blackpoint

ITDR · HISTORICAL SCAN

Uncover Past Risk. Prove Present and Future Value.

To secure what's happening today, you first need to understand what happened yesterday. Microsoft 365 environments often contain indicators of past compromise, from suspicious logins and unauthorized forwarding rules to overprivileged applications. For MSPs, that history is the easiest way to start the security conversation that grows their business.

Historical Scan & Report for M365

Review up to 180 days of activity at onboarding. Get a comprehensive report that is a clear, customer-ready summary of findings and prioritized guidance, demonstrating a strategic partnership.

Uncover Previous Risk

Identifies logins, inbox rules, and forwarding changes that signal a threat.

Map Attacker Behavior

High- and critical-severity findings map directly to MITRE ATT&CK tactics and techniques.

Explain Every Finding

Analysis breaks down each detection in plain language, using the event data behind it.

Prioritize the Response

Each finding includes next steps tied to the specific users, IPs, and applications.

Escalate Confirmed Threats

Malicious findings automatically generate a dedicated Forensic Report for deeper investigation.

Deliver Instantly

Reports are generated automatically with no manual formatting.

SAMPLE FINDING

HIGH SEVERITY

Suspicious Login From New Device and IP

User: jsmith@company.com
Detected: Feb 14, 2026
Detection ID: HS-40217

AI SOC ANALYSIS · BROC

Login originated from a device and location not previously seen for this user. No follow-on persistence activity identified.

MITRE ATT&CK

Valid Accounts · T1078

RECOMMENDED NEXT STEPS

Revoke active sessions, reset credentials, confirm login with the user.

blackpoint

REVEAL. EXPLAIN. RESOLVE.

What Gets Reviewed

- Logins from new or unfamiliar devices and IP addresses.
- Suspicious inbox rule creation and external email forwarding.
- Admin consent granted to verified third-party apps.
- Suspicious external Teams chat activity.
- Up to 180 days of threat activity that would have been detected by the SOC.

Value for the MSP

- Turns onboarding into a value moment, demonstrated on day one.
- No manual investigation or report writing required.
- A documented baseline that supports compliance and cyber insurance reviews.
- Opens the conversation that grows the account.

Value for the Customer

- Anticipates a question they didn't know to ask, "What happened before we were protected?"
- Replaces uncertainty with documented evidence.
- Instills confidence that remediation priorities are based on facts.
- Increased protection against identity threats.

ELIMINATING THREATS WITH AI SPEED AND HUMAN EXPERTISE

1+ BILLION	10+ MILLION	4+ MILLION	2,000+
Total events*	Cloud events*	EDR/AV events*	Disabled accounts for suspicious activity*

*Monthly snapshot of Blackpoint's SOC in action.

For more information, visit blackpointcyber.com