



U.S. Government Solutions

■ MAPPING BRIEF

Zscaler Mapping Brief: DoD Zero Trust Strategy

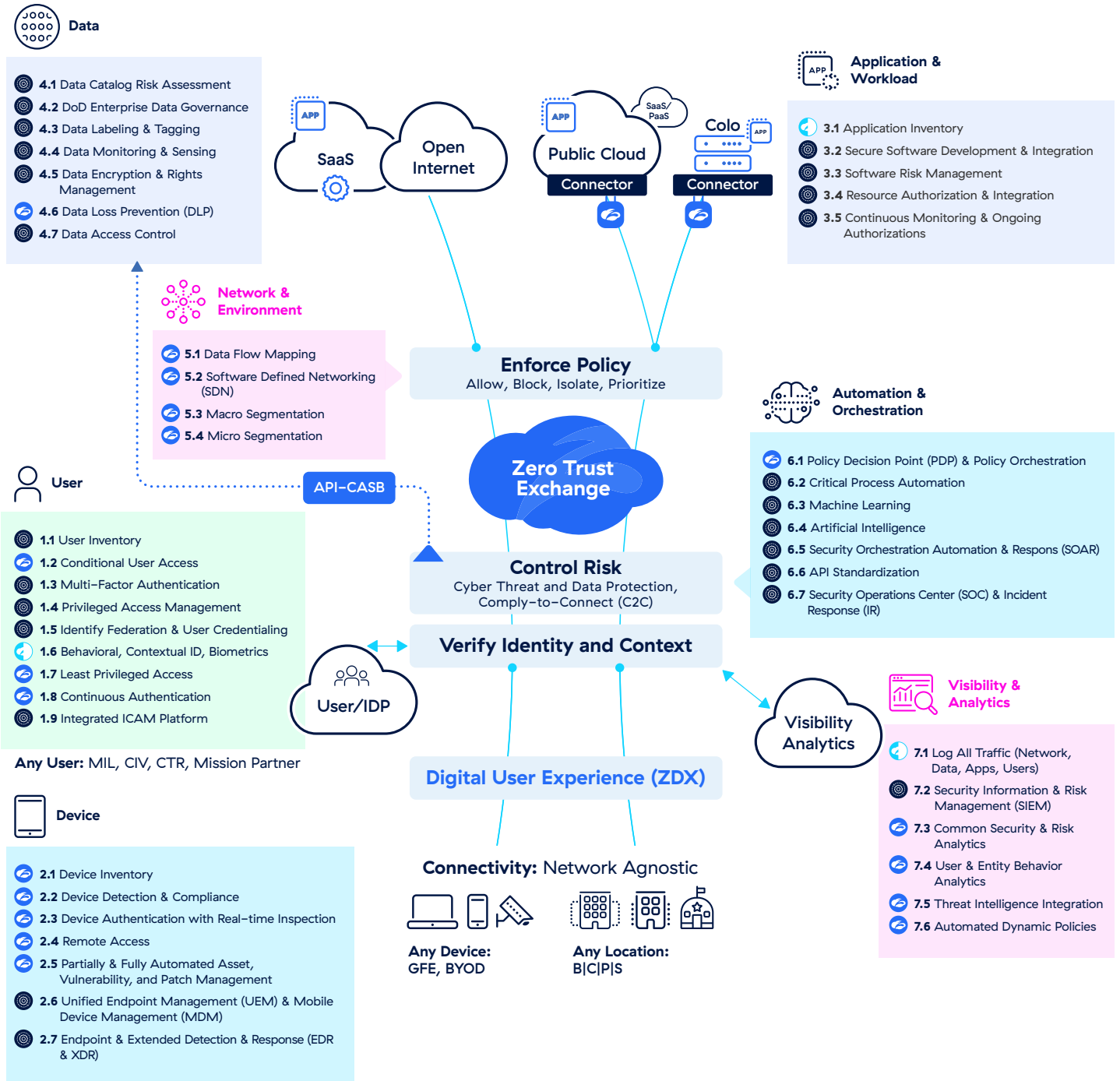
“ Modernization Requires Rethinking.

Implementing ZT requires rethinking how we utilize existing infrastructure to implement security by design in a simpler and more efficient way,” all while improving warfighter performance, increasing interoperability, and enabling unimpeded operations and resiliency.”

—DoD Zero Trust Strategy

What follows is Zscaler’s alignment to each of the DoD’s Zero Trust seven pillar activities, resulting in a cross-pillar integration that enhances each pillar’s cybersecurity mission readiness and visibility **to automate, integrate, and unify security and optimize access control.**

Zscaler-DoD Zero Trust Mapping



ZS-DoD ZT Mapping Legend:

- Meets:** Zscaler can meet the activity's requirement
- Partially Meets:** Zscaler can meet a portion of the activity's requirement
- Supports:** Zscaler integrates with other zero trust ecosystem partners to support this activity




“ Assume a Hostile Environment. There are malicious personas both inside and outside the environment. All users, devices, applications, environments, and all other NPEs are treated as untrusted.”

—DoD Zero Trust Reference Architecture (ZTRA) 2.0












User Pillar 1


Zscaler-DoD Zero Trust Mapping Legend







-  **Partially Meets**
-  **Meets:** Zscaler can meet the activity’s requirement without integration with another zero trust ecosystem partner
-  **Supports:** Zscaler integrates with other zero trust ecosystem partners support this activity
-  **Not Applicable:** Activity is centered on DoD policy, not technology-based
-  **Roadmapped:** Current capabilities and features being developed to meet the activities requirement
-  **Zscaler Internet Access:** Secures access to the Internet & SaaS applications; crowd-sourcing threat intelligence & protection powerhouse
-  **Zscaler Private Access:** SDP/ZTNA capability; secures end-to-end user-to-app traffic; resistant to Attacker-in-the-Middle (AitM/MitM)
-  **Zscaler Digital Experience:** Continuously monitors network performance; enhances troubleshooting and visibility to reshape mission network requirements

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	1.1.1 Authoritative Source of Identity	DoD components utilize enterprise authoritative source of (PE/NPE) identity (PE – AMID, NIS, AFID) and/or establish or augment with local authoritative source. Identity management can be done manually if needed, preparing for automated approach in later stages. Identity source is connected to identity lifecycle management processes (i.e. joiner/mover/leaver/returner). IT Privileged users are clearly identified.	 	<p>ZIA and ZPA can be configured with multiple Identity Providers (IdP) simultaneously to include on-premise and SaaS IdPs using SAML and SCIM-enabled IdPs. This allows agencies to migrate from IdP to IdP in a a secure and consistent manner, ensuring privileges are standardized throughout the transition.</p> <p>Zscaler can leverage the tenant’s IdP to authenticate the user and provide SAML attributes in a signed SAML assertion which is then used as a building block for Access Policy to a resource – no matter if it is an internally managed/hosted resource or SaaS cloud application.</p> <p>Lastly, using Zscaler’s native API and platform integrations with ITSM capabilities like ServiceNow to automate provisioning users. For more information, please ask Zscaler about their “MPE-ServiceNow” demo.</p>

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	1.2.1 Implement App Based Permissions per User	The DoD ICAM governance establishes a basic set of user attributes for authentication and authorization. These are integrated with the “Enterprise Identity Life–Cycle Management Pt1” activity process for a complete enterprise standard. Component authoritative sources are enabled for adding/updating attributes within the solution to better support identity federation. Remaining Privileged Access Management (PAM) activities have attributes that are approved and tailored as specified by the roles.	 	Beyond attributes derived from an ICAM solution, Zscaler’s central position within the network and API integrations allows Zscaler to add to the ICAM solution’s attribute list to create a comprehensive targeting user policy package compiled from additional policies and attributes from other resources (IdP, EDR, SIEM, SOAR, etc.) to secure and authorize access. Furthermore, Zscaler can synchronize user information from DoD’s Global Federated User Directory (GFUD) and incorporate it into Zscaler’s policy enforcement verification checks to secure access to data, applications, and resources while the DoD migrates to a Privileged Access Management (PAM) solution.
Supports 	1.2.2 Rule Based Dynamic Access Pt1	DoD components utilize the rules from the “Periodic Authentication” activity to build basic rules enabling and disabling privileges dynamically. IT Privileged user accounts utilize the PAM solution to move to dynamic privileged access using Just–in–Time access and Just–Enough–Administration methods.	 	Zscaler supports this activity’s criteria at the higher “Rule–Based Dynamic Access Pt2” level (Activity 1.2.3) level. Zscaler’s alignment to Activity 1.2.3: Zscaler combines its role as a Policy Enforcement Point (PEP), its device posture check functionality, and integrations with EDR, SIEM, and SOAR policies and attributes to enforce Comply–to–Connect (C2C) mission policies, develop dynamic risk–scoring, and provide users conditional Adaptive Access (AA). Besides that, agencies can use Zscaler’s open API to get consolidated visibility, engage automation, and increase their security posture.
Supports 	1.2.3 Rule Based Dynamic Access Pt2	DoD Organizations expand the development of rules for dynamic access decision making accounting for risk. Solutions used for dynamic access are integrated with cross pillar Machine Learning and Artificial Intelligence functionality enabling automated rule management.	 	Zscaler combines its role as a Policy Enforcement Point (PEP), its device posture check functionality, and integrations with EDR, SIEM, and SOAR policies and attributes to enforce Comply–to–Connect (C2C) mission policies, develop dynamic risk–scoring, and provide users conditional Adaptive Access (AA). Besides that, agencies can use Zscaler’s open API to get consolidated visibility, engage automation, and increase their security posture.
Supports 	1.2.4 Enterprise Gov’t roles and Permissions Pt1	DoD Organizations federate remaining user and group attributes as appropriate to the Enterprise Identity, Credential and Access Management (ICAM) solution. The updated attribute set is used to create universal roles for Organizations to use.	 	To support this activity, ZIA and ZPA can be configured and integrated with multiple Identity Providers (IdP), simultaneously, to include on–premise and SaaS IdPs using SAML and SCIM–enabled IdPs to secure access to data, applications, and resources.

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	1.2.4 Enterprise Gov't roles and Permissions Pt1	Continued — Core functions of the Identity Provider (IdP) and Identity, Credential and Access Management (ICAM) solutions are migrated to cloud services and/or environments enabling improved resilience and performance.		Continued — Afterward, Zscaler's central position within the network and API integrations allows Zscaler to add to an Enterprise Identity ICAM solution's attribute list to create a comprehensive targeting user policy package compiled from additional policies and attributes from other resources (IdP, EDR, SIEM, SOAR, etc.) to secure and authorize access. Furthermore, Zscaler can synchronize user information from DoD's Global Federated User Directory (GFUD) and incorporate it into Zscaler's policy enforcement verification checks to secure access to data, applications, and resources while the DoD migrates to a Privileged Access Management (PAM) solution.
Supports 	1.2.5 Enterprise Gov't roles and Permissions Pt2 Organizational	DoD Organizations move all possible functions of the Identity Provider (IdP) and Identity, Credential and Access Management (ICAM) solutions to cloud environments. Enclave/DDIL environments local capabilities to support disconnected functions but ultimately are managed by the centralized Identity, Credential and Access Management (ICAM) solutions. Updated roles are now mandated for usage and exceptions are reviewed following a risk-based approach.	 	Agencies can use ZIA and ZPA to integrated with multiple Identity Providers (IdP) and ICAM solutions, on-premise and SaaS IdPs to provide consistent, continuous, and secure access while the DoD transitions identity services from on-premises to the cloud.
Supports 	1.3.1 Organizational MFA/IDP	DoD components leverage enterprise ICAM or procure and implement a a DoD-approved Identity Provider (IdP) solution using approved DoD IL-3 credential or approved alternative Multi-Factor (MFA) solution. The IdP and MFA solution may be combined in a single application or separated as needed assuming automated integration is supported by both solutions. Both IdP and MFA support integration with the Enterprise PKI capability as well enabling key pairs to be signed by the trusted root certificate authorities. Mission/Task-Critical applications and services are utilizing the IdP and MFA solution for management of users and groups.	 	ZIA and ZPA can simultaneously be configured and integrated with multiple Identity Providers (IdP) to include on-premise and SaaS IdPs using SAML and SCIM-enabled IdPs. Zscaler's central position to user access, Agencies can use Zscaler to ensure that DoD users utilize an Identity Provider (IdP) solution that uses DoD's organic Enterprise PKI with Multi-Factor Authentication (MFA) functionality.
Supports 	1.4.1 Implement System and Migrate Privileged Users Pt1	DoD Organizations utilize the inventory of supported and unsupported Applications/Services for integration with privileged access management (PAM) solution to extend integrations. PAM is integrated with the more challenging Applications/Services to maximize PAM solution coverage. Exceptions are managed in a risk-based methodical approach with the goal of migration off and/or decommissioning Applications/Services that do not support PAM solution.	 	Since agencies can integrate Zscaler with a Privileged Access Management (PAM) solution and then use Zscaler to secure access to DoD resources (e.g., devices, applications, services, etc.) that do not support PAM integrations. Afterward, Zscaler will enforce comprehensive policies as a Policy Enforcement Point (PEP).

