

# Identity Threat Protection

Identifizieren Sie im Handumdrehen ungewöhnliches Verhalten dank aussagekräftiger Informationen über die anfälligsten Identitäten, um die Auswirkungen einer Beeinträchtigung zu verringern

Die moderne digitale Umgebung hat sich exponentiell vergrößert, sodass Sicherheitsteams dafür verantwortlich sind, Bedrohungen in hochkomplexen und sich verändernden IT-Umgebungen zu bewerten, zu erkennen und darauf zu reagieren. Angreifer können sich unbemerkt Zugang verschaffen, indem sie legitime Zugangsdaten verwenden, sich als legitime Identität ausgeben und unentdeckt bleiben, bis sie sich zu einem Angriff entschließen.

In vielen Unternehmen fehlen wirksame Sicherheitskontrollen, um die Aktivitäten von Angreifern zu erkennen und einzudämmen, sodass diese die Angriffskette bis zu Ihren sensibelsten Ressourcen durchlaufen können.

Unternehmen sehen Identity Threat Detection and Response (ITDR) als eine unverzichtbare Sicherheitskategorie an, die speziell für den Schutz der Angriffsfläche von Identitäten entwickelt wurde. Identity Threat Protection baut einen Kontext über die Identitätsebene auf, um Bedrohungen in Echtzeit zu erkennen und zu beseitigen. Sie liefert hochwertige Erkenntnisse, die den Sicherheitsverantwortlichen helfen, die Auswirkungen identitätsbezogener Bedrohungen zu begrenzen.

## FUNKTIONSWEISE

### ✓ Ermitteln

Stellen Sie eine Verbindung zu Ihrer gesamten traditionellen, hybriden und Multi-Cloud-Umgebung her, um alle Ihre Identitäten zu finden – menschliche wie maschinelle. Decken Sie Fehlkonfigurationen von Identitäten auf und beheben Sie diese, bevor sie Teil eines Angriffs werden können.

### ✓ Erkennen

Normalisieren Sie das Benutzerverhalten über all Ihre Identitäten hinweg, um anomales Verhalten zu erkennen, das auf eine mögliche Gefährdung hinweist. Nutzen Sie die KI-gesteuerte Risikobewertung, um die Gefahr und die Auswirkungen identitätsbezogener Bedrohungen hervorzuheben.

### ✓ Reagieren

Mindern Sie das Risiko, indem Sie sich einen umfassenden Überblick über die Identität verschaffen, der eine bessere Reaktion mit empfohlenen Maßnahmen oder Automatisierung zur Verringerung der Auswirkungen ermöglicht.

### ✓ Schützen

Verbessern Sie Ihre Identitätssicherheit, indem Sie kontinuierlich Identitätsbedrohungen, neue Benutzer und das sich verändernde Benutzerverhalten erkennen und bewerten.

## Vorteile von Identity Threat Protection



### PROAKTIVE ERKENNUNG

Überwachen Sie anomales Verhalten, um zu verstehen, welche Identitäten am anfälligsten für Kontoübernahmen oder Kompromittierungen sind und beheben Sie diese proaktiv.



### BESEITIGUNG

Beenden Sie im Handumdrehen einen mutmaßlichen Angriff durch das Sperren des Zugriffs, Zurücksetzen von Anmeldedaten oder Anfordern zusätzlicher Authentifizierung und Alarmierung der Sicherheitsabteilung zur Weiterverfolgung



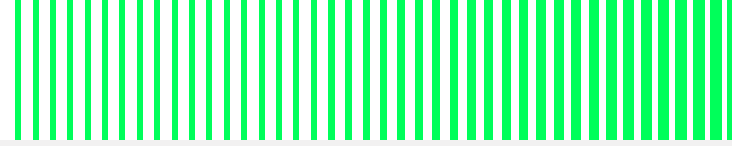
### VERBESSERUNG DER BETRIEBLICHEN EFFIZIENZ

Statten Sie die Sicherheitsabteilungen besser aus, damit diese auf Vorfälle besser reagieren können und verringern Sie die Arbeitsbelastung durch hochwertige Identitätseinblicke und Kontext



### VEREINHEITLICHTE VERWALTUNG

Bereitstellung auf der Cloud-nativen Delinea Plattform mit einer umfassenden Ansicht der Identität für eine beschleunigte Wertschöpfung und geringere Gesamtbetriebskosten

