Identity Is the Attack. ITDR Is the Answer.

The lowest-friction way to stop one of today's top threat vectors and the easiest way to start and grow your business with Blackpoint.

Identities Are Under Siege. Are You and Your Customers Protected?

Today, over 80% of breaches now start with a compromised identity, not malware, making identity threat detection and response (ITDR) one of the fastest growing cybersecurity offerings in the market. MFA bypass, account takeovers, and session hijacking are just a few of the ways threat actors are logging in instead of breaking in through unlocked doors and windows.

Unfortunately, the FUD is Real

> In 2025, there was a **160%** upsurge in credential theft[1] with **1.8B** logins stolen[2], and **$2.7B** in reported business email compromise losses in 2024.[3]

Unfortunately, the threats are real and the impacts are significant. We all know that. Blackpoint is here to help you determine if this is something you need in your tech stack, if this is the right time, and how to share with your clients why they need protection when everyone thought MDR and EDR was enough.

Now Is the Time for ITDR

Most MSPs have focused on EDR and MDR over the last few years. But as identity-based attacks become a growing threat vector, especially with the help of AI, it is where our defenses need to turn.

If you're not sure, here are a few questions you can ask yourself and your IT team to determine if ITDR is a 'now problem' or a 'someday problem' for you and your customers.

Ask Yourself and Your IT Team

1. How many of our clients run their businesses on M365 or Google Workspace? If the answer is "most" or "all," their identity layer is already the primary attack surface, not their endpoints.
2. Is MFA enforced everywhere, or just enabled somewhere? "The CEO has it, accounting doesn't" is the gap attackers and insurers both look for.
3. Have we seen inbox rule changes, forwarding setups, anomalous logins, or credential-stuffing attempts across our client base in the last 6–12 months? If you haven't looked, that itself is an answer.
4. Do we have any 24/7 visibility into identity behavior, or does our monitoring stop at the endpoint? MDR/EDR won't catch an attacker who logs in with a stolen password — there's no malware to flag.
5. Are any of our clients being pushed by cyber insurers to prove MFA enforcement, phishing-resistant auth, or documented identity monitoring at renewal? That requirement is showing up more and it's a forcing function.
6. Have we lost or almost lost a deal because a competitor could say, "we cover identity" and we couldn't?

If the honest answers lean toward "we don't know," "not consistently," or "we'd have a gap," that's the signal ITDR belongs in the stack now rather than on a future roadmap.

It's the New and Easy Entry Point

SMBs are a prime target for cyber criminals who are running businesses that need to meet quotas and revenue targets.

43% of all cyberattacks now target SMBs, 3x more likely than large enterprises.[4]

88% of SMB breaches involve ransomware, most starting with stolen credentials.[5]

Because ITDR is low commitment but high visibility for your prospects, it's more of an easy "yes" if they aren't quite ready for full MDR or they can't see the value in locking all the doors and windows.

What to Look for When Evaluating Your Options

There is a lot of noise in the marketplace from a myriad of vendors saying the same thing to get you to look at their solution. We've devised a few questions to help you effectively evaluate which vendor might be best for your business and security stack.

Evaluate Every Vendor

1. How broad is the identity threat coverage? Just M365 environments or is Google Workspace and Cisco Duo covered?
2. Is it a standalone tool that lacks native correlation with MDR and EDR or full SIEM log aggregation?
3. Is the offering part of a unified platform, or will it create another siloed offering in your stack?
4. What is the vendor's MTTR? Seconds, minutes, hours?
5. Who will triage identity alerts around the clock? Will we need to add new headcount or is the vendor triaging for us?
6. Does the vendor have a 24/7 human-led SOC in your time zone that will triage for us? And do they remediate or simply send alerts our way?
7. Will the vendor be readily available for a phone call or is that a higher tier that requires additional budget to cover?
8. If an account is compromised at 2am on a Saturday, what actually happens, and how long does it take to remediate? Attackers move in minutes; if the honest answer is anything beyond minutes, once someone's awake, that's likely going to cause more damage.

Where Blackpoint Sits and Fits

Blackpoint was the first vendor to deliver a purpose-built and enterprise-grade ITDR offering before the proliferation of identity-based attacks. Here's some key facts about where we sit and fit.

What Sets Blackpoint Apart

First to market with ITDR before it was even a market category. We know this space.

We offer autonomous ITDR containment through our newly launched AI SOC Agent for Identity Threat Detection and Response. Using an AI + human hybrid model, the AI SOC Agent acts on high-confidence threats at machine speed and routes everything else to a human analyst.

Trained on 10+ years of real SOC decisions, IR forensics, and telemetry from over 1M protected accounts.

Human analysts — former NSA, DIA, and CIA operators — always available by phone.

Part of a unified platform, CompassOne: Identity signals and context shared with endpoint and cloud posture.

Broadest coverage in the market, securing M365, Google Workspace, and Cisco Duo with a unified platform.

Ecosystem integration combines ITDR alongside native endpoint, network, and cloud security in a single dashboard.

Faster containment where the automated AI SOC agent averages sub-2-minute containment times (as fast as 21 seconds).

What's In It for You?

You stay the hero to your clients. We're the SOC behind you so you never have to build one.

- ✓ Add a high-margin service line with no SOC to staff, train, or run at 2am.
- ✓ Win the "who's covering identity" conversation before a competitor does.
- ✓ A natural path to cross-sell into full MDR and CompassOne over time.
- ✓ Differentiate against every competitor still selling MDR-only or ITDR-only.
- ✓ The AI SOC Agent is built into every ITDR tier with no additional cost.

Already a Blackpoint partner? Add ITDR to your stack today. New to Blackpoint? Start with ITDR to instantly show value.

Request a Demo: blackpointcyber.com/demo | Start a Free Trial: blackpointcyber.com/free-trial | +1 410-203-1604

Endnotes

1 Check Point Software Technologies. (2025, August). The alarming surge in compromised credentials in 2025. Check Point Blog. https://blog.checkpoint.com/security/the-alarming-surge-in-compromised-credentials-in-2025/

2 Flashpoint. (2025). Global threat intelligence index: 2025 midyear edition. https://flashpoint.io/resources/report/flashpoint-global-threat-intelligence-index-midyear/

3 Internet Crime Complaint Center. (2025). 2024 internet crime report. Federal Bureau of Investigation. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

4 U.S. Small Business Administration. (2023, September). Cyber safety tips for small business owners. https://www.sba.gov/blog/2023/2023-09/cyber-safety-tips-small-business-owners

5 Verizon Business. (2025). 2025 data breach investigations report. https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf