appgate | RADIANT LOGIC

Appgate & Radiant Logic: Solving for Zero Trust Interoperability

Executive Summary

The Department of Defense (DoD) has many operational challenges to ensure secure user access across multiple systems and give the right user the appropriate level of access at the right time. This whitepaper discusses a comprehensive approach that includes Radiant Logic's Master User Record (MUR) for Identity Data Federation, Appgate SDP as the Zero Trust Network Access (ZTNA) solution and an innovative approach to solve for interoperability across the DoDIN, called the Master Zero Trust Record (MZTR) capability.

Appgate and Radiant Logic recognize the DoD's requirement for a robust Identity, Credential and Access Management (ICAM) capability, the need for managing identity data effectively across the organization and the crucial role of ZTNA in ensuring the security of the DoD's information systems. Our ICAM solution and accompanying strategy provides a consistent, unified, and common operating picture for identity data — the MUR, across the organization.

Recognizing the challenges of interoperability, cost and complexity in implementing ICAM and ZTNA across the DoD, we developed this unique MZTR capability. By acting as a universal translator for ZTNA policy definitions, MZTR allows for seamless sharing of resources across branches, eliminating the need for multiple ZTNA agents on user devices and reducing the costs associated with additional software licenses. The MZTR's integration with the existing MUR platform enhances efficiency and control, providing a single, consistent view of both identity and access data across the DoD.

Our solution greatly enhances operational efficiency and mission effectiveness. By enabling seamless sharing of resources and improving interoperability, MZTR ensures that each branch and coalition or mission partner can operate efficiently without silos. This facilitates greater collaboration and coordination, ultimately supporting the overall mission of the DoD. Our approach also future-proofs and safeguards the DoD's investment for subsequent developments in ICAM and ZTNA solutions.

This approach doesn't just solve the current challenges but also sets the stage for a flexible and adaptable future, in alignment with the evolving needs and mission of the DoD.

Alignment with DoD Mission

Implementing a Master User Record (MUR) within an ICAM solution and ZTNA strategy aligns with the DoD's mission in several key areas:

- **Mission Assurance:** By preventing unauthorized access and reducing the likelihood of successful cyber-attacks, this strategy ensures continuity of operations and mission success. It also enables rapid, secure access to critical systems and information when needed, which is crucial during military operations.
- **Efficiency and Cost Savings:** Streamlining identity and access management processes can free up resources and enhance operational efficiency. Over time, these improvements could lead to significant cost savings, enabling the DoD to allocate more resources to its core mission of national defense.
- **Alignment with Coalition Partners and Mission Partners:** Coalition and mission partners often need to share resources and information to achieve common goals. The MUR/ICAM/ZTNA strategy facilitates this secure collaboration.
- **Security Enhancement:** The DoD operates in a high-stakes, often hostile, cybersecurity environment. The MUR/ICAM/ZTNA strategy can significantly improve the security posture by offering robust identity verification, minimizing over-privileged access and implementing real-time, context-aware access decisions.
- **Trust and Security:** By employing a ZTNA approach, the DoD can ensure secure access for its partners. This approach provides confidence that access to shared resources is strictly controlled and monitored, reducing the risk of leaks or breaches.
- **Scalability:** ICAM systems with MUR can manage identities and access rights at scale, allowing for the efficient onboarding and offboarding of users. This is crucial when working with a large number of partners or during joint operations involving many participants.

Why Radiant Logic?

Radiant Logic Introduction

Radiant Logic provides the Identity Data Fabric that forms the foundation for a Zero Trust Architecture. The DoD Digital Modernization Strategy calls for "…multi-attribute-based confidence levels that enable authentication and authorization policies under the concept of least-privileged access." Each ZTA policy enforcement and decision point (PEP, PDP) requires a rich set of attributes on which to authorize access for a person or Non-person Entity (NPE) to a resource. These attributes must be accurate, current, robust, easily consumable and available at scale and under Tactical Air Control/Data Distribution and Integration Lab (TAC/DDIL) conditions. By implementing least-privileged access in a ZTA, the granularity of access and control rests on the breadth and depth of the identity attribute data.

