Secureworks®

Identity Threat Detection and Response (ITDR) Buyer's Guide

The Current State of Identity Threats

90% of organizations experienced an identity breach in the last year as identity attacks have increased in sophistication and prevalence[1]. Organizations depend on their identity infrastructure to facilitate collaboration, remote work, and access to internal systems. This has made identities prime targets for threat actors, posing a significant risk to organizations across all sectors and often serving as a gateway for severe breaches.

95%
of organizations have critical identity misconfigurations that could lead to a cyber-attack

Cybercriminals are continually evolving their tactics to exploit vulnerabilities in identity management systems. These systems are inherently complex, involving multiple components that are constantly changing, including authentication, authorization and user provisioning. This complexity can lead to misconfigurations and security gaps. Analysis of Microsoft Entra ID and Active Directory environments by Secureworks Incident Response team has revealed that 95% are misconfigured, opening the door for cyber-criminals to escalate privileges and carry out identity-based attacks.

90%
of organizations experienced an identity breach in the last year[1]

When it comes to identity threats, it is imperative that organizations are proactive in their defense strategies. Preventative measures, such as maintaining good security hygiene and strengthening identity security posture before an attack occurs, are equally important as detection and response efforts, which involve monitoring for attacks and stopping them once they are underway. Identity threat detection and response (ITDR) solutions can deliver this comprehensive approach to managing identity threats.

Why Identity and Access Management (IAM) Does Not Solve the Problem

Most organization leverage identity and access management (IAM) systems to manage user identities and control access to resources. However, these systems are often insufficient by themselves to fully protect against identity attacks due to five key limitations. IAM systems:

1. Primarily focus on authentication and authorization, which means they can be bypassed if an attacker successfully compromises legitimate credentials through phishing, social engineering, or brute force attacks.
2. Typically rely on static policies and rules that may not adapt quickly enough to detect and respond to sophisticated, evolving threats.
3. Lack comprehensive monitoring and anomaly detection capabilities, making it difficult to identify unusual behavior that could indicate an ongoing attack.
4. Can be complex to configure and manage, leading to potential misconfigurations that attackers can exploit.
5. May not integrate seamlessly with all applications and services within an organization, creating gaps in coverage that attackers can target.

While IAM systems are a critical component of an organization's security strategy, they must be complemented with additional layers of security to effectively mitigate identity attacks. According to Gartner Research, "Conventional identity and access management and security preventive controls are insufficient to protect identity systems from attack. To enhance cyberattack preparedness, security and risk management leaders must add ITDR capabilities to their security infrastructure[2]."

A New Approach to Identity Protection: ITDR

Identity threat detection and response has emerged as the next evolution of identity protection to safeguard against the escalating risks associated with identity-based cyber threats. By continuously monitoring your environment, ITDR solutions can detect anomalies and potential breaches early, enabling a swift response.

ITDR solutions encompass prevention, detection, and response capabilities, providing a comprehensive approach to identity security.

> **Conventional identity and access management and security preventive controls are insufficient to protect identity systems from attack. To enhance cyberattack preparedness, security and risk management leaders must add ITDR capabilities to their security infrastructure[2].**
>
> *Gartner Research*

> **Taegis IDR is uncovering risks in areas that I used to worry about within Azure and the Microsoft ecosystem, like conditional access policy gaps and insecure or over-privileged applications.**
>
> *Senior Information Security Officer*

These solutions continuously assess identity posture to proactively identify and mitigate potential exposures and misconfigurations, ensuring that only authorized users can access critical resources. Advanced threat detection capabilities protect identities against a wide array of threats, while automated response mechanisms enable immediate action to neutralize threats without manual intervention, thereby reducing response times.

Additionally, some ITDR solutions offer dark web monitoring to scan for compromised credentials, and risky user monitoring to identify users whose behavior or credentials may pose a higher risk. This allows for targeted interventions and enhanced security measures, adding an extra layer of protection.

5 "MUST HAVES" FOR YOUR ITDR SOLUTION

Continuous Identity Posture Assessments

Continuously scans your environment to quickly identify misconfigurations and security posture gaps.

Identity Detection

Detects advanced identity-based threats before they can impact your business.

Identity Response

Automated response actions to contain and mitigate identity threats.

Dark Web Monitoring

Monitors and alerts when login credentials have been exposed in data breaches or on the dark web.

Risky User Monitoring

Monitors for abnormal activity associated with the use of stolen credentials.

Questions to Ask a Vendor When Evaluating an ITDR Solution

- Can your solution integrate with our existing identity and access management (IAM) system?
- What kind of visibility would your solution provide into identities?
- Does your solution continuously monitor for misconfigurations and security posture gaps?
- How does your solution help benchmark and monitor security posture over time?
- How many and what types of identity posture checks does your solution perform?
- Does the solution look for security gaps in conditional access policies, apps, and service principles?
- How does your solution detect identity-based threats, and what types of threats can it identify?
- Can your solution detect both known and unknown threats, including zero-day attacks?
- How does your solution leverage artificial intelligence (AI) to help detect the latest threats?

- What automated response actions does your solution support when a threat is detected?
- Does your solution include user behavior analytics (UBA) to identify anomalous activities?
- Does your solution include dark web monitoring to reduce the risk of leaked or stolen credentials?
- Do you offer a centralized XDR platform that your ITDR solution can be integrated with for broader data correlation and threat detection and response?
- What types of reports and dashboards are available?
- How easy is it to deploy and manage the solution, and what kind of ongoing maintenance is required?

Introduction to Secureworks Taegis IDR

Secureworks detects and responds to identity threats that bypass traditional identity security controls, protecting against 100% of MITRE ATT&CK Credential Access techniques[3]. Taegis™ IDR, an ITDR solution designed to improve your security posture, continuously monitors your environment for identity risks and misconfigurations while also providing dark web intelligence on compromised credentials. Uncover your identity risks in under 90 seconds[4] compared to days with legacy solutions and benchmark the reduction of your identity attack surface over time with the Identity Posture Dashboard. Taegis IDR identifies risky user behaviors, monitoring for when stolen or compromised credentials are used to access a system, and identifies unusual login patterns, such as logins from unexpected locations. With Secureworks, you gain comprehensive protection in a single platform across identity, endpoints, network, cloud, email, and other business systems, all without breaking your budget.

> **I am thoroughly impressed with Taegis IDR and how it has improved visibility into our identity risks. Having the information available within XDR is huge.**
>
> ***Richard Hay**, Senior Information Security Officer, First Community Bank*

Next Steps

Read the Taegis IDR Datasheet.

Learn more at secureworks.com/IDR

TRY US TODAY

1. *Identity Defined Security Alliance (IDSA), 2023 Trends in Securing Digital Identities, July 2023*
2. *Based on Secureworks data gathered from thousands of incident response engagements conducted by the Secureworks Counter Threat Unit™*
3. *Based on available Taegis Detectors mapped to the MITRE ATT&CK frame*
4. *Average time to detect identity exposures calculated based on existing Secureworks customer data*

Secureworks®

Secureworks (NASDAQ: SCWX) is a global cybersecurity leader that secures human progress with Secureworks® Taegis™, a SaaS-based, open XDR platform built on 20+ years of real-world detection data, security operations expertise, and threat intelligence and research. Taegis is embedded in the security operations of thousands of organizations around the world who use its advanced, AI-driven capabilities to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist.
secureworks.com