Zero Trust Architecture (ZTA) Vendor Framework Campaign

* Required

Disclaimer:

This Request for Information (RFI) is issued solely for market research purposes and does not represent a commitment to procure, implement, or adopt any specific solution. The technical capabilities described here are comprehensive for evaluation purposes only and may not reflect the organization's current or future infrastructure, architecture, or security environment. Information contained within this RFI should not be used to infer the organization's existing capabilities, controls, or security posture.

Company Information

1. Please provide the company legal name. *

2. Please provide the company address. *

3. If applicable, please provide your Commercial and Government Entity (CAGE) code.

4. If applicable, please provide your North American Industry Classification System (NAICS) code(s).

Point of Contact Information

5. Please provide the name and title of the primary point of contact responsible for this survey response. *

6. Please provide the email address of the primary point of contact responsible for this survey response. *

Solution Overview and Capabilities

7. What is the name of the Zero Trust (ZT) solution you are completing this survey for? *

Please provide information for only one solution per submission. If you would like to provide information for multiple solutions, please complete a separate instance of this RFI survey for each solution.

8. Please provide a brief description of the Zero Trust solution, including its primary purpose, key capabilities, and intended use cases. *

Please enter at most 400 characters

9. Which of the following Zero Trust (ZT) solution categories best describe your solution? (**For definitions and additional context regarding the following categories, please refer to the "General ZTA Reference Architecture" section of the National Institute of Standards and Technology (NIST) Special Publication (SP) 1800-35 supplemental documentation (Web Format):** https://pages.nist.gov/zero-trust-architecture/VolumeB/architecture.html#general-zta-reference-architecture) *

- [ ] Policy Decision Point (PDP) Solution
- [ ] Policy Enforcement Point (PEP) Solution
- [ ] Identity, Credential, and Access Management (ICAM) Solution
- [ ] Endpoint Security Solution
- [ ] Data Security Solution
- [ ] Security Analytics Solution
- [ ] Resource Protection Solution
- [ ] Other

10. Which deployment environments, workloads, or asset types does your Zero Trust solution support? *

- [ ] On-premises infrastructure
- [ ] Private cloud
- [ ] Public cloud
- [ ] Hybrid cloud
- [ ] Multi-cloud
- [ ] Network infrastructure
- [ ] Applications
- [ ] APIs and API gateways
- [ ] Containers and Kubernetes environments
- [ ] Virtual machines
- [ ] Software-as-a-Service (SaaS) applications
- [ ] End-user devices (workstations, laptops, mobile devices)
- [ ] Internet of Things (IoT) devices
- [ ] Operational Technology (OT) / Industrial Control Systems (ICS)
- [ ] Edge computing environments
- [ ] Data and storage resources
- [ ] Identity and directory services
- [ ] Other

Complete this section only if your proposed solution is a PDP and/or a PEP

- The Policy Decision Point (PDP) consists of two logical components: the Policy Engine (PE) and the Policy Administrator (PA). The PE is responsible for making the final decision to grant, deny, or revoke access to a resource for a specific subject based on defined policies and available contextual information. The PA executes the PE's policy decision by sending commands to the PEP to establish and terminate the communications path between the subject and the resource. It generates any session-specific authentication and authorization token or credential used by the subject to access the enterprise resource.
- The Policy Enforcement Point (PEP) protects the trust zone that hosts one or more resources and is responsible for enabling, monitoring, and eventually terminating connections between subjects and resources. It enforces access decisions based on commands received from the PA.

For definitions and additional context, please refer to the "General ZTA Reference Architecture" section of the NIST SP 1800-35 supplemental documentation (Web Format): https://pages.nist.gov/zero-trust-architecture/VolumeB/architecture.html#general-zta-reference-architecture

11. Which of the following functionalities does your solution provide?

- [ ] PDP
- [ ] PEP
- [ ] All of the above

12. If your solution is a PEP solution, which PEP category best describes its primary role within a Zero Trust Architecture?

- [ ] Network PEP – Enforces access policies at the network layer (Layers 3/4). Controls whether a connection can be established between endpoints based on network-level context, such as IP addresses, ports, protocols, and identity. It protects network zones.
- [ ] Application PEP – Enforces access policies at the application layer (Layer 7). Enforces access policies for applications by controlling user access to application resources based on identity, role, authentication status, session context, and application-level policies. it protects applications.
- [ ] API PEP – Enforces access policies for APIs by controlling API authentication, authorization, request validation, rate limits, and API-level access decisions. It protects APIs.
- [ ] Workload/Service PEP – Enforces policies between workloads or services in a distributed application environment.
- [ ] Data PEP – Enforces access policies directly on data assets, such as databases, files, or sensitive information. It protects data.
- [ ] Endpoint PEP – Enforces policies on user or workload endpoints