RadiantOne Identity Data Platform is currently deployed across several branches of the DoD and many Federal Agencies to address the need for a highly available and unified Master User Record. The MUR is a composite of disparate sources of truth of identity data spanning multiple systems, applications and sources of record. The ability of RadiantOne to consume identity data in multiple formats, structures, schemas and protocols enables the aggregation and correlation of identities and attributes from AD, CSP, directories, databases, flat files, applications and other ICAM and ZTA components.

Using a standards-based platform, agnostic schema and data structure, RadiantOne supports not only person identity but NPE's spanning service accounts, applications, bots, devices and IOT. These sources can span coalition partners, contractors and agencies while still keeping confidential data segregated and protected. In addition, the types of attributes and source extends beyond traditional repositories like Human Resources and Active Directory, with the ability to aggregate data from Training Platforms, Clearance Systems, multiple Risk Engines, SIEM systems, Application monitoring solutions and others information systems that enhance the policy enforcement depth and flexibility.

Once identity data across these objects is correlated and disambiguated, RadiantOne can present the data in multiple, simultaneously-available Views. Each View is tailored to the requirements of the application, policy engine or end point that is consuming the data. These Views can be filtered by subset of users in theater, a narrow set of attributes, a specific structure, and data label and schema in the protocol of preference from LDAP, to REST, SCIM2, SOAP and SQL.

RADIANT LOGIC CORE CAPABILITIES

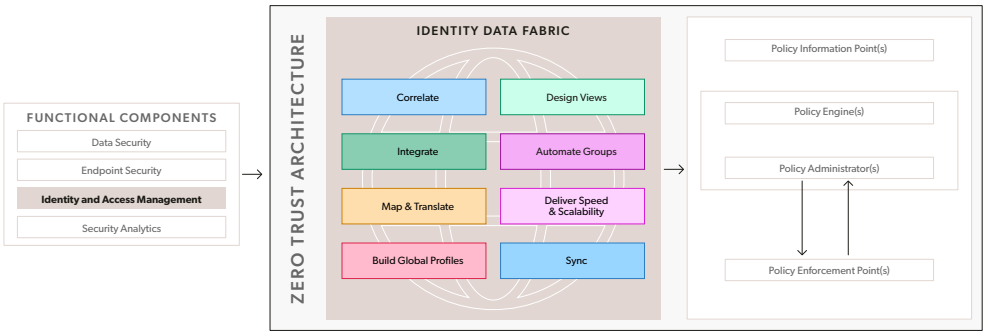
The RadiantOne Identity Data Platform enables an identity-first approach to security decisions. Our core capabilities simplify identity data management, enabling agencies to fully leverage the value of their identity data to implement Zero Trust Architecture.

INTEGRATION
Generate unlimited and flexible virtual views of integrated identity data from across a distributed environment, delivered at speed in the format required.

DIRECTORY STORAGE
Deliver high-performance, scalable, resilient, elastic identity data storage.

SYNCHRONIZATION
Propagate and synchronize identity data bi-directionally across legacy and cloud systems in near-real time.

RadiantOne resides in the middle of the Authentication and Authorization stream, between sources of user data and access management solutions (PDP, PEP) including Appgate SDP, as illustrated in Figure 1. The RadiantOne platform is optimized to scale to hundreds of millions of objects (users and NPEs) with hundreds of thousands of queries per second. The key to a ZTA is delivering the enhanced security of just-in-time authorization based on rich attributes without introducing latency. The combination of RadiantOne and Appgate SDP meets this requirement.



Radiant Logic builds the Master User Record (MUR) to fuel Zero Trust decisions. (Figure 1.)

Why Appgate?

Appgate SDP Introduction

Appgate is a comprehensive universal ZTNA solution that enables the DoD to rapidly adapt how warfighters access their protected resources and applications to execute the mission. It ensures the right user gets access to the right data, under the right conditions, while continuously re-evaluating and monitoring every session. Appgate combines device telemetry and identity attributes (ICAM: human and non-human entities) with a multitude of metrics to include risk score, location, authentication type, geographic, etc. into our Data-Centric policy engine for adaptive risk-based access control. Appgate SDP is built upon the principles of Zero Trust (ZT) with direct alignment to multiple DoD frameworks to include the DoD ZT Reference Architecture and DoD Cloud Native Access Point (CNAP).

