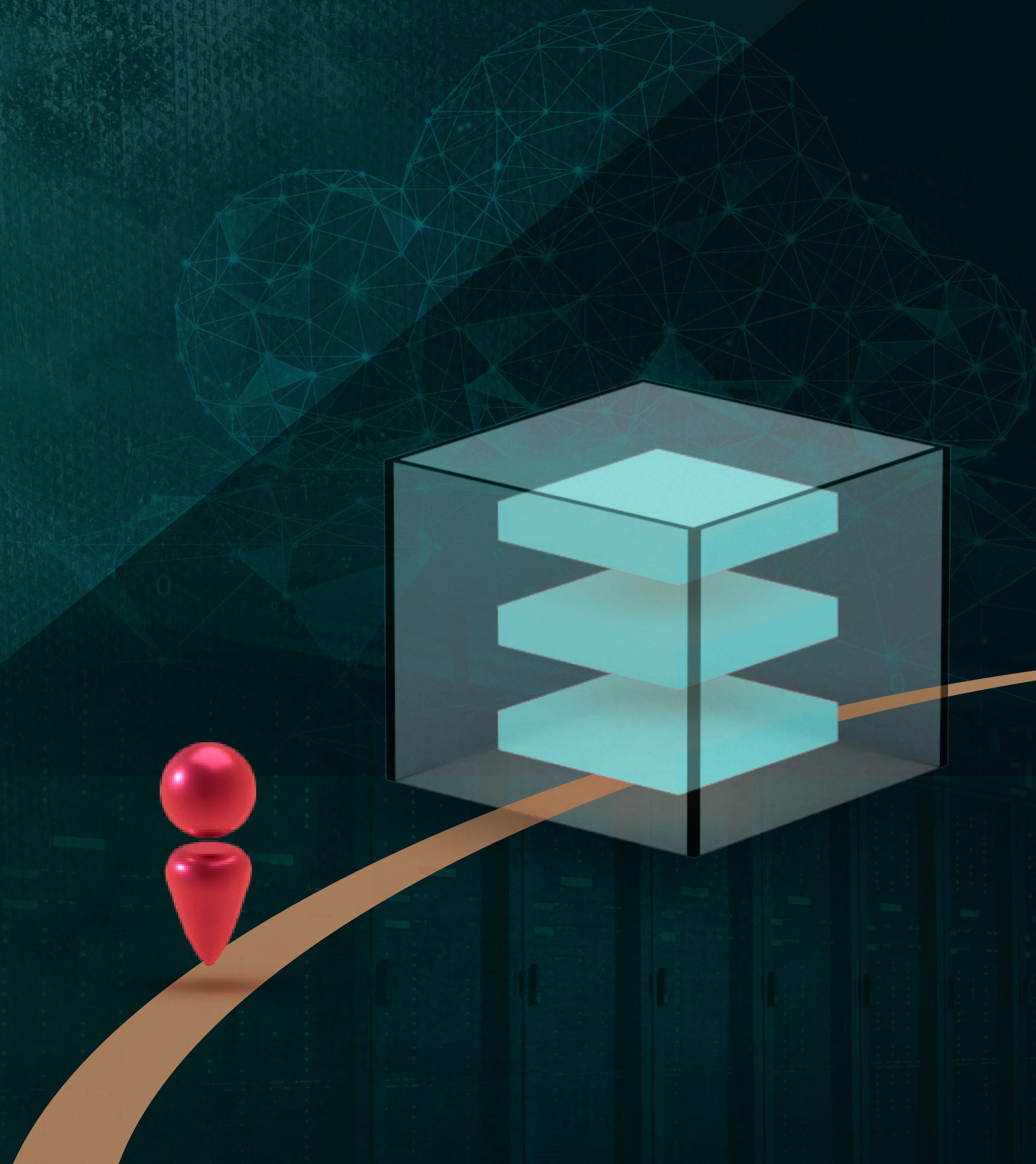




# Identity Threat Detection and Response (ITDR)

Protecting the Exposed  
Identity Attack Surface

eBOOK

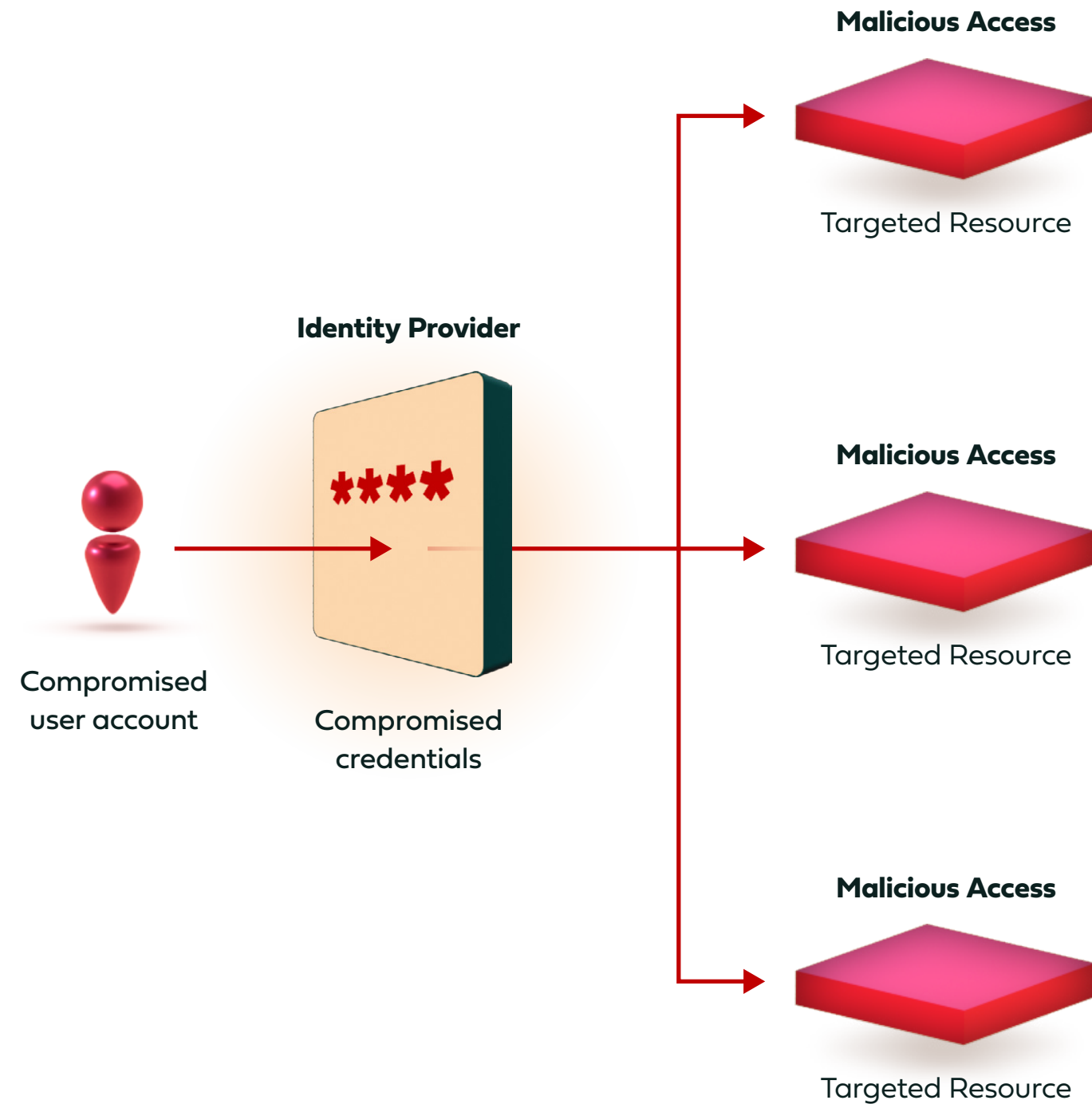




# ITDR: Addressing the Protection Gap of the Identity Attack Surface

**ITDR is an emerging security category that addresses the long-ignored protection gap of the identity attack surface.** An ITDR platform focuses on identity activity, namely user account authentication and access attempts to corporate resources.

**The purpose of ITDR is to provide security teams with the ability to efficiently detect and respond to identity threats, which they haven't had to date.** This eBook provides an analysis of the ITDR category by first explaining what the common identity threats in today's cybersecurity landscape are. It then moves on to explore the limitations of current IAM infrastructure as well as how existing products in the security stack create blind spots that ITDR addresses. Following that is an