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	1.4.2 Implement System and Migrate Privileged Users Pt2	DoD Components utilize the inventory of supported and unsupported Applications/ Services for integration with privileged access management (PAM) solution to extend integrations. PAM is integrated with the more challenging Applications/Services to maximize PAM solution coverage. Exceptions are managed in a risk-based methodical approach with the goal of migration off and/or decommissioning Applications/Services that do not support the PAM solution.	 	Agencies can use Zscaler to secure excepted and unsupported Applications/Services. As the agency migrates/decommissions Applications/Services that do not support PAM solutions, Zscaler can be utilized to manage PAM-unsupported Applications/ Services in a risk-based systematic approach—at the same time. Agencies can use ZPA's Application and Application Server Discovery functionality to discover and cross-reference which applications/services have/have not integrated with the agency's PAM solution. ZDX's Software Inventory capability can provide a snapshot of a users' installed applications and software.
Supports 	1.4.3 Real time Approvals & JIT/JEA Analytics Pt1	Identification of necessary attributes (Users, Groups, etc.) are automated and integrated into the Privileged Access Management (PAM) solution. Privilege access requests are migrated to the PAM solution for automated approvals and denials.	 	As a Policy Enforcement Point (PEP), Zscaler integrates with multiple Policy Decision Points (PDP) to automate and enforce access criteria based on Zscaler's integration with the PAM solution, enforcing and applying Just-in-Time/Just-Enough-Access (JIT/JEA) to all accounts, uniformly, not only high-risk accounts.
Supports 	1.4.4 Real time Approvals & JIT/JEA Analytics Pt2	DoD Organizations establish a process for life cycle management of users both privileged and standard. Utilizing the Organizational Identity Provider (IdP) the process is implemented and followed by the maximum number of users. Any users who fall outside of the standard process are approved through risk-based exceptions to be evaluated regularly for decommission.	 	Zscaler can Integrate with User & Entity Behavior Analytics (UEBA), User Activity Monitoring (UAM), and Privileged Access Management (PAM) solutions to enforce dynamic JIT/JEA. For example, ZPA integrates with EDRs to monitor and create a dynamic risk score that enforces security policies at the mandated risk threshold. Additionally, the Zscaler platform's Insight functionality, Logs, and Reports assist organizations in continuously monitoring organizational systems and system components for anomalous or suspicious behavior (ZIA) and users, applications, and activities (ZPA).
Supports 	1.5.1 Component Identity Life-Cycle Management	DoD Components establish a process for life cycle management of users both privileged and standard. Utilizing an approved Identity Provider (IdP) the process is implemented and followed by the maximum number of users. Any Users falling outside of the standard process are approved through risk-based exceptions to be evaluated regularly for decommission.	 	Zscaler supports this ZT activity's Mission Owner organizational process by performing as a Policy Enforcement Point (PEP). As such, Zscaler can integrate with a Privileged Access Management (PAM) solution and enforce changes in authorization policies based on time and risk.

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	1.5.2 Identity Life-Cycle Management Pt1	Specified policies and supporting process are followed by the DoD Components. DoD Components implement the Enterprise Lifecycle Management process for the maximum number of identities, attributes, groups, credentials, and permissions. Exceptions to the policy are managed in a risk-based methodical approach.	 	As a Policy Enforcement Point (PEP), Zscaler can integrate with a Privileged Access Management (PAM) solution and enforce changes in authorization policies based on time and risk.
Supports 	1.6.1 Implement User & Entity Behavior Activity (UEBA) and User Activity Monitoring (UAM) Tooling	DoD Components procure and implement User & Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) solutions. Initial integration point with Enterprise IdP is completed enabling future usage in decision making.	 	Zscaler Integrates with User & Entity Behavior Analytics (UEBA), User Activity Monitoring (UAM), and Privileged Access Management (PAM) solutions to enforce dynamic JIT/JEA.
Supports 	1.6.2 User Activity Monitoring Pt1	DoD Organizations continue the analytics usage from User & Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) solutions by using generated data for all monitored applications and services when decision making occurs in the Just-in-Time and Just-Enough-Access solution.	 	Zscaler Integrates with User & Entity Behavior Analytics (UEBA), User Activity Monitoring (UAM), and Privileged Access Management (PAM) solutions to enforce dynamic Just-in-Time/Just-Enough-Access (JIT/JEA).
Supports 	1.6.3 User Activity Monitoring Pt2	DoD Organizations continue the analytics usage from User & Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) solutions by using generated data for all monitored applications and services when decision making occurs in the Just-in-Time and Just-Enough-Access solution.	 	Zscaler Integrates with User & Entity Behavior Analytics (UEBA), User Activity Monitoring (UAM), and Privileged Access Management (PAM) solutions to enforce dynamic Just-in-Time/Just-Enough-Access (JIT/JEA).
Supports 	1.7.1 Deny User by Default Policy	DoD Components audit internal user and group usage for permissions and revoke permissions when appropriate. This activity includes the revocation and/or decommission of excess permissions and access for application/service-based identities and groups. Where possible static privileged users are decommissioned or reduced permissions preparing for future rule/dynamic based access.	 	By default, Zscaler provides “deny all” access. Along with this native configuration, Zscaler absorbs the agency’s IdP authorization settings to enforce changes in a user’s level of access. Moreover, agencies can combine Zscaler’s PEP functionality and API integration to leverage attributes and policies from within its ecosystem (EDR, SIEM, SOAR, etc.) to establish and enforce dynamic-based access.

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Meet 	1.8.1 Single Authentication	DoD Components authenticate users and NPEs at least once per session (e.g., login) using CAC and other DoD approved methods. Users being authenticated are managed by the parallel activity “Organizational MFA/IDP” with the Component Identity Provider (IdP). Components do not use application/service-based identities and groups.		<p>ZPA leverages the IdP’s ability to authenticate Users successfully while consuming the SAML attributes in a signed SAML assertion. Afterward, Zscaler uses the SAML assertion as a building block for Access Policy to a resource, whether it is an internally managed/ hosted resource or a SaaS cloud application.</p> <p>ZPA performs as a Policy Enforcement Point (PEP) to broker connections only to an application that has an access policy with all matching SAML identity attribute requirements.</p> <p>An essential aspect of this policy enforcement is that ZPA also acts as a PEP for applications without organic authentications.</p>
Supports 	1.8.2 Periodic Authentication	DoD Components enable periodic authentication for applications and services. Traditionally these are based on duration and/or duration timeout but other period-based analytics can be used to mandate re-authentication of user sessions.	 	<p>Zscaler integrates with multiple Identity Providers (IdP) simultaneously, including on-premise and SaaS IdPs using SAML and SCIM. Afterward, Zscaler can enforce periodic authentication policies for Identity and Data Access Management. Additionally, within Zscaler’s Admin Portal, agencies can configure customizable authentication frequency and timeout policies.</p>
Meet 	1.8.3 Continuous Authentication Pt 1	DoD Organizations’ applications/service utilize multiple session authentications based on security attributes and access requested. Privilege changes and associational transaction requests required additional levels of authentication such as Multi-Factor Authentication (MFA) pushes to users.	 	<p>Zscaler meets this activity’s criteria at the “Continuous Authentication Pt2” level. Please visit Activity ID# 1.8.4.</p> <p>Zscaler performs as a PEP to query and ingest security attributes to create a transaction-based authentication and establishes a dynamic and unique micro-segmented mTLS tunnel. By integrating with cross-pillar technologies, Zscaler monitors user behavior to enforce access based on agency-established application and URL risk profiles.</p>
Meet 	1.8.4 Continuous Authentication Pt 2	DoD Organizations continue usage of transaction-based authentication to include integration such as user patterns.	 	<p>Zscaler performs as a PEP to query and ingest security attributes to create a transaction-based authentication and establishes a dynamic and unique micro-segmented mTLS tunnel. By integrating with cross-pillar technologies, Zscaler monitors user behavior to enforce access based on agency-established application and URL risk profiles.</p>

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	1.9.1 Enterprise PKI/IDP Pt1	The DoD Enterprise works with Components to implement Enterprise Public Key Infrastructure (PKI) solutions in a centralized and/or federated fashion. The Enterprise PKI solution utilizes a single or set of Enterprise level Root Certificate Authorities (CA) that can then be trusted by components to build Intermediate CA's off.	 	Agencies can leverage Zscaler's Identity Providers (IdP) integration to enforce this ZT activity goal for DoD users utilizing an IdP solution with MFA functionality. Moreover, since Zscaler integrates with multiple IdP, as a single solution or a federated set of Organizational IdPs, agencies can integrate their IdPs and PKI Certificated Authorities with the Enterprise IdP and PKI solutions.
Supports 	1.9.2 Enterprise PKI/IDP Pt2	DoD Organizations enable Biometric support in the Identity Provider (IdP) for mission/task-critical applications and services as appropriate. Biometric functionality is moved from Organizational solutions to the Enterprise. Organizational Multi-Factor (MFA) and Public Key Infrastructure (PKI) is decommissioned and migrated to the Enterprise as appropriate.	 	Zscaler can integrate with biometric-enabled Identity Providers (IdP) to enforce biometric attributes and use it as a security overlay for applications and services.
Supports 	1.9.3 Enterprise PKI/IDP Pt3	DoD Organizations integrate the remaining applications/services with Biometrics functionalities. Alternative Multi-Factor (MFA) tokens can be used.	 	Zscaler can integrate with biometric-enabled Identity Providers (IdP) to enforce biometric attributes and use it as a security overlay for applications and services.

“ ZTA validates in real time to ensure any vulnerabilities or rulesets that apply to the device to be validated and corrected to ensure it’s in compliance with the applied policy at the time it tries to access any resource. It is constantly checked against any possible exploits and if any exist, it attempts to remediate and if that’s not possible it will remove it from the environment to mitigate any exploitation.”

—DoD Zero Trust Reference Architecture (ZTRA) 2.0

Devices Pillar 2

Zscaler-DoD Zero Trust Mapping Legend

- Partially Meets**
- Meets:** Zscaler can meet the activity’s requirement without integration with another zero trust ecosystem partner
- Supports:** Zscaler integrates with other zero trust ecosystem partners support this activity
- Not Applicable:** Activity is centered on DoD policy, not technology-based
- Roadmapped:** Current capabilities and features being developed to meet the activities requirement
- Zscaler Internet Access:** Secures access to the Internet & SaaS applications; crowd-sourcing threat intelligence & protection powerhouse
- Zscaler Private Access:** SDP/ZTNA capability; secures end-to-end user-to-app traffic; resistant to Attacker-in-the-Middle (AitM/MitM)
- Zscaler Digital Experience:** Continuously monitors network performance; enhances troubleshooting and visibility to reshape mission network requirements

Zscaler Alignment	DoD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Meet 	2.1.1 Device Health Tool Gap Analysis	DoD Components a manual inventory of devices within the environment. Device attributes tracked in the inventory enable functionality outlined in the ZTA target level.		Using Zscaler’s Digital Experience (ZDX) Monitoring capability, Mission Owners can leverage embedded inventory functionality to view device and device software inventories.
Supports 	2.1.2 NPE/PKI, Device under Management	DoD Components utilize the DoD Enterprise PKI solution/service to deploy x509 certificates to all supported and managed devices. Additional other Non-Person Entities (NPEs) (e.g., web servers, network devices, routers, applications) that support x509 certificates are assigned in the PKI and/or IdP systems.	 	Agencies can integrate Zscaler with an Identity Provider (IdP), which utilizes x509 certificates to create access rules based on x509 certificates and use Zscaler as a security overlay for Non-Person Entities (NPE).


Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	2.1.3 Enterprise IDP Pt1	The DoD Enterprise Identity Provider (IdP) either using a centralized technology or federated organizational technologies integrates Non–Person Entities (NPEs) such as devices and service accounts. Integration is tracked in the Enterprise Device Management solution when applicable as to whether it is integrated or not. NPEs not able to be integrated with the IdP are either marked for retirement or excepted using a risk based methodical approach.	 	While the agency sunsets Non–Person Entities (NPE) that cannot be integrated with DoD Enterprise Identity Provider (IdP), agencies can use Zscaler to secure NPE access to data, applications, and resources during this time of transition.
Meet 	2.1.4 Enterprise IDP Pt2	The DoD Enterprise Identity Provider (IdP) either using a centralized technology or federated organizational technologies adds additional dynamic attributes for NPEs such as location, usage patterns, etc.		Agencies can use ZPA to merge attributes and policies derived from EDR, SIEM, and SOAR signals to enforce Comply–to–Connect mission policies, develop dynamic risk–scoring, and provide users conditional access.
Meet 	2.2.1 Implement C2C	The DoD Enterprise working with the Organizations develops a policy, standard and requirements for Comply to Connect. Once agreement is reached solution procurement is started, a vendor(s) is selected, and implementation begins with base level functionality in ZT Target environments (low risk). Base level checks are implemented in the new Comply to Connection solution enabling the ability to meet ZTA target functionalities.		Agencies can use ZPA to merge attributes and policies derived from EDR, SIEM, and SOAR signals to enforce Comply–to–Connect mission policies, develop dynamic risk–scoring, and provide users conditional access. Upon verification that a device's posture meets Comply–to–Connect criteria, Zscaler can allow or deny access to that DoD resource and recertify authorization continuously. Also, since the baseline of Zero Trust Network Access (ZTNA) is that there is no implicit or explicit trust in a network, Zscaler directly grants access to that DoD resource without direct network access.
Meet 	2.2.2 Implement C2C/ Compliance Based Network Authorization Pt2	DoD Organizations expand the deployment and usage of Comply to Connect to all supported environments required to meet ZT advanced functionalities. Comply to Connect teams integrate their solution(s) with the Enterprise IdP and Authorization Gateways to better manage access and authorizations to resources.		Agencies can use ZPA to merge attributes and policies derived from EDR, SIEM, and SOAR signals to enforce Comply–to–Connect mission policies, develop dynamic risk–scoring, and provide users conditional access. Upon verification that a device's posture meets Comply–to–Connect criteria, Zscaler can allow or deny access to that DoD resource and recertify authorization continuously. Also, since the baseline of Zero Trust Network Access (ZTNA) is that there is no implicit or explicit trust in a network, Zscaler directly grants access to that DoD resource without direct network access.


