



Delinea

Identity Threat Detection and Response (ITDR)

Buyer's Guide

Align ITDR with the NIST Cybersecurity Framework (CSF)

The modern Security Operations Center (SOC) is responsible for detecting threats of all types in a complex hybrid environment, analyzing and prioritizing them based on context, and responding appropriately to protect the organization.

When you are faced with many different threat vectors, where do you begin?

For immediate, measurable impact on risk, it makes sense to prioritize the most common and powerful threat vector attackers employ – identity.

The easiest way for cyber criminals to attack your network isn't through a back door, but by using legitimate credentials to walk in the front. Once they obtain stolen credentials through tactics such as malware, access brokers, or social engineering, threat agents can impersonate authenticated users. Without effective security controls to detect and contain their activities, they can navigate through the attack chain to reach your most sensitive assets.

In response to escalating identity-based attacks, organizations are embracing Identity Threat Detection and Response (ITDR) as a must-have security solution. Unlike other threat detection tools like Managed Detect and Response (MDR), Endpoint Detection and Response (EDR), and Extended Detection and Response (XDR), ITDR is designed specifically to protect your identity attack surface.

If you're responsible for threat detection, incident response, or Identity and Access Management (IAM), and you're considering how ITDR solutions can fit into your security roadmap, this guide is for you.

The information inside will help you:

- ✓ Understand the use cases for ITDR
- ✓ Save you time preparing for conversations with ITDR providers by providing a checklist of questions to ask them
- ✓ Help you compare options and choose the best ITDR solution for your needs
- ✓ Consider ITDR within the context of your overall identity security strategy

| ITDR for the cloud enterprise

Virtually all enterprises today have a mix of on-premise and cloud resources, often spread across data centers and multiple Cloud Service Providers (CSPs). Due to this transformation, sensitive data is now scattered throughout the enterprise, housed in containers and micro-services. What's more, cloud services are created rapidly, outside of central IT control. Unfortunately, misconfigurations are common, leaving sensitive information publicly exposed.

Impact of the cloud on identity security

In a cloud environment, identity security becomes much more complex to manage, for several reasons:

Distributed control: Instead of a small admin group, numerous users and systems now have access to data and resources and may even have the ability to generate new identities.

Machine identities: Non-human identities that run cloud services often operate without sufficient oversight.

Over-privilege: Far too many identities have excessive privileges they don't require to do their job, in violation of least privilege best practices.

Multiple Identity Providers (IdPs): Every cloud application and service may utilize a different identity management process. For example, your organization may rely on Active Directory, other IdPs like Okta or Ping, or federated identities that share tokens with third parties.

It is incredibly difficult to track the potential or actual attack path of a single identity across such a distributed, dynamic, and inconsistent environment.

You cannot structure security operations in a cloud environment the same way you would in an on-premise world. The traditional strategies — network firewalls, common corporate directory services, and static access controls — aren't effective in a modern multi-cloud world.



In response to escalating identity-based attacks, organizations are embracing Identity Threat Detection and Response (ITDR) as a must-have security solution.”

What do incident response teams need to safeguard the cloud?

So that incident response teams can address identity-based attacks quickly and effectively, a security solution must be able to:

- Clearly explain what cloud resources each identity has access to and what they could do with that access (their “effective access”).
- Attribute privileged behavior in the cloud to a unique identity (individual or machine) rather than a group of users with a shared account.
- Incorporate high-quality identity signals that deliver actionable insight to help prioritize alerts and shorten response times.
- Risk scoring that can be applied to triage alerts and point security operations personnel to the riskiest identities and probabilities of an incident occurring.
- Map access and monitor behavior within and across multiple cloud service providers (CSPs), between cloud and on-premise solutions, and between your environment and third parties.
- Easily understand the context behind identities and their behavior to evaluate the level of risk. Detailed assessments of risk account for factors such as usage, accessibility, data sensitivity, and potential consequences of an attack.
- Keep pace with constantly changing identities, assets, and risks.
- Integration into existing Security Operations Center (SOC) tools and workflows, such as a Security Investigation and Event Management (SIEM) solution.
- Automate responses to rapidly contain threats.

ITDR addresses each of these use cases. It breaks through the silos of multi-cloud, Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Identity and Access Management (IAM) to connect the dots across the identity layer.

The faster a cyber event is recognized and understood, the faster it can be mitigated. But what if attackers are more automated than you are? What if they are using Artificial Intelligence (AI) and other means to change their tactics dynamically? You need to be able to detect and respond at the same pace.

