HUNTRESS

The Straightforward Buyer's Guide to ITDR

How to find the right identity threat detection & response (ITDR) solution for your business

Table of Contents

Executive Summary

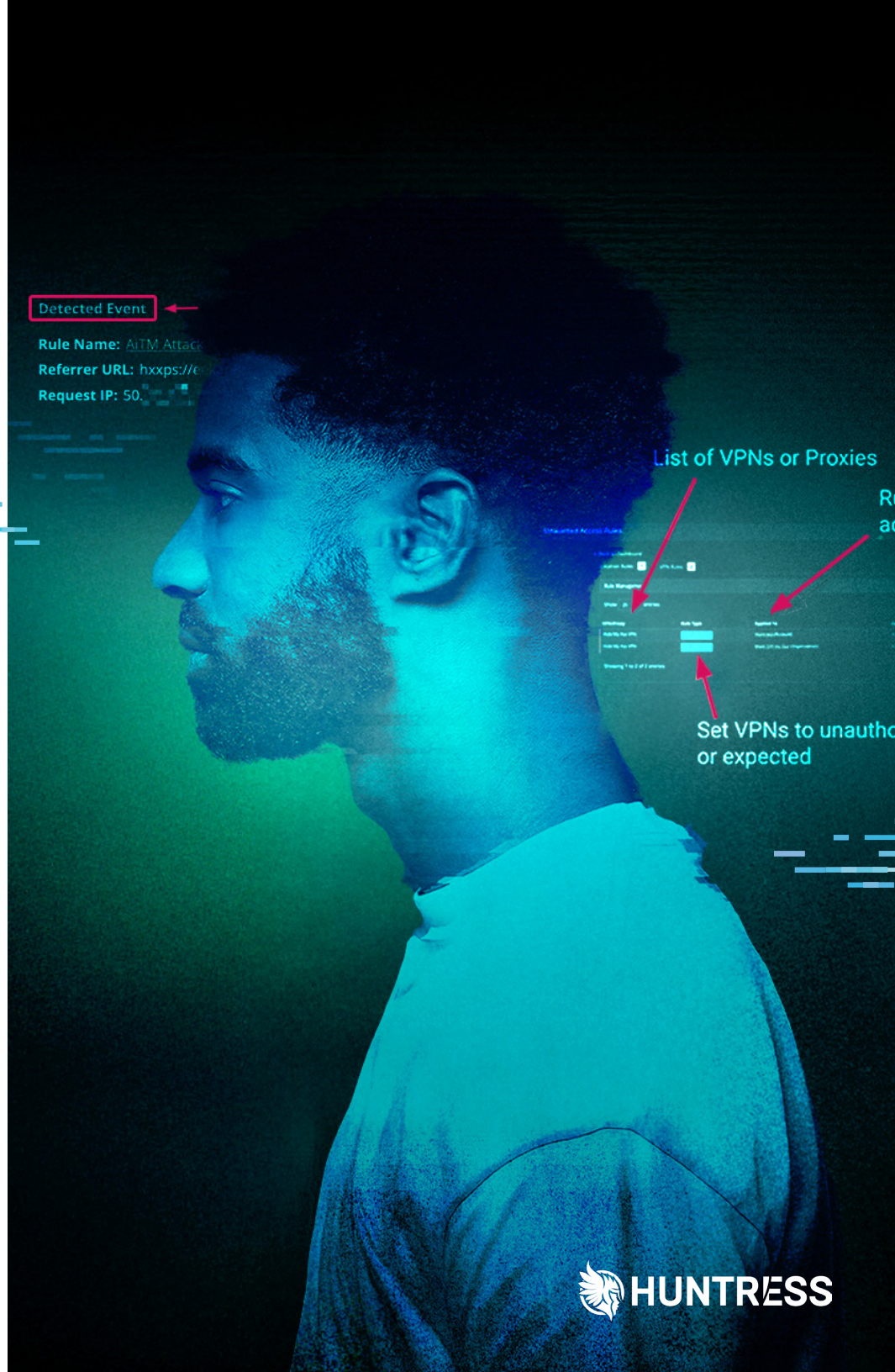
Identity is the new endpoint—and attackers know it. From infostealers and session hijacking to malicious OAuth apps hiding in plain sight, today's breaches aren't caused by breaking in...they're caused by logging in.