Complete this section only if your proposed solution is an ICAM solution

Identity, Credential, and Access Management (ICAM) solutions include the strategy, technology, and governance for creating, storing, and managing subject accounts and identity records and their access to enterprise resources. For definitions and additional context regarding the ICAM solution aspects, please refer to the "General ZTA Reference Architecture" section of the NIST SP 1800-35 supplemental documentation (Web Format):
https://pages.nist.gov/zero-trust-architecture/VolumeB/architecture.html#general-zta-reference-architecture

13. If your solution is an ICAM solution, which of the following functionalities does it provide?

- [ ] Identity Management
- [ ] Access and Credential Management
- [ ] Federated Identity
- [ ] Identity Governance
- [ ] Multi-factor Authentication
- [ ] PAM
- [ ] Other

14. If your solution provides Identity Management functionality, which of the following capabilities does it include?

- [ ] Creation and maintenance of Person Entity (PE) identity records that serves as the authoritative source of identity information, including PE roles and attributes.
- [ ] Creation and maintenance of Non-Person Entity (NPE) identity records that serves as the authoritative source of identity information, including PE roles and attributes.
- [ ] Identity lifecycle management, including provisioning, access modifications and maintenance, monitoring, and deprovisioning.
- [ ] All of the above

15. If your solution provides Access and Credential Management functionality, which of the following capabilities does it include?

- [ ] Authentication to verify subject identity
- [ ] Authorization to manage access to resources
- [ ] Grant access in alignment with the principle of least privilege
- [ ] Conditional user access
- [ ] Risk-based conditional access rules that can trigger MFA
- [ ] All of the above

16. If your solution provides Federated Identity functionality, which of the following capabilities does it include?

- [ ] Aggregation and correlation of identity attributes for access authorization
- [ ] Secure cross-domain (federated) access between separate identity domains
- [ ] Reuse of identity data across domains to reduce redundant user administration
- [ ] Support for federated ICAM communities, including non-enterprise identities
- [ ] All of the above

17. If your solution provides Identity Governance, which of the following capabilities does it include?

- [ ] Use of policy-based centralized automated processes to manage user identity and access control functions
- [ ] Other

18. If your solution provides Multi-Factor Authentication (MFA) functionality, which of the following capabilities does it include?

- [ ] Multi-factor authentication using two or more verification factors
- [ ] Enforcement of MFA before granting access to resources
- [ ] All of the above

19. If your solution provides PAM functionality, which of the following capabilities does it include?

- [ ] Privileged account management
- [ ] Credential vaulting
- [ ] Approval workflows for elevated access
- [ ] Just-in-Time (JIT) access
- [ ] Just Enough Access (JEA)
- [ ] Session management
- [ ] Privileged activity monitoring
- [ ] All of the above

Complete this section only if your proposed solution is an Endpoint Security solution

For definitions and additional context regarding the Endpoint Security aspects, please refer to the "General ZTA Reference Architecture" section of the NIST SP 1800-35 supplemental documentation (Web Format): https://pages.nist.gov/zero-trust-architecture/VolumeB/architecture.html#general-zta-reference-architecture

20. If your solution is an Endpoint Security solution, which of the following functionalities does it provide?

- [ ] Endpoint Detection and Response (EDR)/Endpoint Protection Platform (EPP)
- [ ] Unified endpoint management (UEM)/mobile device management (MDM)
- [ ] Continuous diagnostics and mitigation (CDM)
- [ ] Other

21. If your solution provides EDR/EPP functionality, which of the following capabilities does it include?

- [ ] Host firewall Functionality: Preventing unauthorized inbound traffic to endpoints by allowing only explicitly permitted communications, reducing exposure to malware and malicious traffic
- [ ] Malware protection Functionality: Detecting and mitigating malicious software using signature-based or non-signature-based methods (e.g., Machine Learning/Artificial Intelligence (ML/AI)), including quarantining, disabling, and remediating infected files, and providing alerts with remediation and mitigation guidance
- [ ] Vulnerability and threat mitigation Functionality: Identifying vulnerabilities in endpoint software and configurations and providing alerts with recommended remediation and mitigation actions
- [ ] Host intrusion prevention Functionality: Monitoring endpoints for suspicious or malicious activity, blocking or stopping potential intrusions, logging events, alerting stakeholders, and preventing future malicious traffic
- [ ] All of the above

22. If your solution provides UEM/MDM functionality, which of the following capabilities does it include?

- [ ] Endpoint compliance: Ensuring endpoints meet enterprise requirements for approved hardware, firmware, software, and configurations, and do not contain unauthorized components
- [ ] Application protection: Enforcing security policies to protect application data and control how data is accessed and used within applications
- [ ] Data protection enforcement: Ensuring data stored on endpoints is protected in accordance with enterprise security policies
- [ ] All of the above

