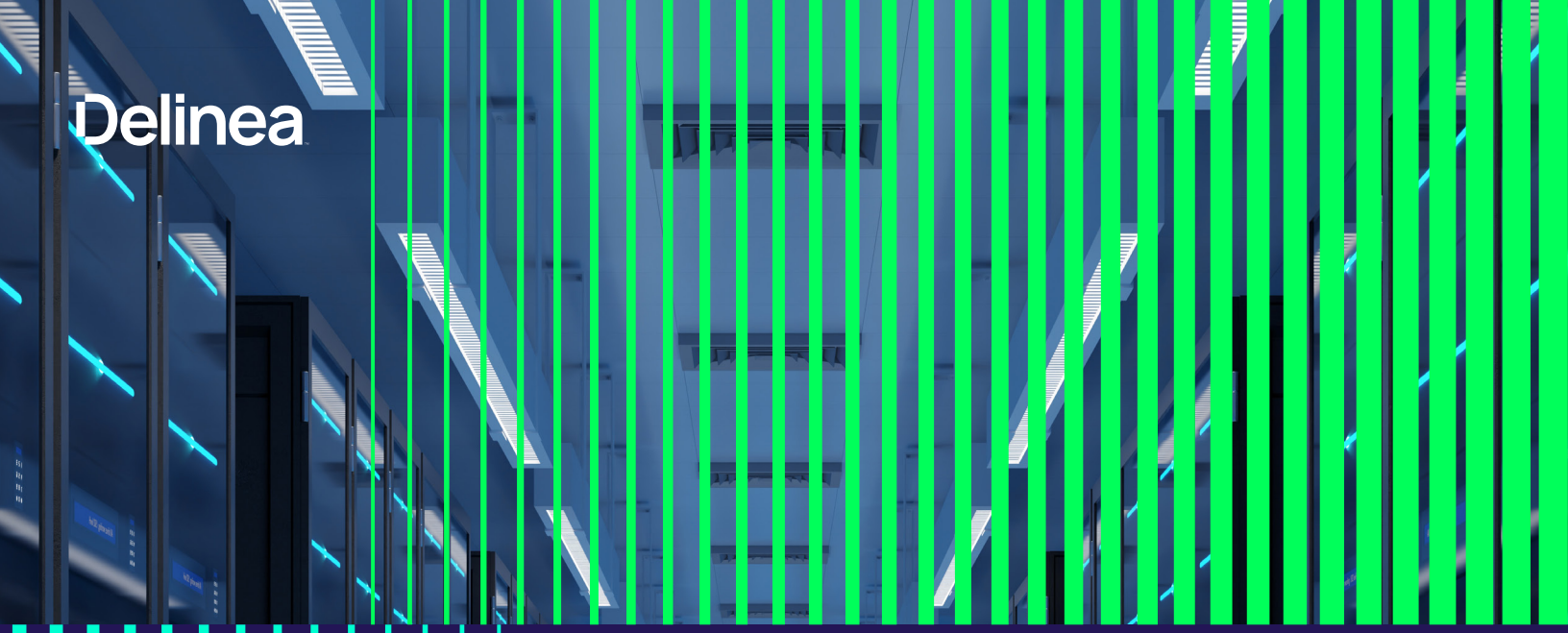
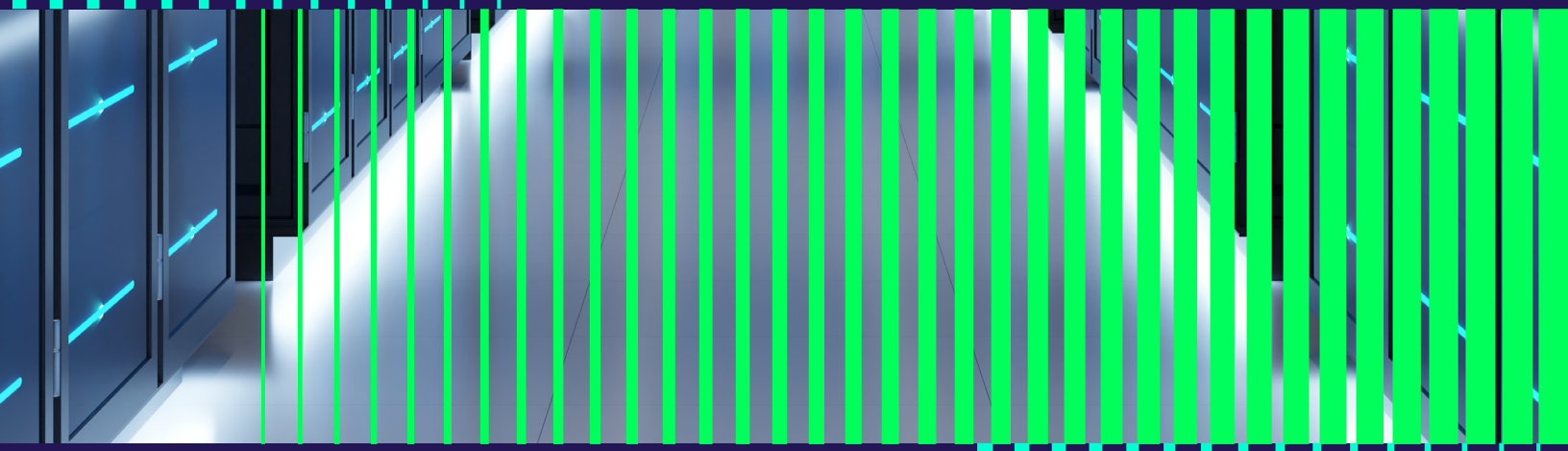
Delinea



Insights into Enhanced Cybersecurity Insurance Requirements

Meeting the demands of cyber risk insurers



WHITEPAPER

Insights into Enhanced Cybersecurity Requirements: Meeting the demands of cyber risk insurers

As cyberattacks continue unabated and the cost of ransomware increases, insurance claim payouts exceed insurance premiums. The insurance industry can't sustain these conditions and is working to right the ship.