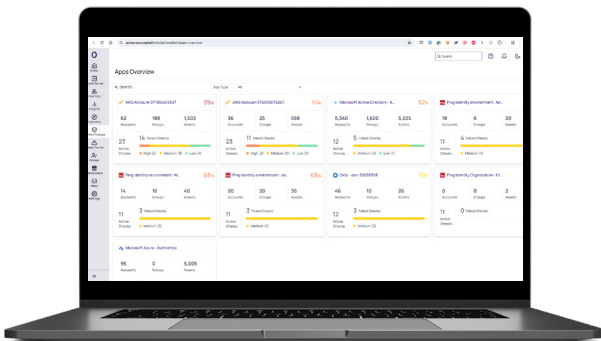


## Identity Threat Detection wird auf der Delinea Plattform bereitgestellt, um identitätsbezogene Bedrohungen proaktiv zu erkennen und zu bekämpfen.

Identity Threat Protection baut einen Kontext über die Identitätsebene auf, um Bedrohungen in Echtzeit zu erkennen und zu beseitigen. Sie liefert hochwertige Erkenntnisse, die den Sicherheitsverantwortlichen helfen, die Auswirkungen identitätsbezogener Bedrohungen zu begrenzen.

Verkürzung der Reaktionszeiten durch eine Einzelansicht der Identitätsdaten mit kontinuierlicher Überwachung von Aktivitäten, wodurch die Auswirkungen von Kontoübernahmen wie MFA-Angriffen, Brute-Force-Angriffen und ähnlichen Vorfällen über Systeme, Software-as-a-Service (SaaS), und die Cloud reduziert werden. Integrieren Sie wertvolle Erkenntnisse über Identitätsbedrohungen nahtlos in Ihre bestehenden Sicherheitssignale.

Identity Threat Detection bietet den Sicherheitsteams den entscheidenden Identitätskontext, den sie benötigen, um Angriffe schnell zu untersuchen und zu beheben.



### KONTINUIERLICHE ERKENNUNG

Erkennen Sie Fehlkonfigurationen von Identitäten und anomales Verhalten bei föderierten und lokalen Identitäten.

### BEREITSTELLUNG VON KONTEXT

Visualisieren Sie Identitätszugriffspfade über Identitätssysteme, Software-as-a-Service (SaaS)-Anwendungen, die Cloud und herkömmliche Infrastrukturen hinweg.

### BESEITIGUNG VON BEDROHUNGEN

Ergreifen Sie empfohlene Maßnahmen, oder automatisieren Sie Reaktionen, um die Auswirkungen eines Angriffs zu verringern.

## Flexibel und agil, sodass Sie Ihre PAM-Sicherheitskontrollen nach Ihren eigenen Anforderungen skalieren können



### Essentials

Identifizieren, verwalten und sichern Sie privilegierte Konten mit der Möglichkeit, Regeln für den Zugriff auf Zugangsdaten festzulegen und privilegierte Remote-Zugriffssitzungen zu überwachen und zu prüfen.



### Standard

Setzen Sie Ihre PAM-Reise fort, indem Sie sich vor Identitätsbedrohungen schützen, Just-in-Time- und Just-enough-Berechtigungen anwenden und MFA im Detail erzwingen.



### Enterprise

Erhöhen Sie die Automatisierung und Intelligenz Ihrer Autorisierungsrichtlinien, um identitätsbezogene Risiken weiter zu reduzieren und die Produktivität zu steigern.

Erfahren Sie mehr über Delinea Identity Threat Protection unter [Delinea.com/de](https://delinea.com/de)

## Delinea

Delinea ist ein Vorreiter bei der Sicherung von Identitäten durch zentralisierte Autorisierung und macht Unternehmen sicherer, indem es ihre Interaktionen in modernen Unternehmen nahtlos steuert. Delinea nutzt Kontext und Intelligenz während des gesamten Identitätslebenszyklus, über Cloud- und traditionelle Infrastrukturen, Daten und SaaS-Anwendungen hinweg, um identitätsbezogene Bedrohungen zu beseitigen. Delinea bietet eine einzigartige intelligente Autorisierung für alle Identitäten, die eine präzise Benutzeridentifizierung, eine angemessene Zugriffszuweisung, die Überwachung von Interaktionen und eine schnelle Reaktion auf Unregelmäßigkeiten ermöglicht. Die Delinea-Plattform beschleunigt die Einführung und steigert die Produktivität, da sie innerhalb von Wochen und nicht Monaten bereitgestellt werden kann und im Vergleich zu anderen Anbietern nur 10 % der Ressourcen benötigt. Erfahren Sie mehr über Delinea auf [delinea.com](https://delinea.com), [LinkedIn](#), [X](#), und [YouTube](#).