

A woman with dark, wavy hair and glasses is looking out a window. She is wearing a dark, sleeveless collared shirt. The background is a blurred view of a cityscape with buildings and trees. A large white semi-circle is overlaid on the bottom left of the image, containing the text.

AHEAD

An Overview of AHEAD's Secure Access Solution

Security & Compliance

Benefits of Using Delinea PAM Solution

Delinea is a robust solution designed to secure, control, and monitor privileged access to critical systems and data. It provides a centralized platform for managing privileged accounts, ensuring that only authorized users have access to sensitive information and systems.

Introduction

AHEAD is committed to providing top-tier digital platform solutions, ensuring the highest standards of security and compliance for our customers. As part of this commitment, AHEAD engineers use the [Delinea Privileged Access Management \(PAM\)](#) solution to access customer systems. This whitepaper details the benefits of using Delinea PAM, emphasizing the security and compliance advantages it offers to AHEAD customers.

Overview

Delinea provides remote access to a secure system within the client environment, using a tool called a Remote Access Support (RAS) Engine. An RAS engine is similar to a “jump box,” midserver, or access server. When an AHEAD engineer authenticates through the Delinea Platform and connects to the access server, they are securely operating in the environment with the privileges that the account provides.

Security Benefits

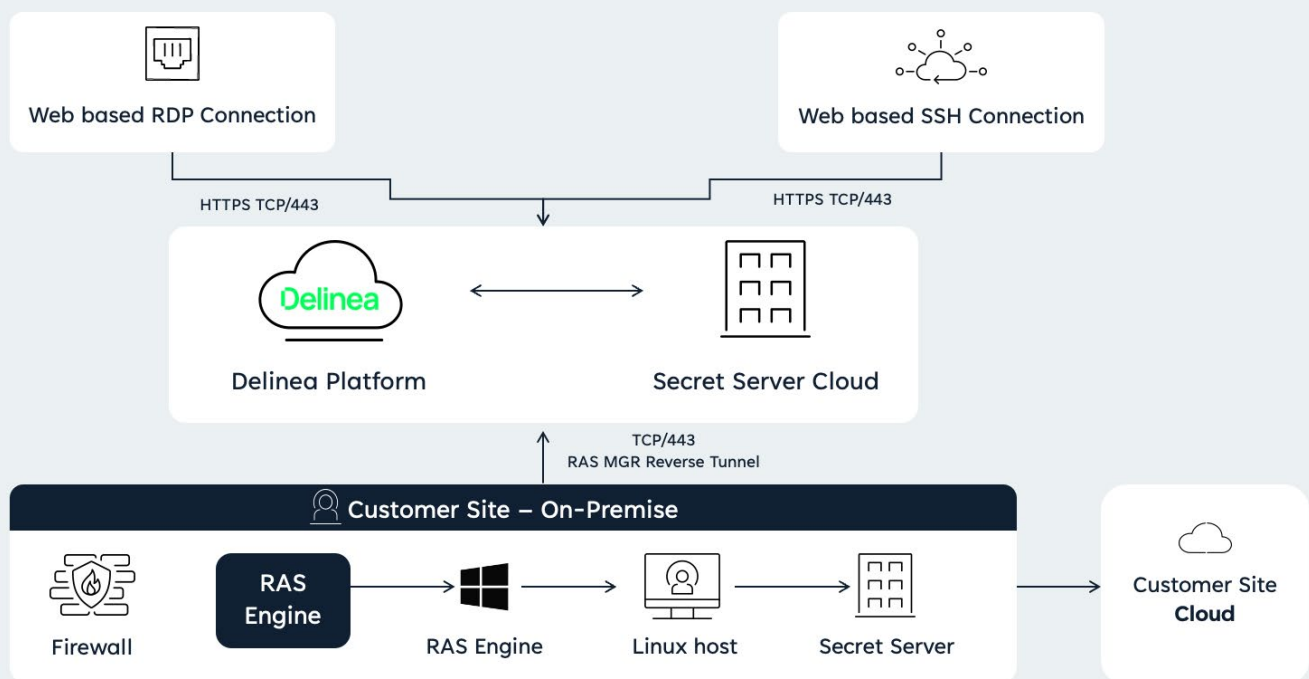
Security by Design

Delinea adheres to industry standards and frameworks while ensuring that security testing is performed as a critical component of the software development processes along with continuous Quality Assurance (QA) checks.

Delinea's cybersecurity defense measures address key components, including intrusion detection, distributed denial-of-service (DDoS) attack prevention, penetration testing, behavioral analytics, anomaly detection, machine learning, and a [Security Operations Center \(SOC\)](#). Delinea also monitors and protects against critical web application security risks, incorporating [OWASP Top 10](#) and [Automated Top 20 threats](#).

Customer data is fully isolated and encrypted both in transit and at rest, using the AES-256 standard encryption algorithm and PBKDF2-HMAC-SHA256 hashing algorithm. Delinea uses private encryption keys for each customer, with third-party key management support (AWS KMS). Secrets are systematically "salted" before being hashed and encrypted with their own unique Initialization Vector and Key.