In this paper, we explore the state of cyber risk insurance and how insurers react to the current threat landscape. Specifically, we examine more stringent insurer requirements for Privileged Access Management (PAM). Why is PAM so important that it can make or break your ability to get insurance and avoid denied claims and premium hikes?

To stay afloat, providers are more frequently declining coverage and denying claims. But those tactics only go so far if they want to participate in the growing cyber insurance market and satisfy their customers.

That's why providers and brokers are trying to assess risk exposure and help their clients become more cyber resilient by increasing scrutiny and imposing requirements before granting or renewing cyber insurance policies more accurately. The strategy is simple: help clients fortify their defenses to reduce the impact of a cyber incident and lower the number and cost of claims.

For example, detailed ransomware supplemental applications now accompany new business cyber risk insurance applications. When applying for new insurance or a renewal, you might see something like this:

> "This supplemental application must be completed by a Chief Information Security Officer (CISO), or equivalent authorized company representative, that has sufficient oversight of the applicant's information security governance."

Some insurers will probe more deeply than others. Some have built internal cyber risk assessment teams, while others partner with third-party cybersecurity assessors to validate that the appropriate security controls are deployed, operational, and doing their job.

Addressing their requirements isn't a choice. It's a demand that significantly affects your ability to get new insurance, extend an existing policy, and avoid increased premiums.

The challenge for you is knowing what questions insurance providers will pose and what security measures will be required. Unfortunately, there's no industry-wide regulation like HIPAA or PCI-DSS to provide consistency. Rather, in our research of more than a dozen questionnaires, we found many variations because each insurer chooses its path to assess risk. This can make it more difficult for you to navigate the choppy waters.

One cybersecurity practice consistently highlighted as a fundamental requirement in most cyber insurance evaluations is PAM. To contain risk, insurers are mandating that clients have PAM controls, including multi-factor authentication (MFA), password management, access control, privilege elevation, session management, least privilege, and zero trust policies in place, and can demonstrate evidence of their use.

This paper can help you anticipate the questions cyber insurance providers and brokers will likely ask and demonstrate the necessary security controls to prevent denials in coverage or claims, increased premiums, and delays in coverage.

How Privileged Access Management reduces cyber risk

Contrary to Hollywood storylines, cyberattacks are rarely carried out by legions of highly sophisticated coders who have gone rogue. Reality paints a very different picture: cyber adversaries apply simple tactics, techniques, and procedures — often called TTPs — to pursue the weakest link in the attack chain, leveraging tactics such as password theft, phishing, and ransomware.

Thus, implementing an effective enterprise cybersecurity strategy requires understanding TTPs and basic cyber hygiene, including PAM. Compromised privileged identities are the most common cause of data breaches, making securing privileged access critical to reducing risk.

At a high level, PAM is an identity-centric solution to this problem. It reinforces best practices like the Principle of Least Privilege, Zero Trust, and zero standing privileges. The essential moving parts to PAM include:

- A **credential and secrets vault** to strictly control access to privileged accounts, SSH keys, API keys, and DevOps secrets and manage login sessions to servers and network devices.
- **Workstation protection** and application control.
- **Server protection** and privileged application/ command elevation.
- Supporting PAM capabilities, including **multi-factor authentication (MFA), just-in-time access request workflows**, and **behavioral analytics.**

Meet and exceed cyber insurance requirements with Delinea

Delinea makes security seamless for the modern, hybrid enterprise. Our industry-leading PAM solutions empower organizations to secure critical data, devices, code, and cloud infrastructure to help reduce risk, ensure compliance, and simplify security.

The next chapter references Delinea PAM products. Below is a short description of each one. Click on the links to open product pages on our website for more detailed information.

Protect Privileged Access	Secure Endpoints and Devices	Enable Remote Work
Secret Server Discover, manage, protect, and audit privileged account access.	**Server PAM** Manage identities and policies on servers.	**Connection Manager** Monitor, record, and control privileged sessions.
Privileged Behavior Analytics Detect anomalies in privileged account behavior.	**Privilege Manager** Manage workstation privileges with application control.	**Remote Access Service** Secure remote access for vendors and third parties.
Account Lifecycle Manager Discover, secure, provision, and decommission service accounts.		
DevOps Secrets Vault Manage credentials for applications, databases, CI/CD tools, and services.		

The mapping below aggregates requirements from insurance questionnaires sourced from public-facing documents and information provided by insurance companies and brokers (see Appendix). We have organized requirements according to common cybersecurity categories. You'll see how PAM capabilities and Delinea products satisfy each requirement.

One final note before you dig in: be aware of other areas that insurers may turn to next. While today their eyes are focused almost exclusively on the human identity side of the risk equation, non-human service accounts may be next in the spotlight. The **Cyber Insurance Academy** warns that:

> "…this developing cyber risk should concern all insurance professionals, but cyber underwriters must be especially aware of the implications that poorly managed service accounts could have on a policy."

In anticipation, Delinea **Account Lifecycle Manager** has you covered.

