Blackpoint's Enrichment Engine for ITDR

Stop cloud identity attacks before they become breaches.

Modern attackers don't break in. They blend in with normal traffic by logging in with stolen credentials and using legitimate-looking workflows. Most MDR tools miss this because they're built for endpoints, not the identity layer where cloud attacks actually happen.

Blackpoint's enrichment engine gives our SOC the context to catch what others miss.

Every authentication event gets enriched in real time across numerous categories, including but not limited to: autonomous sources, user agents, VPN and proxy usage, geolocation, and connected applications. Our analysts use that intelligence to separate real threats from noise, disable compromised accounts fast, and keep your clients protected around the clock.

ITDR Detection in Action

ITDR correlates signals across dozens of identity threats. Here are five common examples of what it catches for your customers.

Category	What it catches
Autonomous Sources & Systems	Logins from infrastructure that shouldn't be there
User Agents	Abnormal or known-risky agents used during authentication
VPN & Proxy	Anonymizing services masking credential misuse
Geolocation	Logins that deviate from a user's behavioral baseline
Applications	Unauthorized apps connected to accounts before they become a breach path

These five categories are a sample. ITDR continuously correlates signals across authentication, device, geolocation, application, and behavioral data, catching the slow, staged attacks that single-event logic misses, and extend enrichment into SIEM log sources.

What It Means For Your Clients

Cloud identity attacks move fast. Blackpoint's SOC moves faster. With continuous enrichment, our SOC catches threats early and prevents a full-blown security incident from happening so your clients stay protected.

Talk to your Blackpoint rep to learn how we can help you protect your clients' cloud identities.