The problem? Traditional defenses like EDR and MFA weren't built to detect identity abuse in Microsoft 365, Azure AD, or cloud-based infrastructure. Even native Microsoft tools often miss stealthy persistence and unauthorized access, leaving organizations exposed long after the initial compromise.

Managed Identity Threat Detection and Response (ITDR) fills this critical gap. It's not just about seeing events—it's about detecting and disrupting identity-based attacks before they turn into full-blown incidents.

This guide walks you through what to look for in a modern ITDR solution, how to separate signal from noise, and why Huntress delivers the only managed offering built specifically for mid-market IT teams and MSPs. If you're still relying on EDR alone, it's time to rethink your frontline defenses.

Let's get into it.

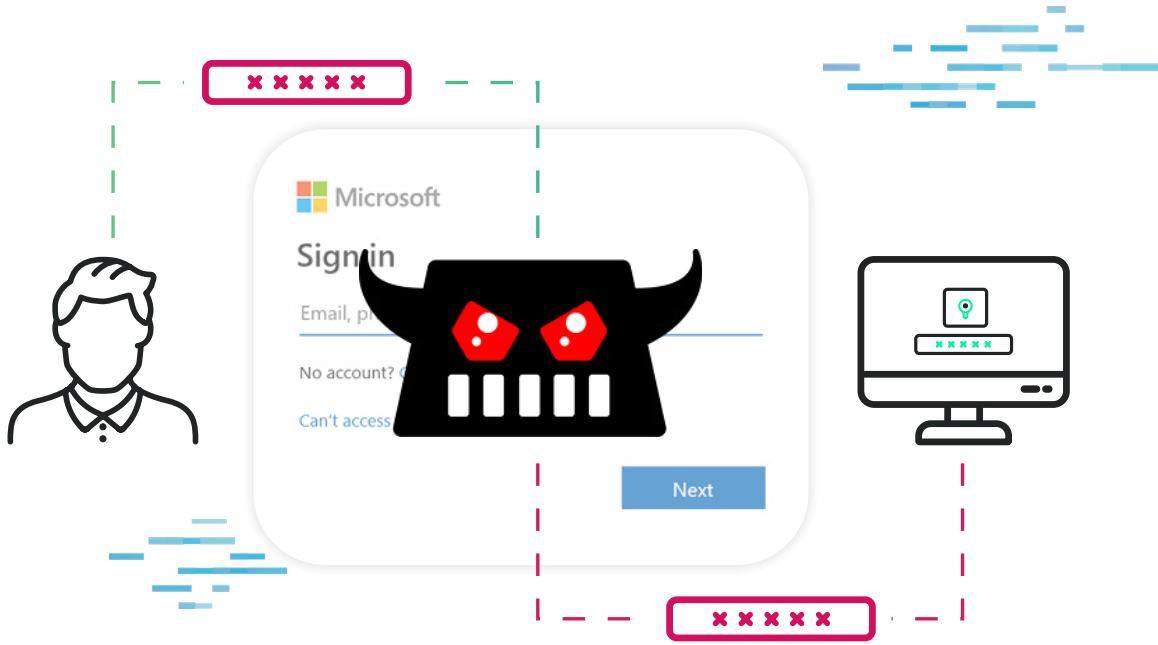


The Identity Threat Landscape

Attackers aren't dropping malware—they're hijacking sessions, abusing trust, and logging in with stolen credentials. According to Huntress data, **over 78% of breaches now involve identity-based techniques**, making credentials more valuable than zero days. Infostealers siphon login data in bulk, selling it on the dark web for pennies per identity. Malicious OAuth apps silently embed themselves in Microsoft 365. Adversaries-in-the-middle hijack sessions without ever triggering an endpoint alert.

And once they're in? They blend in, escalating privileges, maintaining persistence, and quietly exfiltrating data. These tactics don't trip antivirus or EDR tools because they aren't malware—they're abuse of identity and access.

The result: threats go undetected for days, weeks, or longer. The identity layer has become the new battleground, and most defenses were never designed for this.