Appgate SDP Capabilities

Appgate SDP ZTNA provides robust protections to connect users and systems to mission systems (CONOS, OCONUS and forward deployed assets) with a low probability of interception and detection. It is agnostic to the underlying infrastructure and can be automatically deployed to user machines, mobile devices, servers, containers and non-traditional IT (IoT/OT/SCADA/Weapons Platforms). Appgate SDP also applies condition-based access policies that are continually monitored and re-evaluated throughout each session.

Traditional network security approaches are failing to adequately secure the DoD enterprise. Trust is presumed to allow the user to "connect first, athenticate second," and network access is typically binary in nature (access is granted to everything or nothing). The DoDIN must defend against open listening ports exposed to adversarial reconnaissance, denial of service, unauthorized users consuming unauthorized services, inherited over-entitlement and a broad attack surface.

Appgate SDP employs principles of Zero Trust by taking an Identity, Device and Data-Centric approach to security. Users, devices and mission systems must be "pre-authorized" and "pre-authenticated" before they are allowed to connect. Authorized users and systems must meet access criteria and the appropriate conditions before access is granted. These criteria are continuously re-evaluated and monitored during all sessions. See Figure 2.

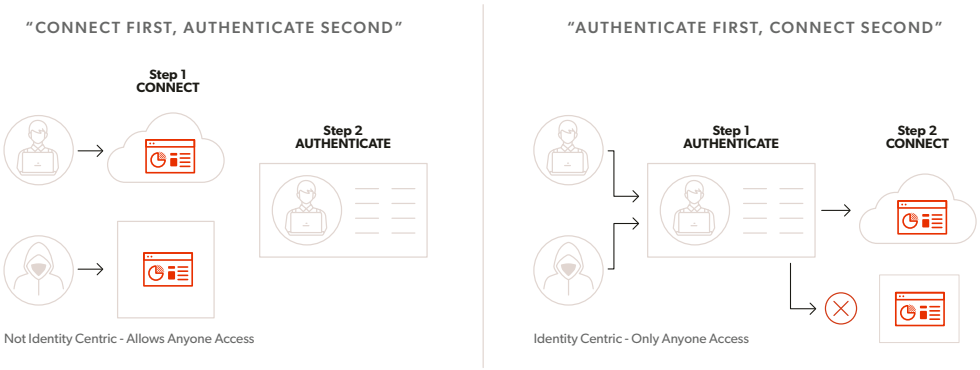
APPGATE CORE CAPABILITIES

Enable a Data Centric approach for resource authorization; consuming meta-data tags/labels for policy alignment.

Unify Policy across the operating environment. A distributed and elastic Policy Enforcement & Decision Points that leverages ICAM attributes, device posture telemetry for Common Client Health and C2C, meta-data tags/labels and additional context derived from other security or mission tools — continuously.

Cloak the Enterprise Edge (making it undiscoverable to the adversary) to reduce the overall attack surface.

Mitigate multiple vulnerabilities to include Compromised Credentials & Access Tokens, Imposter Devices and Man-in-the-Middle attacks using SPA (Single Packet Authorization) and mutual TLS.



(Figure 2.)

To make the DoD's enterprise edge undiscoverable, Appgate SDP uses Single Packet Authorization (SPA) technology, a sophisticated version of port knocking, to enforce the "authenticate-first, connect second" approach. SPA cloaks infrastructure so that it is invisible to port scans and network reconnaissance. It ensures that only authorized users can connect to network resources. Appgate SDP's use of SPA and FIPS certified mutual **TLS 1.3** have been proven to mitigate man-in-the-middle, denial of service and stolen credentials/access tokens.

Single Packet Authorization in combination with mutual TLS is specifically called out in the DoD's CNAP Reference Design.

- https://dodcio.defense.gov/Portals/0/Documents/Library/CNAP_RefDesign_v1.0.pdf (Page 13)

Why combine Radiant Logic and Appgate?

