the complete lifecycle of identities from dynamic access controls, governance, APIs, and storing authoritative data – consumable in any cloud or hybrid environment. The company is privately held, and headquartered in San Francisco, California, with offices around the world. For more information and free downloads, visit www.forgerock.com or follow ForgeRock on social media.

Follow Us

ForgeRock

Peraton

WHITEPAPER

ENHANCED CYBERSECURITY VIA ZERO TRUST

EXECUTIVE SUMMARY

Organizational leaders are fast discovering how digital transformation benefits their mission critical programs and business processes. Multitasking remote workers are increasingly teaming virtually, any time and from anywhere, confidently and safely leveraging efficient cloud platforms to achieve timely results. Data scientists now apply AI/ML capabilities to swiftly discern actionable trends from oceans of collected data. Technologists exploit autonomous processes to streamline previously labor-intensive tasks. Watch standers respond decisively to enterprise threats revealed in real-time on single pane displays for hyper situational awareness. These and many other welcome transformations help enable modern work environments. However, they demand high performance from the organization's cyber and information technology professionals.

Chronic shortages of expert staff, burdensome upkeep of unsafe legacy infrastructure, and overtasked program managers with little bandwidth or resources to apply to new initiatives challenge even the most dedicated teams. Additionally, the need for reliability, resilience, and security has never been greater. The audacity of sophisticated cyber actors spying on sensitive programs, disrupting business processes, or extorting fees for ransomed data increases with every successful compromise. Still, the future is bright as we are in this together. Information sharing and cooperation among partners—federal, state, local and tribal governments, the private sector, academia, as well as our international allies—will be key to our mutual success in navigating the digital road ahead.

On May 12, 2021 the Biden administration issued a new executive order (EO)[1] to enhance our nation's cybersecurity posture which notably includes coordinating partnerships with the private sector to support the EO execution. The EO represents a significant number of activities that will require directed actions and significant effort significant effort among all U.S. federal government agencies and government contractors/subcontractors.

The new EO requirements make cybersecurity and securely managing government data more important than ever before. Peraton welcomes this opportunity to further our trusted partnership with the Federal Civilian Executive Branch (FCEB) agencies, Department of Defense (DOD), and the Intelligence Community (IC) in support of their mission accomplishment. This whitepaper highlights Peraton's capabilities that can directly enhance implementation of the EO.

[1] Executive Order on Improving the Nation's Cybersecurity (May 12, 2021) Presidential Actions

THE WORLD WE LIVE IN

During 2020, information technology (IT) software and services providers suffered a significant increase in supply chain cyberattacks. The year ended with the December 2020 announcement by SolarWinds of a sophisticated nation-state sponsored cyberattack on three of their Orion network monitoring software upgrade releases indicating that the trend would continue into 2021. Numerous U.S. federal government agencies and thousands of government contractors who implemented the SolarWinds software as a part of their network monitoring are reporting varying degrees of data compromise and exfiltration.

The rampant cybersecurity concerns touched off by the SolarWinds cyberattack continue to flourish across many U.S. federal government agencies (defense, intelligence, civilian and health), government contractors and commercial companies worldwide. As a result, many organizations are taking additional measures to verify, authenticate and test software patches and upgrades from supply chain partners to ensure they are the original software version and do not contain Trojan horse malware.

CYBERSECURITY REPORTED INCIDENTS BY U.S. FEDERAL AGENCIES

In FY 2019, there were 28,591 cybersecurity incidents reported by the U.S. federal executive branch civilian agencies to the U.S. Department of Homeland Security (DHS). Further, in the past several years GAO made over 3,000 recommendations to U.S. federal agencies and as of September 2020, about 600 of those have not been fully implemented. GAO designated 75 of the 600 outstanding recommendations as cybersecurity priority recommendations, meaning that GAO believes these recommendations warrant priority attention from the leaders of the U.S. departments and agencies. Until these 75 priority recommendations are fully implemented, U.S. federal IT systems and data will be increasingly susceptible to cyber threats, cyberattacks and costly data breaches. One of the top cybersecurity recommendations made by GAO and numerous leading IT consulting firms to enhance U.S. federal government cybersecurity is to implement zero trust (ZT) concepts and a zero trust architecture (ZTA).

WHAT IS ZERO TRUST?

Said simply, ZT is a cybersecurity concept based on the premise to "never trust and always verify", as it relates to identity, credentials and data access management—in other words, workplace, workforce, workflow and the associated data access requirements.

Additional definitions

To support a strong understanding of the concept, the following bullets offer some additional explanation:

- The National Institute of Standards and Technology (NIST) Special Procedure (SP) 800-207 says: "Zero-Trust (ZT) is the term for an evolving set of cybersecurity paradigms that move network defenses from static, network-based perimeters to focus on users, assets, and resources."
- Forrester Research states: "A Zero Trust Architecture (ZTA) abolishes the idea of a trusted network inside a defined corporate perimeter. ZT mandates that enterprises create micro-perimeters of control around their sensitive data assets to gain visibility into how they use data across their information ecosystem to win, serve, and retain customers."
- Gartner Group says: "Zero Trust network access replaces traditional technologies, which require organizations to extend excessive trust to employees and partners to contract and collaborate."