in-depth discussion of the building blocks of ITDR in order to better understand exactly what detection, response, and coverage capabilities an ITDR solution should have, including a decision process framework to easily shortlist and determine what ITDR is the best fit to your environment.

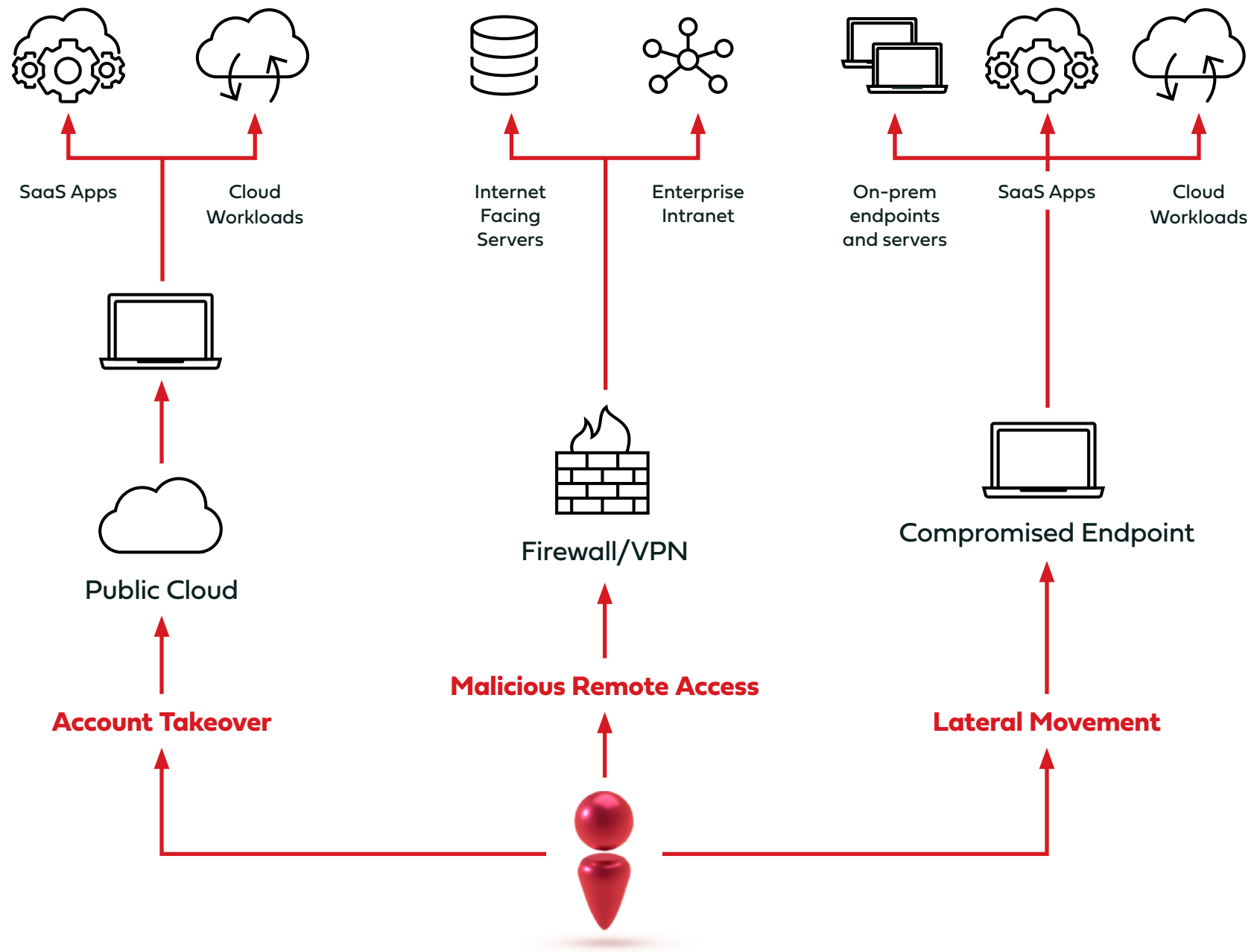




# What are Identity Threats?

Identity threats is the term used to describe **any type of adversarial activity that targets the identity attack surface by using compromised user account credentials for malicious access** to on-prem and cloud resources. This can happen during the initial access phase of a cyberattack (such as with an account takeover of SaaS apps and cloud workloads) or at the post-compromise persistence and lateral movement stages. Credential theft is a necessary condition for launching an identity threat and is often accompanied by privilege escalation. However, it is the actual malicious access that creates the threat that ITDR addresses directly.