Zscaler Alignment	DoD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Meet 	2.3.1 Entity Activity Monitoring Pt1	Using the developed User and Device baselines, DoD Organizations utilize the implemented User and Entity Behavioral Activity (UEBA) solution to integrate baselines. UEBA device attributes and baselines are available to be used for device authorization detections.		As the Policy Enforcement Point (PEP), Zscaler can consume host-based posture intelligence from various host-based sources to aggregate UEBA device attributes and baselines. Additionally, if UEBA, FIM, Application control data, or Next generation Anti-Virus & Anti-Malware technologies can feed log data to a SIEM to determine if the aggregated device risk posture is out of tolerance for access to a specific DAAS entity. In such cases, Zscaler will deny the user access from that device.
Meet 	2.3.2 Entity Activity Monitoring Pt2	DoD Organizations utilize the User and Entity Behavioral Activity (UEBA) solution with network access solutions to mandate UEBA attributes (e.g., device health, logon patterns, etc.) for accessing environments and resources.		As the Policy Enforcement Point (PEP), Zscaler can consume host-based posture intelligence from various host-based sources to aggregate UEBA device attributes and baselines. Additionally, if UEBA, FIM, Application control data, or Next generation Anti-Virus & Anti-Malware technologies can feed log data to a SIEM to determine if the aggregated device risk posture is out of tolerance for access to a specific DAAS entity. In such cases, Zscaler will deny the user access from that device.
Supports 	2.3.3 Implement Application Containment & File Integrity Monitoring (FIM) Tools	DoD Components procure and implement File Integrity Monitoring (FIM) and Application containment solutions. FIMs ensures any data altered is authorized and unauthorized changes are detected by FIM. Application containment is used to isolate any suspicious behaviour or permissions to prevent any malicious later movement, expanding the capabilities and response than traditional executable containment. Both FIMS and Application containment continues the development of the device, data, and application pillar.		Zscaler integrates with File Integrity Management vendors, enabling real-time detections and alerts to trigger to initiate automated, targeted policies in Zscaler. This enables swift action in response to critical security events, changes in a system's hardening status, or when the system fails to meet DISA STIGs/CIS Benchmarks.











Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Meet 	2.3.4 Integrate NextGen AV Tools with C2C	DoD Components procure and implement Next Generation Anti-Virus solutions. NextGen AV should have the capabilities to use artificial intelligence, behavioral detection, machine learning, and mitigate exploits so zero days, signatureless, fileless, provide Network Access Control and known/unknown threats can be prevented. These solutions are orchestrated with the C2C or EDR solution for baseline status checks of signatures, updates, etc.	       	<p>Zscaler's inherent Device Posture Check functionality allows Mission Owners to develop and configure Device Posture profiles to enforce device configuration policies, compliance, changes in status, and unauthorized activity, which includes aggregating information regarding anti-virus and EDR data. Zscaler's integration with Microsoft Defender, Crowdstrike, and CarbonBlack EDRs provides additional visibility regarding unauthorized activity and dynamic risk scoring to enforce Just In Time/Just Enough Access if the users' risk exceeds the mission's risk threshold.</p> <p>Zscaler's Device Posture profile is a set of criteria evaluated on devices. Agencies can configure ZIA and ZPA's policies based on the outcome of this evaluation. For example, if you specify a file path in a device posture profile, the User can access the application if the User's system has the file specified in the C2C posture profile. Zscaler's device posture profiles provide the following benefits and allow Mission Owners to:</p> <p>*Determine access to resources and applications based on the C2C mission policies.</p> <p>*Ensure a security-specific level is present on the device before allowing access.</p>
Meet 	2.3.5 Fully Integrate Device Security stack with C2C as appropriate	DoD Organizations continue the deployment of Application Control to all environments and in prevention mode. File Integrity Monitoring (FIM) and Application Controls analytics are integrated into Comply to Connect for expanded access decision making data points. Comply to Connect analytics are evaluated for further device/endpoint security stack data points such as UEDM and are integrated as necessary.	   	<p>Zscaler's inherent Device Posture Check functionality allows Mission Owners to develop and configure Device Posture profiles to enforce device configuration policies, compliance, changes in status, and unauthorized activity, which includes aggregating information regarding anti-virus and EDR data. Zscaler's integration with Microsoft Defender, Crowdstrike, and CarbonBlack EDRs provides additional visibility regarding unauthorized activity and dynamic risk scoring to enforce Just In Time/Just Enough Access if the users' risk exceeds the mission's risk threshold.</p> <p>Agencies can integrate ZIA's Data Loss Protection (DLP) subcomponents: 1) Exact Data Match (EDM) and 2) Indexed Document Match (IDM) to support their File Integrity Monitoring (FIM) efforts.</p>

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Meet 	2.3.5 Fully Integrate Device Security stack with C2C as appropriate	Continued		Continued— <ul style="list-style-type: none"> ZIA's DLP Exact Data Match (EDM) capability allows the Zscaler service to identify a record from a structured data source that matches predefined criteria. To do this, Zscaler identifies and correlates multiple tokens contributing to a particular record to identify data ownership for regulated data types (CUI, PII, PHI, etc.) and protect them from intentional or unintentional data loss. ZIA's DLP Indexed Document Match (IDM) capability allows agencies to fingerprint your organization's critical documents that contain sensitive data. By fingerprinting and indexing your documents, agencies can create a document repository that the Zscaler service can use to identify wholly or partially matching documents when evaluating outbound traffic with the Mission Owner's (MO) Data Loss Prevention (DLP) policy. Roadmapped: Zscaler is releasing ZIA Data tagging solution for unstructured data in ZIA's commercial cloud, which is backed and supported with AI and ML technology and is a roadmap item. This will provide organizations greater perspective on data in flight and at rest for users in organizations and their interactions with the internet and public applications.
Supports 	2.3.6 Enterprise PKI Pt1	The DoD Enterprise Public Key Infrastructure (PKI) is expanded to include the addition of NPE and device certificates. NPEs and device that do not support PKI certificates are marked for retirement and decommission starts.	 	As a Policy Enforcement Point (PEP), Zscaler fully supports PKI validation on an asset as a component of Zscaler's risk-based decision analysis.
Supports 	2.3.7 Enterprise PKI Pt2	DoD Organizations utilize certificates for device authentication and machine to machine communications. Unsupported devices complete retirement and exceptions are approved using a risk based methodical approach.	 	As a Policy Enforcement Point (PEP), Zscaler fully supports PKI validation on an asset as a component of Zscaler's risk-based decision analysis.

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	2.4.1 Deny Device by Default Policy	DoD Enterprise sets standards and requirements for overall policy, with components to tailor pertaining to specific environment. DoD Components will block all unmanaged remote and local device access to resources. Compliant managed devices are provided risk based methodical access following ZTA target level concepts.	 	<p>Along with using Zscaler to block all unmanaged remote and local device access to resources, agencies use Zscaler to enforce Mission Owner (MO) policies to provide compliant managed—and unmanaged—devices risk-based controlled application-specific access following DoD's ZTA Target and Advanced level concepts.</p> <p>By default, Zscaler's Policy Enforcement Point core functionality only allows access to DoD resources once the authenticated user and device have established approved baselines. MOs can configure granular baselines to adapt access based on the user, device, network location, UEBA, and other PDP resources. These adaptive access baselines allow MOs to grant access to additional DoD resources incrementally. For example, agencies have used Zscaler's Browser-based Access to flex DoD users to view a DoD resource or website through a controlled browser environment.</p>
Meet 	2.4.2 Managed and Limited BYOD & IOT Support	DoD Components utilize Enterprise Device Management Solution to ensure that managed Bring Your Own Device (BYOD) and Internet of Things (IoT) devices are fully integrated with Enterprise IdP. Enabling user and device-based authorization is supported. Device access requires dynamic access policies and the practice of least privilege.	 	<p>Zscaler integrates with the Mission Owner (MO) Identity Provider (IdP), no matter enterprise or tactical, to manage BYOD and Internet of Things (IoT) devices.</p> <p>However, by default, Zscaler's native functionality only allows access to DoD resources once the authenticated user and device have established approved baselines. MOs can configure granular baselines to adapt access based on the user, device, network location, UEBA, and other PDP resources. These adaptive access baselines allow MOs to grant access to additional DoD resources incrementally. For example, agencies have used Zscaler's Browser-based Access to flex DoD users to view a DoD resource or website through a controlled browser environment.</p>
Meet 	2.4.3 Managed and Full BYOD & IOT Support Pt1	DoD Organizations utilize Unified Endpoint and Device Management (UEDM) and similar solutions to enable access for managed and approved devices to Mission and Operational Critical services/applications using dynamic access policies. BYOD and Internet of Things (IoT) devices are required to meet standard baseline checks before authorization.	 	<p>Zscaler integrates with the Mission Owner (MO) Identity Provider (IdP), no matter enterprise or tactical, to manage BYOD and Internet of Things (IoT) devices.</p> <p>ZIA and ZPA can leverage device posture checks, and MO pre-defined device posture profiles are criteria evaluated on devices. ZIA and ZPA policies can be configured based on the outcome of this evaluation. For example, if you specify a file path in a device posture profile, the user can access the application if the user's system has the file specified in the posture profile. The posture profiles are used for configuring access policies in the ZPA Admin Portal and for adding posture profile trust levels for ZIA.</p>

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	2.4.4 Managed and Full BYOD & IOT Support Pt2	DoD Organizations utilize Unified Endpoint and Device Management (UEDM) and similar solutions to enable access for unmanaged devices meeting device checks and standard baselines. All possible services/applications are integrated to allow access to managed devices. Unmanaged devices are integrated with services/applications based on risk driven methodical authorization approach.	 	As a cybersecurity overlay, agencies can use Zscaler to enable secure access for authenticated users using unmanaged devices to authorized DoD resources. Facilitated secure access is granted only after the endpoint first meets mission device posture check criteria and standard baselines. EDR integrations like CrowdStrike, Microsoft Defender, and Carbonblack bolster Zscaler's device posture check functionality to create a dynamic risk scoring weighed against the Mission Owners (MO) configured risk profiles. It includes additional attributes correlated from the Zscaler administrator console and the SIEM and SOAR policies.
Meet 	2.5.1 Implement Asset, Vulnerability and Patch Management Tools	DoD Components implement solution(s) for managing assets/devices configurations, vulnerabilities, and patches. Using minimum compliance standards (e.g., STIGs, C2C, UEM etc.) teams can confirm or deny managed device compliance. As part of the procurement and implementation process for solutions, APIs or other programmatic interfaces will be in scope for future levels of automation and integration.	 	<p>Zscaler integrates with the Mission Owner (MO) Identity Provider (IdP), no matter enterprise or tactical, to manage BYOD and Internet of Things (IoT) devices.</p> <p>Zscaler can limit user access to DAAS based on the need for patch updates to the endpoint or platform and limit a DoD user's access based on contextual risk-based policies and analysis to that DoD resource.</p> <p>Additionally, Zscaler has API integrations with ITSM capabilities, like ServiceNow, to automate Incident Response, patching, and remediation. Internally, as a cloud service, Zscaler automatically automates and delivers its patches to our services and assets, eliminating the need for DoD personnel, planning, or intervention.</p> <p>ZIA and ZPA can leverage device posture checks, and MO pre-defined device posture profiles are criteria evaluated on devices. ZIA and ZPA policies can be configured based on the outcome of this evaluation. For example, if you specify a file path in a device posture profile, the user can access the application if the user's system has the file specified in the posture profile. The posture profiles are used for configuring access policies in the ZPA Admin Portal and for adding posture profile trust levels for ZIA.</p>

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Meet 	2.6.1 Implement UEM or equivalent Tools	DoD Components will work closely with the “Implement Asset, Vulnerability, and Patch Management tools” activity to procure and implement a Unified Endpoint Management (UEM) solution ensuring that requirements are integrated with the procurement process. Once a solution is procured the UEM team(s) ensure that critical ZT target functionalities such as minimum compliance, asset management, and API support are in place.	  	<p>Zscaler integrates with the Mission Owner (MO) Unified Endpoint and Device Management (UEDM) or Mobile Device Management (MDM) tool to ensure Zscaler can limit user access to the DoD resource based on the need for patch updates to the endpoint or platform and limit a DoD user's access based on contextual risk-based policies and analysis of that DoD resource.</p> <p>Additionally, Zscaler has API integrations with ITSM capabilities, like ServiceNow, to automate Incident Response, patching, and remediation. Internally, as a cloud service, Zscaler automatically automates and delivers its patches to our services and assets, eliminating the need for DoD personnel, planning, or intervention. ZIA and ZPA can leverage device posture checks, and MO pre-defined device posture profiles are criteria evaluated on devices.</p> <p>ZIA and ZPA can leverage device posture checks and MO pre-defined device posture profiles to evaluate and validate if the MOs endpoint devices meet its access control policy criteria.</p> <p><small>*As a supplemental toolset to asset management systems, agencies can use ZDX's native device inventory functionality to verify the asset management system's device inventory.</small></p>
Meet 	2.6.2 Enterprise Device Management Pt1	DoD Enterprise sets standards and policies for DoD Components migrate the manual device inventory to an automated approach using a Enterprise Device Management solution. Approved devices are able to be managed regardless of location. Devices part of critical services are mandated to be managed by the Enterprise Device Management solution supporting automation.		In place of managing a different asset management system, agencies can use ZDX's native device inventory functionality to verify managed and unmanaged device inventory automatically.
Supports 	2.6.3 Enterprise Device Management Pt2	DoD Components migrate the remaining devices to Enterprise Device Management solution. EDM solution is integrated with risk and compliance solutions as appropriate.		As a supplemental toolset to the Enterprise Device Management solution, agencies can use ZDX's native device inventory functionality to automatically collect device inventory and cross-reference afterwards.









Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	2.7.1 Implement Endpoint Detection & Response (EDR) Tools and Integrate with C2C	DoD Components procure and implement Endpoint Detection and Response (EDR) solution(s) within environments. EDR is protecting, monitoring, and responding to malicious and anomalous activities enabling ZT Target functionality and is sending data to the Comply to Connection solution for expanded device and user checks.	 	Beyond meeting NextGen AV performance requirements, ZIA prevents compromise, lateral movement, and data exfiltration. Zscaler integrates with the Mission Owner's (MO) EDR tool to consume the EDR's threat intelligence and propagate throughout Zscaler's Zero Trust Exchange. Afterward, Zscaler can limit user access to the DoD resource based on the need for patch updates to the endpoint or platform and limit a DoD user's access based on contextual risk-based policies and analysis of that DoD resource.
Supports 	2.7.2 Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt1	DoD Component procure and implement Extended Detection & Response (XDR) solution(s). Integration points with cross pillar capabilities (network, cloud services, applications) are identified and prioritized based on risk. XDR should be in alignment with C2C. XDR capabilities would either supplement or replace EDR implementation activity . Analysis and correlation capabilities are sent from the XDR solution stack to the SIEM.	  	As a Policy Enforcement Point (PEP), Zscaler integrates with all of DoD's Zero Trust pillar (IdP, EDR, SIEM, etc.) capabilities to enhance each pillar's cybersecurity and secure data access and data-in-transit.
Supports 	2.7.3 Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt2	XDR solution stack completes identification of integration points expanding coverage to the fullest amount possible. Exceptions are tracked and managed using a risk based methodical approach for continued operation. Extended analytics enabling ZT Advanced functionalities are integrated into the SIEM and other appropriate solutions.	 	Zscaler integrates with the Mission Owner (MO) Endpoint Detection & Response (EDR), SIEM and SOAR tools to consume EDR threat intelligence and propagate throughout Zscaler's Zero Trust Exchange.




“ The approach to full Zero Trust implementation begins with preparatory discovery and assessment tasks. **The initial discovery process will identify critical DAAS as well as access and authorization activity existing within the architecture.** [...] To do this, the relationships between workloads, networks, devices, and users must be discovered.”

—DoD Zero Trust Reference Architecture (ZTRA) 2.0

Applications & Workloads Pillar 3

Zscaler-DoD Zero Trust Mapping Legend

-  **Partially Meets**
-  **Meets:** Zscaler can meet the activity’s requirement without integration with another zero trust ecosystem partner
-  **Supports:** Zscaler integrates with other zero trust ecosystem partners support this activity
-  **Not Applicable:** Activity is centered on DoD policy, not technology-based
-  **Roadmapped:** Current capabilities and features being developed to meet the activities requirement
-  **Zscaler Internet Access:** Secures access to the Internet & SaaS applications; crowd-sourcing threat intelligence & protection powerhouse
-  **Zscaler Private Access:** SDP/ZTNA capability; secures end-to-end user-to-app traffic; resistant to Attacker-in-the-Middle (AitM/MitM)
-  **Zscaler Digital Experience:** Continuously monitors network performance; enhances troubleshooting and visibility to reshape mission network requirements

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	3.1.1 Application/Code Identification	DoD Components create an inventory of approved applications and code being used including open source, commercial, and in-house developed. Each organization will track the supportability (i.e., active, legacy, etc.) hosted location (i.e., cloud, on-premise, hybrid, etc.) and record important data (i.e. name, version, team responsible, licensing and support, mapped dependencies)	 	Agencies can use ZDX Software Inventory embedded capability to provide a snapshot of the DoD user devices’ installed applications and software. Use the filters at the top of the page to narrow the search for a specific application or software. For enterprise applications, agencies can use ZPA’s application and application discovery to discover dynamically and inventory and agencies enterprise applications.

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Roadmap 	3.2.1 Build DevSecOps Software Factory Pt1	The DoD enterprise provide best practices for modern DevSecOps processes and CI/CD pipelines. The concepts are applied in a standardized technology stack across DoD Components able to meet future Application Security requirements which includes requirements gathering, design, development, testing and deploying.	 	ZIA and ZPA used in combination with Zscaler's Cloud Connector and Branch Connector appliances provide the ability to manage potential workload vulnerabilities in the following ways: <ul style="list-style-type: none"> Secure app-to-web and app-to-app traffic across cloud and data center environments Eliminate lateral threat movement within VPCs/VNets Providing zero trust connectivity across multi-cloud and hybrid cloud infrastructure, securing workload-to-internet, workload-to-workload, and workload-to-data center communications.
Supports 	3.2.2 Build DevSecOps Software Factory Pt2	DoD Components use their approved CI/CD pipelines to develop most new applications. Any exceptions will follow a standardized approval process to be allowed to develop in a legacy fashion. DevSecOps processes are also used to develop all new applications and update existing applications. Continual validation functions are integrated into the CI/CD pipelines and DevSecOps processes and integrated with existing applications.	 	ZPA's RESTFul API allows for automated policy creation and modification on the fly and the ability to create new Application Segment definitions to support CI/CD pipelines. ZIA has the ability to integrate with third party Development applications to gain continuous visibility and governance for the applications and third-party add-ons installed in your environment, take remediation actions, and automate your vetting and governance processes. This allows you to apply granular policies that dictate what users are able to do within each application.
Supports 	3.2.3 Automate Application Security & Code Re- mediation Pt1	A standardized approach to application security including code remediation is implemented across the DoD enterprise. Part one (1) of this activity includes the integration of a Secure API gateway with applications utilizing API or similar calls. Code reviews are conducted in a methodical approach and standardized protections for containers and their infrastructure are in place. Additionally, any serverless functions where the 3rd party manages the infrastructure such as Platform as a Service utilize adequate serverless security monitoring and response functions. Code Reviews, Container and Serverless security functions are integrated into the CI/CD and/or DevSecOps process appropriate.		ZPA's RESTFul API allows for automated policy creation and modification on the fly and the ability to create new Application Segment definitions to support CI/CD pipelines.

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	3.3.2 Vulnerability Management Program Pt1	The DoD Enterprise works with Components to establish and manage a Vulnerability Management program. The developed program includes at a minimum the tracking and management of public vulnerabilities based on DoD applications/services. Components establish a vulnerability management team with key stakeholders where vulnerabilities are discussed and managed following the Enterprise policy and standards.		As an active US-CERT and DC3//DCISE partner, agencies can use Zscaler to enhance the agency vulnerability management program.
Supports 	3.3.3 Vulnerability Management Program Pt2	Processes are established at the DoD Enterprise level for managing the disclosure of vulnerabilities in DoD maintained/operated services both publicly and privately accessible. DoD Components expand the vulnerability management program to track and manage closed vulnerability repositories such as DIB, CERT, and others.		As an active US-CERT and DC3//DCISE partner, agencies can use Zscaler to enhance the agency vulnerability management program.
Meet 	3.3.4 Continual Validation	DoD Components implement a continuous validation approach for application development where security is constantly assessed throughout the development, integration, and deployment. Validation includes security principles when planning and designing, security testing (to include code reviews), incident response, and SIEM alerting/logging. These principles are integrated and continuously executed with CI/CD pipeline. Applications developed outside of CI/CD process should still adhere to continuous validation in an Ad Hoc/Manual manner.	  	<p>While the agency sunsets applications that cannot integrate continual validation into their CI/CD process, agencies can use Zscaler to restrict access to those applications and provide secure access to applications with exceptions to policy. Additionally, to support the discovery of unsanctioned applications, agencies can use Zscaler capability features to validate that only sanctioned applications are in use.</p> <p>Agencies can use ZIA's Shadow IT Report to show the number of sanctioned and unsanctioned applications being used and their number of users. It also shows the application categories, the risk index, and the certifications for each application.</p> <p>Agencies can use ZPA's Application and Application Server Discovery functionality to discover and cross-reference which applications/services have/have not integrated with the agency's PAM solution.</p> <p>Agencies can use ZDX's Software Inventory page to provide a snapshot of your users' installed applications and software. Use the filters at the top of the page to narrow your search for a specific application or software.</p>

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Meet 	3.4.1 Access Control Decision Pt 1	The DoD Enterprise standardizes on policy enforcement approaches (e.g., Software Defined Perimeter) with the components. At a minimum the access gateways will be integrated with identities and devices once authentication is achieved. Components deploy approved resource authorization gateways and enable for external facing applications/services. Additional applications for migration and applications unable to be migrated are identified for exception or decommission.		
Meet 	3.4.2 Access Control Decision Pt 2	Policy enforcements and decisions are used for all possible applications/services. Application unable to utilize gateways are either decommissioned or excepted using a risk based methodical approach.		
Meet 	3.4.4 SDC Resource Authorization Pt2	Applications which support software-based configuration and management have been transitioned to a production/live environment and are in normal operations.	  	<p>While the agency sunsets applications that cannot support software-based configuration and management, agencies can use Zscaler to restrict access to those applications and provide secure access in a JIT/JEA fashion. Moreover, the following Zscaler capabilities and Open API for cloud application management can support the agency's SDC environment.</p> <p>Agencies can use ZIA's Shadow IT Report to show the number of sanctioned and unsanctioned applications being used and their number of users. It also shows the application categories, the risk index, and the certifications for each application.</p> <p>Agencies can use ZPA's Application and Application Server Discovery functionality to discover and cross-reference which applications/services have/have not integrated with the agency's PAM solution.</p> <p>Agencies can use ZDX's Software Inventory page to provide a snapshot of your users' installed applications and software. Use the filters at the top of the page to narrow your search for a specific application or software.</p>

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	3.4.5 Enrich At-tributes for Resource Authoriza-tion Pt1	Initial attributes from sources such as User and Entity Activity Monitoring, Micro-segmentation services, DLP and DRM are integrated into the Resource Authorization technology stack and policy. Any additional attributes for later integration are identified and planned. Attributes are used to create basic risk posture of users, NPEs and devices allowing for authorization decisions.	  	<p>As a Policy Enforcement Point (PEP), Zscaler integrates attributes from sources such as User and Entity Activity Monitoring, Micro-segmentation services, DLP, and DRM.</p> <p>Zscaler's inherent Comply-to-Connect (C2C) functionality can incorporate EDR and aggregated policies to establish a risk posture and develop and monitor a dynamic-risk (confidence) scoring that facilitates an automated throttling of authorization per the user, device, network, and mission policies.</p>
Meet 	3.4.6 Enrich At-tributes for Resource Authoriza-tion Pt2	Extended identified attributes are integrated with the resource authorization technology and policy. Confidence scoring is introduced across the attributes to create a more advanced method of authorization decision making in an automated fashion.		<p>As a Policy Enforcement Point (PEP), Zscaler can absorb Extended identified attributes from the other digital ecosystem components (IdP, EDR, SIEM, SOAR, etc.) and perform as the resource authorization technology or integrate with the respective resource authorization technology to enforce its policies.</p> <p>As is today, Zscaler's inherent Device Posture Check functionality incorporates EDR and aggregated policies to establish a dynamic-risk (confidence) scoring that facilitates an automated throttling of authorization per the User, device, network, and mission policies.</p>



“ This ZT security model re-thinks the implementation of security access to resources and is determined by dynamic policy, including observable state of user and endpoint identity, application/service, and the requesting asset. All capabilities within the Pillars must work together in an integrated fashion to **secure effectively** the Data Pillar, which is central to the model.”