Use Case	Questions	How Delinea Helps
Access Control	Procedures ensure authorized user access and prevent unauthorized access to systems and services.	Delinea PAM security controls ensure that access and privilege are allowed only to authorized users specified in Delinea PAM policies. They encompass log in, MFA, privilege elevation, application access, and Secret access as follows: • Server Suite: Dictate who can log in to the vault, what they can view, and what secrets they can access (for example, a Windows Administrator password Secret used for brokered login to a Windows server in AWS) • Server PAM: Dictate who can log in directly to a Windows, Unix, or Linux server and what privileged commands and applications they can run. • Privilege Manager: Dictate who can log in to a workstation and what privileged commands and applications they can run. • DevOps Secrets Vault: Dictate who can access DevOps secrets and secure access to DevOps tools. You can also tie PAM policies to service accounts.
Access Control	Establish granular policies for privilege elevation.	Delinea Server PAM and Delinea Privilege Manager enforce elevation policies on servers and workstations. The security controls these solutions provide are local at the operating system level. Centralized PAM policies are granular, addressing login, elevation, and MFA.
Access Control	Ensure all connections required for privileged operations are mutually authenticated with cryptographic credentials.	Delinea Server PAM uses a server-resident client to enroll the server in the Delinea Platform and enable mutual authentication between the server and the Platform. Cryptographic credentials ensure they can mutually authenticate to mitigate the risk of a rogue server attempting to access the Delinea Platform or a rogue entity trying to supply the server with unsanctioned PAM policies to facilitate a breach.
Access Management	Eliminate local accounts via identity consolidation for Unix and Linux.	A best practice for Delinea Server PAM is identity consolidation. This requires eliminating additional individual privileged accounts typically created by administrators locally on servers (primarily Linux and Unix). It ensures administrators have only one individual account used for privileged activities (either their enterprise account or a secondary "alternative admin" account.) The result is better enforcement of the least privilege, attack surface reduction, and full accountability of privileged activities tied to a single user. For local accounts that can't be eliminated (for example, "root" or 3rd-party application accounts), Delinea Server PAM can migrate local accounts to Active Directory for centralized management, and/or Delinea Secret Server can vault the accounts to control who can access them and to rotate the passwords on a schedule.
Access Management	Domain Administrator Accounts are managed and monitored through just-in-time access, are time bound, and require approvals to provide privileged access.	Delinea best practice is that you protect domain administrator account passwords in the Delinea Secret Server vault and control access to them. Admins can request break-glass emergency access via self-service workflow. If approved, access is granted for a limited time, automatically deprovisioned when the time expires (or via manual check-in).

Use Case	Questions	How Delinea Helps
Access Management	Role-based access controls have been implemented to assign access based on a user's specific job duties or business needs (users should not have access rights or functions that do not directly relate to their job).	Delinea PAM solutions support Role-Based Access Controls to assign access based on a user's job duties or business needs. Since Delinea PAM also embraces the Principle of Least Privilege, requests for elevated rights are constrained to only the permissions necessary for the task, i.e., not elevating to full administrative rights. Organizations can adjust roles and privileges via third-party IGA solutions such as SailPoint, with changes pushed to Delinea PAM.
Access Management	Access rights must be revoked in a timely manner for terminated employees.	Delinea PAM centralizes the administration of access and permissions. If you terminate an employee, you can revoke access immediately or constrain access to a subset of resources if the employee continues to work off a notice period.
Access Management	Is VPN-less secure access supported for remote users?	Delinea Secret Server supports several secure remote access methods, including SSH and RDP clients and browser-based (VPN-less). The latter is ideal for vendor access, avoiding the risks associated with VPNs, such as limited granular access controls, physical network attachment, virus and malware exposure, and exposure to the broader target network.
Access Management	Virtual Private Network (VPN) connections require Multi-Factor Authentication (MFA).	Delinea's best practice is to not use VPNs for remote access to mitigate risks such as limited granular access controls, physical network attachment, virus and malware exposure, and exposure to the broader target network. If using VPNs for remote access, Delinea PAM can augment any native VPN-level MFA by enforcing MFA at the server level to help mitigate the risk that a threat actor uses a valid credential to fly under the radar. Delinea Server PAM can enforce MFA at login or when users try to elevate rights to run privileged applications or commands and move laterally.
Access Management	Do you have remote desktop protocol (RDP) connections?	Delinea Secret Server strictly controls who can establish RDP sessions to Windows servers. The RDP sessions can be end-to-end, i.e., initiated by a user running an RDP client (such as Microsoft Remote Desktop) on their workstation or tunneled through a browser (for VPN-less remote access). To further reduce risk, you can enforce MFA at login to Delinea Secret Server to prevent access to a threat actor with a valid (compromised) credential. You can also enforce MFA with Delinea Server PAM at the Windows server operating system level, during login, and during privilege elevation when attempting to run a privileged application or command.
Access Management	Do you have secure shell protocol (SSH) connections?	Delinea Secret Server controls who can establish SSH sessions to Windows servers. The RDP sessions can be end-to-end, i.e., initiated by users running an RDP client (such as PuTTY) on their workstation or tunneled through a browser (for VPN-less remote access). To further reduce risk, you can enforce MFA at login to Delinea Secret Server to prevent access to a threat actor with a valid (compromised) credential. You can enforce MFA using Delinea Server PAM at the Linux and Unix server operating system level, during login, and during privilege elevation when attempting to run a privileged application or command.