**The steep rise in account takeovers, malicious remote connections, and lateral movement attacks implies that sound protection against identity threats is clearly beyond the scope of current security practices and tools.**



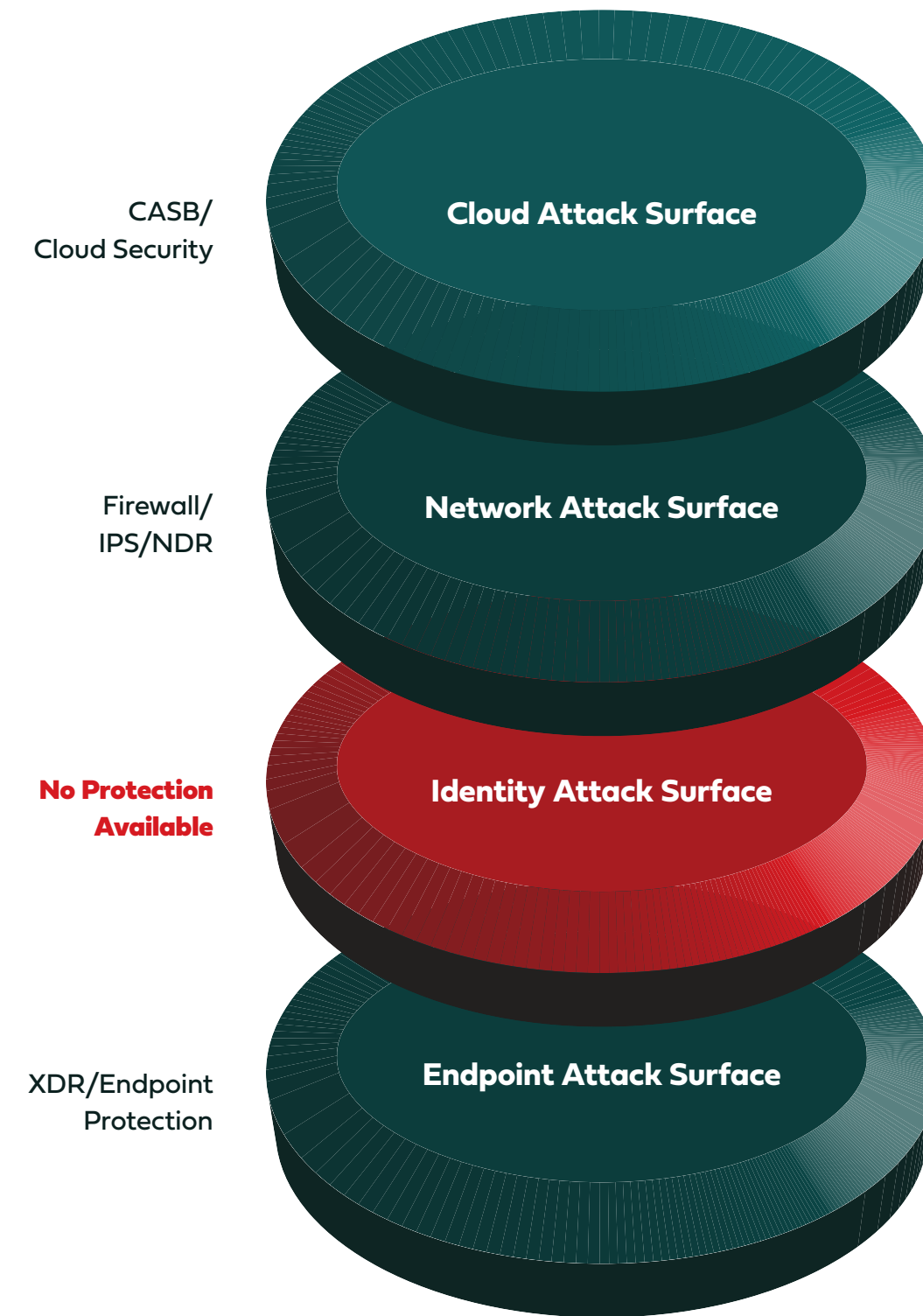


# What Makes Identity Threats a Blind Spot in Today's Security Architecture?

Protection against cyber threats entails the ability to monitor a certain activity within the IT environment, detect whether an instance of this activity is malicious, and take steps to mitigate the threat if so. Ideally, this response would result in the automated termination of that activity.

On the identity control plane, this activity specifically means user authentication and access attempts. The blind spot of identity protection here stems from the fact that there is no product in the security stack dedicated to this activity. While running processes are covered by the Endpoint Protection Platform (EPP), network traffic by the firewall, interaction with data files by the Data Loss Prevention (DLP) solution, **there is actually no security product that addresses the core attack surface of user identity.**

ITDR aims to fill this gap.

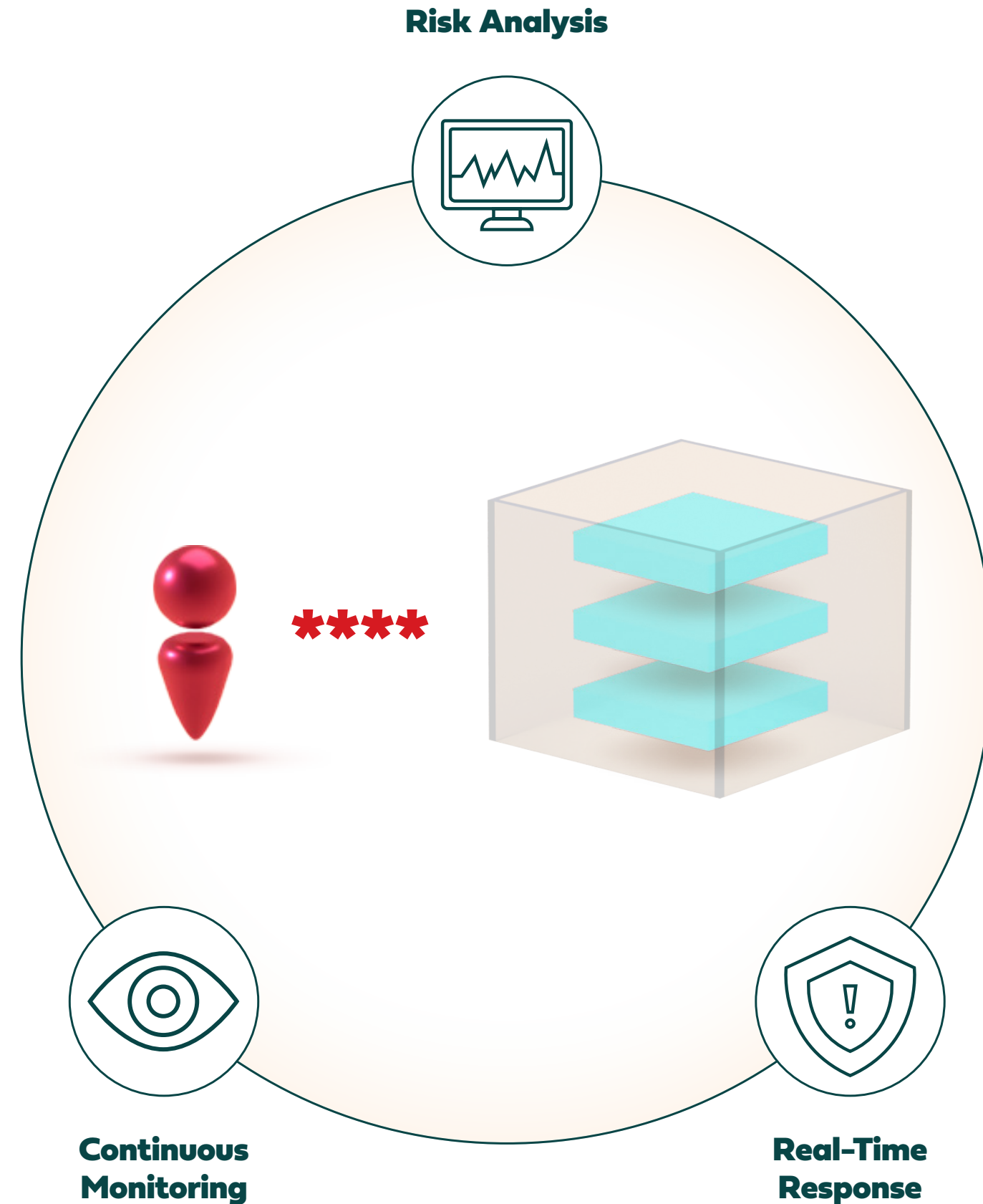




# The Definition of ITDR

ITDR is a security solution that **focuses primarily on continuous monitoring, risk analysis, and active protection of user authentication and access attempts.** The core activity that ITDR analyzes is user authentication and access attempts to organizational resources. The purpose of this analysis is to **uncover when a seemingly legitimate access is, in fact, malicious and block it in real time.** In this way, ITDR can protect enterprise resources against malicious access using compromised credentials as well as against abuse of the identity infrastructure itself.

**In the following pages we'll explore how this goal is achieved.**

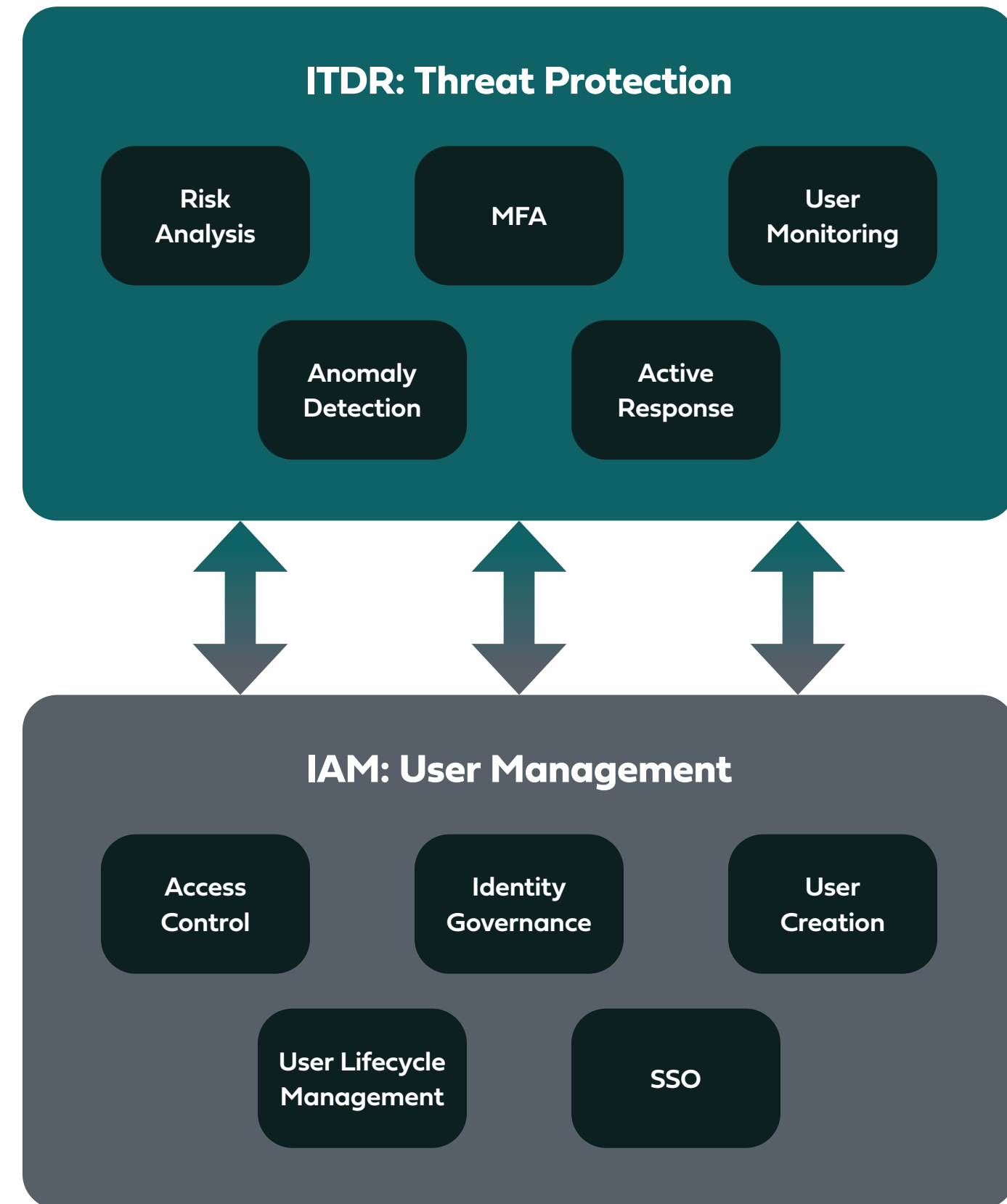




# What's the Relationship Between ITDR and IAM?

**ITDR must maintain a close integration with the IAM infrastructure** – Active Directory, cloud identity providers (IdPs), federation servers, VPNs, and every other component that processes user authentications. This is because the **ITDR doesn't replace the IAM layer but instead acts as a security layer on top of it.** In this way, the IAM solutions within the environment can keep attending to user management functionality while the **ITDR handles the security side** – analyzing each authentication to ensure that it is indeed the actual user providing the credentials and not an adversary who has compromised them.

