STAY AHEAD OF THE ATTACK TIMELINE WITH MDR ESSENTIALS

BLACKPOINT DELIVERS ESSENTIAL THREAT COVERAGE WHERE IT MATTERS MOST, RIGHT BETWEEN COMPROMISE AND DAMAGE.

MDR Essentials provides real-time detection, active response, and expert investigation to stop threat actors before they can cause significant damage.

Aligned with the NIST Cybersecurity Framework, Blackpoint covers the core functions of Detect and Respond, while also supporting Identify, Protect, and Recover. Whether in the cloud or on the endpoint, Essentials closes the gap so you are not reacting to breaches, you are preventing them.

Identify

Understand your environment, assets, and risks.

CLOUD MDR:

- Cloud identity mapping and login activity tracking
- Continuous monitoring of cloud assets

MDR:

- Endpoint visibility and behavioral baselining
- Asset inventory support through agent and network data

Detect

Identify cybersecurity events quickly and accurately.

CLOUD MDR:

- Suspicious login detection (e.g., from new geo or device)
- Impossible travel, MFA bypass attempts, OAuth abuse
- Identity-linked threat detection (when integrated with Identity Response)

MDR:

- Detection of malware (e.g., DarkGate), lateral movement, LOLBins
- Real-time detection via endpoint and network telemetry
- Identity-linked threat detection (when integrated with Identity Response)

Protect

Implement safeguards to limit or contain potential threats.

CLOUD MDR:

- Automated enforcement (e.g., session revocation, account lockout)

MDR:

- Endpoint policy enforcement
- Device isolation in response to high-risk behavior

Respond

Take action to contain or eliminate active threats.

CLOUD MDR:

- Revoke cloud sessions
- Lock or suspend compromised accounts
- Human-led incident handling through the SOC

MDR:

- Endpoint containment (host isolation)
- Adversary pursuit and guided remediation steps
- SOC-driven incident analysis, alerting, and real-time response

LEFT OF BOOM

RIGHT OF BOOM

Recover

Restore capabilities and document the incident.

CLOUD MDR:

- Post-incident reporting for compliance evidence

MDR:

- Response documentation to support recovery workflows
- Forensics to understand scope and prepare for recurrence

ESSENTIAL DEFENSE ACROSS THE ATTACK SURFACE

blackpoint

Stop Threats Others Miss

Go beyond basic EDR with behavior-based detection, identity correlation, and proactive threat disruption.

Unified Security Across Environments

Protect on-prem and cloud assets, including Office 365, Google Workspace, and Duo, with a single, integrated solution.

Faster Response, Fewer Breaches

Patented technology blocks lateral movement and privilege abuse before attackers gain control.

Human-Led SOC, Always-On

Around-the-clock threat monitoring and response by Blackpoint's expert analysts

MSP-Friendly by Design

Multi-tenant support, partner access to dashboards, and seamless integrations streamline operations and scale with your business.