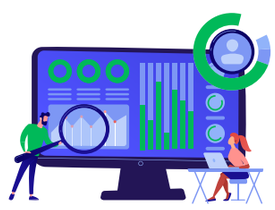
What is the Delinea Identity Threat Solution?

Delinea ITP stands for Identity Threat Protection, a feature within the Delinea Platform, which is designed to enhance identity security for organizations. It is part of Delinea's broader Privileged Access Management (PAM) and identity security solutions, aimed at protecting against identity-based attacks in modern, hybrid environments, including cloud infrastructure and SaaS applications.

Specifically, Delinea ITP helps organizations by:

Detecting Threats:

It provides capabilities to identify suspicious behavior and potential identity-based risks, such as privilege escalation or unauthorized access attempts.



Improving Visibility:

It discovers and monitors identities, accounts, groups, and access permissions across integrated systems, giving organizations a clearer picture of their identity landscape.

Responding to Risks:

It supports automated or manual remediation of threats, such as suspending accounts or adjusting permissions, to mitigate risks in real time.

ITP is often paired with Privilege Control for Cloud Entitlements (PCCE) on the Delinea Platform, combining Identity Threat Detection and Response (ITDR) with Cloud Infrastructure Entitlement Management (CIEM). This integration allows organizations to secure privileged access to cloud services, manage entitlements, and reduce the risk of over-privileged accounts—all while maintaining a seamless experience unified with Delinea's secrets vault and other PAM tools.

In essence, Delinea ITP is a proactive tool for safeguarding identities, focusing on threat detection and response to bolster an organization's cybersecurity posture in today's complex digital environments.

Can Delinea's ITP Block Access?

Yes, Delinea ITP can facilitate blocking access, but its ability to do so directly depends on how it's configured, the integrations in place, and whether you're leveraging its full ecosystem (e.g., the Delinea Platform, Secret Server, or third-party identity providers). ITP itself is primarily a detection and response tool, focused on identifying identity threats and providing actionable insights, but it can trigger access-blocking actions through automated responses or manual intervention. Here's how:

Direct Blocking Capabilities

ITP doesn't natively "block access" in the sense of being a standalone firewall or access gatekeeper sitting inline between users and resources. Instead, it detects threats and initiates blocking via integrations or workflows. Key mechanisms include:

Automated Response via Integrations:

Identity Providers: ITP integrates with identity platforms like Microsoft Entra ID (Azure AD), Okta, or other IdPs. When a threat is detected (e.g., anomalous login attempts), ITP can trigger an API call to:

- Disable a user account.
- Revoke active sessions.
- Enforce step-up authentication (e.g., MFA challenge).
- **Example:** If ITP detects a privileged account logging in from an unusual location, it can signal Entra ID to terminate the session or lock the account.

Secret Server Integration:

ITP works with Delinea Secret Server to manage privileged credentials. If a threat is tied to a vaulted secret (e.g., a compromised admin password), ITP can:

- Rotate the password immediately, effectively blocking access with the old credential.
- Flag the secret for check-in if checked out, preventing further use.
- **Example:** "User X accessed a secret abnormally; rotate it now."

For more content like and follow me:  **@bertblevins**

What is the Delinea Identity Threat Solution?

Delinea

Privilege Control for Cloud Entitlements (PCCE):

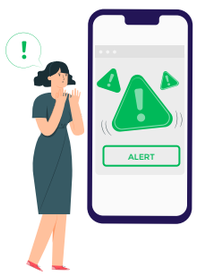
- Paired with ITP on the Delinea Platform, PCCE manages cloud permissions. ITP can recommend or trigger PCCE to revoke excessive entitlements (e.g., remove an over-privileged AWS IAM role), blocking access to specific resources.
- Example: “This service account has unused S3 admin rights; revoke them.”

Workflow Automation:

- Using connectors like Power Automate or Delinea’s internal workflows, ITP can execute predefined actions to block access when thresholds are met (e.g., too many failed logins).
- Example: A flow disables a user in Active Directory after ITP flags a brute-force attempt.