This also implies that **an ITDR's protection capabilities are only as good as its integration depth with the IAM infrastructure.** The deeper the integration, the easier it will be for the ITDR to incorporate itself in the access attempt flow and provide accurate, real-time protection.





# How to Choose an ITDR Solution?

There are various technologies and approaches to achieve the goal of ITDR. To choose the path that best fits your needs, it's imperative to keep in mind the reason why this category has emerged – to protect against identity threats.

There are three evaluation factors when determining an ITDR solution's ability to deliver the protection it promises:



## Coverage

**What is the scope of the ITDR protection,** and does it integrate with all IAM infrastructure, both on-prem and in the cloud?



## Detection

**What is the range of identity threats** the ITDR solution can identify and what is its level of accuracy?



## Response

**What action does the ITDR take upon detection of identity threat?** Does it generate an alert retroactively or can it block the malicious activity in real time?

**Let's dive deeper into each of these factors to better understand what's entailed in each of them.**



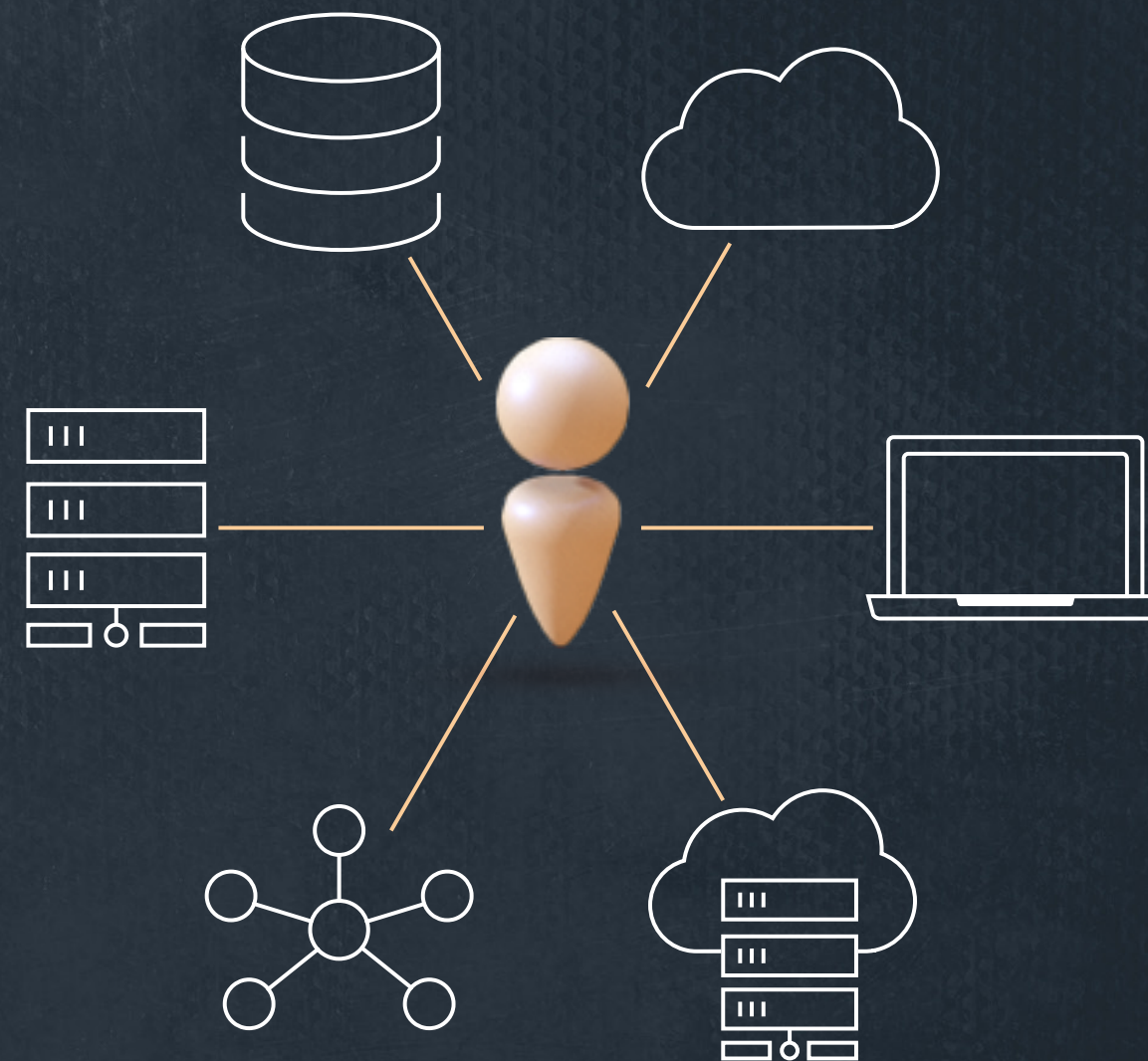


# Evaluation Factor #1: Breadth of Coverage

Over 90% of organizational environments today are hybrid, containing both on-prem and cloud resources. In terms of identity infrastructure, this means there are at least two (and often more) IAM providers in the environment. The most common architecture includes Active Directory for on-prem resources and either a federation service (such as Microsoft AD FS, PingFederate, etc.) or a cloud-native IdP (such as Entra ID (formerly Azure AD), Okta, etc.) for the SaaS apps.

**Adversarial activities** take advantage of this fragmented architecture, as evidenced by the increasing number of attacks leveraging compromised user credentials to **traverse between the on-prem and cloud environments.**

In terms of protection against identity threats, this means the **ITDR must integrate with every IAM solution in the environment so that it has visibility into every authentication and access attempt** that takes place, both on-prem and in the cloud. Failure to achieve this coverage by implementing either an AD-focused or SaaS-centric ITDR solution would inevitably fail to provide the required foundation for sound detection and response capabilities.