Radiant Logic and Appgate SDP provide a well-integrated solution that can improve an organization's security posture, reduce risk levels, enhance cyber readiness and provide overall value in terms of improved operational efficiency and cost savings. Radiant Logic is foundational to providing the rich set of identity data aggregated across multiple disparate sources of truth. These sources span traditional identity stores such as ADFS and extended sources including training platforms, risk engines and clearance systems. By providing a highly performant and available rich source of attributes and groups to Appgate SDP and updating changes in near real-time, the policies governing access across the gateways can be applied to meet the requirements of multiple scenarios and environments.

Radiant Logic provides a unified and consistent identity profile (Master User Record, MUR) by consolidating multiple identity data sources. It can also track and manage an individual's or a device's access rights and attributes across various systems, platforms and applications. When this is coupled with a ZTA strategy, which assumes no inherent trust for any user or device, regardless of whether they are inside or outside the network perimeter, it results in a robust defense mechanism. With ZTA, each access request is validated, authenticated and encrypted, and these decisions are made in real-time based on the MUR. This dual-level security mechanism significantly improves the organization's security posture.

The MUR can be used to create granular access policies which can be enforced through a ZTA framework built on Zero Trust Network Access, validating the user/device, their access rights, and the context of access before granting access to any resources. This helps to reduce the risk of unauthorized access, insider threats and data breaches, as the access is granted on a need-to-know basis and can be immediately revoked when no longer required. By eliminating over-privileged access, risk levels are significantly reduced.

Our approach enhances cyber readiness, allowing for real-time tracking and monitoring of user/device behavior. Unusual patterns or activities can be identified and acted upon swiftly, helping in early threat detection and mitigation. MURs can also store and process historical access data, providing valuable insights for proactive threat hunting and enhancing cyber readiness. Further, the transparency provided by this solution empowers agencies to adhere to regulatory compliance, proactively address audit concerns and expose comprehensive root cause analysis.

APPGATE CORE CAPABILITIES cont.

DevSecOps Enablement – Directly Integrates into CI/CD pipelines enabling GitOps. Security policy operation and management is orchestrated with Rest APIs and K8 Operators that can be maintained in version-controlled code repositories.

Robust security policy automation (SOAR) for automated threat detection, response and recovery - ELICSAR.

Meet and exceed performance requirements at each site 10gbps and elastically scale to 100+ gpbs per site.

Interoperability Challenge

ICAM and ZTNA interoperability has been a significant challenge for the DoD, preventing it from reaching its desired Zero Trust target state. Different ZTNA solutions have different policy definitions, and translating these policies between solutions is often complex, time-consuming and error-prone. MZTR, with its universal translation capability, eliminates these challenges.

The benefits of this approach are significant. By eliminating the need for multiple ZTNA agents, we reduce system complexity and the potential for compatibility issues. By avoiding the need for additional software licenses, we reduce costs. And by providing a mechanism for seamless policy translation and sharing, we greatly enhance the flexibility and utility of the DoD's ZTNA capabilities.

As the DoD begins to deploy ICAM and Zero Trust technologies to create secure and flexible operating environments that can dynamically adapt to the evolving threat landscape: the lack of interoperability between the multitude of vendor ZT platforms is hindering the overall operational effectiveness across the services branches and mission partners:

- Current ZT solutions are siloed
- Information-sharing inhibited
- Multiple end-user software agents creates complexity for associated management infrastructure
- Warfighters have different experiences for connecting (such as loading VPN clients or authenticating differently)
- Separate policy engines require IT teams to set and manage policy in multiple places, increasing likelihood of inconsistency
- Swivel-chair troubleshooting across multiple consoles

Appgate and Radiant Logic have developed a capability to directly solve for the lack of interoperability across the DoDIN, called the Master Zero Trust Record (MZTR). This capability was made possible due to the joint investment in automation, orchestration and delivering "everything as code."