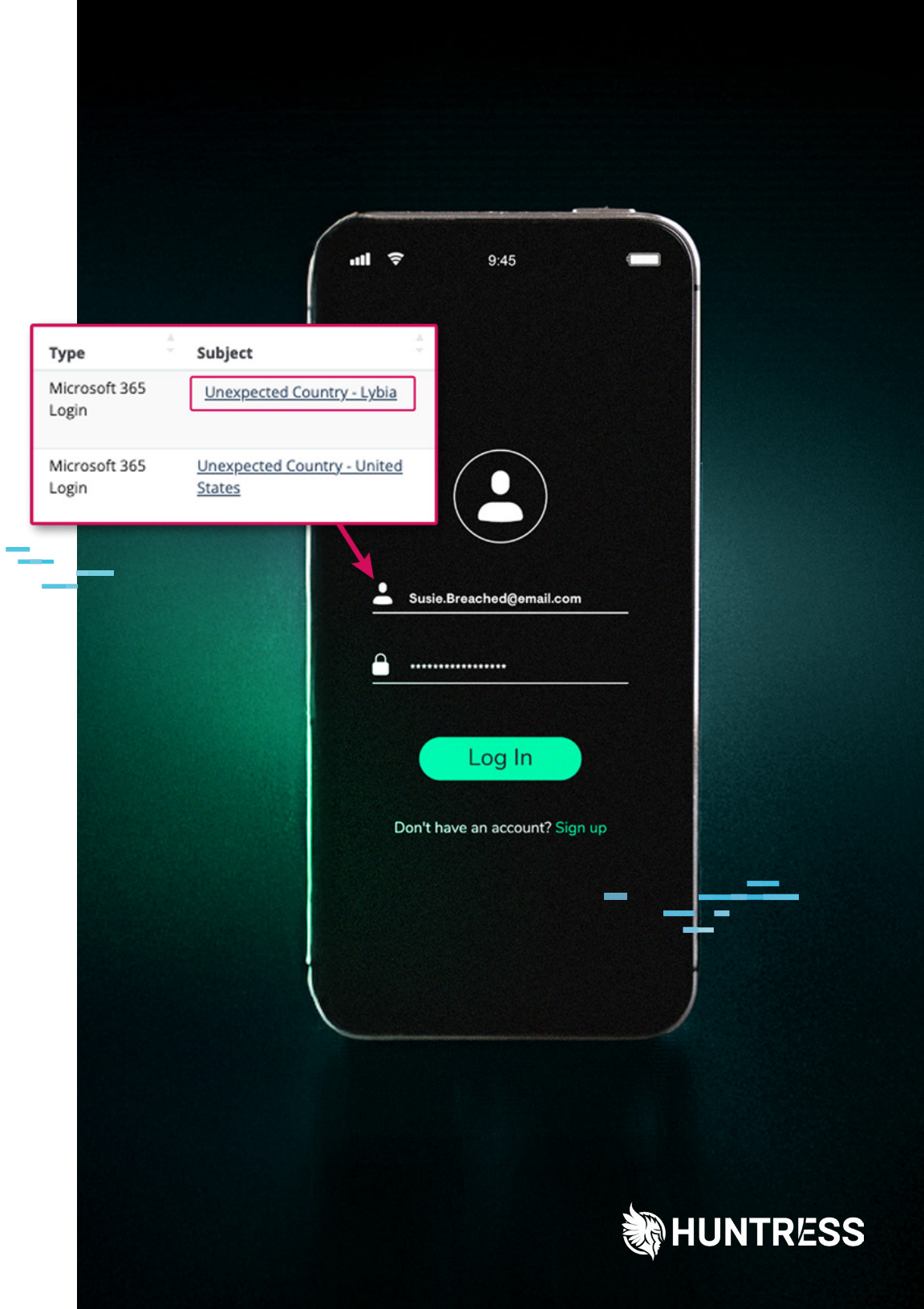
HUNTRESS

What is ITDR, and Why Do You Need It?

Identity Threat Detection and Response (ITDR) is a security discipline focused on finding, investigating, and responding to identity-based threats: think stolen credentials, session hijacking, malicious OAuth applications, and abuse of legitimate access. Unlike traditional tools that monitor endpoints or networks, ITDR zeroes in on the identity layer: your users, accounts, permissions, and how they're being used (or misused) across cloud and hybrid environments.