Use Case	Questions	How Delinea Helps
Access Management	Remote administration of systems is performed over secure channels.	Remote login sessions initiated via Delinea Secret Server are over secure SSH, RDP, or HTTPS channels.
Access Management	Expand remote access control to vendors and contractors without creating AD accounts.	Delinea Secret Server can link (federate) a user's identity in an external Identity Provider (IdP) via SAML. Once authenticated to their local IdP (such as Microsoft Active Directory Federation Services), the external user can single-sign on to Delinea Secret Server without requiring an Active Directory account at the Service Provider.
Access Management	Does the applicant support federated login (i.e., SAML) for remote access?	Delinea Secret Server can link (federate) a user's identity in an external Identity Provider (IdP) via SAML. Once authenticated to their local IdP (such as Microsoft Active Directory Federation Services), the external user can single-sign on to Delinea Secret Server without requiring an Active Directory account at the Service Provider. Delinea Secret Server supports unlimited federated partnerships.
Access Management	Establish a secure administrative environment for both local and remote sessions.	Delinea Secret Server's Remote Access Service supports VPNless remote sessions. Thus, the user workstation is not network-attached (as would be the case with a VPN connection), resulting in a "clean source" secure administrative environment that prevents any viruses or malware from spreading.
Access Management for Service Accounts	Service account provisioning and deprovisioning are managed.	Delinea Account Lifecycle Manager manages non-human privileged accounts used by applications and services. This solution provides complete lifecycle management, including discovery, provisioning, delegation, and decommissioning. Account Lifecycle Manager is a cloud-native service. It integrates with Active Directory and Azure Active Directory. It integrates with Delinea Secret Server for account credential vaulting and scheduled password rotation without service interruption.
Access Management for Service Accounts	There is a process in place to review the current requirements for each service associated with privileged service accounts to verify the service still requires the permissions the service account has (and deprivilege if not).	Delinea Account Lifecycle Manager templates support review/expiration periods for service accounts. A re-approval setting will result in the Account Owner (and, optionally, a configured System Administrator) being notified of password expiration and having the option to re-approve, adjust settings, or deprovision the service account.
Account Classification	Discover, classify, and manage local accounts, servers, Groups, roles, and security configuration files that might grant privileges across all assets.	Delinea Secret Server, Privilege Manager, and Account Lifecycle Manager solutions can automatically find AD machines, AD and Azure AD user accounts, local Windows accounts, Group Managed Service accounts, dependencies on an AD domain, VMware ESX/ESXi, AWS Access Keys, AWS Console Accounts, Google Cloud Platform (GCP) service accounts and VM instances, Unix machines, Unix non-daemon accounts, and Unix local accounts. Delinea's Extensible Discovery allows custom scanners to be written in PowerShell to discover additional accounts and dependencies not addressed by the built-in scanners.

Use Case	Questions	How Delinea Helps
Account Classification	Discover and classify service accounts. Implement service account discovery, provisioning, and governance across identity and cloud service providers.	Delinea Secret Server, Privilege Manager, and Account Lifecycle Manager can discover and vault Active Directory, Azure Active Directory, or Group Managed Service accounts using predefined workflow templates. You specify owners and attributes during the discovery process. Administrators can set attribute values to update in Active Directory/ Azure AD or leave the values blank so they inherit the values already present. You can assign owners per account or the same group of owners to all accounts. Users and groups can be added or removed from the account.
Application Control	Applicant implements application controls across workstations to only allow for the execution of authorized applications. Unauthorized applications are blocked.	Application Control in Delinea Privilege Manager allows administrators to manage all application activity on workstation endpoints. Privilege Manager can automatically elevate trusted applications and block untrusted or malicious applications.
Approval Workflow	Initial user access to systems is approved by the manager, or delegate, who is responsible for the system and correlated data (i.e., the "System Owner").	You can configure PAM policies through Delinea UIs or push to Delinea PAM via third-party integration. For example, access request and approval workflows in an Identity Governance and Administration (IGA) solution such as SailPoint with approved changes pushed to Delinea. Issue access requests and use multi-step approval workflows via: • Secret Server: request access to secrets. • Server PAM: request access to log in to a server and elevate privilege. • Privilege Manager: request approval to elevate privilege.
Approval Workflow	Integration with ITSM to drive access control request workflows tied to help desk tickets.	Although we have built access request/approval workflows into Delinea Secret Server, customers can use ServiceNow as an alternative workflow. Using the ServiceNow catalog, they can request access for a limited time. Approvers can review requests and approve or deny them from within ServiceNow. If an approver grants a request, ServiceNow interacts automatically with Delinea PAM to adjust roles and permissions as necessary. Delinea Secret Server will automatically revoke incremental permissions once the time limit has expired.
Auditing and Reporting	Integrate with User and Entity Behavior Analytics tools (UEBA).	Delinea Secret Server can integrate with UEBA solutions such as IBM QRadar and Splunk.
Auditing and Reporting	Systems are configured to issue a log entry and alert when an account is added to or removed from a domain administrators' group or when a new local administrator account is added on a system.	Delinea Server PAM and Delinea Privilege Manager control who can elevate privilege to add a new local admin account to a server or workstation. Server PAM logs these actions and can generate alerts. Adding or deleting a user from a domain administrator group requires administrative rights and can also be controlled by these Delinea solutions. Delinea Server PAM will log approved actions (e.g., via access request approval workflow.)

Use Case	Questions	How Delinea Helps
Auditing and Reporting	Systems are configured to issue a log entry and alert on any unsuccessful login to an administrative account.	Successful or unsuccessful login attempts are logged by: • Delinea Secret Server: when logging into Secret Server • Delinea Server PAM: when logging into a Windows, Linux, or Unix server or Linux workstation • Delinea Privilege Manager: when logging into a Windows workstation
Auditing and Reporting	Logging and monitoring is in place for changes to existing user accounts (e.g., password reset, modification to access levels or groups, etc.).	Delinea PAM solutions log any changes to user accounts. Delinea PAM can forward logged events to a SIEM solution such as Splunk for monitoring and alerting.
Auditing and Reporting	Logging and monitoring are in place for the creation of new user accounts and associated access permissions assigned.	Delinea PAM logs the creation of new user accounts performed by Delinea PAM Solutions. Delinea PAM can forward logged events to a SIEM solution such as Splunk for monitoring and alerting.
Auditing and Reporting	Does your firm monitor user accounts to identify and eliminate inactive users?	Formal management is typically a function of your Identity Management solution, such as Active Directory. However, you can also monitor privileged accounts vaulted in Delinea Secret Server and service/application accounts managed by Delinea Account Lifecycle Manager.
Auditing and Reporting	Logs are sent to a centralized logging system, such as a SIEM.	Delinea PAM maintains events centrally for reporting and alerting. It can also forward events to a Syslog server or a third-party SIEM solution such as Splunk, Microsoft Sentinel, and Exabeam Fusion.
Auditing and Reporting	Functionality or procedures have been implemented to ensure event/audit entries are not overwritten prior to backup or other archiving. This includes properly sizing of audit log files and storage space to ensure events are not overwritten.	Delinea provides customers with recommendations on audit log sizing, rotation, and disk requirements to ensure events are preserved for the required amount of time. By default, Delinea PAM does not delete any audit data.
Auditing and Reporting	Enforce host-based session, file, and process auditing with integration to SIEM.	Delinea Server PAM captures all administrative and privileged activity events centrally for reporting and alerting. It can also forward events to a Syslog server or a third-party SIEM solution such as Splunk. Delinea Server PAM captures events and records sessions locally on each host server to ensure visibility and granularity (capturing at the process/shell level). Local event data is forwarded securely to the Delinea Server PAM Audit Collector, where events and sessions can be centrally audited, queried, and reviewed. Delinea Advanced Monitoring can also watch for file modifications and command execution (directly or in scripts) of particular interest.