23. If your solution provides CDM functionality, which of the following capabilities does it include?

- [ ] Collecting information about enterprise assets and their current state
- [ ] Applying updates to enterprise asset configurations and software components to maintain compliance and security posture
- [ ] Providing the policy engine with asset-related information to support access control decisions
- [ ] All of the above

Complete this section only if your proposed solution is a Data Security solution

Data Security includes the policies that an enterprise needs to secure access to enterprise resources, as well as the means to protect data at rest and in transit. For definitions and additional context regarding the Data Security aspects, please refer to the "General ZTA Reference Architecture" section of the NIST SP 1800-35 supplemental documentation (Web Format): https://pages.nist.gov/zero-trust-architecture/VolumeB/architecture.html#general-zta-reference-architecture

24. If your solution is a Data Security solution, which of the following functionalities does it provide?

- [ ] Data Discovery
- [ ] Data Classification, Labeling, and Sanitization
- [ ] Data Encryption
- [ ] Data Integrity Protection
- [ ] Data Availability Protection
- [ ] Data Access Protection and Exfiltration Prevention
- [ ] Auditing and compliance
- [ ] Other

25. If your solution provides Data Discovery functionality, which of the following capabilities does it include?

- [ ] Scanning and Identifying digital assets
- [ ] Identifying and classifying structured and unstructured data assets
- [ ] All of the above

26. If your solution provides Data Classification, Labeling, and Sanitization functionalities, which of the following capabilities does it include?

- [ ] Applying security classifications and labels to data
- [ ] Sanitizing data in accordance with organizational policies
- [ ] All of the above

27. If your solution provides Data Encryption functionality, which of the following capabilities does it include?

- [ ] Data at rest encryption
- [ ] Data in transit encryption
- [ ] Other controls (e.g., watermarking) to prevent unauthorized disclosure or tampering
- [ ] All of the above

28. If your solution provides Data Integrity Protection functionality, which of the following capabilities does it include?

- [ ] Data at rest integrity protection
- [ ] Data in transit integrity protection
- [ ] All of the above

29. If your solution provides Data Availability Protection functionality, which of the following capabilities does it include?

- [ ] Ensuring authorized users can access data when needed
- [ ] Protecting against unauthorized deletion or disruption
- [ ] All of the above

30. If your solution provides Data Access Protection and Exfiltration Prevention functionality, which of the following capabilities does it include?

- [ ] Data Loss Prevention (DLP)
- [ ] Digital Rights Management (DRM)
- [ ] All of the above
- [ ] Other

31. If your solution provides Data Auditing and compliance functionality, which of the following capabilities does it include?

- [ ] Monitoring data security controls
- [ ] Auditing, and reporting on data security controls
- [ ] All of the above

Complete this section only if your proposed solution is a Security Analytics solution

Security Analytics encompasses threat intelligence, security monitoring, and behavioral analytics capabilities across the enterprise environment. It continuously collects and analyzes security-relevant data from users, devices, applications, networks, and other assets to identify threats, detect anomalous or malicious activity, and support incident response. Security analytics outputs may also provide contextual risk information to policy engines, enabling dynamic and risk-based access decisions. For definitions and additional context regarding the Security Analytics aspects, please refer to the "General ZTA Reference Architecture" section of the NIST SP 1800-35 supplemental documentation (Web Format):
https://pages.nist.gov/zero-trust-architecture/VolumeB/architecture.html#general-zta-reference-architecture

32. If your solution is a Security Analytics solution, which of the following functionalities does it provide?

- [ ] Security Information and Event Management (SIEM)
- [ ] Security Orchestration, Automation, and Response (SOAR)
- [ ] Vulnerability scanning and assessment
- [ ] Network Discovery
- [ ] Security Controls Validation
- [ ] Identity Monitoring
- [ ] Security Monitoring
- [ ] Application Protection and Response
- [ ] Cloud Access Permission Manager
- [ ] Cloud Security Analytics and Access Monitoring
- [ ] Network Monitoring
- [ ] Traffic Inspection
- [ ] Endpoint Monitoring
- [ ] Threat Intelligence
- [ ] User Behavior Analytics
- [ ] Firmware Assurance
- [ ] Centralized Management
- [ ] Other

33. If your solution provides Network Discovery functionality, which of the following capabilities does it include?

- [ ] Discover the risk posed by devices, services, and users on the network
- [ ] Classify and asses the risk posed by devices, services, and users on the network
- [ ] All of the above

34. If your solution provides Security Controls Validation functionality, which of the following capabilities does it include?