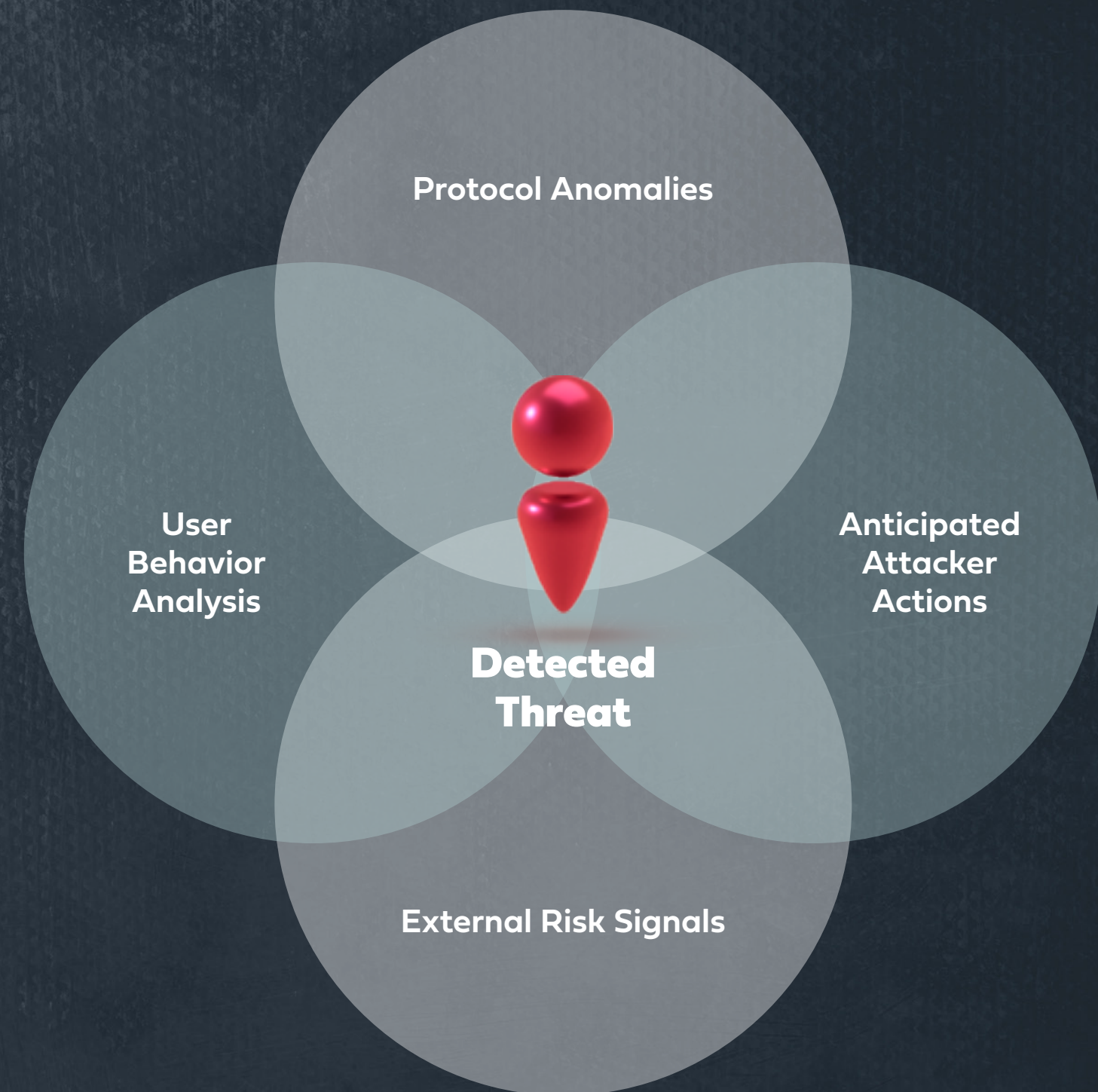




## Evaluation Factor #2: Accuracy of Detection

Detection factor relates to an ITDR's ability to **identify an access attempt as malicious while achieving the lowest possible rate of false positives.**

Like any other malicious activity, identity threats generate anomalies that differentiate them from legitimate resource access. These anomalies come in various types and can range from a simple impossible geolocation of a user accessing a SaaS app to a slight alteration of an on-prem authentication protocol or a service account performing an interactive login. **ITDR's detection capability is measured by the range of anomalies it can identify and validate as malicious.** This is achieved first and foremost with the ITDR's risk engine, but can also be supplemented by ingesting signals from other security components such as EPP, SIEM, CASB and others.