Connections to Delinea cloud services are protected via Transport Layer Security (TLS). Distributed Engine communications are also secured with an additional encryption key that is unique to each tenant.



Enhanced Access Control

Delinea PAM provides granular access control, allowing AHEAD to define and enforce strict access policies. This guarantees that only authorized engineers can access customer systems, reducing the risk of unauthorized access.

- **Role-Based Access Control (RBAC):** Assign permissions based on user roles, ensuring that engineers only have access to the systems and data necessary for their tasks.
- **Just-In-Time (JIT) Access:** Grant temporary access to privileged accounts, reducing the attack surface by ensuring that privileges are not left open indefinitely.

Multi-Factor Authentication (MFA)

To further secure access, Delinea PAM incorporates MFA, requiring each accessing engineer to verify their identity through multiple authentication methods. This adds an additional layer of security, making it more difficult for unauthorized users to gain access.

Session Monitoring & Recording

Delinea PAM provides comprehensive session monitoring and recording capabilities. All actions performed by AHEAD engineers during their sessions are logged and recorded, ensuring full visibility and accountability.

- **Real-Time Monitoring:** Enable real-time oversight of privileged sessions, allowing immediate response to suspicious activities.
- **Detailed Auditing:** Generate detailed audit logs and session recordings, based on logged actions, to create a detailed image of events throughout the platform and facilitate thorough reviews and investigations.



Secure Credential Management

Delinea PAM securely manages and rotates credentials for privileged accounts, reducing the risk of credential theft and misuse.

- **Automated Password Rotation:** Regularly change passwords for privileged accounts (on a schedule or upon completion of a remote session), ensuring that credentials are always secure.
- **Secure Vaulting:** Store credentials in an encrypted vault, protecting them from unauthorized access and cyber threats. By default, the password is not visible to users, and is instead invisibly and silently passed into the remote sessions.

Compliance Benefits

Regulatory Compliance

Using Delinea PAM helps AHEAD and its customers meet various regulatory requirements, including those specified by GDPR, HIPAA, and PCI-DSS. The solution's comprehensive access controls, auditing, and reporting capabilities facilitate compliance with industry standards and regulations.

- **Access Control & Reporting:** Ensures that access policies align with regulatory requirements and provides detailed reports to demonstrate compliance.
- **Audit Trails:** Maintains detailed records of all privileged access and actions, supporting compliance audits and investigations.



Nonrepudiation

The combination of session recording and detailed audit logs ensures nonrepudiation, meaning that actions taken by AHEAD engineers can be indisputably attributed to them. This is crucial for both security and compliance purposes, as it provides clear evidence of user activities.

- **Immutable Logs:** Confirms that audit logs and session recordings cannot be tampered with, providing reliable evidence for compliance audits.
- **User Accountability:** Clearly links actions to specific users, supporting accountability and transparency.

Policy Enforcement

Delinea PAM allows AHEAD to enforce consistent security policies across all customer environments. This standardization helps specify that all systems meet the same high level of security and compliance.

- **Centralized Policy Management:** Facilitates the creation, deployment, and enforcement of security policies from a single platform.
- **Consistent Enforcement:** Mandates that security policies are uniformly applied across all systems and environments.

Third-Party Compliance Validation

AHEAD builds and manages digital platforms that power the most successful organizations in the world. We are committed to upholding the highest standards of cybersecurity and data protection for our clients. The frameworks, regulations, and certifications that support AHEAD services include:

- **PCI DSS**
- **ISO 27001**
- **SOC 2**

Delinea's compliance program includes the following:

- **ISO 27001**
- **SOC 2**





Final Thoughts

By utilizing Delinea PAM, AHEAD ensures that its engineers have secure, controlled, and monitored access to customer systems. The solution's robust security features and compliance capabilities provide significant benefits, enhancing the overall security posture and helping clients meet regulatory requirements. AHEAD remains dedicated to delivering secure and compliant digital platform solutions, leveraging advanced technologies like Delinea PAM to protect our clients' critical systems and data.

As we pursue additional operational and security tools to support our clients, the use of PAM and RAS solutions will continue to be evaluated, and future enhancements and changes will reflect this pursuit of excellence.

Contributing Author:

David Kidd, Director, Managed Services Governance, Risk & Compliance

AHEAD

Combining cloud-native capabilities in software and data engineering with an unparalleled track record of modernizing infrastructure, we're uniquely positioned to help accelerate the promise of digital transformation.

[Contact Us](#)

National Hubs

CHICAGO

444 W. Lake Street
Suite 3000
Chicago, IL 60606

NEW YORK

500 Fifth Avenue
Suite 1500
New York, NY 10110

ATLANTA

1117 Perimeter Center
Suite W406
Atlanta, GA 30338

SAN FRANCISCO

2000 Crow Canyon Place
Suite 250
San Ramon, CA 94583