Organizations need ITDR because attackers have shifted tactics. Instead of exploiting software vulnerabilities, they're exploiting human ones—phishing for passwords, stealing tokens, or using infostealers to quietly harvest credentials. Sometimes the attack is simply reading an email. Once inside, they can blend in by using the same tools and access as legitimate users. These threats often fly under the radar of legacy defenses because they don't trigger malware alerts or endpoint detections.

In short, ITDR helps organizations spot and stop the kinds of stealthy, identity-driven attacks that traditional security stacks were never designed to catch.



How ITDR Is Different from EDR

Endpoint Detection and Response (EDR) and **Identity Threat Detection and Response (ITDR)** are both critical components of a modern security stack, but they solve different problems.

EDR focuses on devices. It monitors for malware, exploits, and suspicious activity on endpoints like laptops and servers. It's great at spotting ransomware, backdoors, and hands-on-keyboard activity—and only if the threat lands on a machine you control.

But attackers have evolved. They don't always need malware or an endpoint. Modern threats often start with a stolen credential, a malicious OAuth app, or a hijacked session token - bypassing the endpoint entirely. That's where ITDR comes in.

ITDR monitors identity systems—like Microsoft 365, Azure AD, Google Workspace, and cloud access—for signs of unauthorized or stealthy access. It detects persistence techniques that EDR simply can't see because they don't touch the device.

ITDR vs. EDR: What They Cover

Feature/Focus	EDR	ITDR
Primary Focus	Endpoint and host activity	Identity systems and access behaviors
What It Detects	Malware, exploits, process anomalies	Stolen credentials, OAuth abuse, session hijacking
Common Data Sources	OS-level telemetry, agents, files	Sign-in logs, identity metadata, session activity
Attack Surface Coverage	Devices (laptops, servers)	Cloud identities, accounts, sessions
Visibility into SaaS/Cloud Threats	Limited or none	Deep, continuous monitoring
Detects Rogue OAuth Apps	✗	✓
Detects Unwanted Access / Lateral Movement via Identity	✗	✓
Requires Endpoint Presence	✓	✗ (can detect even if no endpoint is involved)
Best For	Malware-based attacks	Identity-based attacks
Response Capabilities	Stop process, isolate endpoint	Disable user, revoke sessions/apps

HUNTRESS

How ITDR is Different from Point Solutions

Point solutions like spam filters, MFA, and conditional access policies are essential, but they're not enough. They help prevent some attacks, but they don't offer the visibility or response needed when attackers bypass those controls (and they do!)

Identity Threat Detection and Response (ITDR) steps in after prevention fails. It continuously monitors your identity infrastructure, detects stealthy and sophisticated threats in real time, and enables rapid containment and remediation—something most point tools weren't designed to do.

TL;DR

- Spam filters try to stop phishing, but can't stop what happens when a phish succeeds.
- Conditional Access helps enforce policy, but attackers can still work around it with stolen sessions or trusted apps.
- MFA is critical, but adversaries-in-the-middle (AiTM) and token theft still bypass it.

ITDR closes the gap. It doesn't replace your point solutions—it makes them smarter by detecting what they miss and responding when they fail.

ITDR vs. Point Solutions: What They Cover

Feature/Focus	Point Solutions (MFA, CA, Spam Filters)	ITDR
Primary Goal	Prevention	Detection and Response
Stops Known Threats	✓	✓
Detects Stealthy Persistence (e.g. Rogue Apps)	✗	✓
Detects MFA Bypass / Session Hijacking	✗	✓
Monitors OAuth Application Behavior	✗	✓
Investigates Suspicious Identity Activity	✗	✓
Provides Threat Context and Timelines	✗	✓
Takes Remediation Actions (e.g., disable identity)	✗	✓
Best For	Blocking known attacks and risky access	Detecting, containing, and responding to advanced identity threatsattacks

HUNTRESS

How ITDR Works

Integration & Data Collection

ITDR solutions integrate with identity systems like Microsoft 365, Azure AD, Entra ID, and hybrid Active Directory to continuously gather essential telemetry like user sign-ins, OAuth app usage, mailbox rule changes, session metadata (IP, device, location), and more. Logs flow in near real-time for ongoing analysis.