- [ ] Validation of implemented ZTA cybersecurity controls
- [ ] Other

35. If your solution provides Identity Monitoring functionality, which of the following capabilities does it include?

- [ ] Monitors identities and credentials to detect indicators of compromise, account revocation, and sign-in risks, and generates alerts for suspicious or unauthorized activity.
- [ ] Other

36. If your solution provides Security Monitoring functionality, which of the following capabilities does it include?

- [ ] Monitor and detect malicious or suspicious user and device actions
- [ ] Other

37. If your solution provides Application Protection and Response functionality, which of the following capabilities does it include?

- [ ] Protect applications from phishing attacks
- [ ] Protect applications from spam attacks
- [ ] Protect applications from malware attacks
- [ ] All of the above
- [ ] Other

38. If your solution provides Cloud Access Permission Manager functionality, which of the following capabilities does it include?

- [ ] Provide visibility of permissions used by identities in various cloud services
- [ ] Provide control of permissions used by identities in various cloud services
- [ ] All of the above
- [ ] Other

39. If your solution provides Cloud Security Analytics and Access Monitoring functionality, which of the following capabilities does it include?

- [ ] Monitor cloud resource access sessions for conformance to policy.
- [ ] Other

40. If your solution provides Network Monitoring functionality, which of the following capabilities does it include?

- [ ] Network telemetry collection and aggregation
- [ ] Network traffic analysis and visibility
- [ ] Threat detection through network monitoring
- [ ] On-premises network monitoring
- [ ] Cloud network monitoring
- [ ] Network-based incident detection and response
- [ ] All of the above
- [ ] Other

41. If your solution provides Traffic Inspection functionality, which of the following capabilities does it include?

- [ ] Network traffic interception
- [ ] Network traffic inspection and analysis
- [ ] Traffic logging and recording
- [ ] Deep Packet Inspection (DPI)
- [ ] Metadata-based traffic analysis
- [ ] Policy-based traffic inspection
- [ ] All of the above
- [ ] Other

42. If your solution provides Endpoint Monitoring functionality, which of the following capabilities does it include?

- [ ] Endpoint discovery and inventory
- [ ] Continuous endpoint monitoring
- [ ] Software version monitoring
- [ ] Endpoint configuration assessment
- [ ] Host (devices or virtual machines (VMs)) information collection and analysis
- [ ] All of the above
- [ ] Other

43. If your solution provides Firmware Assurance functionality, which of the following capabilities does it include?

- [ ] Firmware version monitoring
- [ ] Firmware update monitoring
- [ ] Firmware change detection
- [ ] Firmware security monitoring
- [ ] Firmware compliance assessment
- [ ] All of the above
- [ ] Other

44. If your solution provides Centralized Management functionality, which of the following capabilities does it include?

- [ ] Centralized security policy management
- [ ] Centralized security component administration
- [ ] Centralized security configuration management
- [ ] Centralized security component integrity management
- [ ] Centralized distribution and update management
- [ ] All of the above
- [ ] Other

Complete this section only if your proposed solution is a Resource Protection solution

Resource Protection includes technologies that safeguard enterprise resources through monitoring, inspection, access mediation, and policy enforcement. These capabilities may be deployed on-premises or in the cloud and include proxy-based protections, secure access solutions, and secure desktop/workstation technologies. For definitions and additional context regarding the Resource Protection aspects, please refer to the "General ZTA Reference Architecture" section of the NIST SP 1800-35 supplemental documentation (Web Format):
https://pages.nist.gov/zero-trust-architecture/VolumeB/architecture.html#general-zta-reference-architecture

45. If your solution is a Resource Protection solution, which of the following functionalities does it provide?

- [ ] Application Connector
- [ ] Cloud Workload Protection
- [ ] Cloud Security Posture Management
- [ ] Other

46. If your solution provides Application Connector functionality, which of the following capabilities does it include?

- [ ] Provides secure proxy-based access to on-premises resources, enabling access control without exposing the resource directly to the network
- [ ] Provides secure proxy-based access to cloud-hosted resources, enabling access control without exposing the resource directly to the network.
- [ ] All of the above

47. If your solution provides Cloud Workload Protection functionality, which of the following capabilities does it include?

- [ ] Cloud application traffic monitoring
- [ ] Cloud data leakage prevention
- [ ] Cloud workload threat protection
- [ ] Real-time threat detection and alerting
- [ ] All of the above

48. If your solution provides Cloud Security Posture Management functionality, which of the following capabilities does it include?

- [ ] Continually assess the security posture of cloud resources
- [ ] Other

This content is neither created nor endorsed by Microsoft. The data you submit will be sent to the form owner.

Microsoft Forms