—DoD Zero Trust Strategy


Data Pillar 4





Zscaler-DoD Zero Trust Mapping Legend




-  **Partially Meets**
-  **Meets:** Zscaler can meet the activity’s requirement without integration with another zero trust ecosystem partner
-  **Supports:** Zscaler integrates with other zero trust ecosystem partners support this activity
-  **Not Applicable:** Activity is centered on DoD policy, not technology-based
-  **Roadmapped:** Current capabilities and features being developed to meet the activities requirement
-  **Zscaler Internet Access:** Secures access to the Internet & SaaS applications; crowd-sourcing threat intelligence & protection powerhouse
-  **Zscaler Private Access:** SDP/ZTNA capability; secures end-to-end user-to-app traffic; resistant to Attacker-in-the-Middle (AitM/MitM)
-  **Zscaler Digital Experience:** Continuously monitors network performance; enhances troubleshooting and visibility to reshape mission network requirements

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	4.3.1 Implement Data Tagging & Classification Tools	Components implement a solution to create new rules, modify existing rules, delete existing rules, check for rule collision, rule deviation, or compound rule inconsistency, and testing of collective rule sets for an outcome. Tools must be adaptable to advanced analytic techniques.		Agencies can integrate ZIA’s Data Loss Protection (DLP) with data tagging and labeling capabilities like Microsoft Information Protection (MIP) to provide sensitivity labels that identify and protect files with sensitive content. Roadmapped: Zscaler is releasing ZIA Data tagging solution for unstructured data in ZIA’s commercial cloud, which is enhanced by AI and ML technology. This provides agencies greater perspective on data-in-transit and at-rest for users in and their interactions with the internet and public applications.

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	4.3.2 Data Tagging Pt1	Components map DoD Enterprise ZT tags to local labeling to meet minimum essential metadata criteria for ZT compliance.		Agencies can integrate ZIA's Data Loss Protection (DLP) with data tagging and labeling capabilities like Microsoft Information Protection (MIP) to provide sensitivity labels that identify and protect files with sensitive content. Roadmapped: Zscaler is releasing ZIA Data tagging solution for unstructured data in ZIA's commercial cloud, which is enhanced by AI and ML technology. This provides agencies greater perspective on data-in-transit and at-rest for users in and their interactions with the internet and public applications.
Supports 	4.3.3 Manual Data Tagging Pt2	DoD organizational specific data level attributes are integrated into the manual data tagging process. DoD enterprise and organizations collaborate to decide which attributes are required to meet ZTA advanced functionality. Data level attributes for ZTA advanced functionality are standardized across the enterprise and incorporated.		Agencies can integrate ZIA's Data Loss Protection (DLP) with data tagging and labeling capabilities like Microsoft Information Protection (MIP) to provide sensitivity labels that identify and protect files with sensitive content. Roadmapped: Zscaler is releasing ZIA Data tagging solution for unstructured data in ZIA's commercial cloud, which is enhanced by AI and ML technology. This provides agencies greater perspective on data-in-transit and at-rest for users in and their interactions with the internet and public applications.
Supports 	4.3.4 Automated Data Tagging & Support Pt1	DoD Organizations use data loss prevention, rights management, and/or protection solutions to conduct scanning of data repositories. Standardized tags are applied to supported data repositories and data types. Unsupported data repositories and types are identified.		Agencies can integrate ZIA's Data Loss Protection (DLP) with data tagging and labeling capabilities like Microsoft Information Protection (MIP) to provide sensitivity labels that identify and protect files with sensitive content. Roadmapped: Zscaler is releasing ZIA Data tagging solution for unstructured data in ZIA's commercial cloud, which is enhanced by AI and ML technology. This provides agencies greater perspective on data-in-transit and at-rest for users in and their interactions with the internet and public applications."


Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	4.3.5 Automated Data Tagging & Support Pt2	Remaining supported data repositories have basic and extended data tags which are applied using machine learning and artificial intelligence. Extended data tags are applied to existing repositories. Unsupported data repositories and data types are evaluated for decommissioning using a risk based methodical approach. Approved exceptions utilize manual data tagging approaches with data owners and/or custodians to manage tagging.		Agencies can integrate ZIA's Data Loss Protection (DLP) with data tagging and labeling capabilities like Microsoft Information Protection (MIP) to provide sensitivity labels that identify and protect files with sensitive content. Roadmapped: Zscaler is releasing ZIA Data tagging solution for unstructured data in ZIA's commercial cloud, which is enhanced by AI and ML technology. This provides agencies greater perspective on data-in-transit and at-rest for users in and their interactions with the internet and public applications.
Supports 	4.4.1 DLP Enforcement Point Logging and Analysis	DoD Components identify business rules for managing data loss prevention (DLP) enforcement points such as specific services and user endpoints. Using the established DoD Enterprise cybersecurity incident response standard, DoD organizations ensure the appropriate detail of data is captured. Additionally, protection, detection, and response use cases are developed to better outline solution coverage.		Agencies can integrate ZIA's Data Loss Protection (DLP) with data tagging and labeling capabilities like Microsoft Information Protection (MIP) to provide sensitivity labels that identify and protect files with sensitive content. Roadmapped: Zscaler is releasing ZIA Data tagging solution for unstructured data in ZIA's commercial cloud, which is enhanced by AI and ML technology. This provides agencies greater perspective on data-in-transit and at-rest for users in and their interactions with the internet and public applications.
Supports 	4.4.2 DRM Enforcement Point Logging and Analysis	DoD Components identify business rules for managing the accepted use of the digital asset managing Data Rights Management (DRM) enforcement points such as specific services and user endpoints. Using the established DoD Enterprise cybersecurity incident response standard, DoD organizations ensure the appropriate detail of data is captured. Additionally, protection, detection, and response use cases are developed to better outline solution coverage.	  	ZIA, ZPA, and ZDX utilize a standardized logging schema, forwarding and integrating with a Mission Owner's (MO) SIEM to correlate Incident Response and post-mortem activities.
Supports 	4.4.3 File Activity Monitoring Pt1	DoD Components utilize File Monitoring tools to monitor the most critical data classification levels in applications, services, and repositories. Analytics from monitoring is fed into the SIEM with basic data attributes to accomplish ZT Target functionality.	 	As a Policy Enforcement Point (PEP), Zscaler secures, allows, or restricts access to the front door to unstructured, semi-structured, and structured data repositories based upon aggregated attributes and risk data about the user, endpoint, network, and mission policies.

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	4.4.4 File Activity Monitoring Pt2	DoD Components utilize File Monitoring tools to monitor all regulatory protected data (e.g., CUI, PII, PHI, etc.) in applications, services, and repositories. Extended integration is used to send data to appropriate inter/intra-pillar solutions such as Data Loss Prevention, Data Rights Management/Protection and User & Entity Behavior Analytics.	 	As a Policy Enforcement Point (PEP), Zscaler secures, allows, or restricts access to the front door to unstructured, semi-structured, and structured data repositories based upon aggregated attributes and risk data about the user, endpoint, network, and mission policies.
Supports 	4.4.5 Database Activity Monitoring	DoD Organizations procure, implement, and utilize Database Monitor solutions to monitor all databases containing regulated data types (CUI, PII, PHI, etc.). Logs and analytics from the database monitoring solution are fed to the SIEM for monitoring and response. Analytics are fed into cross pillar activities such as “Enterprise Security Profile” and “Real Time Access” to better direct decision making.	 	As a Policy Enforcement Point (PEP), Zscaler secures, allows, or restricts access to the front door to unstructured, semi-structured, and structured data repositories based upon aggregated attributes and risk data about the user, endpoint, network, and mission policies. Agencies can integrate ZIA’s Data Loss Protection (DLP) with data tagging and labeling capabilities like Microsoft Information Protection (MIP) to provide sensitivity labels that identify and protect files with sensitive content. Roadmapped: Zscaler is releasing ZIA Data tagging solution for unstructured data in ZIA’s commercial cloud, which is enhanced by AI and ML technology. This provides agencies greater perspective on data-in-transit and at-rest for users in and their interactions with the internet and public applications.
Supports 	4.4.6 Comprehensive Data Activity Monitoring	DoD Organizations expand monitoring of data repositories including databases as appropriate based on a methodical risk approach. Additional data attributes to meet the ZT Advanced functionalities are integrated into the analytics for additional integrations.	 	Agencies can integrate ZIA’s Data Loss Protection (DLP) with data tagging and labeling capabilities to provide sensitivity labels that identify and protect files with sensitive content. Additionally, agencies can leverage ZPA’s SDP functionality to validate data and application access activity and ZDX’s in-depth visibility of the DoD user’s network, application, and data pathways to provide a unified view of monitoring across data repositories. Lastly, as a Policy Enforcement Point (PEP), Zscaler can secure, allow, and restrict access to unstructured, semi-structured, and structured data repositories based upon aggregated attributes and risk data about the user, endpoint, network, and mission policies. Roadmapped: Zscaler is releasing ZIA Data tagging solution for unstructured data in ZIA’s commercial cloud, which is enhanced by AI and ML technology. This provides agencies greater perspective on data-in-transit and at-rest for users in and their interactions with the internet and public applications.

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	4.5.1 Implement DRM and Protection Tools Pt1	DoD Components procure and implement DRM and Protection solution(s) as needed following the DoD Enterprise standard and requirements. Newly implement DRM and protection solution(s) are implemented with high risk data object	 	Zscaler can integrate with Adobe DRM to create a dual path from clients to data and DRM tools to create more manageable enforcement of DRM. In this example, the Zscaler client connector would create a ZPA tunnel to the Adobe DRM service for direct secure interaction, then on a separate tunnel in our integration, create a ZIA tunnel to AVVS workspaces to implement DRM relative to file interactions in that workspace. Additional integrations are possible and forthcoming as Zero Trust use cases present themselves.
Meet 	4.6.1 Implement Enforcement Points	Data loss prevention (DLP) is aligned to and strengthened by Data Privacy and Protection (DPP). Then through attribution, attributes can be injected that address where data is coming from, its movement across ZT control boundaries, and the invocation of protection measures (encryption, obfuscation, etc.). Collaboration with cyber functions should occur with respect to any observed data loss activity.		<p>ZIA offers the ability to provide Network DLP, at scale, for all internet and Public Application traffic, inclusive of SSL decrypted traffic.</p> <p>ZIA's DLP Exact Data Match (EDM) capability allows the Zscaler service to identify a record from a structured data source that matches predefined criteria. To do this, Zscaler identifies and correlates multiple tokens contributing to a particular record to identify data ownership for regulated data types (CUI, PII, PHI, etc.) and protect them from intentional or unintentional data loss.</p> <p>ZIA's DLP Indexed Document Match (IDM) capability allows agencies to fingerprint your organization's critical documents that contain sensitive data. By fingerprinting and indexing your documents, agencies can create a document repository that the Zscaler service can use to identify wholly or partially matching documents when evaluating outbound traffic with the Mission Owner's (MO) Data Loss Prevention (DLP) policy.</p> <p>If your organization had a third party DLP solution, Zscaler can forward information about transactions that trigger DLP policies to your third party solution. Zscaler uses secure Internet Content Adaptation Protocol (ICAP) to do this. However, the Zscaler service does not take ICAP responses from your DLP solution. Zscaler only monitors or blocks content according to the policy you configure, then forwards information about transactions so that your organization can take any necessary remediation steps.</p>

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	4.6.2 DLP En– forcement via Data Tags and Analytics Pt1	Data loss prevention (DLP) solution is updated from monitor only mode to prevention mode. Zero Trust tagging should incorporate indicators to facilitate DLP through cooperative cyber enforcement.	  	<p>ZIA, ZPA, and ZDX utilize a standardized logging schema, forwarding and integrating with a Mission Owner's (MO) SIEM to correlate Incident Response and post-mortem activities.</p> <p>Agencies can integrate ZIA's Data Loss Protection (DLP) with data tagging and labeling capabilities like Microsoft Information Protection (MIP) to provide sensitivity labels that identify and protect files with sensitive content.</p> <p>Roadmapped: Zscaler is releasing ZIA Data tagging solution for unstructured data in ZIA's commercial cloud, which is enhanced by AI and ML technology. This provides agencies greater perspective on data-in-transit and at-rest for users in and their interactions with the internet and public applications.</p>
Supports 	4.6.3 DLP En– forcement via Data Tags and Analytics Pt2	Data loss prevention (DLP) solution is updated to include extended data tags based on parallel Automation activities.		<p>Agencies can integrate ZIA's Data Loss Protection (DLP) with data tagging and labeling capabilities like Microsoft Information Protection (MIP) to provide sensitivity labels that identify and protect files with sensitive content.</p> <p>Roadmapped: Zscaler is releasing ZIA Data tagging solution for unstructured data in ZIA's commercial cloud, which is enhanced by AI and ML technology. This provides agencies greater perspective on data-in-transit and at-rest for users in and their interactions with the internet and public applications.</p>
Supports 	4.6.4 DLP En– forcement via Data Tags and Analytics Pt3	Data loss prevention (DLP) solution is integrated with automated data tagging techniques to include any missing enforcement points and tags.		<p>Agencies can integrate ZIA's Data Loss Protection (DLP) with data tagging and labeling capabilities like Microsoft Information Protection (MIP) to provide sensitivity labels that identify and protect files with sensitive content.</p> <p>Roadmapped: Zscaler is releasing ZIA Data tagging solution for unstructured data in ZIA's commercial cloud, which is enhanced by AI and ML technology. This provides agencies greater perspective on data-in-transit and at-rest for users in and their interactions with the internet and public applications.</p>