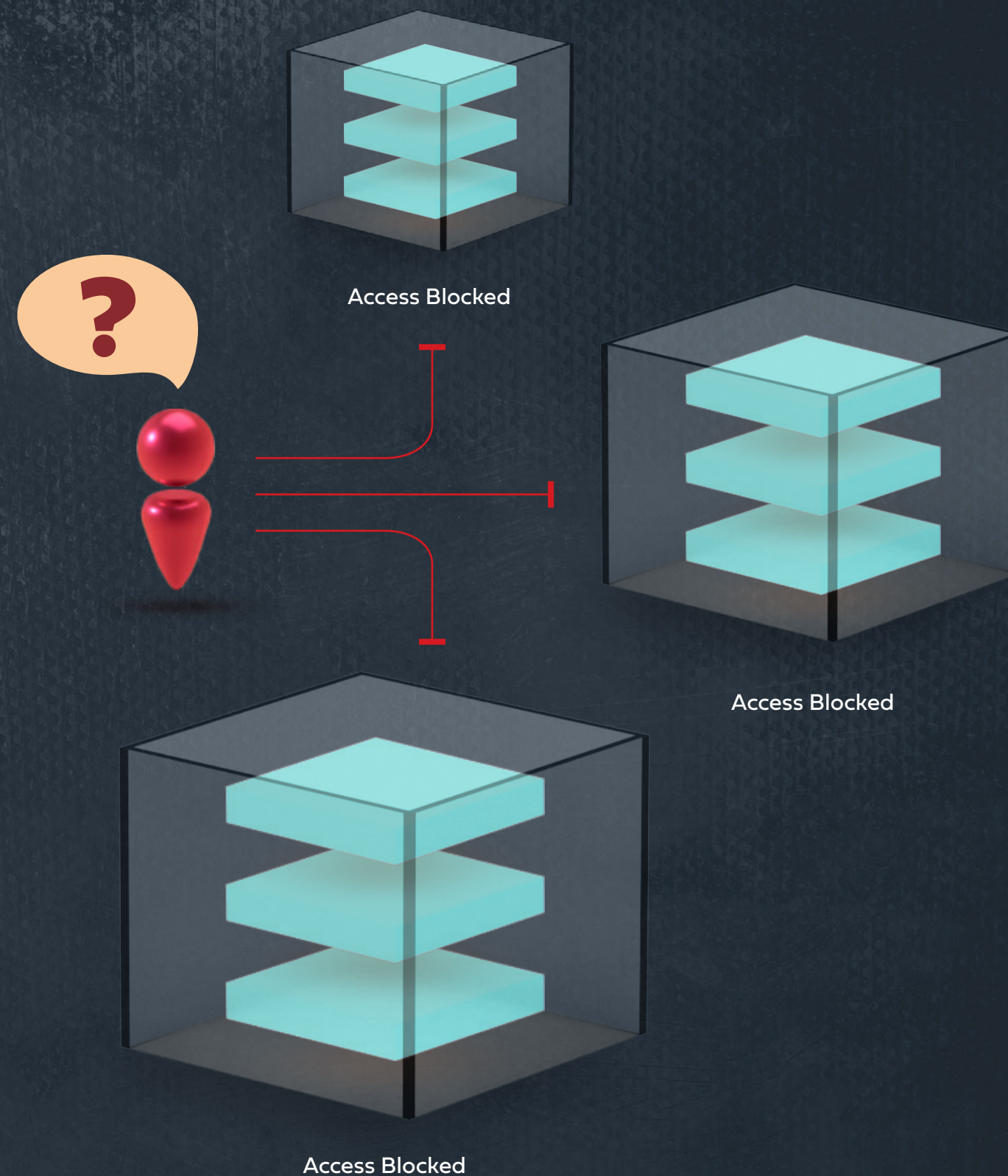




## Evaluation Factor #3: Efficiency of Response

Once an identity threat is detected and confirmed, the ITDR should take action to mitigate the threat. The efficiency of the response's action depends on the level of the ITDR's integration with the IdP in the environment. Typically, there are two main options:

- 1. Real-time blocking:** The ITDR is integrated into the IdP's user authentication flow. In this case, the IdP waits for the ITDR verdict prior to granting or denying access, so if the ITDR detects a threat it will inform the IdP to deny access, therefore **blocking the adversary altogether**.
- 2. Reactive alert:** The ITDR is not integrated into the IdP's user authentication flow, ingesting logs of authentications and access attempts after they've occurred. In this case, the ITDR cannot block the malicious authentication but instead alerts the security team about an **active identity threat that should be manually validated, investigated, and resolved**.











# Evaluation Factor #2 Revisited: What Makes MFA the Ultimate ITDR Game Changer

Incorporating multifactor authentication (MFA) in the detection stage exponentially increases ITDR effectiveness and operability, and is the key to automating a validation processes that otherwise consumes precious SecOps time.

Realistic planning should always take into account that false positives may happen. **MFA is the ultimate measure to minimize the impact of any false positives because** it crowdsources the immediate response to the entire workforce, ensuring that only verified threats land on the SecOps team's desk. The table below shows the clear advantage that MFA provides in such scenarios.

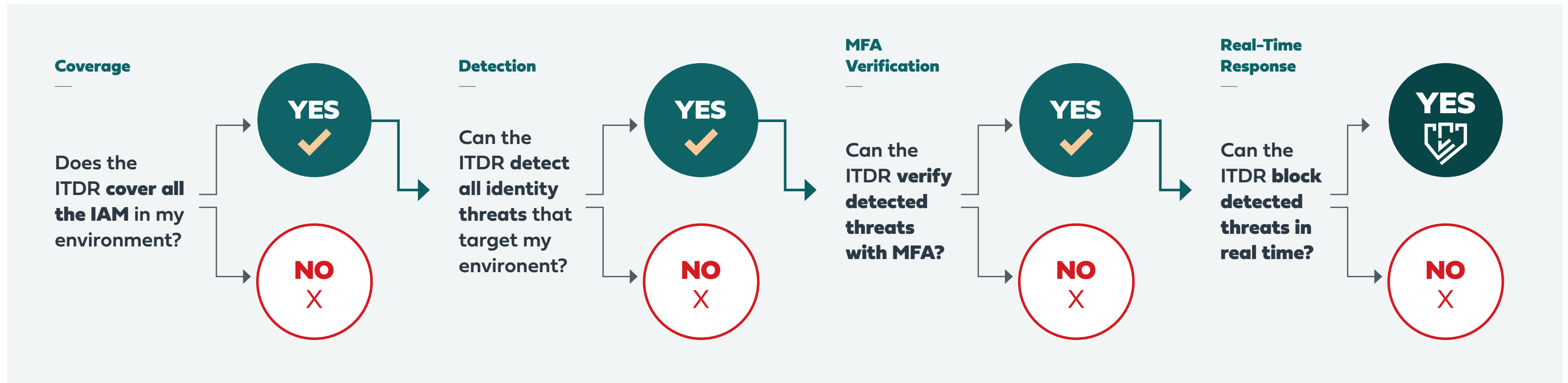
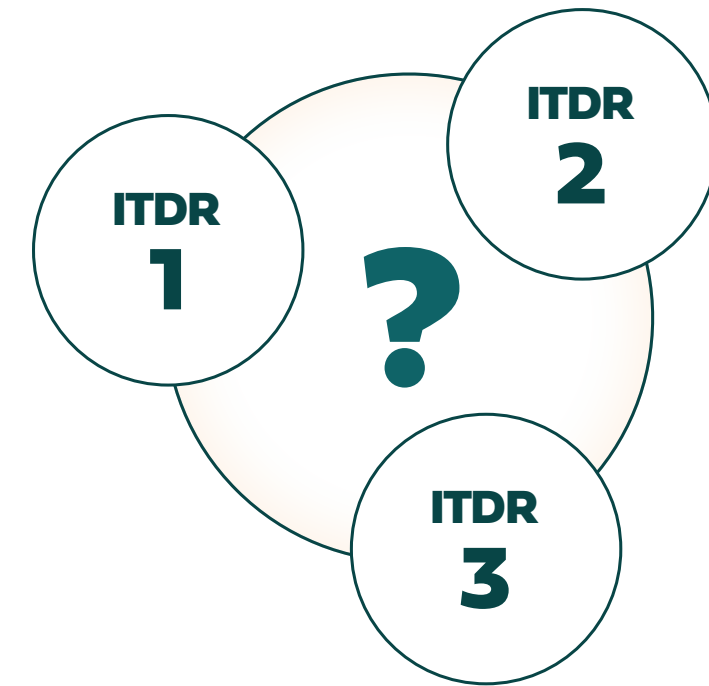
	ITDR Without MFA		ITDR With MFA
	Alert	Block Access	Verify User Identity
False Positive	 Waste of precious SecOps investigation time until the alert is validated as false alarm	 Legitimate user's access is blocked	 Zero SecOps effort required, since the immediate response is crowdsourced to the employee who only loses a few seconds of time
True Positive	 Another alert added to the SecOps queue that requires manual triage and investigation while the attack is in full gear	 Attack blocked. SecOps must investigate rapidly to validate that it's not a false positive before actual remediation can take place	 Attack is blocked and validated in real time. SecOps gets immediate insight into the compromised user and resources, facilitating immediate remediation efforts





# The ITDR Decision Process

By incorporating everything discussed, we can now define a straightforward evaluation framework in order to shortlist the ITDR solution that best fits the identity protection needs of your environment.

