strongdm

Infrastructure Access Management

AN RFP CHECKLIST

Managing, securing, and auditing infrastructure access requires an end-to-end set of capabilities that encompasses both legacy and modern stacks. An effective solution must support cloud-native, hybrid, multi-cloud, and on-premises environments across a broad range of resources (e.g., databases, servers, containers, clusters, clouds)—and to do so from a single control plane. Additionally, the ability to preserve DevOps' workflows and to support enterprise-scale workloads are critical.

The following RFP checklist includes requirements spanning several key categories to help you evaluate the vendors under consideration. Think of this checklist as a prescriptive document that can be tailored to fit your company's specific requirements.

Infrastructure Access Management Requirements

DEPLOYMENT

- [ ] The product must be able to support on-premises, hybrid, cloud-native, and/or multi-cloud environments.
- [ ] The product must not require the use of agents on target resources.
- [ ] For on-prem environments, the product must support an automated installer on the organization's standard OS images.
- [ ] For hybrid environments, the product's architecture must support multiple datacenters spanning both private (including on-prem) and public cloud resources.
- [ ] For multi-cloud environments, the product must be fully deployable in AWS, Azure, and/or GCP.
- [ ] The product must be hypervisor-agnostic and not rely on physical or virtual appliances.
- [ ] The product must be container orchestrator-agnostic (e.g., OpenShift, Tanzu).

ARCHITECTURE

- [ ] The product must provide authentication, authorization, connectivity, and auditing capabilities.
- [ ] The product must be built around industry-standard infrastructure, allowing it to be easily scaled and maintained, without the need for vendor's professional services.
- [ ] The product must not rely on non-standard or proprietary components such as non-commercially available databases or network protocols.
- [ ] The product must be able to support a modern infrastructure stack (e.g., modern databases and servers, clusters, containers, cloud platforms, internal web apps, etc.).
- [ ] The product must include components to distribute workloads across an environment.
- [ ] The product must be able to scale easily.
- [ ] The product must support a high-availability architecture.
- [ ] The product must have disaster recovery features.
- [ ] The product must support automatic updates.

AUTHENTICATION

- [ ] The product must have a native integration with an identity provider such as Okta or Azure AD.
- [ ] The product must support an easy-to-use, intuitive scripting framework, which allows application owners to extend credential management functions to technical staff.
- [ ] The product must support federation protocols such as OIDC.
- [ ] The product must support MFA.
- [ ] The product must support UI and CLI interfaces for user authentications.
- [ ] The product must support local authentication & local role-based access control groups.
- [ ] The product must support SSH certificates and password-based authentication for SSH connections on any type of Unix/Linux systems.
- [ ] The product must support seamless integration with existing 3rd-party secrets managers (e.g., HashiCorp Vault, GCP Secret Manager, AWS Secrets Manager) for externalizing credential management.

POLICY MANAGEMENT & WORKFLOWS

- [ ] The product must support a single pane of glass for policy configuration across an entire deployment.
- [ ] The product must support role-based access control (RBAC) policies.
- [ ] The product must support attribute-based access control (ABAC) policies
- [ ] The product must support just-in-time (JIT) access policies.
- [ ] The product must support temporary (i.e., time-based) policies.
- [ ] The product's approval workflows must support optionally validating case/tickets with an external ticketing system during the justification and approval process.
- [ ] The product must support custom ticket system integrations.
- [ ] The product must support account lockouts.
- [ ] The product must be able to enforce segregation of duties (i.e., apply controls based on the type of accounts being used by the end user to access a resource).
- [ ] The product must offer hooks to integrate with external systems such as ticketing systems.
- [ ] The product must support ChatOps platforms to manage access to resources via automated approval workflows (e.g., via Slack, Microsoft Teams, Jira, PagerDuty).

PRIVILEGED SESSIONS

- [ ] The product must support transparently connecting a user from the web portal to a target resource through RDP, SSH, or an application.
- [ ] The product must support monitoring a session without notifying the connected user.
- [ ] The product must support terminating an active user session.
- [ ] The product must provide pre-configured applications for SSH session launching.
- [ ] The product must support launching to sessions without disclosure of the password.
- [ ] The product must support the automatic recording of sessions with and without notification to the user.
- [ ] The product must support offloading recordings to a SAN, NAS, or other network share while still being encrypted.
- [ ] The product must support a configuration where RDP & SSH sessions do not require a "jumpbox" component to facilitate connections.
- [ ] The product must be able to manage and interact with multiple remote sessions for both RDP and SSH in a unified environment.
- [ ] The product must be able to manage multiple sessions active at once, using different connection protocols and a variety of privileged accounts.
- [ ] The product must be able to launch and configure sessions across multiple environments with credentials automatically injected into sessions as needed.
- [ ] The product must not require more hardware or additional licensing for terminal connection features.

NETWORKING

- [ ] The product must support network segmentation capabilities between user segments and other security boundaries that may involve one or two hops between user and target resource network segments.
- [ ] The product must support end-to-end encryption and security protocols (e.g., TLS 1.2 or later) when communicating within the product's components.
- [ ] The product must support remote session management for multiple standard network ports/protocols, including SSH, RDP, HTTPS, UDP, TCP, and several other commerically available databases across multiple cloud and datacenter platforms.
- [ ] The product must support tunneling via OpenSSH.

Section continues on next page →

NETWORKING (cont'd)

- [ ] The product must support concurrent client connections to either the same target resource or a different resource, but each connection/session must be protected and isolated.
- [ ] The product must support "break-glass" access to its components during disaster situations and provide an access path to the target resources.

AUDITING AND REPORTING

- [ ] The product must include a tamper-proof, comprehensive audit of all activities within and against the platform.
- [ ] The product must support the capture of user sessions for user keystrokes and audit events (i.e., the who, what, where, and when of activities).
- [ ] The product must support forwarding logs to any SIEM platform.
- [ ] The product must support keystroke capture for Linux, Unix, and Windows operating systems.
- [ ] The product must support text-based search and allow for export to a CSV file.
- [ ] The product must support centralized audit collection and review.
- [ ] The product must support session recordings (SSH, RDP, Kubernetes, etc.).
- [ ] The product must provide an audit trail for service account workflows and governance enforcement.

SECURITY

- [ ] The product must protect data at rest.
- [ ] The product must protect data in motion.
- [ ] The product must provide a user audit report, enabling admins to see what accounts an offboarded individual interacted with.
- [ ] The product must allow the customer to hold the encryption keys.
- [ ] The product must support zero information disclosure error messages to prevent logs from displaying sensitive information.
- [ ] The product must support configuration to allow for non-standard ports.
- [ ] The product must support a customizable password complexity and rules policies engine.

Section continues on next page →

SECURITY (cont'd)

- [ ] The product must provide a single-pane of glass interface for all access and configurations for all functions (e.g., administration, auditing, reporting, vaulting, access policies, privileged sessions, discovery, and API).
- [ ] The product must not require browser plugins (Flash, Java, etc.) for any function of access, initiation, review, administration, or management.
- [ ] The product's user experience must be the same for all users but only be restricted by roles and permissions to streamline training and adoption.
- [ ] The product's administration and user experience must be intuitive.
- [ ] The product's account segregation must mimic a systems file system explorer to streamline training and adoption.
- [ ] The product's account segregation hierarchy must support an inheritance model for resources and policies.
- [ ] The product must provide ephemeral storage of any Personally Identifiable Information (PII) and remove data automatically once processes are completed.

RESOURCE SUPPORT

- [ ] The product must support major databases types - relational, Key-Value, NoSQL in AWS (RDS, Aurora, RedShift, & EC2), GCP, and Azure cloud platforms.
- [ ] The product must support major databases types, including relational and NoSQL engines hosted on a compute (virtual/physical) resource in a datacenter setting.
- [ ] The product must support a variety of client connections to major databases such as MySQL, Oracle, PostgreSQL, SQL Server, Snowflake, MongoDB, Cassandra, DynamoDB, Aurora, RDS, RedShift, etc. seamlessly.
- [ ] The product must support direct SSH access to containers hosted on Kubernetes clusters.
- [ ] The product must allow for configuration of external web and other services without needing development.

API & SDKs

- [ ] The product must offer an extensive web services API with create, read, update, and delete functions.
- [ ] The product must offer a SDK or programming libraries for inclusion within the source code of internally developed software.

Section continues on next page →

API & SDKs (cont'd)

- [ ] The product's SDK or CLI client audit must be accessible within the platform.
- [ ] The product must provide a SCIM interface/connector for integration into IAM platforms.
- [ ] Workflows must support API calls, both to internal and external REST APIs.
- [ ] The product must offer APIs for externalizing workflows for registration/de-registration of resources and users.
- [ ] The product must offer APIs for monitoring the health of the product.
- [ ] The product must offer APIs for reporting on existing security controls and access controls in the product (policies, administrative controls, who has access to what, number of databases and user accounts).

SLAs

- [ ] The vendor must provide regular, automated software updates.
- [ ] The vendor must provide standard security updates as necessary.
- [ ] The vendor must provide support via a help desk ticketing system.
- [ ] The vendor must provide 24x7x365 support.