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	4.7.2 Integrate DAAS Access w/ SDS Policy Pt2	DoD Organizations implement the DAAS policy in an automated fashion.	 	As a Policy Enforcement Point (PEP), Zscaler integrates with the DoD's multiple Policy Decision Points (PDP) to automate DAAS policy implementation. Through API integration, Zscaler can integrate Security orchestration, automation, and response (SOAR) capabilities to accept SOAR-based risk scoring to securely allow or block access between Users and resources.
Meet 	4.7.3 Integrate DAAS Access w/ SDS Policy Pt3	Newly implemented SDS technology and/or functionalities are integrated with the DAAS policy in a risk-based fashion. A phased approach should be taken to during implementation to measure results and adjust accordingly.	 	Through API integration, agencies can use ZPA to not only integrate Software-defined Storage (SDS) technology with DAAS policy but correlate attributes, signals/triggers, and mission policies from other Policy Decision Points (PDP), i.e., IdP, EDR, SIEM, SOAR, etc. to enforce a comprehensive, secure access posture across SDS assets.
Meet 	4.7.4 Integrate Solution(s) and Policy with Enterprise IDP Pt1	DoD Components integrate attributes associated with access control and data location, and create means for interoperability across DLP, DRM, and SDS solutions with Enterprise IDP	 	Through API integration, agencies can use ZPA to not only integrate Software-defined Storage (SDS) technology with DAAS policy but correlate attributes, signals/triggers, and mission policies from other Policy Decision Points (PDP), i.e., IdP, EDR, SIEM, SOAR, etc. to enforce a comprehensive, secure access posture across SDS assets.
Supports 	4.7.5 Integrate Solution(s) and Policy with Enterprise IDP Pt2	Newly implemented SDS technology and/or functionalities are integrated with the Enterprise Identity Provider (IdP) following the integration plan. Identity attributes required to meet ZT Target functionalities are required for integration.		Through API integration, agencies can use ZPA to not only integrate Software-defined Storage (SDS) technology with DAAS policy but correlate attributes, signals/triggers, and mission policies from other Policy Decision Points (PDP), i.e., IdP, EDR, SIEM, SOAR, etc. to enforce a comprehensive, secure access posture across SDS assets.
Supports 	4.7.6 Implement SDS Tool and/or integrate with DRM Tool Pt1	Depending on the need for a Software Defined Storage tool, a new solution is implemented or an existing solution is identified meeting the functionality requirements to be integrated with DLP, DRM/Protection, and ML solutions.	 	<p>Zscaler can integrate its DLP with a DRM to create a dual path from clients to data and DRM tools to create more manageable enforcement of DRM. Agencies can integrate ZIA's Data Loss Protection (DLP) with data tagging and labeling capabilities like Microsoft Information Protection (MIP) to provide sensitivity labels that identify and protect files with sensitive content.</p> <p>ZIA's DLP Exact Data Match (EDM) capability allows the Zscaler service to identify a record from a structured data source that matches predefined criteria. To do this, Zscaler identifies and correlates multiple tokens contributing to a particular record to identify data ownership for regulated data types (CUI, PII, PHI, etc.) and protect them from intentional or unintentional data loss.</p>

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	4.7.7 Implement SDS Tool and/or integrate with DRM Tool Pt2	DoD Organizations configure the SDS functionality and/or solution to be integrated with the underlying DLP and DRM/Protection infrastructure as appropriate. Lower-level integrations enable more effective protection and response.	<div>ZIA</div> <div>ZPA</div>	<p>If the software-defined storage (SDS) has an OpenAPI, Zscaler can integrate with the DoD's SDS and IdP to support existing DAAS access and policy implementation.</p> <p>Zscaler can integrate with a DRM to create a dual path from clients to data and DRM tools to create more manageable enforcement of DRM. Additionally, agencies can integrate ZIA's Data Loss Protection (DLP) with data tagging and labeling capabilities like Microsoft Information Protection (MIP) to provide sensitivity labels that identify and protect files with sensitive content.</p> <p>ZIA's DLP Exact Data Match (EDM) capability allows the Zscaler service to identify a record from a structured data source that matches predefined criteria. To do this, Zscaler identifies and correlates multiple tokens contributing to a particular record to identify data ownership for regulated data types (CUI, PII, PHI, etc.) and protect them from intentional or unintentional data loss.</p>




“ A ZT environment dispenses with the distinction between “internal” and “external” users. An internal user should have no implicit trust associated with it than an external user. All users are untrusted. **One outcome that can follow is the removal of VPN.** In a ZT environment, all users are effectively “external” or untrusted and therefore must undergo the same rigorous authentication and authorization processes.”

—DoD Zero Trust Reference Architecture (ZTRA) 2.0

Network & Environment Pillar 5

Zscaler-DoD Zero Trust Mapping Legend


-  **Partially Meets**
-  **Meets:** Zscaler can meet the activity’s requirement without integration with another zero trust ecosystem partner
-  **Supports:** Zscaler integrates with other zero trust ecosystem partners support this activity
-  **Not Applicable:** Activity is centered on DoD policy, not technology-based
-  **Roadmapped:** Current capabilities and features being developed to meet the activities requirement
-  **Zscaler Internet Access:** Secures access to the Internet & SaaS applications; crowd-sourcing threat intelligence & protection powerhouse
-  **Zscaler Private Access:** SDP/ZTNA capability; secures end-to-end user-to-app traffic; resistant to Attacker-in-the-Middle (AitM/MitM)
-  **Zscaler Digital Experience:** Continuously monitors network performance; enhances troubleshooting and visibility to reshape mission network requirements

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	5.2.2 Implement SDN Infra-structure	Following the API standards, requirements and SDN API functionalities, DoD Components will implement Software Defined Networking (SDN) infrastructure to enable automation tasks. Segmentation Gateways and Authentication Decision Points are integrated into the SDN infrastructure along with output logging into a standardized repository (e.g., SIEM, Log Analytics) for monitoring and alerting.	 	Since Zscaler natively leverages user-to-app micro-segmentation, agencies can use Zscaler as a Segmentation Gateway. As such, agencies can leverage Zscaler’s central position to user access to ensure agencies receive end-to-end monitoring and alerting log collection. Additionally, as a Policy Enforcement Point (PEP), Zscaler can integrate with Authentication Decision Points (IdP, PDP), SDN infrastructure, and if needed, other Segmentation Gateways and stream logs to multiple standardized repositories (e.g., SIEM, Log Analytics), simultaneously.

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	5.2.2 Implement SDN Infra-structure	Continued		Continued — All policies, reports, and logs are available via standard/published web APIs. Over ten types of logs, i.e., web, firewall, DNS, tunnel, failed SSL, CASB, etc., are available in near real-time and can be tailored per log stream feed.
Supports 	5.2.3 Segment Flows into Control, Manage-ment, and Data Planes	Network infrastructure and flows are segmented either physically or logically into separate and distinct control, management, and data planes. Basic segmentation using IPv6/VLAN approaches is implemented to better organize traffic across data planes. Analytics and NetFlow from the updated infrastructure is automatically fed into Operations Centers and analytics tools.	 	Because Zscaler is network agnostic, produced logs are not limited to IP/TCP tuples. Zscaler can provide a hop-by-hop path along with performance metrics. While data and information are not sent via IPFix/NetFlow, telemetry of the user, application, path, and performance can be gathered via standard API.
Supports 	5.2.4 Network Asset Discovery & Optimiza-tion	DoD Organizations automate network asset discovery through the SDN infrastructure limiting access to devices based on risk based methodical approaches. Optimization is conducted based on the SDN analytics to improve overall performance along with provide necessary approved access to resources.	 	Agencies can use ZPA to enhance the SDN infrastructure's ability to limit device access based on automated network asset discovery. ZPA's Comply-to-Connect functionality enables MOs to authorize device access based on aggregated risk-based policies that extend past the IP network and boundary. Additionally, MOs can cross-reference the ZPA's Application and Application Server Discovery, and ZDX's embedded device and software inventory functionality cross-reference the network asset database. Within ZDX's device inventory dashboard, device models are arranged and color-coded according to device and size, indicating the number of device models relative to other models. Beyond device/asset discovery, ZDX can provide a drill-down into GFE characteristics (CPU, memory, Wifi, etc.), user information, and applications accessed.
Meet 	5.2.5 Real-Time Access Decisions	SDN Infrastructure utilizes cross Pillar data sources such as User Activity Monitoring, Entity Activity Monitoring, Enterprise Security Profiles and more for real-time access decisions. Machine learning is used to assist decision making based on advanced network analytics (full packet capture, etc.). Policies are consistently implemented across the Enterprise using unified access standards.	 	Zscaler performs as a Policy Enforcement Point (PEP) and integrates today across DoD pillar assets and policies, e.g., C2C, enterprise, and mission/non-mission security profiles. As such, agencies can incorporate Zscaler PEP functionality with the SDN infrastructure to develop, review, and automate real-time access decisions.

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Meet 	5.2.5 Real-Time Access Decisions	Continued		<p>Continued— All packets, encrypted and unencrypted that make up the transition are examined for context and intent. Zscaler's Single Scan Multi-Action (SSMA) allows Zscaler to inspect all traffic, encrypted and unencrypted, transaction and perform multiple checks at the same time. This simultaneous multithreaded threat checking allows Zscaler to scale to hundreds of billions of daily transactions. As of March 2023, Zscaler is processing over 1.5Tbps of encrypted traffic and 12PBytes of daily transactions.</p> <p>Furthermore, the Zscaler SDP can also utilize cross-Pillar data sources such as User Activity Monitoring, Entity Activity Monitoring, Enterprise Security Profiles, and more for real-time access decisions. Zscaler uses Machine learning to assist decision-making based on advanced network analytics from DPI and threat patterns. Policies are consistently implemented across the Enterprise using unified access standards. Open APIs allow policy within the SDP to be modified in real-time to provide situational aware access.</p> <p>https://www.zscaler.com/ThreatLabz/encrypted-traffic-dashboard</p>
Supports 	5.3.1 Macro segmentation	DoD Components implement service-based architectures to restrict lateral movement between public and private components of a solutions architecture. Proxy and/or enforcement checks are integrated with the SDN solution(s) based on device attributes and behavior.	  	<p>Zscaler's DoD IL5 zero-trust solution currently creates a per-user per-app micro-segmentation. Furthermore, Zscaler's solution removes the TCP listener from the server's path, ensuring that only authenticated and authorized users can communicate with authorized servers, and requires no refactoring on the user or the server.</p> <p>All policies, reports, and logs are available via standard/published web APIs. Zscaler has over ten types of logs, i.e., web, firewall, DNS, tunnel, failed SSL, CASB, etc., available in near real-time and can be tailored per log stream feed. Typically, each log contains 50+ tuples of information for use by operations.</p> <p>Roadmapped: Zscaler's commercial cloud has additional micro-segmentation capabilities to regulate East-West traffic. This additional micro-segmentation capability is expected to migrate to the Zscaler DoD IL5 cloud infrastructure in 2023.</p>

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	5.3.2 Mission-based Macro segmentation	DoD Components implement mission/organization-based macro-segmentation using logical network zones limiting lateral movement. Proxy and/or enforcement checks are integrated with the SDN solution(s) based on device attributes and behavior.	 	As a DoD IL5 Zero Trust solution, Zscaler eliminates the need for segmentation at the B/P/C/S end-user level, as Zscaler removes the user and the application from the network and creates a secure segmented per-user-per-app TLS tunnel on demand. This connection model allows Zscaler's solution to provide zero trust even if the network is compromised, as the network is leveraged for its core functionality: a transport mechanism only. Also, adversaries cannot compromise the certificate-pinned tunnel. As a result, remote and local users cannot move laterally. This approach simplifies the design, reduces complexity and risk, and accelerates the agency's zero-trust rollout.
Meet 	5.4.1 Implement Micro segmentation	DoD Components implement Micro-Segmentation infrastructure into SDN environment enabling basic segmentation of service components (e.g., web, app, db), ports and protocols. Basic automation is accepted for policy changes including API decision making. Virtual hosting environments implement micro-segmentation at the host/container level.	 	Zscaler implements the application Micro-Segmentation allowing authenticated entities to only connect to authorized resources. Using API policy updates and embedded C2C capabilities, Zscaler brokers secure data access using a dynamically established and terminated user-to-app micro-segmented tunnel. The host-based zero-trust solution further eliminates lateral movement by B/P/C/S endpoints. Moreover, extensive API capability allows Zscaler to be a force multiplier as it implements a dynamic need-to-know capability. With IdP, EDR, and data-specific solutions, Zscaler can prevent, limit, or allow per-user per-app applications.
Meet 	5.4.2 Application & Device Micro segmentation	DoD Components utilize Software Defined Networking (SDN) solution(s) to establish infrastructure meeting the ZT Target functionalities — logical network zones, role, attribute and conditional based access control for user and devices, privileged access management services for network resources, and policy-based control on API access.	 	<p>Zscaler's Zero Trust Exchange – Software Defined Perimeter (SDP) dedicated to zero trust – absorbs identity, role, and machine attributes, among others, and provides conditional-based access control for users and devices. Zscaler's ZTE seamlessly provides the following:</p> <ul style="list-style-type: none"> Privileged access management services for network resources. Rate-limiting on logs. Policy-based control on API access. <p>Rate-limiting for logs is critical to avoid overwhelming the SIEM/SOAR solutions. Zscaler high-fidelity log data can be tuned up or down to accomplish the SOAR/SIEM requirements. For reference, all of Zscaler's ZTE internal capabilities leverage APIs.</p>

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Meet 	5.4.3 Process Micro seg- mentation	DoD Organizations utilize existing micro-segmentation and SDN automation infrastructure enabling process micro-segmentation. Host-level processes are segmented based on security policies and access is granted using real-time access decision making.	 	Zscaler's host-based processes are segmented on a per-application basis, mandating one-way communication for servers without using hardware mechanisms as defined by AC-4(7). Furthermore, continuously monitoring user behavior achieves the SC-7(20) dynamic isolation requirement. For example, a user's web access can be switched to browser isolation or terminated as needed. Zscaler satisfies the AC-4(17) security control since it uses AD, ADFS, or integrating with IdPs using SAML insertions to ensure secure access provided using real-time and continuous decision-making.
Meet 	5.4.4 Protect Data In Transit	Based on the data flow mappings and monitoring, policies are enabled by DoD Organizations to mandate protection of data in transit. Common use cases such as Coalition Information Sharing, Sharing Across System Boundaries and Protection across Architectural Components are included in protection policies.	 	Zscaler encrypts traffic using a certificate-pinned TLS tunnel on a per-user/per-app basis that is dynamically established and terminated. This modus operandi allows the transaction to transit any network because user-level access and application transcend network access control.