Use Case	Questions	How Delinea Helps
Auditing and Reporting	Leverage audit data, machine learning, behavioral analytics, and automation to detect, track, and alert to threats.	Delinea Privileged Behavior Analytics is a behavioral baselining and analytics solution that uses machine learning to detect anomalous activity. It warns of potentially malicious activity by comparing actions against a behavioral norm for accounts established over time, with continuous adjustment. It requires no external connectors, is low maintenance, serverless at the back end, and consumed as a SaaS service, so the customer is spared the high compute demands to run the algorithms.
Auditing and Reporting	Implement real-time session recording and security access control policies for server endpoints.	Server login sessions can be initiated through the Delinea Secret Server or via direct login to servers. In either case, Delinea PAM can capture privileged session activity. In the former, session activity is recorded by Delinea Secret Server as a proxy. In the latter, session activity is recorded at the server operating system level by Delinea Server PAM. Security access controls for servers are provided by Delinea Server PAM, with the controls residing on each host. Security access controls for workstation endpoints are provided by Delinea Privilege Manager, with the controls residing on each workstation.
Auditing and Reporting	Applicant monitors for unauthorized remote access to "Vital Assets."	A Delinea best practice for remote access to internal resources is central session management via Delinea Secret Server. Secret Server has complete control and visibility if you initiate all remote sessions from here. Role-Based Access Control policies prevent users from seeing assets (passwords, secrets, and server resources) they're not authorized to view. All access to the remainder - authorized assets - is logged. Login sessions to servers can also be recorded for subsequent review or monitored in real-time.
DevSecOps	Automate privilege security in DevOps workflows and tooling.	With Delinea DevOps Secrets Vault, you can manage credentials for applications, databases, CI/CD tools, and services.
DevSecOps	Remove hard-coded credentials and config data from applications and scripts.	Plaintext credentials and configuration data embedded in code increase the breach risk. With Delinea DevOps Secrets Vault, you can instead secure this information inside the Delinea Secret Server vault. Developers can then replace the sensitive data with API calls to programmatically obtain the data at run-time versus being exposed on disk.
Identity Management	Internal systems use an approved centralized identity/single sign-on solution such as Active Directory or OKTA.	Several on-premise and cloud directories, including Active Directory, OpenLDAP, Okta, Ping, or Azure AD, can be accessed by Delinea Secret Server, Delinea Server PAM, and Delinea Privilege Manager to authenticate a user during login to the vault, workstation, and Windows, Linux, or Unix servers.
Identity Management	Does the Applicant use Microsoft Active Directory for directory services, identity providers (IdP), federation, and/or rights management?	Delinea Secret Server, Server PAM, and Privilege Manager can use Microsoft Active Directory as an IdP, allowing users to log in with their AD account. Delinea PAM can also authenticate external users logging into Delinea Secret Server via SAML-based federated login such as Active Directory Federation Services (ADFS).

Use Case	Questions	How Delinea Helps
Identity Management	Prohibit privileged access by any client system that isn't known, authenticated, properly secured, and trusted.	A Delinea best practice is configuring Delinea Secret Server as the only trusted launch point for server access. As such, its Role-Based Access Controls ensure that the only servers visible to administrators are known and secured with Delinea Server PAM. Deploying Delinea Server PAM on a server establishes a trust relationship with the Delinea Platform. Once logged into a server, Delinea Server PAM can prevent users (or adversaries) from moving laterally to known or unknown servers (e.g., shadow IT or adversarial servers).
Incident Response	What steps are you taking to detect and prevent ransomware attacks?	A ransomware assault can be avoided, detected, and stopped by Delinea PAM. Since the ransomware attack chain includes numerous touchpoints, including workstations, servers, domain controllers, network devices, end users, administrators, and supply-chain partners, Delinea's ransomware prevention is multi-layered. Delinea Secret Server protects access to privileged account credentials and secrets and supports secure remote access sessions. Delinea Server PAM prevents lateral movement and safeguards access to Windows, Linux, and Unix servers on-premise or in the cloud. Delinea Privilege Manager focuses on protecting access to user workstations and application control. The Delinea Platform provides shared services to them all, such as session recording, MFA, and behavioral analytics. Example capabilities include: • Consolidating identities and vaulting shared privileged accounts for emergencies to decrease the attack surface. • Enforcing the Principle of Least Privilege ensures that any compromised credential has minimum rights and that no one can advance vertically or laterally. • Using Privileged Behavior Analytics to deny access, enforce MFA, or notify IT Security when ransomware-related behavior is abnormal for the account. • Application control to stop privileged programs from running. • Workflows for access requests to allow privilege elevation only for authorized users and tasks.
Incident Response	How is privileged activity logged and suspicious activity identified?	All Delinea PAM products capture privileged activity in log files. Also, Delinea Secret Server can record interactive login sessions at the proxy level, and Delinea Server PAM can record at the server operating system level for more granularity. You can use these events and session recordings detectively to report suspicious activity. You can also feed events to external Security Information and Event Management (SIEM) solutions such as Splunk for intel enrichment, correlation, and near real-time alerting. Delinea Privileged Behavior Analytics can detect activity that is abnormal for the account. Based on a computed risk score, access can be allowed, denied, or challenged with a second factor.
Least Privilege	Access to a system is authorized only if based upon legitimate business need for access and the least amount of access needed to perform job duties (i.e., "Least Privilege" access).	Delinea PAM supports Role Based Access Controls (RBAC) and the Principle of Least Privilege, allowing just enough access to be defined based on job function. You can assign permanent roles to users and grant temporary access just-in-time via self-service access request/approval workflows. Issue access requests and use multi-step approval workflows via: • Secret Server: request access to secrets. • Server PAM: request access to log in to a server and elevate privilege. • Privilege Manager: request approval to elevate privilege.