Indirect Blocking (Manual or Policy-Driven)

ITP’s primary strength is threat detection and visibility, so some blocking actions rely on human intervention or preconfigured policies:



Alerts and Recommendations:

ITP notifies admins via the Delinea Platform UI, email, or integrations (e.g., Microsoft Teams) with details like “Account Y is at risk—disable it?” An admin must then act manually.

Policy Enforcement:

ITP can enforce just-in-time (JIT) access policies, ensuring no standing privileges exist to block by default unless explicitly granted.

How It Works

Detection:

ITP uses AI-driven analytics (e.g., AIDA) and behavioral baselines to spot threats (e.g., unusual login times, privilege misuse).

Decision:

It assesses risk based on configured rules or machine learning models.

Action:

Depending on setup:

- Automated: Triggers an API call or workflow to block (e.g., via Entra ID, Secret Server).
- Manual: Alerts an admin to intervene.
- Hybrid: Suggests blocking with an approval step (e.g., “Block this? Yes/No”).

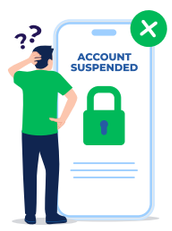
Limitations

Not Real-Time Inline:

Unlike a network firewall, ITP doesn’t sit in the access path to block requests in real time. Blocking happens reactively after detection, via downstream systems.

Dependency on Integrations:

Blocking requires configured connections (e.g., Entra ID, AWS IAM) and sufficient permissions to execute changes.



Granularity:

It’s better at account-level blocking (e.g., disabling a user) than resource-level blocking (e.g., denying access to one file), unless paired with PCCE or other tools.

For more content like and follow me:  **@bertblevins**

What is the Delinea Identity Threat Solution?

Delinea

Examples of Blocking Scenarios

Compromised Account:

ITP detects multiple failed logins on an admin account and triggers Entra ID to lock it.

Leaked Credential:

ITP flags a secret exposed on the dark web (via external feeds) and rotates it in Secret Server, blocking the old password.

What Does Delinea ITP Detect?

Yes, Delinea ITP can facilitate blocking access, but its ability to do so directly depends on how it's configured, the integrations in place, and whether you're leveraging its full ecosystem (e.g., the Delinea Platform, Secret Server, or third-party identity providers). ITP itself is primarily a detection and response tool, focused on identifying identity threats and providing actionable insights, but it can trigger access-blocking actions through automated responses or manual intervention. Here's how:

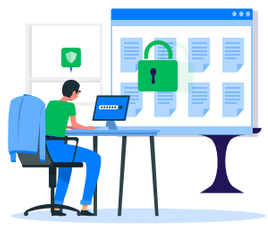
01 Anomalous User Behavior

Unusual Login Patterns:

- Logins from unrecognized locations, devices, or IP ranges.
- Example: An admin logs in from Russia when they're based in the US.

Time-Based Anomalies:

- Access outside normal working hours or unexpected frequency.
- Example: A user logs in at 3 AM when they typically work 9-5.



Suspicious Session Activity:

- Atypical commands or resource access during privileged sessions.
- Example: An account runs destructive scripts it never used before.

02 Credential Misuse or Compromise

Failed Login Attempts:

- Multiple unsuccessful logins suggesting brute-force or credential stuffing attacks.
- Example: 10 failed logins in 5 minutes on a privileged account.

Leaked Credentials:

- Matches credentials against external threat feeds (e.g., dark web scans) to detect exposure.
- Example: An admin password found in a breach dump.

Shared or Stale Credentials:

- Identifies secrets or accounts used by multiple entities or left unchanged too long.
- Example: A service account password unchanged for 6 months.

03 Over-Privileged Accounts

Excessive Permissions:

- Detects users or accounts with more access than needed (violating least privilege).
- Example: A developer with full admin rights to an AWS S3 bucket.

Shadow Admins:

- Finds accounts with indirect admin privileges via group memberships or nested roles.
- Example: A user in a group that inherits Global Admin rights in Entra ID.

Unused Privileges:

- Flags entitlements not exercised recently, indicating potential over-provisioning.
- Example: An account with Azure VM admin rights unused for 90 days.

For more content like and follow me:  **@bertblevins**

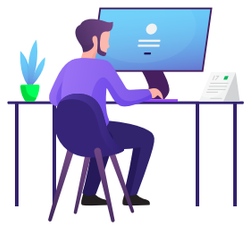
What is the Delinea Identity Threat Solution?

Delinea

04 Configuration Risks

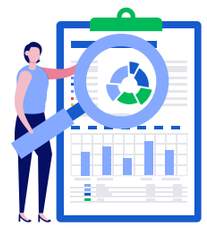
Missing MFA:

- Identifies privileged accounts without multi-factor authentication enabled.
- Example: An admin in Secret Server without MFA configured.



Unmanaged Accounts:

- Spots privileged accounts not vaulted or monitored by Secret Server.
- Example: A local admin account on an AWS EC2 instance not in the vault.



Weak Policies:

- Detects lax access policies, like unrestricted JIT durations or no session timeouts.
- Example: A JIT approval set to 24 hours instead of 1 hour.

05 Lateral Movement Risks

Privilege Escalation Attempts:

- Detects efforts to gain higher privileges (e.g., via misconfigured roles or exploits).
- Example: A user tries to elevate from read-only to admin in Azure.

Cross-System Access:

- Flags abnormal access across linked systems (e.g., from on-prem AD to cloud SaaS).
- Example: An AD account suddenly accessing Salesforce excessively.

06 Cloud-Specific Threats

Unsecured Cloud Identities:

- Identifies misconfigured IAM roles, orphaned accounts, or exposed API keys in AWS, Azure, Google Cloud, etc.
- Example: An AWS IAM user with a public key not rotated in a year.

SaaS App Risks:

- Detects over-privileged users in SaaS platforms integrated with the Delinea Platform.
- Example: A user with admin rights in Okta who rarely logs in.

07 Session-Based Threats

Suspicious Privileged Sessions:

- Monitors recorded sessions (via Secret Server) for risky actions using AI-Driven Audit (AIDA).
- Example: An SSH session deleting critical files unexpectedly.

Session Hijacking Indicators:

- Detects signs of session takeover, like multiple concurrent logins from different IPs.
- Example: An account active in two countries simultaneously.

08 Compliance Violations

Policy Non-Compliance:

- Flags deviations from standards like NIST, GDPR, or SOC 2 (e.g., no audit trail for a privileged action).
- Example: A secret accessed without logging the requester.

Orphaned Accounts:

- Identifies accounts tied to departed employees still active.
- Example: A terminated user's account still has vault access.

For more content like and follow me:  **@bertblevins**

What is the Delinea Identity Threat Solution?

Delinea

How ITP Detects These Threats

AI and Machine Learning:

- Uses behavioral baselines (e.g., “What’s normal for this user?”) to spot deviations.
- Employs AIDA (AI-Driven Audit) to analyze session data in real time.

Continuous Discovery:

Scans identity stores (e.g., Entra ID, AD, cloud IAM) to build an inventory of accounts and privileges.

Integration:

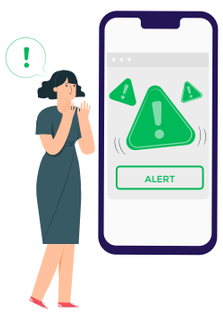
Pulls data from Secret Server, Privilege Manager, and external feeds (e.g., dark web monitoring).

Rules and Policies:

Applies predefined or custom rules (e.g., “Alert if MFA is off for admins”) to flag risks.

Output of Detection

When ITP detects something:



Alerts:

Notifies admins via the Delinea Platform UI, email, or integrations (e.g., Teams).

Risk Scores:

Assigns severity levels to threats (e.g., “High risk: Exposed credential”).

Recommendations:

Suggests actions (e.g., “Disable this account” or “Vault this secret”).

Automation:

Can trigger responses (e.g., lock an account) if configured with integrations like Entra ID or Power Automate.

Examples of What ITP Detects

“Admin logs in from a different country at 2 AM, no MFA enabled” ➔ Flags as high-risk anomaly.

“Service account with S3 full access hasn’t been used in 120 days” ➔ Over-privilege warning.

“Root secret accessed 5 times in 10 minutes” ➔ Potential misuse alert.

“User tries to elevate privileges in Azure” ➔ Escalation attempt detected.

For more content like and follow me:  **@bertblevins**