Intelligent Detection Logic

Advanced behavioral analytics and detection rules examine the telemetry for identity-focused threats:

- Contextual login anomalies
- Use of unauthorized or malicious OAuth apps
- Evidence of session hijacking or token misuse
- Unauthorized mailbox rule modifications

These detections often leverage cloud-scale visibility and threat intelligence to identify subtle signs of identity abuse.

Signal Escalation & Triage

When a suspicious event is spotted, it generates a prioritized signal (or alert). In human-backed models, analysts triage these signals - reviewing context, pulling in more data, and validating whether the activity is benign or malicious.

Analysis & Investigation

Analysts (or automated systems) investigate each suspicious event, pinpointing details such as login location, device details, OAuth app permissions, or mailbox activity. They may also run forensic tools to gather deeper insight, such as session tokens and access patterns.

Remediation & Containment

Once confirmed, containment steps are taken:

- Disabling or suspending compromised accounts
- Blocking or revoking rogue OAuth applications

These measures aim to eliminate attack persistence without disrupting normal operations.

Incident Reporting & Guidance

The outcome should be documented in a clear incident report, including:

- The timeline of malicious activity
- What the detection revealed
- Which remediation steps were taken (or recommended)
- Further actions (e.g., credential rotation, threat-hunting follow-up)

Continuous Improvement & Threat Hunting

The system refines its detection logic over time, using insights and feedback to tune alert thresholds and add coverage for emerging identity threats. Proactive threat-hunting exercises optionally search for hidden or stealthy attacks that may not yet trigger standard alerts.

Basically, ITDR continuously monitors and analyzes identity activity, escalates suspicious behaviors, investigates with contextual clarity, and gives you targeted remediation to stop identity-based attacks that bypass traditional endpoint or network defenses.

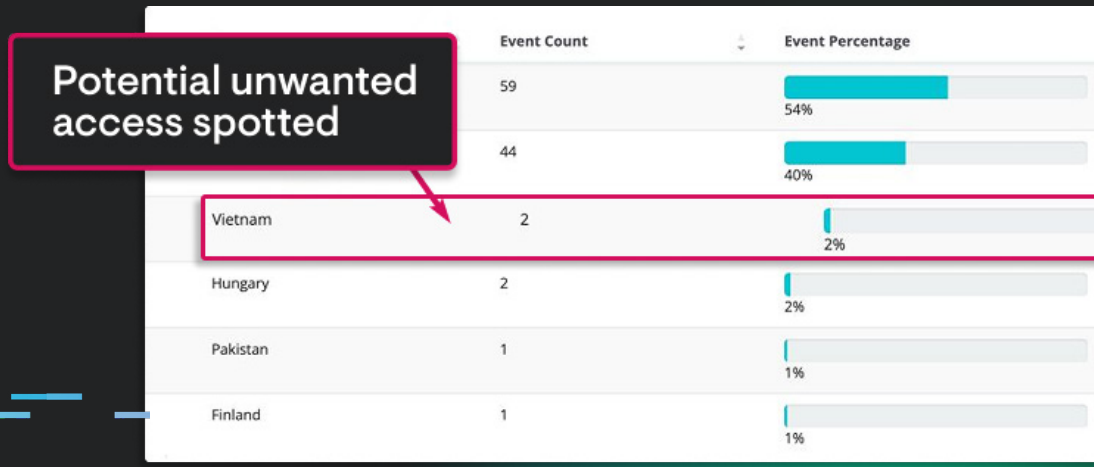
HUNTRESS

Must-Have Capabilities in an ITDR Solution

- Continuous Microsoft 365 monitoring
- Rogue/malicious OAuth app detection and remediation
- Unwanted access and anomaly detection
- Session hijacking and suspicious sign-in tracking
- 24/7 Human-led investigation and response
- Identity disablement for Microsoft 365 and AD synced identities
- Support for all Microsoft licensing tiers
- Fast time-to-value and easy deployment
- Partner- and practitioner-friendly experience

What Do You Want from Your ITDR Solution?

Use the self-assessment on the next page to help you figure out what you want and need from an ITDR solution. Answering "Yes" or "No" will help guide you toward an ITDR solution that best matches what you're looking for.