Use Case	Questions	How Delinea Helps
Least Privilege	Establish just-in-time, just-enough privileges.	Delinea PAM supports the Principle of Least Privilege. Incremental rights (for example, to log in to a server or elevate privileges to run a privileged application or command) can be requested just in time by the user. Upon approval, Delinea PAM provisions additional roles/rights to satisfy the need without overprovisioning (i.e., just-enough privileges vs. unfettered rights). Issue access requests and use multi-step approval workflows via: • Secret Server: request access to secrets. • Server PAM: request access to log in to a server and elevate privilege. • Privilege Manager: request approval to elevate privilege.
Least Privilege	No user's regular, everyday account is in the Administrator's group or has local admin access to their workstation.	Delinea best practice is that you protect local admin account passwords in the Delinea Secret Server vault, and you control access to them. Admins can request break-glass emergency access via self-service workflow. With Delinea Privilege Manager, You can set PAM policies to define which accounts (if any) are members of any local groups (including local Administrators). Delinea PAM can automatically reverse any unsanctioned changes to group membership.
Least Privilege	Do any of the Applicant's users have persistent administrative access to servers and/or workstations other than their own?	Delinea best practice is to enforce the Principle of Least Privilege, which includes removing standing privileges (persistent administrative access). Delinea Server PAM and Delinea Privilege Manager controls enforce such policies on servers and user workstations.
Least Privilege	The number of privileged user accounts has been limited to the bare minimum needed to support the system and is based upon a clear business need (i.e., the Principle of Least Privilege)	Delinea best practice is to eliminate all unnecessary privileged user accounts ("identity consolidation") to reduce the attack surface. Admins have a single, low-privilege enterprise account used to log in everywhere. They can request elevated rights just in time, for a limited time, to perform sanctioned activities that require elevated privileges. The Delinea Platform can support several Identity Providers to authenticate users, such as Active Directory and OpenLDAP on-premise and cloud directories, such as Azure AD, Google Cloud Directory, Ping Directory, and Okta.
Least Privilege	Generic and/or test accounts must not be created or enabled on production systems, unless specifically authorized by the relevant information asset owners.	By enforcing the Principle of Least Privilege, Delinea PAM ensures that users cannot create new accounts on production systems unless granted elevated rights through explicit access request/approval workflow. On workstations, Delinea Privilege Manager enforces this. On servers (on-premise or cloud-hosted instances,) Delinea Server PAM enforces this.
Least Privilege	Active Directory administrator accounts and local administrator accounts are only used to perform administrative functions.	The Delinea Secret Server vault stores and strictly control access to passwords for Active Directory administrator and local admin accounts. Admins can use self-service workflow to request break-glass access. Delinea PAM aligns with the Principle of Least Privilege to ensure administrators log in using their enterprise account and request enhanced rights on a case-by-case basis rather than utilizing unrestricted administrator accounts.

Use Case	Questions	How Delinea Helps
Least Privilege	Segregation of duties (SOD) has been analyzed and implemented for operation and support of the application to guard against an independent malicious actor's ability to circumvent security controls and commit fraud.	Delinea Secret Server's Folders and Roles and Server PAM's patented Zone Technology simplify permission management and the separation-of-duties security model. They allow customers to manage access and define a custom governance model.
MFA	Processes are in place to detect and respond effectively to suspicious or anomalous logins. An example of an acceptable control is prompting the user for out-of-band authentication when a logon is attempted from an unregistered device.	Delinea PAM supports static and dynamic policies to control access. You can manually create static policies to identify specific users and specific conditions. Dynamic policies leverage Delinea Privileged Behavior Analytics and machine learning to compare a user's historical behavior to the current state. In this way, Privileged Behavior Analytics can recognize abnormal activity, allowing (for example) Delinea PAM to enforce MFA policies to assure the user's identity.
MFA	Is MFA required to access the vault?	Delinea MFA policies are optional and can be enabled in Delinea Secret Server to enforce MFA on login to Secret Server.
MFA	Is MFA required to check out a vaulted secret?	Delinea MFA policies are optional and can be enabled in Delinea Secret Server to enforce MFA when checking out a vaulted Secret in Secret Server.
MFA	Is MFA required to log in to a server directly?	Delinea MFA policies are optional and can be enabled in Delinea Server PAM to enforce MFA when logging directly into a Windows, Linux, or Unix server.
MFA	Is MFA required to log in to a server indirectly via a vault proxy?	Delinea MFA policies are optional and can be enabled in Delinea Secret Server to enforce MFA when a login session is established indirectly via Delinea Secret Server.
MFA	Is MFA required to run a privileged application or command on a workstation?	Delinea MFA policies are optional and can be enabled in Delinea Privilege Manager to enforce MFA before elevating privilege to run privileged applications on Windows workstations and similarly in Delinea Server PAM for Linux workstations.
MFA	Is MFA required to run a privileged application or command on a server?	Delinea MFA policies are optional and can be enabled in Delinea Server PAM to require MFA before elevating privilege to run a privileged application or command on Windows, Unix, or Linux servers.
MFA	Is MFA required to log in to a server directly?	Delinea MFA policies are optional and can be enabled in Delinea Server PAM to enforce MFA when logging directly into a Windows, Linux, or Unix server.
MFA	Is MFA required to log in to a server indirectly via a vault proxy?	Delinea MFA policies are optional and can be enabled in Delinea Secret Server to enforce MFA when a login session is established indirectly via Delinea Secret Server.