“ Cybersecurity and intelligence analysts working on the front lines of the Department’s security operations centers struggle to maintain an enterprise view of common threats and vulnerabilities and to communicate effectively when incidents emerge. Siloed domains and manual interventions are par for the course in today’s conventional architectures and result in increased security risks and inconsistent policies, data, logs, and analytics. **With Zero Trust executed, these analysts in the Department’s cybersecurity operations centers will have the ability to maintain dynamic security monitoring, receive real-time alerts, and automatic incident response —providing the best chance of keeping malicious actors out, and getting them off DoD’s networks.**”

—DoD Zero Trust Strategy

Visibility & Analytics Pillar 6

Zscaler-DoD Zero Trust Mapping Legend



-  **Partially Meets**
-  **Meets:** Zscaler can meet the activity’s requirement without integration with another zero trust ecosystem partner
-  **Supports:** Zscaler integrates with other zero trust ecosystem partners support this activity
-  **Not Applicable:** Activity is centered on DoD policy, not technology-based
-  **Roadmapped:** Current capabilities and features being developed to meet the activities requirement
-  **Zscaler Internet Access:** Secures access to the Internet & SaaS applications; crowd-sourcing threat intelligence & protection powerhouse
-  **Zscaler Private Access:** SDP/ZTNA capability; secures end-to-end user-to-app traffic; resistant to Attacker-in-the-Middle (AitM/MitM)
-  **Zscaler Digital Experience:** Continuously monitors network performance; enhances troubleshooting and visibility to reshape mission network requirements

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	6.1.2 Component Access Profile Rules	DoD Components develop basic access profile rules for mission/task and non-mission/task DAAS access using the data from the User, Data, Network, and device pillars. The DoD Enterprise works with the Organizations to develop an Enterprise Security Profile Rules using the existing Component security profiles to create a common access approach to DAAS. A phased approach can be used in organizations to limit risk to mission/task critical DAAS access once the security profile(s) are created.	 	As a Policy Enforcement Point (PEP), Zscaler can receive the decision from the PDP & Policy orchestration solution via API integration and enforce additional policies from its administrative UI to facilitate an automated throttling of authorization per the User, device, network, and mission policies.

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Meet 	6.1.3 Enterprise Security Profile Rules Pt1	The Enterprise Security profile rules covers the User, Data, Network and Device pillars initially. Existing Component security profile rules are integrated for non-mission/task DAAS access following an iterative approach to tuning access.	 	Since Zscaler natively performs as a Policy Enforcement Point (PEP) and cybersecurity overlay, agencies can use Zscaler to develop, test, isolate, and transition users, devices, networks, and environments to integrated Organizational Security Profiles are integrated for non-mission/task DAAS access.
Meet 	6.1.4 Enterprise Security Profile Pt2	The minimum number of Enterprise Security Profile(s) exist granting access to the widest range of DAAS across Pillars within the DoD Organizations. Mission/task organization profiles are integrated with the Enterprise Security Profile(s) and exceptions are managed in a risk based methodical approach.	 	Agencies can leverage Zscaler's inherent capability as a cybersecurity overlay to integrate Enterprise Security and Mission/Task Critical profiles and dynamically apply configured profiles when specific attributes and policies are triggered.
Supports 	6.2.2 Enterprise Integration & Workflow Provisioning Pt1	The DoD enterprise establishes baseline instrument interoperability within the Security Orchestration, Automation and Response solution (SOAR) required to enable target level ZTA functionality where actionable and relevant information resides. DoD components identify instrument interoperability points and prioritization per the DoD enterprise baseline.	 	Zscaler performs as a centralized Policy Enforcement Point (PEP) that crosscuts each DOD Zero Trust Pillar to secure and optimize routing and information, enhance visibility, and create synergy across each domain. This high-touch cybersecurity awareness simultaneously feeds tailored logs to SIEM/SOAR capabilities e.g., Splunk>Phantom, Demisto, Exebeam, etc. and SOC and Incident Response teams so that they may establish SOAR baselines required to enable target and advanced-level Zero Trust Access functionality.
Supports 	6.5.1 Response Automation Analysis	DoD Components identify and enumerate all response activities that are executed both manually and in an automated fashion. Response activities are organized into automated and manual categories.	  	Zscaler supports integrations with all leading SOAR platforms, which help SOC teams enforce and automate event lookups, reputation checks, blocking actions, and other response activities. By delivering a streamlined SOAR and Zscaler workflow, security teams can ensure real-time enforcement of updated and automatable policies for better protection of users, on or off-network. SOAR vendors can ingest Zscaler's standardized logs (from engines including firewall, IPS, etc.) and alerts and automate enforcement/threat intel actions via the Zscaler API.

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	6.5.2 Plan SOAR Tools Implementation	DoD enterprise working with components to develop a standard set of requirements for security orchestration, automation, and response (SOAR) tooling to enable target level ZTA functions. DoD Components use approved requirements to procure a SOAR solution. Basic infrastructure integrations for future SOAR functionality is completed.	  	Zscaler supports integrations with all leading SOAR platforms, which help SOC teams enforce and automate event lookups, reputation checks, blocking actions, and other response activities. By delivering a streamlined SOAR and Zscaler workflow, security teams can ensure real-time enforcement of updated and automatable policies for better protection of users, on or off-network. SOAR vendors can ingest Zscaler's standardized logs (from engines including firewall, IPS, etc.) and alerts and automate enforcement/threat intel actions via the Zscaler API.
Supports 	6.5.3 Implement Playbooks	DoD organizations review all existing playbooks to identify for future automation. Existing manual and automated processes missing playbooks have playbooks developed. Playbooks are prioritized for automation to be integrated with the Automated Workflows activities covering Critical Processes. Manual processes without playbooks are authorized using a risk based methodical approach.	 	From a playbook perspective, agencies can leverage Zscaler's threat intelligence, Cloud Sandbox reports, and cloud misconfiguration information to enrich incident tickets and quickly respond via automated workflows. These automated workflows reduce response time by minimizing manual triage tasks, increasing the IT team's speed and productivity. Remediate incidents instantly or create alert tickets in the ITSM of choice as artifacts for streamlined workflows. From a SOAR perspective, Zscaler supports integrations with all leading SOAR platforms, which help SOC teams enforce and automate event lookups, reputation checks, blocking actions, and other response activities. SOAR vendors can ingest Zscaler's standardized logs (from engines including firewall, IPS, etc.) and alerts and automate enforcement/threat intel actions via the Zscaler API.
Supports 	6.6.1 Tool Compliance Analysis	Automation and Orchestration tooling and solutions are analyzed for compliance and capabilities based on the DoD Enterprise API machine-readable patterns and protocols.	  	Zscaler's supports DoD Enterprise programmatic interface standard by using REST APIs.
Supports 	6.6.2 Standardized API Calls & Schemas Pt1	The DoD enterprise works with components to establish machine readable protocols and patterns for programmatic interfaces (e.g., API) to enable target ZTA functionalities. DoD Components update programmatic interfaces to the new machine readable protocols and patterns.	  	Zscaler's supports DoD Enterprise programmatic interface standard by using REST APIs.

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	6.6.3 Standardized API Calls & Schemas Pt2	DoD Components will ensure that all ZT services and applications are using protocol and pattern interfaces.	ZIA ZPA ZDX	Zscaler's supports DoD Enterprise programmatic interface standard by using REST APIs.
Supports 	6.7.1 Workflow Enrichment Pt1	DoD Enterprise works with Components to establish cybersecurity incident response guidance using industry best practices such as NIST and a list of approved threat data sources as specified in "Cyber Threat Intelligence Program Pt 1". DoD Components enable workflows for security events using internal context, past threat events, and other threat intelligence. Approved external sources of enrichment are identified for future integration. These workflows are used to determine incident response procedures.	ZIA ZPA ZDX	<p>Although this activity seems to be by formulating a policy first, Agencies can leverage Zscaler's threat intelligence, Cloud Sandbox reports, and cloud misconfiguration information to enrich incident tickets and quickly respond via Zscaler's automated workflows. Moreover, Zscaler integrates with ITSM capabilities to inform and augment ITSM automation workflows.</p> <p>Zscaler supports integrations with all leading SOAR platforms so that SOC teams can enforce and automate event lookups, reputation checks, blocking actions, and other response activities. SOAR vendors can ingest Zscaler's standardized logs (from engines including firewall, IPS, etc.) and alerts and automate enforcement/threat intel actions via the Zscaler API.</p>
Supports 	6.7.2 Workflow Enrichment Pt2	DoD Components identify and establish extended workflows for additional incident response types. Initial enrichment data sources are used for existing workflows. Additional enrichment sources are identified for future integrations.	ZIA ZPA ZDX	<p>Agencies can leverage Zscaler's threat intelligence, Cloud Sandbox reports, and cloud misconfiguration information as an enriched threat intelligence data source deepen incident response visibility and automate workflows. Moreover, Zscaler supports integrations with all leading SOAR platforms so that SOC teams can enforce and automate event lookups, reputation checks, blocking actions, and other response activities. SOAR vendors can ingest Zscaler's standardized logs (from engines including firewall, IPS, etc.) and alerts and automate enforcement/threat intel actions via the Zscaler API.</p>



Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	6.7.3 Workflow Enrichment Pt3	DoD organizations use final enrichment data sources on basic and extended threat response workflows.		Zscaler's Zero Trust Architecture (ZTA) processes over 300 billion transactions, enforces over 10 billion policies, and blocks over 139 million threats—on average, daily. This feat, Zscaler's active US-CERT and DC3//DCISE partnership, and its 40+ threat intelligence feeds allow agencies to leverage Zscaler's threat intelligence apparatus to enhance the DoD's basic and extended threat intel data sources.
Supports 	6.7.4 Automated Workflow	DoD organizations focus on automating Security Orchestration, Automation and Response (SOAR) functions and playbooks. Manual processes within security operations are identified and fully automated as possible. Remaining manual processes are decommissioned when possible or marked for exception using a risk based approach.	  	Zscaler supports integrations with all leading SOAR platforms (Splunk>Phantom, Demisto, Exebeam, etc.), which help SOC teams enforce and automate event lookups, reputation checks, blocking actions, and other response activities. By delivering a streamlined SOAR and Zscaler workflow, security teams can ensure real-time enforcement of updated and automatable policies for better protection of users, on or off-network. SOAR vendors can ingest Zscaler's standardized logs (from engines including firewall, IPS, etc.) and alerts and automate enforcement/threat intel actions via the Zscaler API.





“ Real-time, Risk-based Response. ZT accelerates the shift from compliance-based to risk-based security approaches as the complexity of threats and vulnerabilities increases. **This acceleration is imperative to address future performance and interoperability expectations** for initiatives such as JADC2.”