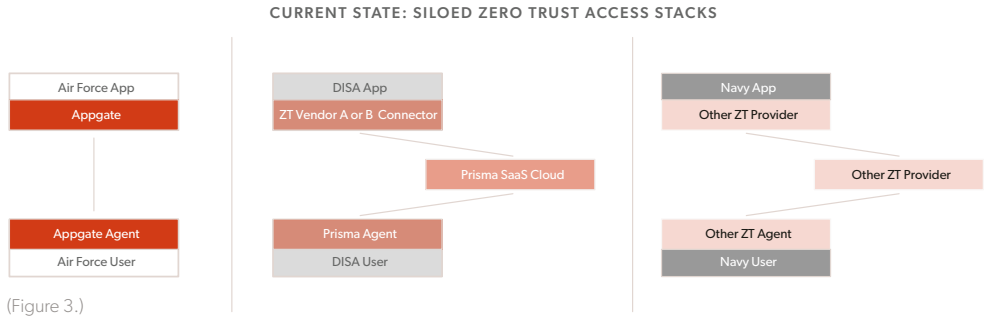
The same interoperability challenges existed with user identity (authorization and authentication) across the DoDIN, which is being solved through federation and normalization of identity objects with ICAM. Our MZTR solution has adapted similar processes and methodologies used to solve multiple problems from siloed identities in ICAM to Zero Trust Access platform interoperability.

This combined approach will enable each service component to leverage their own ZT Technologies, while enabling direct interoperability all without using multiple agents. This will enable each service branch with different vendor technology stacks to achieve maximum operational effectiveness. The benefits include:

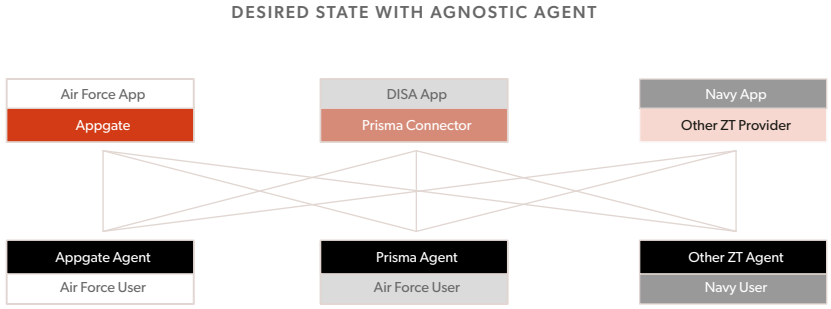
- Single security policy that spans across the DoDIN
- Common experience for warfighters
- Simpler troubleshooting (i.e., one solution versus multiple)
- Better economics and efficiency

Current Approach

As DISA, Service Branches and COCOMS go down their own Zero Trust access paths, this inhibits information sharing and creates complexitiy and siloed architectures… in short, creating 4X the complexity and cost. Figure 3 depicts an example of where the "current state" of the DoD could be as they leverage multiple Zero Trust Solutions.



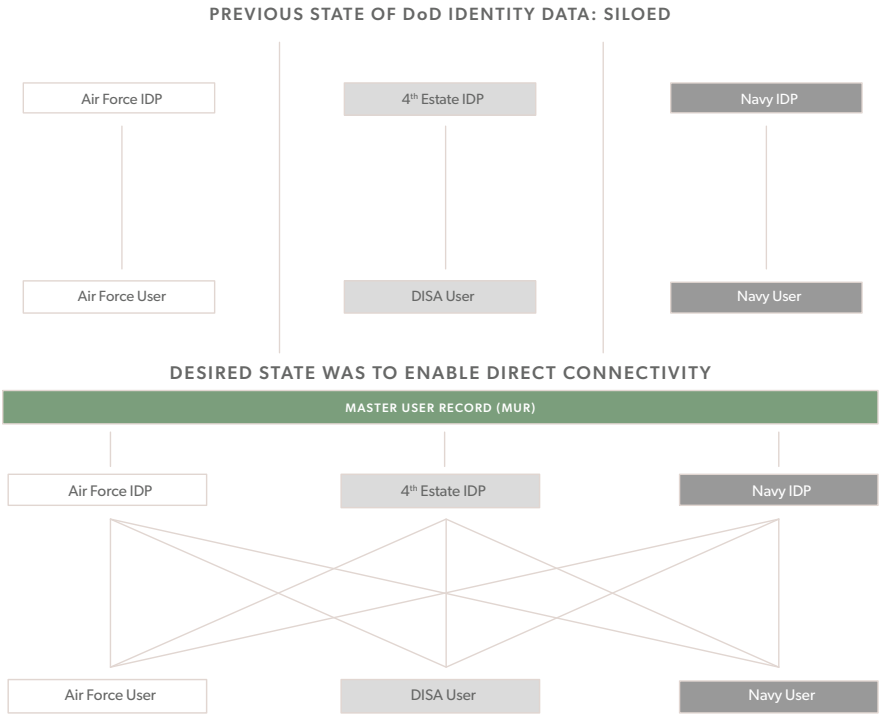
(Figure 3.)