ITDR helps you align to NIST CSF (Cyber Security Framework)

In this next section, you will learn how ITDR solutions align with the gold standard for risk-based cybersecurity decision-making, the [National Institute of Standards and Technology's \(NIST CSF\) Cybersecurity Framework](#). By aligning with NIST CSF, you can demonstrate to your leadership team, external auditors, and cyber insurance companies that you're following best practices for risk-based cybersecurity management.

NIST CSF has five functions

1 Identify

The Identify function leads organizations to understand all assets and environments and associated risks, define the current and desired states of controls to protect those assets, and create a plan to go from current to desired states of security.

2 Protect

The Protect function is when the Framework becomes more proactive. It includes implementing preventive security controls for authentication and authorization to reduce the risk of identity-related attacks.

3 Detect

The Detect function requires appropriate information to recognize the occurrence of a cybersecurity event. It includes a collection of meaningful data on activities and events, supported by continuous monitoring.

4 Respond

The Respond function supports your ability to contain the impact of a potential cybersecurity incident through communications, risk-based analysis, and mitigating controls.

5 Recover

The Recover function involves developing and implementing appropriate activities to maintain cyber and business resilience and restore any impaired capabilities or services caused by a cybersecurity event.

Let's dig into how ITDR capabilities align with each of the NIST five functions. In the next section, you'll find questions to ask any ITDR solution provider as part of your vendor assessment.

1 Identify

These ITDR capabilities lay the groundwork for your cybersecurity actions by providing end-to-end visibility of your identity attack surface.

ITDR capability	Questions to ask an ITDR Provider
Discover human identities	Do you support multiple IdPs (Okta, Azure Active Directory, PingOne, etc.)? Can you connect to HR systems to track Joiner-Mover-Leaver (JML) changes and partial offboarding?
Discover machine identities	Can you discover machine identities such as application programming interfaces (APIs) and workloads?
Discover federated identities	Can you discover federated identities that are generated externally and joined to your IdP via token exchange? Can you tie activity in Amazon Web Services (AWS) to federated users so that I can track them?
Discover all critical cloud services and apps and their current state	Does your coverage include Identity-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS)? Can you see all identities across a complex multi-cloud, hybrid cloud environment? Which CSPs do you cover? Can you detect sensitive folders that are publicly accessible? How about our homegrown systems?
Discover permissions and privileges for all types of identities	Can you show what permissions are granted to whom and how in a centralized view? Can you provide granular, file-level visibility of access permissions? Can you detect over-privileged human and machine identities? How do you discover hidden privileges granted via groups, privilege escalation paths, and misconfigurations? Can you show me which contractors and third parties retain access to assets with their own identities?
Merge identities	Can you merge identities, including those not in our identity provider but with access to our assets?
Continuous discovery	How does the system discover new identities and assets as they're created so they can quickly be brought under management?
Discover dormant identities and standing privileges	How do you determine when an identity or privileged access is no longer required? Can you show access privilege usage, detecting unused privileges over specified periods?
Discover effective access across environments	How do you trace access paths and entitlement permissions across systems and environments (on-premise, and multi-cloud)? Do you provide end-to-end visibility from the Identity Provider to the asset? Can you show me privilege escalation paths like role chaining, the granting of temporary access to resources, in Amazon Web Services? How do you create visualizations of access paths so they're easy to understand immediately?

2 Protect

These ITDR capabilities help you implement preventive security controls to reduce the potential blast radius of an identity-based attack.

ITDR capability	Questions to ask an ITDR Provider
Authentication support	Can you show me which privileged identities MFA enabled and at what levels? Can you uncover and fix IAM misconfigurations? Can you detect risky misconfigurations that would expose us to leaking clear text passwords or user impersonation?
Authorization support	Can you show me how users gain access to assets through group membership (ex. nested groups, public groups)? How do you limit privileged access? How do you eliminate privilege escalation paths to contain attacks?

3 Detect

These ITDR capabilities help you uncover identity-based attacks in progress, including attempts to gain initial access with compromised credentials or escalate privileges if attackers are already inside.

ITDR capability	Questions to ask an ITDR Provider
Detecting Tactics, Techniques, and Procedures (TTPs)	Can you detect MFA bombing/fatigue attacks? Can you detect brute-force attacks? Can you detect failed login attempts using credential stuffing across multiple applications that may indicate related attacks on an identity? Can you detect session hijacking?
Suspicious activity	Can you detect when new privileged identities are created? Can you detect dormant accounts that become active again? Can you detect unexpected/unwanted privilege elevation or escalation? Can you detect the connection of new upstream identity data sources like additional Identity Providers (IdPs) or Human Resources (HR) applications? Can you generate a risk score that indicates the probability an identity may be attacked as well as the impact ("blast radius") such an attack may result in? Can you detect newly created malicious misconfigurations at the IdP level? Can you detect changes users make to logs in our IdP that may indicate they're hiding their activity?