Use Case	Questions	How Delinea Helps
MFA	Is MFA required for administrator and privileged access	You can set Delinea Server PAM and Delinea Privilege Manager to require MFA for administrator/privileged access (login) and privilege elevation across all managed servers and workstations, respectively. You can also enable MFA at Secret Server login and when admins access vaulted secrets.
MFA	Authenticator Assurance Levels (AAL) 1, 2, and 3 are supported for login (NIST Special Publication 800-63B).	With Delinea Platform "Authentication Profiles," you can configure the authentication challenges allowed by Delinea Secret Server during vault login and Secret access and by Delinea Server PAM during server login and privilege elevation. You can configure one or two challenges, plus a variety of second factors. These include the Delinea mobile authenticator, phone call, text message confirmation code, email confirmation code, OATH OTP client, third-party RADIUS authentication, and FIDO2 authenticator. Thus, you can configure authentication profiles solely using NIST AAL1, AAL2, or AAL3 second factors.
Password Management	Privileged user accounts and/or passwords are unique to each user (user accounts are not shared amongst users, and duplicate user accounts are not accepted by the system).	Privileged user accounts are vaulted and managed by Delinea Secret Server. To maintain good complexity and uniqueness and avoid re-use, password rotation policies use quality of service rules to change the passwords on a set timetable automatically.
Password Management	System administrators at the Applicant have a unique, privileged credential for administrative tasks (separate from their user credentials for everyday access, email, etc.).	Delinea PAM supports an alternative admin (or "dash-a") account model, where administrators have two accounts. One is their "business card" account, which is visible to the public and used for normal end user activities like email. They are assigned minimum rights to align with zero standing privileges. Through Delinea Server PAM, admins can request temporarily elevated rights just-in-time for the dash-a account via a self-service request workflow.
Password Management	Shared privileged service account passwords are frequently rotated.	Delinea Account Lifecycle Manager discovers, secures, provisions, and deprovisions Microsoft Windows service account passwords. Delinea Secret Server automatically vaults discovered accounts and can apply password rotation policies.
Password Management	Privileged Service Accounts have password lengths of at least 8 characters.	Delinea Account Lifecycle Manager discovers, secures, provisions, and deprovisions Microsoft Windows service account passwords. Delinea Secret Server automatically vaults discovered accounts and can apply quality of service policies, including password length.
Password Management	User account passwords meet minimum password length requirements.	Delinea Secret Server is used to vault privileged user accounts and assume management. Password rotation policies can automatically change the passwords on a schedule and apply quality of service rules to ensure appropriate complexity and uniqueness and prevent re-use.
Password Management	Passwords are not re-used frequently. System prevents the re-use of the last X passwords.	Privileged user accounts are vaulted and managed by Delinea Secret Server. To maintain good complexity and uniqueness and to avoid re-use, password rotation policies can use quality of service rules and automatically change the passwords on a set timetable.

Use Case	Questions	How Delinea Helps
Password Management	User accounts are automatically locked by the system after 3 unsuccessful password attempts.	User account policies, such as locking accounts after failed login attempts, are a function of the underlying Identity Management system, such as Active Directory.
Password Management	Accounts remain locked until reset by an authorized system administrator or reset through an approved self-service password reset function.	User account policies, such as locking accounts after failed login attempts and manual reset by an authorized individual, are a function of the underlying Identity Management system, such as Active Directory. However, access to the systems, applications, or commands necessary to reset the password can be governed and controlled by Delinea PAM.
Password Management	Service, System, or Test/Monitor account passwords are required to be changed routinely.	Delinea Secret Server is used to vault privileged service, system, and test/monitor account passwords and assume management. Password rotation policies can automatically change the passwords on a schedule and apply quality of service rules to ensure appropriate complexity and uniqueness and prevent re-use.
Password Management	Service, System or Test/Monitor accounts passwords are unique.	Delinea Secret Server is used to vault privileged service, system, and test/monitor account passwords and assume management. Password rotation policies can automatically change the passwords on a schedule and ensure uniqueness.
Password Management	System accounts, service accounts, and any other required shared privileged accounts have the associated password stored in the enterprise password escrow system product.	You can protect system, service, or any other required shared privileged accounts in the Delinea Secret Server vault and access controlled.
Password Management	Do you provide users with a password manager software?	Delinea Secret Server securely vaults account passwords and strictly controls access via Role-Based Access Controls. Secret Server can automatically inject passwords for login without exposing the password to the user. Secret Server also supports break-glass access to reveal the password to the user. You can protect access by a workflow requiring approval to expose the password in an emergency. Password rotation policies can automatically change the passwords after use and on a schedule, applying quality of service rules to ensure appropriate complexity and uniqueness and prevent re-use.
Password Management	How do you protect privileged accounts (such as Server Administrator accounts)	Delinea Secret Server securely vaults shared privileged account passwords (such as Server Administrator) and controls access via Role-Based Access Controls. Secret Server can automatically inject passwords for login without exposing the password to the user. Secret Server also supports break-glass access to reveal the password to the user. You can protect this access by a workflow requiring approval to expose the password in an emergency. Password rotation policies can automatically change the passwords after use and on a schedule, applying quality of service rules to ensure appropriate complexity and uniqueness and prevent re-use. With shared privileged accounts protected, Delinea Server PAM and Delinea Privilege Manager enforce the Principle of Least Privilege at the server and workstation, respectively. Users and administrators can request elevated privileges to perform legitimate administrative tasks using their enterprise accounts.

