blackpoint

SLICK SHEET

Behind the Scenes of Managed EDR

The Power of the SOC and APG

Managed EDR | Streamlined managed endpoint security

There are two teams within Blackpoint Cyber that make our integrations with third-party endpoint security solutions possible: our 24/7 security operations center (SOC) team and expert-led threat hunters within the Adversary Pursuit Group (APG). Knowing that data integration and workflow automation was not enough, we set out to fully manage the alerts your endpoint security solution generates.

Managed EDR surpasses metadata ingestion, complementing the integration with 24/7 triage and response capabilities. This capability derives from Blackpoint's in-house technology, SNAP-Defense, to combine endpoint security with network visualization, insider threat monitoring, anti-malware, behavior analysis, and traffic analysis. Our team of experts take your data one step further, staying ahead of adversaries on all fronts.

MEET THE TEAMS

The Security Operations Center

Our SOC is comprised of a team of industry-qualified specialists providing 24/7 coverage across a global landscape. Their mission is to monitor your and your clients' networks and detain advanced threats before they can spread laterally. As they collect and monitor your data sources, they add context to make the information actionable within the overall threat management process. With a precise lens into these movements, they can accurately identify real threats, producing a very low false positive rate and preventing interruption in your business.

The Adversary Pursuit Group

Blackpoint's SOC is supported by the APG which is comprised of threat researchers with experience in the military, intelligence community, and Fortune 500 companies. The team, led by David Rushmer, has a mandate to monitor and evaluate the constant evolving threat landscape, react to changes by reverse engineer binaries, and study threat actor behaviors. These efforts are translated into further protection within our product line and broader awareness for the cybersecurity community.

MANAGED EDR SOLUTIONS

Bitdefender · CROWDSTRIKE · CYLANCE

Malwarebytes · Microsoft Defender for Endpoint · SentinelOne

SOPHOS · WEBROOT opentext Business Solutions

MICROSOFT DEFENDER FOR ENDPOINT

Within our product bundle, Blackpoint Response, get the most out of your Microsoft 365 investment with Managed Defender for Endpoint. Directly within the Blackpoint portal, you can manage and apply Defender for Endpoint policies to multiple customers at once. Best practices informed by our APG are also available for quick setup.

MANAGED EDR, LIVE IN ACTION

Blackpoint Cyber Detains Qakbot Information-Stealing Malware

With Webroot's total endpoint protection and Blackpoint's true, 24/7 MDR, IMPACT Technology Group (IMPACT) closed the gap in threat detection for their end client. When a Qakbot detection was triggered from Webroot, Blackpoint was able to respond immediately. This Managed EDR team-up led to a heroic save missed by other security vendors in November 2022.

Play-by-Play of Our Managed EDR Response

Timeline of Attack – Nov. 14, 2022

3:03 P.M. EST	Blackpoint Security Operations Center (SOC) alerted to a Qakbot detection.
3:20 P.M. EST	An MDR analyst began triaging the event.
3:21 P.M. EST	The MDR analyst escalated for potential Qakbot activity.
3:22 P.M. EST	A Senior MDR analyst began investigation and isolated for potential Qakbot activity.
3:38 P.M. EST	The Blackpoint SOC called IMPACT and informed them of the incident.
4:10 P.M. EST	The SOC sent IMPACT an Incident Response (IR) report with recommended post-incident actions.

Industry-Leading Response Times

TIME BETWEEN INITIAL ALERT INVESTIGATION AND HOST ISOLATION:

2 minutes

Leverage Blackpoint's security ecosystem for expert-led analysis, up-to-date response capabilities, and a unified front.

BOOK A DEMO TODAY

blackpointcyber.com