—DoD Zero Trust Reference Architecture (ZTRA) 2.0




Automation & Orchestration Pillar 7













Zscaler-DoD Zero Trust Mapping Legend

-  **Partially Meets**
-  **Meets:** Zscaler can meet the activity's requirement without integration with another zero trust ecosystem partner
-  **Supports:** Zscaler integrates with other zero trust ecosystem partners support this activity
-  **Not Applicable:** Activity is centered on DoD policy, not technology-based
-  **Roadmapped:** Current capabilities and features being developed to meet the activities requirement
-  **Zscaler Internet Access:** Secures access to the Internet & SaaS applications; crowd-sourcing threat intelligence & protection powerhouse
-  **Zscaler Private Access:** SDP/ZTNA capability; secures end-to-end user-to-app traffic; resistant to Attacker-in-the-Middle (AitM/MitM)
-  **Zscaler Digital Experience:** Continuously monitors network performance; enhances troubleshooting and visibility to reshape mission network requirements

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	7.1.1 Scale Con-siderations	DoD Components conduct analysis to determine current and future needs of scaling for monitoring, detection, and response. This requires a prioritization plan aligned with component business/mission considerations with associated risk alignment. Scaling is analyzed following common industry best practice methods and is in line with ZT Pillar requirements.	  	<p>As a platform, Zscaler provides intra- and inter-data center redundancy for its production cloud distributed across CONUS cloud service providers and three physical on-premises colocations from three different vendors. In addition, the Zscaler cloud can be extended globally via an on-premises solution that can project the cloud protection to on-premises.</p> <p>This infrastructure foundation allows collection of 150+ tuples of information and over 10 different types of logs that can be streamed and stored for integration into all industry leading SIEM and logging solutions.</p>






Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	7.1.1 Scale Con- siderations	Continued		Continued— Zscaler elastically scales bandwidth and security, enabling Mission Owners (MO) to add new services without performance degradation, even when combined with including processing-intensive services such as 100% SSL/TLS-encrypted traffic deep-packet inspection, URL inspection or when utilizing DLP and a cloud sandbox.
Supports 	7.1.2 Log Parsing	DoD Components identify and prioritize log and flow sources (e.g., Firewalls, Endpoint Detection & Response, Active Directory, Switches, Routers, etc.) and develop a plan for collection of high priority logs first then low priority. An open industry-standard log format is agreed upon at the DoD Enterprise level with the Components and implemented in future procurement requirements. Existing solutions and technologies are migrated to this format on a continual basis.	  	Zscaler logs over 150+ log fields to enable detailed analysis of user and machine traffic; this includes User Web Traffic, Firewall traffic, DNS Traffic, and Device/machine traffic. Zscaler can stream data to a SIEM at the agency's location cannot be tampered with in transit. It supports industry standard formatting such as CSV and JSON. In addition, Zscaler provides granular obfuscation function on a per field basis to suppress PII data, if required.
Supports 	7.1.3 Log Analysis	Enterprise develops common user and device activities. Components identify and prioritized activities based on risk. Activities deemed the most simplistic and risky have analytics created using different data sources such as logs. Trends and patterns are developed over longer periods of time.	 	Zscaler can Integrate with User & Entity Behavior Analytics (UEBA), User Activity Monitoring (UAM), and Privileged Access Management (PAM) solutions to monitor and establish common user and device activities. For example, ZPA integrates with EDRs to observe and create a dynamic risk score that enforces security policies at the mandated risk threshold. Zscaler's Insights, Logs, and Reports assist organizations in continuously monitoring organizational systems and system components for anomalous or suspicious behavior (ZIA) and users, applications, and activities (ZPA). Logging data is automatically forwarded throughout the transaction to the agency's SIEM for further analysis.

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	7.2.1 Threat Alerting Pt1	DoD Components utilize existing Security Information and Event Management (SIEM) solution to develop basic rules and alerts for common threat events (malware, phishing, etc.) Alerts and/or rule firings are fed into the parallel “Asset ID & Alert Correlation” activity to being automation of responses.	 	<p>Zscaler’s Nanolog Streaming Service (NSS) can stream web traffic logs in real-time, enabling real-time alerting. The Zscaler ZTA protects against advanced threats by using multiple inspection techniques for identifying web threats that traditional anti-malware engines wouldn’t typically block. Zscaler ZTA offers native real-time alerting that covers, but not limited to, the following scenarios</p> <ul style="list-style-type: none"> • Incoming Adware/Spyware/Malware/Unscannable • Outgoing Spyware/Malware/Unscannable • Botnet callback • Browser exploit • Chat file transfer • Cross-site scripting (XSS) • Crypto-mining • Custom DLP violation • GLBA/HIPAA/PCI violation • Unscannable files, Malicious content • Patient zero • Peer-to-peer traffic • Phishing, Policy violation • Sandbox activity • Social networking activity • Streaming activity • Suspicious content • Unauthorized communication • URL filtering block, Web spam (Webmail attachment)
Supports 	7.2.2 Threat Alerting Pt2	DoD Organizations expand threat alerting in the Security Information and Event Management (SIEM) solution to include Cyber Threat Intelligence (CTI) data feeds. Deviation and anomaly rules are developed in the SIEM to detect advanced threats.	  	<p>ZIA, ZPA, and ZDX utilize a standardized logging schema, forwarding and integrating with a Mission Owner’s (MO) SIEM to correlate Incident Response and post-mortem activities.</p> <p>Zscaler’s proprietary Single Scan, Multi-Action (SSMA) technology automates global threat intelligence collection and protection organically or absorbed threat intelligence from up to 60+ threat feeds sources.</p>

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	7.2.3 Threat Alerting Pt3	Threat Alerting is expanded to include advanced data sources such as Extended Detection & Response (XDR), User & Entity Behavior Analytics (UEBA), and User Activity Monitoring (UAM). These advanced data sources are used to develop improved anomalous and pattern activity detections.	 	<p>Zscaler's Zero Trust Architecture (ZTA) processes over 420 billion transactions per day, enforces over 10 billion policies per day, and blocks over 139 million threats per day. This feat, Zscaler's active US-CERT and DC3//DCISE partnership, and its 40+ threat intelligence feeds allow agencies to leverage Zscaler's threat intelligence apparatus to enhance the DoD's advanced threat intel data sources to develop improved anomalous and pattern activity detections.</p> <p>Additionally, Zscaler's ZTA leverages APIs to leverage data sources such as UEBA, XDR, and UAM solutions, allowing Zscaler ZTA to develop and adapt to new threats and patterns continuously. Afterward, Zscaler's logs can be streamed back to a SIEM for further analysis and investigation for the next steps.</p>
Supports 	7.2.4 Asset ID & Alert Correlation	All assets in SIEM are identified and correlated to alerts in order to provide security teams with the accurate and detailed information. This information contributes to the incident response speed. Asset ID's also allow better visibility performing vulnerability assessments.	 	Agencies can use Zscaler to respond to common threat events and we are able to stream logs, in near realtime, to industry standard SIEM. This allows the DoD organization to develop further rules for basic asset and alert data.
Supports 	7.2.5 User/Role Baselines	DoD components develop a User/Role Baseline approach based off typical pattern and behavior in activity "Establish User Behavior Pattern" This approach will serve as a benchmark for security when identifying and responding to abnormal malicious activity.	 	<p>Zscaler can synchronize user information from DoD's Global Federated User Directory (GFUD) and incorporate it into Zscaler's policy enforcement verification checks. In addition, all cloud based Identity Provider solutions are supported.</p> <p>Zscaler merges GFUD user attributes, information, and policies derived from EDR, SIEM, and SOAR signals to develop and aggregate user and device baselines and enforce enforce Comply-to-Connect mission policies, dynamic risk-scoring, and provide users conditional access.</p>
Supports 	7.3.2 Establish User Behavior Pattern	Utilizing the analytics tools implemented, user behavior patterns are analyzed to identify patterns and deviations from normality. Techniques in analytics involve machine learning and UEBA.	 	Zscaler's Zero Trust Architecture can integrate with User and device baseline analytic tools. Zscaler can apply this baseline to a set of users. The Zscaler ZTA solution leverages ML functionality to continuously and automatically assess user and device activity against the initial baseline from the Mission Owner's (MO) pre-configured risk profile.

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	7.4.1 Risk Profiling Pt1	Utilizing the baselines developed in the User/ Role Baseline activity, Threat Profiles are created to assess the level of risk for individual users associated to the overall component security.	 	ZIA and ZPA can leverage device posture checks, and Mission Owner (MO) pre-defined device posture profiles are criteria evaluated on devices. ZIA and ZPA policies can be configured based on the outcome of this evaluation. For example, if you specify a file path in a device posture profile, the user can access the application if the user's system has the file specified in the posture profile. Other posture check includes, but not limited to, valid certificate, encrypted disk, etc. The posture profiles can be used for ZIA and ZPA.
Supports 	7.4.2 Baseline & Profiling Pt2	DoD Organizations expand baselines and profiles to include unmanaged and non-standard device types including Internet of Things (IoT) and Operational Technology (OT) through data output monitoring. These devices are again profiled based on standardized attributes and use cases. Analytics are updated to consider the new baselines and profiles accordingly enabling further detections and response. Specific risky users and devices are automatically prioritized for increased monitoring based on risk. Detection and response are integrated with cross pillar functionalities.	 	Zscaler integrates with the Mission Owner (MO) Identity Provider (IdP), no matter enterprise or tactical, to manage BYOD and Internet of Things (IoT) devices. ZIA and ZPA can leverage device posture checks, and Mission Owner (MO) pre-defined device posture profiles are criteria evaluated on devices. ZIA and ZPA policies can be configured based on the outcome of this evaluation. For example, if you specify a file path in a device posture profile, the user can access the application if the user's system has the file specified in the posture profile. The posture profiles are used for configuring access policies in the ZPA Admin Portal and for adding posture profile trust levels for ZIA.
Supports 	7.4.3 UEBA Baseline Support Pt 1		 	Zscaler integrates with the Mission Owner (MO) solutions leverages ML and AI to continuously improve detection and response. ZIA and ZPA can leverage embedded C2C functionality, and Mission Owner (MO) predefined C2C profiles are criteria evaluated on devices. ZIA and ZPA policies can be configured based on the outcome of this evaluation. For example, if you specify a file path in a device posture profile, the user can access the application if the user's system has the file specified in the posture profile. The posture profiles are used for configuring access policies in the ZPA Admin Portal and for adding posture profile trust levels for ZIA.

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	7.4.4 UEBA Baseline Support Pt 2	User & Entity Behavior Analytics (UEBA) within DoD Organizations completes its expansion by using traditional and machine learning (ML) based results to be fed into Artificial Intelligence (AI) algorithms. Initially AI based detections are supervised but ultimately using advanced techniques such as neural networks, UEBA operators are not part of the learning process.	 	Zscaler integrates with the Mission Owner (MO) solutions leverages ML and AI to continuously improve detection and response. ZIA and ZPA can leverage embedded C2C functionality, and Mission Owner (MO) predefined C2C profiles are criteria evaluated on devices. ZIA and ZPA policies can be configured based on the outcome of this evaluation. For example, if you specify a file path in a device posture profile, the user can access the application if the user's system has the file specified in the posture profile. The posture profiles are used for configuring access policies in the ZPA Admin Portal and for adding posture profile trust levels for ZIA.
Supports 	7.5.1 Cyber Threat Intelligence Program Pt1	The DoD Enterprise works with the Components to develop and Cyber Threat Intelligence (CTI) program policy, standard and process. Components utilize this documentation to develop organizational CTI teams with key mission/task stakeholders. CTI Teams gather intelligence from common data feeds across ZT Pillars and aggregate all intelligence to a centralized SIEM.	  	ZIA, ZPA, and ZDX utilize a standardized logging schema, forwarding and integrating with a Mission Owner's (MO) SIEM to correlate Incident Response and post-mortem activities. Zscaler's proprietary Single Scan, Multi-Action (SSMA) technology automates global threat intelligence collection and protection organically or absorbed threat intelligence from up to 60+ threat feeds sources.
Supports 	7.5.2 Cyber Threat Intelligence Program Pt2	DoD Components expand their Cyber Threat Intelligence (CTI) teams to include new stakeholders as appropriate. Threat Intel is analyzed and appropriate actions and controls are enforced across ZT Pillars. Threat Intel Program adapts strategy over time with expansion of threat intel developed in solutions and program maturity.	  	ZIA, ZPA, and ZDX utilize a standardized logging schema, forwarding and integrating with a Mission Owner's (MO) SIEM to correlate Incident Response and post-mortem activities. Zscaler's proprietary Single Scan, Multi-Action (SSMA) technology automates global threat intelligence collection and protection organically or absorbed threat intelligence from up to 60+ threat feeds sources.

Zscaler Alignment	DOD Zero Trust Activity Mappings		Zscaler Platform Core Capabilities	
	Activity ID# and Name	Activity Description	Zscaler Capability	Zscaler Alignment
Supports 	7.6.1 AI-enabled Network Access	DoD Organizations utilize the SDN Infrastructure and Enterprise Security Profiles to enable Artificial Intelligence (AI)/Machine Learning (ML) driven network access. Analytics from previous activities is used to teach the AI/ML algorithms improving decision making.		Independent of 'network access,' Zscaler leverages its embedded AI/ML to allow authenticated users to access authorized DoD applications and resources. Agencies accomplish this granular per user/per application access without exposing the agency's IP network.
Supports 	7.6.2 AI-enabled Dynamic Access Control	DoD Organizations utilize previous rule based dynamic access to teach Artificial Intelligence (AI)/Machine Learning (ML) algorithms to make access decision to various resources. The "AI-enabled Network Access" activity algorithms are updated to enable broader decision making to all DAAS.	 	Other than aggregating attributes and policies from the ZTA environment's analytics, Zscaler combines its embedded AI/ML cybersecurity, device posture checks, and dynamic risk profiling capabilities and AI/ML signals from multiple Policy Decision Points (PDP) capabilities to enforce and apply Just-in-Time/Just-Enough-Access (JIT/JEA) to all accounts, not only high-risk accounts.



About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at [zscaler.com](https://www.zscaler.com) or follow us on Twitter [@zscaler](https://twitter.com/zscaler).

© 2024 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™, Zscaler Digital Experience, and ZDX™, and other trademarks listed at [zscaler.com/legal/trademarks](https://www.zscaler.com/legal/trademarks) are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.