ITDR capability	Questions to ask an ITDR Provider
Usage monitoring	Can you provide a baseline of activity to determine a user's normal entitlement usage, so that we'll know when behavior outside of the norm occurs? Is monitoring continuous vs. sporadic or ad-hoc?
Flexibility	How will you help me extend my existing detection capabilities for new IdPs and apps in my next merger and acquisition? Describe to me your flexibility in shifting scope or adding detection policies for the newly acquired company or its users.

4 Respond

Automating data flows and workflows helps you rapidly remediate potential risks and contain suspected cyberattacks. Look for flexible remediation recommendations and options that won't disrupt business or IT operations.

ITDR capability	Questions to ask an ITDR Provider
Right-sizing	Can you provide recommendations for right-sizing identities and permissions?
Policy creation	Can you create new policies for permissions or roles?
Alerting	How do you integrate with my security tools for monitoring, analysis, and alerts, such as my SIEM? Can you send webhooks or open tickets in IT workflow systems like JIRA or ServiceNow?
Refactoring	Can you automatically refactor AWS/Azure/Google Cloud Platform (GCP) permissions to be more secure based on actual usage?
Mitigating actions	Can you automate alerting users to change passwords when their credentials are compromised? Can you automatically log users out of current sessions to avoid hijacking attacks from stolen tokens? Can you challenge the user via additional MFA when they perform a suspicious or privileged activity? Or based on their changing identity risk level? Can you remove third-party access? Can you dynamically adjust conditional access based on risk level? Can you automate remediation workflows?
Personnel	Can you reduce the time it takes for security operations to respond to incidents?

5 Recover

In the context of ITDR solutions, the Recover phase can be understood as performing mass clean-ups and getting rid of the misconfigurations or privilege escalation paths that you may have discovered during a breach. Ideally, your ITDR solution can help you to snap back to your regular operations, showing you the state you should revert to and even assisting in restoring configurations as they were before your incident.

ITDR capability	Questions to ask an ITDR Provider
Backups	Can you provide a backup of my IAM elements and controls for restoration?
Forensics	Can you provide me with a forensic log of IAM changes? Can you show deleted identities and assets? Can you show responders what was accessed during an incident? Can you assist with post-event forensics to provide high quality identity insight to help with an investigation?

| Partnership also matters

Beyond the NIST CSF functions, a key aspect of selecting the right vendor is feeling confident that you'll have a relationship built for the long run. A true partner should understand your identity security strategy and help you achieve your goals, not just sell you an ITDR tool.

The fact is, ITDR by itself isn't a silver bullet to improve your identity security posture. It's part of a comprehensive approach. Just as ITDR breaks down silos in the cloud, it also breaks down silos in your organization. It brings IAM, security, and incident response teams together because they have a complete, accurate picture of identity and access in the cloud, a shared understanding of risk, and clear steps for remediation.

Look for a vendor who understands all your identity needs and can deliver the outcomes you expect in a timely way. To avoid unwelcome surprises, ask them these questions upfront.

Vendor capability	Questions to ask an ITDR Provider
Time to value	How long does deployment take? Can I see functional results within 1-2 days? How will you help me decrease incident response time?
Usable security	What native connectors do you have? Do you have an open API? Is there any need to write scripts to operate your solution? What do you require from my side for deployment or integration? Can I adjust security policies to track and alert on risky accounts without the need for professional services or new feature development?
Strategic support	How do you see ITDR fitting into my overall identity security strategy? How can you help me build alignment across teams?
Responsiveness	Are you going to pick up the phone when I have questions or feature requests? How easy is it to access your technical documentation? Will I have a dedicated success manager? Can I get insight into your roadmap?

About Delinea Identity Threat Protection



Delinea Identity Threat Protection builds context across the identity layer to discover and remediate threats in real-time, delivering high-quality insight that helps Security Operations leaders limit the impact of identity-related threats.

Proactively reduce risk by identifying anomalous behavior, understanding the most vulnerable identities, determining the potential impact if compromised, and taking appropriate actions. 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 identity systems, SaaS and cloud. Integrate high-quality identity threat insight seamlessly into your existing security operations signals. Delivered on the cloud-native Delinea Platform, you can reduce workload, stress, cost, and uncertainty as part of the single source of truth for authorization across all identities.

To learn more, visit our website to see an interactive demo of [Delinea Identity Threat Protection in action](#).



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 [LinkedIn](#), [X](#), and [YouTube](#).

© Delinea ITDR-BG-0424-EN

