Identity Threat Protection

Quickly identify unusual behaviors with high-quality insights into the most vulnerable identities to reduce the impact of compromise

The modern digital environment has expanded exponentially, making security teams responsible for assessing, detecting, and responding to threats in highly complex and changing IT environments. Bad actors can blend in by using legitimate credentials to walk in the front door, impersonate a legitimate identity, and go undetected until they decide to attack.

Many organizations lack effective security controls to detect and contain bad actors' activities, enabling them to navigate the attack chain to reach your most sensitive assets.

Organizations are embracing Identity Threat Detection and Response (ITDR) as a must-have security category designed specifically to protect your identity attack surface. Identity Threat Protection builds context across the identity layer to discover and remediate threats in real-time, delivering high-quality insights that help Security Operations leaders limit the impact of identity-related threats.

Using a powerful built-in AI engine, Identity Threat Protection analyzes the amount of privilege that a user has as well as the accounts they have access to. It then analyzes their activity and discovers threats to their account security to determine their risk score and impact associated with a potential breach. The engine quickly delivers an easily consumable and actionable report, including a risk score and potential damage, along with summarized recommended next steps to reduce vulnerabilities and remediate incidents.

HOW IT WORKS

✓ Discover
Connect into your entire traditional, hybrid, and multi-cloud environment to find all your identities — human and machine. Uncover and fix identity misconfigurations before they can become part of an attack.

✓ Detect
Normalize or baseline user behavior across your identities to detect anomalous behavior indicative of a potential compromise. Use AI-driven risk scoring to highlight the danger and impact of identity-related threats.

✓ Respond
Mitigate risk with a comprehensive view of identity, enabling improved response with recommended actions or automation to reduce the impact. Utilize natural language AI queries to easily gain insight into identity-related incidents.

✓ Protect
Elevate your identity posture by continuously discovering and evaluating identity threats, new users, and evolving user behavior.

Identity Threat Protection Benefits

PROACTIVELY DETECT
Monitor for anomalous behavior to understand which identities are most vulnerable to account takeover or compromise and fix them proactively

REMEDIATE
Rapidly shut down a suspected attack in progress by pulling access, resetting credentials, or requiring additional authenticaiton, and alert security operations for follow up
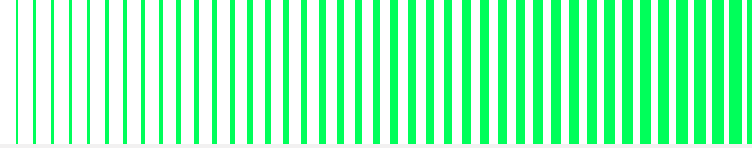
IMPROVE OPERATIONAL EFFICIENCY
Better equip security operations to respond to incidents and reduce the workload with high-quality identity insight and context

UNIFY ADMINISTRATION
Delivered on the cloud-native Delinea platform with a comprehensive view of identity for fast time-to-value and lower total cost of ownership

Identity Threat Detection is delivered on the Delinea Platform to detect and address identity-related threats proactively.

Build context across the identity layer to discover and remediate threats in real-time, delivering high-quality insights that help Security Operations leaders limit the impact of identity-related threats.

Decrease response times through a single view of identity data with continuous monitoring of activities, reducing the impact of account takeovers such as MFA bombings, brute-force attacks, and related incidents across systems, software-as-a-service (SaaS) and cloud. Integrate high-quality identity threat insight seamlessly into your existing security operations signals.

Identity Threat Detection gives Security Operations teams the vital identity context they require to quickly investigate and remediate attacks.
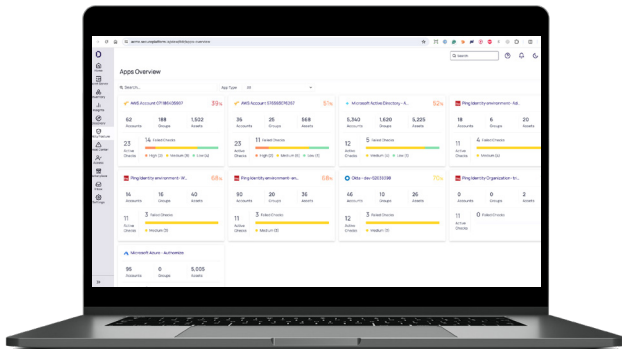
CONTINUAL DETECTION
Discover identity misconfigurations and anomalous behavior across federated and local identities.

BUILD CONTEXT
Visualize identity access pathways across identity systems, software-as-a-service (SaaS) applications, the cloud, and traditional infrastructure.

REMEDIATE THREATS
Take recommended actions or automate responses to reduce the impact of an attack.

The flexibility and agility to scale PAM security controls on your own terms

Essentials
Get started by identifying, managing, and vaulting privileged accounts, with the ability to set rules to request access to credentials and monitor and audit privileged remote access sessions.

Standard
Continue your PAM journey by protecting against identity threats, applying just-in-time and just enough privileges, and enforcing MFA at depth.

Enterprise
Increase automation and intelligence across your authorization policies to further reduce identity-related risk and improve productivity.

Learn more about the Delinea Identity Threat Protection by visiting Delinea.com

Delinea

Delinea is a pioneer in securing identities through centralized authorization, making organizations more secure by seamlessly governing their interactions across modern enterprise. It applies context and intelligence throughout the identity lifecycle, covering cloud and traditional infrastructure, data, and SaaS applications to eliminate identity-related threats. Delinea uniquely provides intelligent authorization for all identities, allowing precise user identification, appropriate access assignment, interaction monitoring, and swift response to irregularities. The Delinea Platform accelerates adoption and boosts productivity, deploying in weeks, not months, requiring just 10% of the resources compared to competitors. Discover more about Delinea on **delinea.com**, **LinkedIn**, **X**, and **YouTube**.

© Delinea   ITP-DS-0824-EN