HUNTRESS

ITDR Checklist

Statement	Yes	No
We're concerned about credential theft, session hijacking, or token misuse in Microsoft 365.	☐	☐
We need to detect and stop malicious OAuth and Rogue Apps before they gain access to sensitive data.	☐	☐
We want visibility into identity activity beyond just login attempts (e.g., mailbox rule changes, MFA bypasses).	☐	☐
We manage a hybrid identity environment (cloud + on-prem Active Directory).	☐	☐
We need to be able to disable compromised user accounts quickly - without jumping between tools.	☐	☐
We prefer human-led triage over purely automated alerts.	☐	☐
We want straightforward incident reports: what happened, how it was contained, and how to prevent it.	☐	☐
We don't want to rely on premium Microsoft licensing to get the visibility we need.	☐	☐
We want a provider who can detect identity threats that EDR and email security tools miss.	☐	☐
We want business-level visibility into identity risks and remediation performance (e.g., MTTR, dwell time).	☐	☐
We use (or plan to use) both Microsoft 365 and Google Workspace.	☐	☐
We're overwhelmed by the number of alerts we get—or aren't confident in which ones to act on.	☐	☐
We need a partner that can handle identity response 24/7, - even when we're offline.	☐	☐

HUNTRESS

How to Evaluate Your ITDR Needs

Choosing the right ITDR partner means cutting through the buzzwords and getting clear on capabilities, coverage, and outcomes. Use this checklist to guide your process and check if your vendor is just watching identity threats and not actually doing something about them.

Core Evaluation Questions

- Do you monitor for threats beyond login activity like OAuth abuse, session hijacking, and mailbox rule manipulation?
- Can you detect and remediate malicious OAuth or Rogue Apps?
- How do you identify session hijacking or token-based persistence?
- Do you support hybrid environments with both cloud and on-prem Active Directory?
- Can you disable compromised identities directly, both cloud-only and AD-synced?
- Do your analysts review and confirm identity threats, or are alerts fully automated?
- What's your average response time once an identity threat is found?
- Do you need Microsoft E5 licensing or other premium subscriptions?

Analyst-Driven vs. Alert Cannon

- Do you give contextual investigation with human-led triage?
- Will we get incident reports with root cause, timeline, and remediation steps?
- Can you take direct containment actions like account disablement or app revocation?

HUNTRESS

Integration and Coverage

- Which identity providers and cloud platforms do you integrate with (e.g., Microsoft 365, Entra ID, Google Workspace)?
- How deep are your integrations: do they have telemetry ingestion or alert-forwarding only?
- Can your solution operate without requiring SIEM, EDR, or Microsoft add-ons?

Analyst-Driven vs. Alert Cannon

- What metrics do you give us (e.g. MTTR, false positive rate)?
- How do you measure false positives and missed detections?
- Can you demonstrate real-world identity threat detections and outcomes?