(Figure 4.)

The "Desired State" shown above in Figure 4 would solve the interoperability with an agnostic agent. The probability of all vendors creating an "agnostic agent" in the short term is highly unlikely, due to the lack of standardization via IETF/RFC.

Appgate and Radiant have solved this type of challenge before through our ICAM offering, using technologies for identity federation and creating a Master User Record. The once siloed Identity Providers can now have all their identities, roles and attributes aggregated, normalized and then made globally available in a centralized repository as depicted in Figure 5.



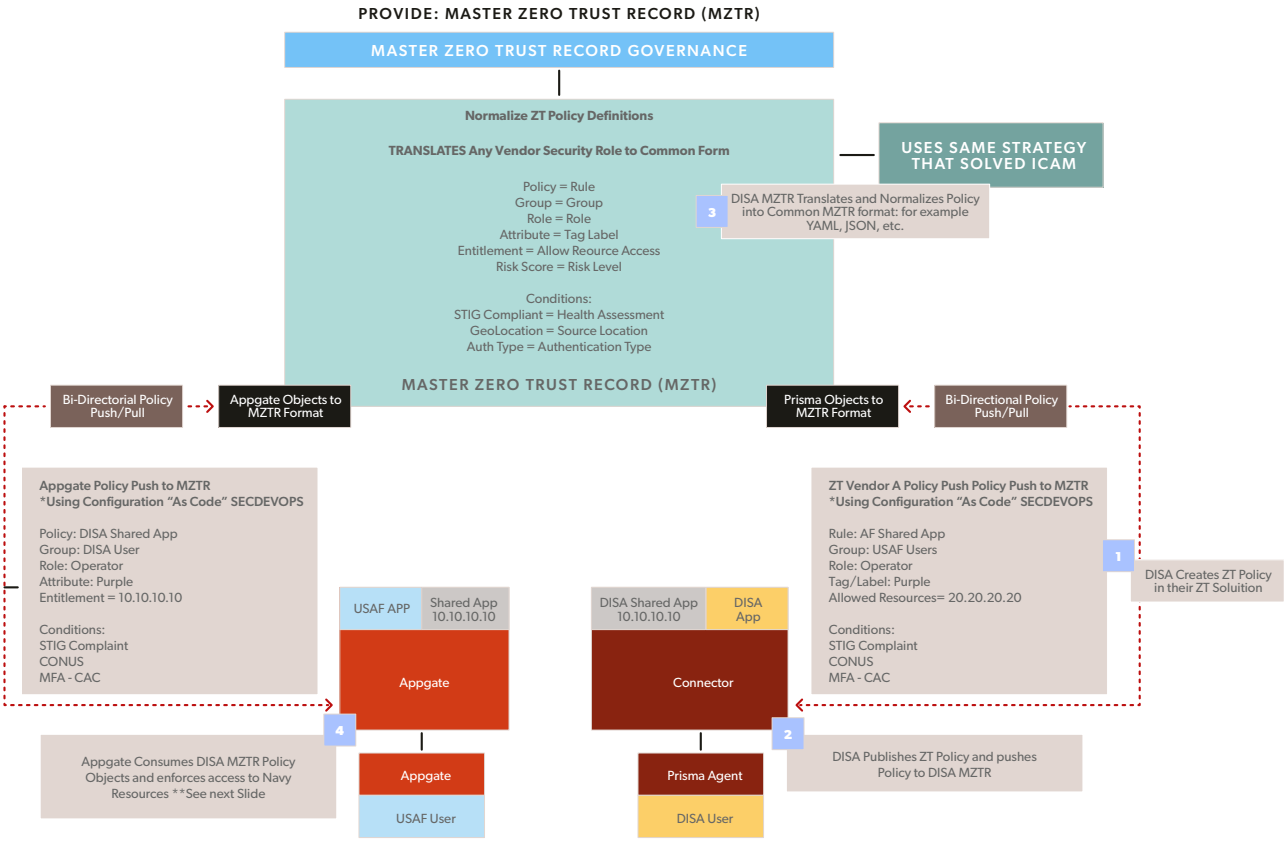
(Figure 5.)