Zero trust concepts

NIST Special Procedure (SP) 800-207 provides extensive guidance on ZT concepts and the design and implementation of a ZTA. The ZT concepts include:

- Focus the data architecture on restricting access to data and resources to only those individuals with a valid need to access data and then grant the minimum privileges (e.g., read, write, delete) needed to perform the mission.
- Implement data segmentation or data compartmentalization combined with micro-perimeters, which prevents unauthorized access to data, resources and services coupled with making the access control enforcement as detailed as possible.
- Ensure authorized and approved subjects (combination of users, applications and devices) can access the data to the exclusion of all other subjects (cyberattackers).

Zero trust design tenets

NIST Special Procedure (SP) 800-207 provides the following seven ZT design tenets for policies, plans, procedures and architecture including:

- **All resources are in-scope:** all data sources and computing services are considered resources
- **Secure all communications:** all communications are secured regardless of network location
- **Access is on a per session basis:** access to individual enterprise resources are granted on a per session basis
- **Access is determined dynamically:** access to resources is determined by dynamic policy, including the observable state of client identity, application and the requesting asset—and may include other behavioral attributes
- **Secure and monitor assets:** the enterprise ensures that all owned and associated devices are in the most secure state possible and monitors assets to ensure they remain in the most secure state possible
- **Strictly enforce dynamic authentication and authorization:** all resource authentication and authorization are dynamic and strictly enforced before access is allowed
- **Gather and use as much information as possible:** the enterprise collects as much information as possible about the current state of network infrastructure and communications and uses it to improve its security posture

NIST SP 800-207: Zero trust architecture

In addition to describing the seven basic design tenets guiding the ZT principles, NIST SP-800-207 defines the logical components that make up the architecture, reviews typical ZTA deployment scenarios and provides guidance for transitioning to a ZTA. A core component of ZTA, the policy enforcement point (PEP) tightly controls access to enterprise resources based on business rules maintained and executed in a policy decision point (PDP)—basically establishing a gated access between the user or application and the enterprise system, data or application being requested that requires authentication and authorization in real-time in order to gain access. Separating policy decision and enforcement functions allows organizations to implement access controls close to enterprise resources, while preserving centralized administration and management. The approach restricts lateral movement and reduces security vulnerabilities by shrinking implications.

Additionally, a ZTA is ideal for cloud-centric, geographically distributed organizations that leverage public compute, storage and networking infrastructure. A ZTA can help government agencies adopt cloud applications and services in accordance with the U.S. Cloud Smart initiative as well as help agencies overcome security limitations associated with traditional Cybersecurity Infrastructure Services Agency (CISA) Trusted Internet Connections (TIC) architectures that rely on perimeter-based defenses.

The NIST SP 800-207 provides several potential use cases for government organizations including:

- Distributed enterprises with remote offices and teleworkers
- Multicloud implementations
- Enterprises extending services to contractor workers or visitors
- Enterprises sharing resources with outside organizations for joint R&D programs or other collaboration activities

Zero trust technologies and tools

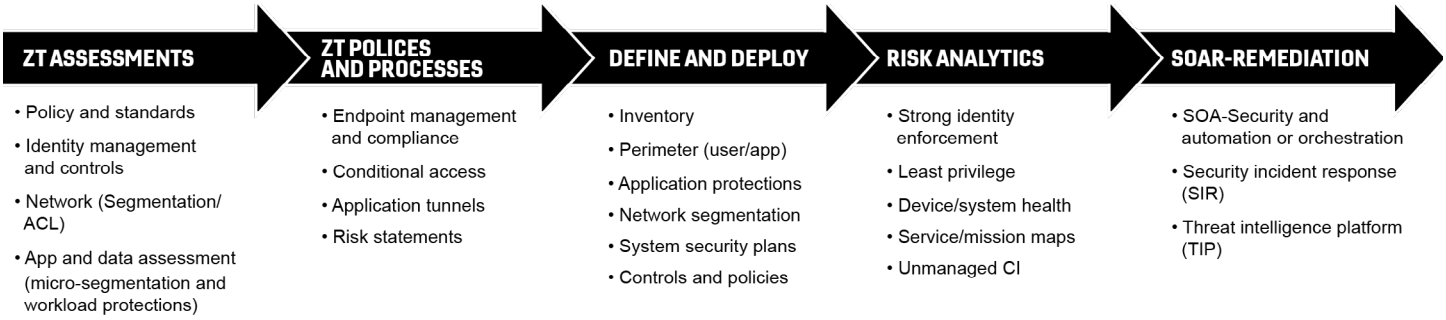
The concept of ZT has become extremely popular in the world of IT and cybersecurity. As a result of the hype, many software developers and software re-sellers often portray their respective products to be the single-point ZT solution for cyber defense. Unfortunately, no single software product can truly serve as a total solution to this complex, multifaceted cybersecurity challenge. Establishing a true ZT enterprise solution requires the system integration of numerous software technologies including:

- Identity verification (IV)
- Access control (AC) and access management (AM)
- Data architecture and data segmentation (DS)
- Micro-perimeters/firewalls
- Cyber threat intelligence (CTI)
- Monitoring, detection and response (MDR)
- Endpoint detection and response (EDR)/security to the edge
- Information technology service management (ITSM)
- Security information and event management (SIEM)
- Security orchestration, automation and response (SOAR)

There are thousands of software applications or tools which address one or more of the above stated technologies required to create a ZT solution—yet, no single software application or tool which addresses all of the technologies and their respective capabilities.

PERATON'S APPROACH TO DEVELOPING A ZT SOLUTION

Given that most U.S. federal, state and local governments have already invested in numerous software applications to perform some or most of the above stated IT functions, the development of a zero trust solution begins with determining how to properly assess the organization's current cybersecurity state against the ZT concept tenets to create a customized ZTA with the right software applications effectively integrated into a cost-effective cyber defense solution. As stated in NIST SP 800-207, when ZT is balanced with existing cybersecurity policies and best practices including identity, credential, and access management, cyber threat intelligence, continuous monitoring and a ZTA, it can provide protection against common cyber threats and improve upon an organization's existing security posture.



COMPREHENSIVE ZT BUILD STRATEGY THAT ALIGNS WITH ENTERPRISE AND MISSION OBJECTIVES FOR DEPLOYMENT, INTEGRATION AND O&M

Peraton has developed a unique five-step process approach to help U.S. federal, state and local government agencies build a customized and integrated ZT solution:

1. **Conduct a NIST SP 800-207-based zero trust assessment:** Peraton will evaluate the agency's cybersecurity ZT-related policies, plans and procedures against NIST SP 800-207 and related U.S. federal government: NIST SP 800-63 Digital Identity Guidelines, NIST Privacy Framework, NIST Cybersecurity Risk Management Framework (RMF), DHS -Continuous Diagnostics & Mitigation (CDM) and Trusted Internet Connections (TIC) 3.0 requirements. Peraton will provide a ZT gap assessment for the agency with specific recommendations to enhance cybersecurity via ZT.
2. **Develop enterprise-wide ZT policies, plans and procedures:** Peraton will support the organization in the development, communications and implementation of customized ZT policies, plans and procedures to create a secure data environment based upon a ZTA including data segmentation, micro-perimeters, privilege access management, continuous monitoring and dynamic access analysis combined with cyber threat intelligence, incident detection and response services.
3. **Create and implement a customized ZTA:** Peraton will work with the agency to develop and implement a customized ZTA, which will protect the data, resources and assets in a cost-effective manner leveraging a privilege access management provider such as CyberArk or Symantec.
4. **Provide continuous cyber threat intelligence, cybersecurity monitoring, detection and incident response services:** Peraton will either enhance the agency's existing threat intelligence, monitoring, detection and response (MDR) capabilities to support ZT or will integrate managed security services via a leading cyber threat intelligence firm such as CrowdStrike.
5. **Conduct systems integration of the identity, credential and access management (ICAM) and security information into a software services platform:** Peraton will provide appropriate systems integration services to leverage the ZTA-related ICAM and security information into a software services platform such as ServiceNow or Trusted Agent. As requested, Peraton will integrate the appropriate security information into a customer selected security information and event management (SIEM) system such as Splunk or ArcSight. This final step provides the agency with a fully integrated and customized cybersecurity dashboard to manage, operate, and maintain a ZT security environment enterprise-wide.

Peraton's five-step approach to a ZT solution offers a comprehensive, flexible, integrated and turn-key approach that can be customized based on the specific capabilities, needs and budget of each U.S. federal, state or local government agency.

SUMMARY

The concept of zero trust is a real paradigm shift in the design of security for information systems and vital data assets. If an organization truly wants to enhance cybersecurity via zero trust, then it is important to begin with a complete assessment of their current information security policies, plans and procedures. Then, follow the NIST SP 800-207 guidance to use the zero trust design tenets to create a customized zero trust architecture for improved cyber defense.

It is also essential that the new zero trust architecture, designed to protect critical data assets, be fully integrated with the following software systems and capabilities:

- Identity, credential and access management (ICAM)
- Monitoring, detection and response (MDR)
- Cyber threat intelligence (CTI)
- Security information and event management (SIEM)
- Security orchestration and automated response (SOAR)
- Information technology services management (ITSM) platform

Effective implementation of zero trust requires a comprehensive and systems integrated approach that ties together all of the key components of cybersecurity.

Peraton

Learn more at

PERATON.COM