HUNTRESS

Buyer's Checklist

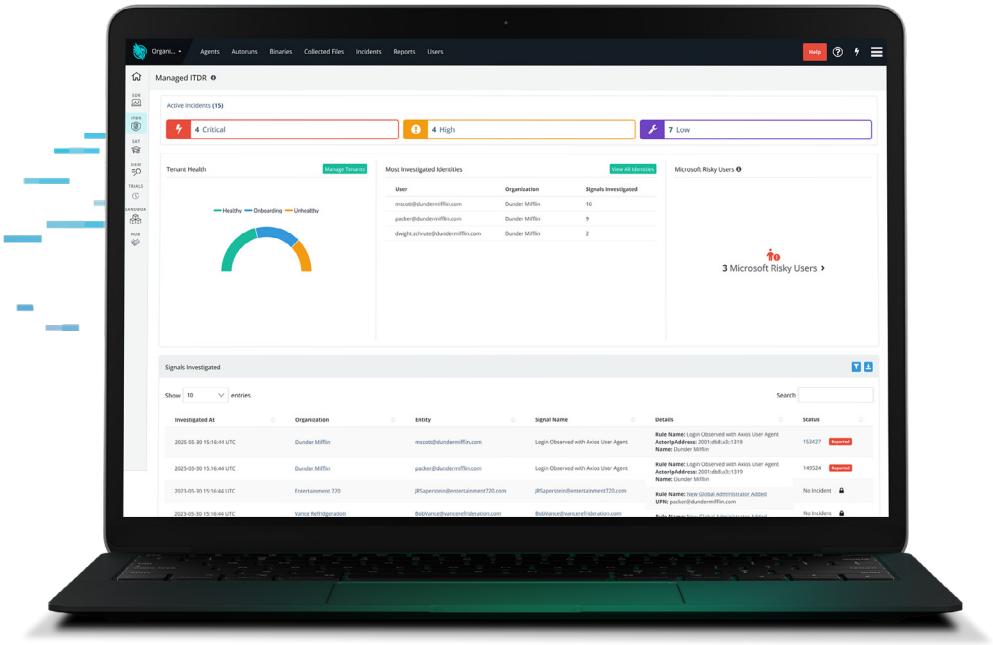
Capability	Must-Have	Nice-to-Have	Not Needed
Provides 24/7 monitoring and response	☐	☐	☐
Detects credential theft and suspicious sign-ins	☐	☐	☐
Identifies malicious OAuth and Rogue Apps	☐	☐	☐
Detects session hijacking and token misuse	☐	☐	☐
Enables tuning for VPN and location-based anomalies	☐	☐	☐
Monitors cloud-only and AD-synced identities	☐	☐	☐
Supports automatic and assisted identity disablement	☐	☐	☐
Offers human-led triage and incident analysis	☐	☐	☐
Provides detailed incident reporting and timelines	☐	☐	☐
Integrates with Microsoft 365 and Google Workspace	☐	☐	☐
Requires no premium Microsoft licensing	☐	☐	☐
Delivers business-level metrics and visibility	☐	☐	☐

HUNTRESS

Why Huntress Managed ITDR

Because identity is the new endpoint—and Huntress is built to defend it.

Attackers aren't just dropping malware anymore. They're logging in with stolen credentials, abusing OAuth apps, hijacking sessions, and lurking in cloud platforms like Microsoft 365. Most tools miss this activity because it doesn't trigger a traditional endpoint alert, and by the time someone notices, the damage is done.



Location-based and VPN Anomalies

Expose unusual login locations and VPNs to ensure only authorized users have access to your data.

Malicious Inbox & Forwarding Rules

Spot shady activity and protect your inbox.

Session Hijacking

Stop hackers from exploiting your systems and bypassing your 2FA/MFA.

Credential Theft

Keep cybercriminals out by locking down and monitoring your identity assets.

Rogue Apps

Hunt and stop malicious OAuth apps lurking in your Microsoft 365 environment.

HUNTRESS

Key Outcomes

Always-on Identity Protection
Sleep easier knowing our team of relentless identity experts monitors your Microsoft 365 environment 24/7, identifying and mitigating threats.

Block Unwanted Access
Detection and response to combat credential theft, session hijacking, and AiTM attacks to protect your most critical assets.

Uncover Rogue Apps
Detection and response to combat credential theft, session hijacking, and AiTM attacks to protect your most critical assets.

Combat Shadow Workflows
Neutralize malicious inbox and forwarding rules to protect your business from pervasive business email compromise (BEC) attempts.

No Noise. Just Results.
Every alert we send is actionable, human- verified, and built to keep you two steps ahead of the attackers. Our low false positive rate puts us ahead of others in the industry.

The ROI?