Solution Overview

The traditional MUR capability is expanded by implementing a MZTR, which is built upon the MUR foundation. The decision to implement MZTR on the existing MUR platform is a strategic one. The MUR is already a globally available data store for identity objects, so it makes sense to add ZTNA policy objects to it. This not only simplifies the architecture but also enhances efficiency, as ZTNA policies are intrinsically linked to user identities.

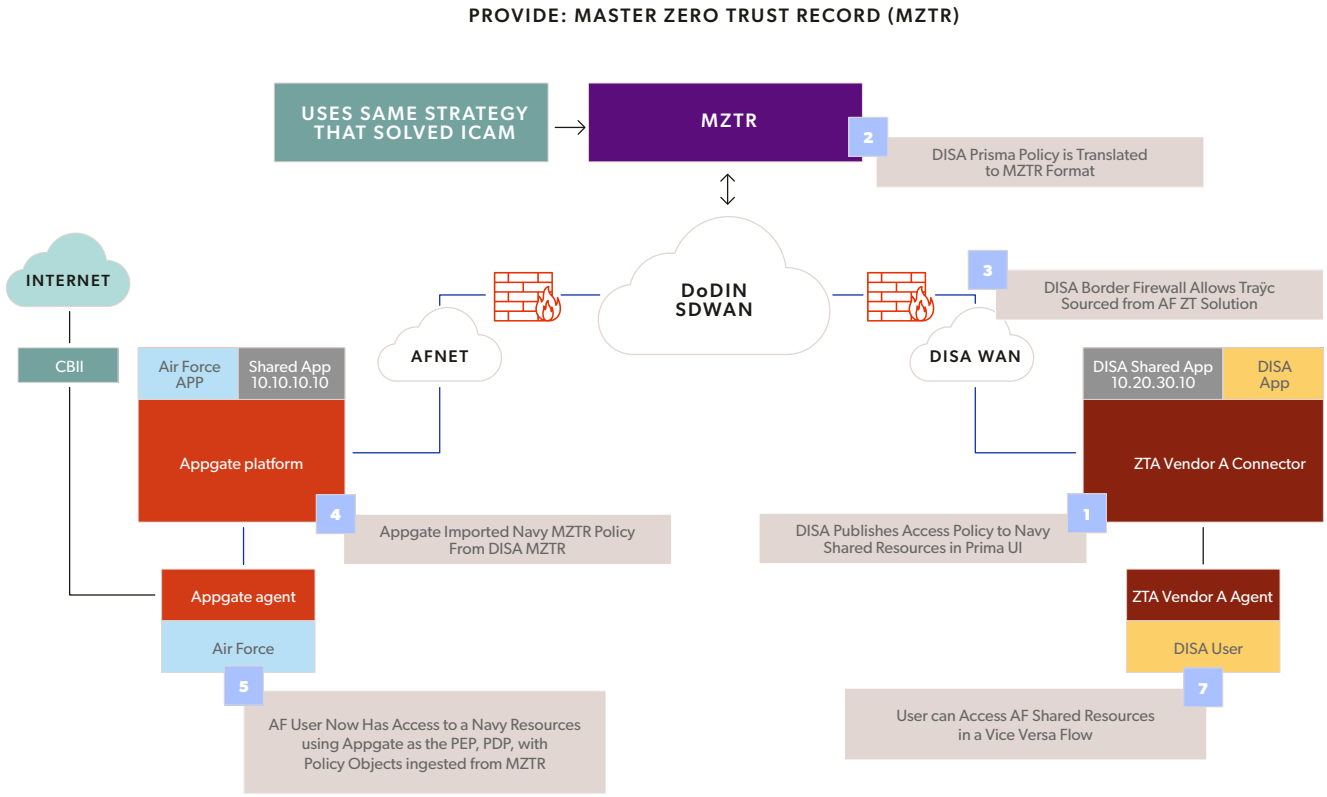
Furthermore, by integrating MZTR and MUR, we can provide a single, consistent view of both identity and access data. This not only simplifies management and reporting but also improves visibility and control, enhancing security. This would allow any organization (Service Branch, COCOM, Mission Partner, etc.) to use any Zero Trust Access solution without inhibiting interoperability.