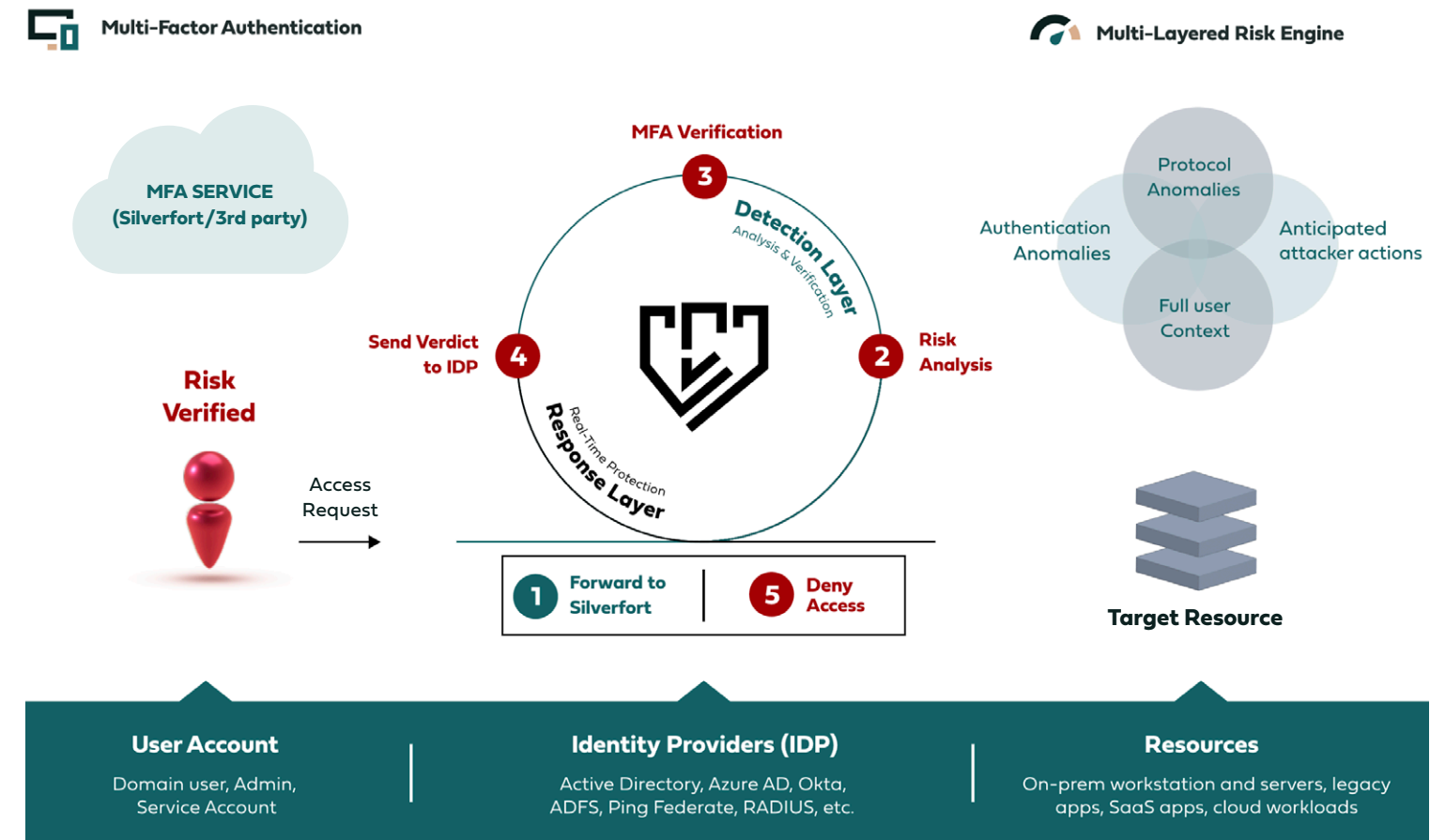




# The Silverfort ITDR Way: Real-Time Protection Against All Identity Threats

Silverfort's Unified Identity Protection platform is the first to introduce a full set of ITDR capabilities with native integration into all IdPs (including AD, Azure AD, ADFS, Okta, and PingFederate). Silverfort's ITDR natively integrates into the authentication flow of these IdPs, which forward every incoming access request to Silverfort for risk analysis, then await its verdict before granting or denying access.

In addition, Silverfort ITDR is the only solution that can extend MFA to all legacy and on-prem authentication, including legacy applications, command-line access to workstations and servers, file shares, and many other systems that could not have been protected in this way before. This makes Silverfort's ITDR solution the ultimate protection against lateral movement and ransomware attacks in AD environments.



## How Silverfort's real-time ITDR protection works:

1. Adversary attempts to access a resource, providing the IdP valid, yet compromised, user credentials. The IdP forwards the access request to Silverfort for risk analysis.
2. Silverfort's risk engine suspects a compromise may have occurred.
3. Silverfort instructs the MFA service to send an MFA verification to the user, that verifies whether the user attempted to access the resource.
4. Based on the MFA response, Silverfort determines that the user account is indeed compromised and instructs the IdP to block access.
5. The IdP denies the malicious access, and the attack is blocked.



# About Silverfort

Silverfort has pioneered the first-ever Unified Identity Protection platform, which protects enterprises against identity-based attacks that utilize compromised credentials to access enterprise resources. Using innovative agentless and proxyless technology, Silverfort natively integrates with all existing IAM solutions to extend secure access controls such as Risk-Based Authentication and MFA across all on-prem and cloud resources. This includes assets that could never have been protected in this way before, such as homegrown/legacy applications, IT infrastructure, file systems, command-line tools, machine-to-machine access, and more. Silverfort continuously monitors all access attempts by users and service accounts, and analyzes risks in real-time using an AI-based engine to enforce adaptive access policies.

**For more information, visit [silverfort.com](https://silverfort.com)**