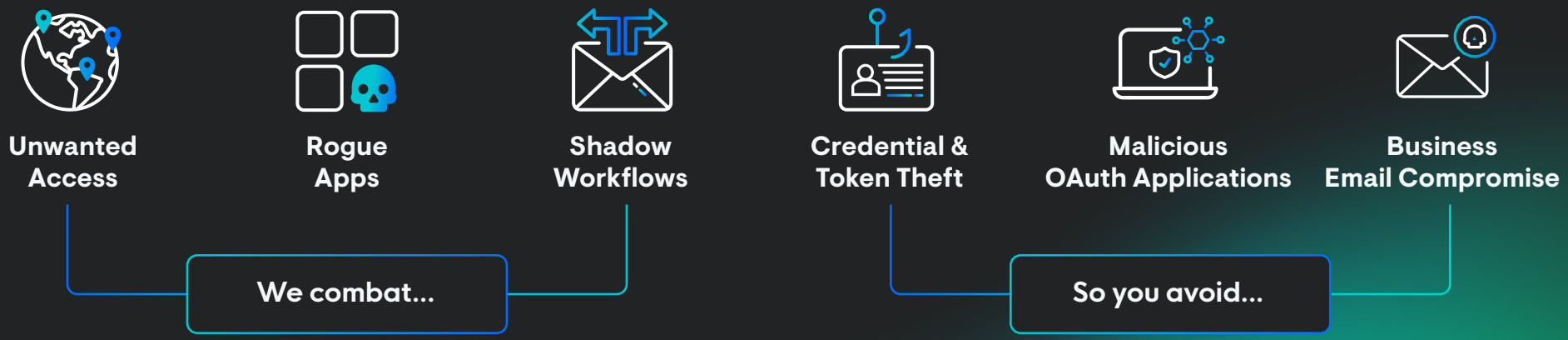
- Fewer breaches by detecting attacks that other tools miss
- Low false positive rate with a 3-minute mean-time-to-respond (MTTR)
- Faster containment with built-in remediation for both cloud and hybrid identities
- Lower resource strain with an expert, 24/7 SOC triaging and responding on your behalf
- No hidden costs—no premium licensing, no SIEM complexity, no sprawling security stack to maintain

HUNTRESS

Whether you're an internal IT/security team or MSP, Huntress Managed ITDR gives you identity security that works out of the box and pays for itself in speed, simplicity, and reduced risk.

> I was skeptical because the price seemed too good to be true, but Managed ITDR has been a game-changer. The visibility into Microsoft 365 identities, the speed of detection, and now Rogue Apps? Total no-brainer.
>
> Ryan Rowbottom
> Director of IT Services | PCS

Huntress Managed ITDR stops identity-based threats in Microsoft 365



HUNTRESS

Getting Started with Huntress Managed ITDR

Ready to stop identity threats before they spiral?

Getting started with Huntress Managed ITDR is fast and frictionless. It doesn't require premium Microsoft licensing or complex infrastructure changes. You don't need an E5 license, a SIEM, or weeks of planning—just connect your Microsoft 365 tenant, and we'll handle the rest.

Once you're up and running, Huntress will immediately start monitoring for credential theft, session hijacking, rogue OAuth applications, and signs of unwanted access across your environment. Our security experts will triage suspicious activity and guide you through any necessary response—or take direct action when time is critical.

In your trial, you'll:

- Understand how Huntress can slot into your existing security stack without the overhead5
- Experience how fast and easy it is to contain identity-based threats
- See real-time visibility into your identity attack surface
- Get alerts backed by human investigation

Identity attacks aren't slowing down. Neither should your defenses.

Start Your Free Trial

HUNTRESS

About Huntress

Huntress is a global cybersecurity company on a mission to make enterprise-grade products accessible to all businesses. Purpose-built from the ground up, Huntress' technology is specifically designed to continuously address the unique needs of security and IT teams of all sizes. From Endpoint Detection and Response (EDR) and Identity Threat Detection and Response (ITDR) to Security Information and Event Management (SIEM) tools and Security Awareness Training (SAT), the platform provides targeted protection for endpoints, identities, data, and employees, delivering trusted outcomes and valuable peace of mind.

Its 24/7, AI-assisted Security Operations Center (SOC) is powered by a team of world-renowned engineers, researchers, and security analysts, dedicated to stopping cyber threats before they can cause harm. Huntress is often the first to respond to major hacks and incidents, with its expert security team sharing real-time tradecraft analysis and actionable advisories with the community. Currently safeguarding over 4 million endpoints and 6.8 million identities, Huntress empowers security teams, IT departments, and Managed Service Providers (MSPs) worldwide to protect their businesses with enterprise-grade security accessible to everyone.

As long as hackers keep hacking, Huntress keeps hunting. Join the hunt at www.huntress.com

Contact us to learn more.

Cosmistack, Inc.

support@cosmistack.com

https://cosmistack.com

In partnership with cosmistack and HUNTRESS