The MZTR allows the normalization of proprietary security policies from each Zero Trust Vendor into a unified format, much like ICAM can assimilate identities from various sources such as Active Directory, LDAP Repositories, and Oracle Identity Manager and then standardize them for utilization across the DoDIN.



(Figure 6.)

SAME SILOED CHALLENGE EXISTED WITH ENTERPRISE IDENTITY: ICAM



(Figure 7.)

The MZTR approach will enable the DoD secure information sharing and interoperability across the DoDIN and any MPE environments.

MZTR Solution

By solving the ICAM/ZTNA interoperability problem, each military branch accelerates their ZTNA initiatives without fear of interoperability issues. This will not only improve security but also facilitate greater collaboration and resource sharing across branches, enhancing operational efficiency.

1. **Interoperability:**
   The ability of different ZTNA solutions to function cooperatively is a major issue. For instance, without interoperability, DISA using Prisma cannot easily access resources secured by Appgate SDP ZTNA for the U.S. Army and Air Force and visa versa. The MZTR provides an unprecedented solution by serving as a universal translator for ZTNA policy definitions, enabling any branch's ZTNA solution to understand and implement policy data from other branches. This kind of interoperability is crucial for fostering collaboration and coordination among the different branches of the military.
2. **Complexity and Cost:**
   Without a solution like MZTR, each branch of the military would need to deploy multiple ZTNA agents on user devices to ensure access to resources secured by different ZTNA solutions. This adds not only technical complexity and increased risk of conflicts between the different ZTNA agents, but also leads to significant cost increases due to licensing for multiple solutions. MZTR eliminates the need for multiple ZTNA agents and reduces costs, while still ensuring secure access to necessary resources.

3. **Mission Efficiency:**
   The MZTR addresses mission efficiency by enabling seamless sharing of resources across different branches of the military, enhancing the ability of the DoD to execute its mission. Without this capability, each branch would operate in a silo, which could lead to duplicated efforts, decreased efficiency and a potential negative impact on the mission.
4. **Consistency and Control:**
   By integrating MZTR and MUR, we offer a consistent and unified view of identity and access data, improving visibility and control across all branches. This enhanced view facilitates more accurate and effective decision-making regarding access and security.
5. **Future-proofing:**
   MZTR ensures that as new capabilities emerge or existing ones evolve, the DoD can easily adapt without needing to overhaul its entire system. This flexibility safeguards the DoD's investment in its ICAM/ZTA strategy against future developments.

By demonstrating a deep understanding of the specific needs and challenges facing the DoD, Appgate and Radiant positions its MZTR as a vital component of any successful ICAM/ZTNA solution for the department. Implementing an ICAM/ZTNA solution without addressing these challenges with a capability like MZTR maintains access silos, increasing risk to the DoD's mission.

In summary, our solution does not merely offer a technical solution: it provides a strategic approach that aligns with the DoD's mission and operational needs. We're not just selling a product - we're offering a partnership for the future of secure, efficient and cost-effective ICAM/ ZTNA in the Department of Defense.

COMPARATIVE ADVANTAGE:

While alternative solutions are capable of providing ICAM and ZTNA, this joint Radiant Logic and Appgate solution has several key advantages that make it the superior choice for the DoD.

Seamless Integration: Radiant Logic and Appgate SDP are natively integrated and designed to work seamlessly with a wide range of systems and platforms, ensuring easy integration with your existing IT infrastructure. This reduces the risk of implementation issues, minimizes disruption to ongoing operations and maximizes the return on your current IT investments.

Interoperability: MZTR is a unique capability that solves many challenges today, eliminates vendor lock-in and future-proofs the DoD as their mission needs evolve.

appgate