Use Case	Questions	How Delinea Helps
Password Management	The Company maintains a password policy which requires regular resets, minimum length, and minimum complexity (for example special characters).	Privileged user account passwords are vaulted and managed by Delinea Secret Server. Policies for password rotation can schedule automatic password changes and apply custom quality of service rules to ensure appropriate length, complexity, and uniqueness and prevent re-use.
Password Management	Establish an accurate inventory of administrative privileged accounts and passwords.	Delinea Secret Server can discover, and inventory administrative privileged accounts and passwords and securely vault them.
Password Management	Vault Linux and local administrative credentials (passwords and SSH keys).	Delinea Secret Server can vault and protect access to Linux and local administrative credentials, including passwords and SSH keys. Secret Server controls access to these secrets. Secret Server can automatically inject a credential to log the user into a Linux server without revealing the password or SSH key. Admins can reveal credentials in an emergency via a self-service access request that requires explicit approval.
Password Management	Vault Active Directory and Azure privileged accounts and manage privileged account Groups.	Delinea Secret Server stores and strictly controls access to privileged Active Directory and Azure accounts. Admins can use self-service workflow to request break-glass access. With Delinea Privilege Manager, you can establish PAM policies to define which accounts (if any) are members of any local groups (including local Administrators). Delinea PAM can automatically reverse any unsanctioned changes to local group membership.
Role-Based Access Control	Integrate with Identity Governance and Administration (IGA) tools for attestation reporting and risk-based approvals.	Although Delinea Secret Server includes reports you can use for attestation, you can also use SailPoint as an alternative. The integration gives SailPoint visibility into Delinea Secret Server's users, roles, and entitlements. These can be presented to users during a SailPoint certification process and adjusted as necessary. Once approved, changes are pushed from SailPoint to Delinea Secret Server and applied.
Server Protection	Applicant's endpoint security tool(s) is/are deployed on all servers (excluding hypervisor hosts).	Delinea Server PAM can be deployed on all Windows, Linux, and Unix servers to enforce least privilege and allow you to control which privileged applications and commands admins can run with elevated rights.
Server Protection	Where and how is endpoint protection applied for servers?	Delinea Server PAM provides endpoint protection for servers via local security controls on each server. The local client enrolls the server with the Delinea Platform or Active Directory to establish a trust relationship and provide a unique machine identity. Login, elevation, and MFA policies are centrally defined and managed in Active Directory or the Delinea Platform.
Server Protection, Least Privilege	Applicant has host-level security controls to prevent lateral movement	Delinea Server PAM deploys host-level security controls to enforce Delinea PAM policies, enforce the Principle of Least Privilege, and prevent lateral movement.

Use Case	Questions	How Delinea Helps
Session Management	In addition to being kept in a password safe, "Domain Administrator Accounts" are not exposed to the administrative user when "checked out," and access is recorded through a session manager.	Suppose you grant permission to allow users to log in to a server with a vaulted domain administrator account. In that case, Delinea Secret Server can create the session without revealing the password to the user. Delinea Server PAM can capture a visual recording of all session activity for any session initiated through Secret Server. Delinea Server PAM can also record session activity at the server OS level for more granular detail.
Workstation Protection	Applicant's endpoint security tool(s) is/are deployed on all workstations and laptops.	Delinea Privilege Manager can be deployed on all user Windows endpoints to enforce least privilege and control which applications can be run and elevated.
Workstation Protection	Where and how is endpoint protection applied for workstations?	Delinea Privilege Manager provides workstation endpoint protection via local security controls on each workstation. Login, elevation, and MFA policies are centrally defined and managed via Privilege Manager's cloud-based UI.

Appendix

The public documents listed below constitute the bulk of information used in this study. There was a considerable amount of replication. We reviewed more than a dozen additional sources not cited below, as they didn't bring any new or original questions to the corpus.

- **Great American Insurance Group: Ransomware Prevention Supplemental Application**
- **AIG: CyberEdge Ransomware**
- **AXIS Insurance: Cyber Ransomware Supplemental Application**
- **Capitol Specialty: Ransomware Supplemental Application**
- **CNA Canada: Ransomware Supplement**
- **The Hartford: Supplemental Ransomware Application**
- **Travelers Multi-Factor Authentication Attestation**
- AXA: CyberRiskConnect New Business Application (not public)
- AXA: XL Supplemental Application (not public)
- Delinea internal cybersecurity assets (various)

Delinea

Securing identities at every interaction

Delinea is a pioneer in securing identities through centralized authorization, making organizations more secure by seamlessly governing their interactions across the modern enterprise. Delinea allows organizations to apply context and intelligence throughout the identity lifecycle across cloud and traditional infrastructure, data, and SaaS applications to eliminate identity-related threats. With intelligent authorization, Delinea provides the only platform that enables you to discover all identities, assign appropriate access levels, detect irregularities, and immediately respond to identity threats in real-time. Delinea accelerates your teams' adoption by deploying in weeks, not months, and makes them more productive by requiring 90% fewer resources to manage than the nearest competitor. With a guaranteed 99.99% uptime, the Delinea Platform is the most reliable identity security solution available. Learn more about Delinea on **delinea.com**, **LinkedIn**, **X**, and **YouTube**.