Blackpoint Cyber



Who is Blackpoint Cyber?

- 2014: Founded
- 2019: Launched 24/7 MDR, strong market fit with MSPs
- 2021: Launched industry's first cloud MDR offering
- 2025: Introduced CompassOne, The Unified Security Posture and Response Platform

Blackpoint Cyber Today

1,800
MSP partners worldwide

1 Million +
endpoints protected globally

1 Million +
Cloud Users protected

Leadership Heritage

NSA | CSS

U.S. Department of Defense

tenable

Microsoft

CISCO

Investment Partners

BainCapital

Accel

Today's Cybersecurity Challenges

Lack of Unified Visibility Across Attack Surface

Siloed information, disjoint platforms, and continuing expansion of connectivity and IT convergence.

Difficulty Prioritizing Risk & Threats

Too many alerts and vulnerabilities make it hard to identify what matters most and maximize resources.

Increasing Compliance Demands

Expanding compliance requirements continue to add workload, costs, and risks.

Security Operations at Scale

Managing security at scale, especially in multi-tenant environments, requires the right mix of technology, processes, and automation.

Cybersecurity Maturity is Difficult to Show ROI

No consistent and easy way to measure maturity and risk or how investments have made tangible improvements.

Rapidly Evolving Threat Landscape

Building and maintaining in-house expertise and capabilities with 24/7 monitoring and response is expensive and detracts from core business.

How CompassOne Solves Today's Challenges

Asset Visibility

CompassOne unifies prevention, detection, response, and recovery into a single platform, eliminating the need to juggle disconnected tools.

Prioritization

Security and IT teams spend their time addressing legitimate threats, improving security without burnout.

Effective Compliance

CompassOne provides the visibility, reporting, and posture scoring needed to help meet and maintain compliance requirements with less effort.

Scalability

The platform scales protection across clients and environments without adding operational burden or headcount.

Showing ROI

With built-in posture ratings and incident reporting, CompassOne makes it easy to demonstrate measurable value to clients.

24/7 Proven Security

CompassOne in collaboration with the SOC, filters noise and only escalates real threats, dramatically reducing alert fatigue and manual triage.

FOCUS ON SECURITY MATURITY NOT JUST TACTICS

Navigate your security posture

Underprepared

Organizations lacking necessary information to take effective action; unaware or unable to respond to current or emerging issues

Reactive

Organizations have basic platforms and structures to react to business requirements; cannot proactively prevent problems from arising

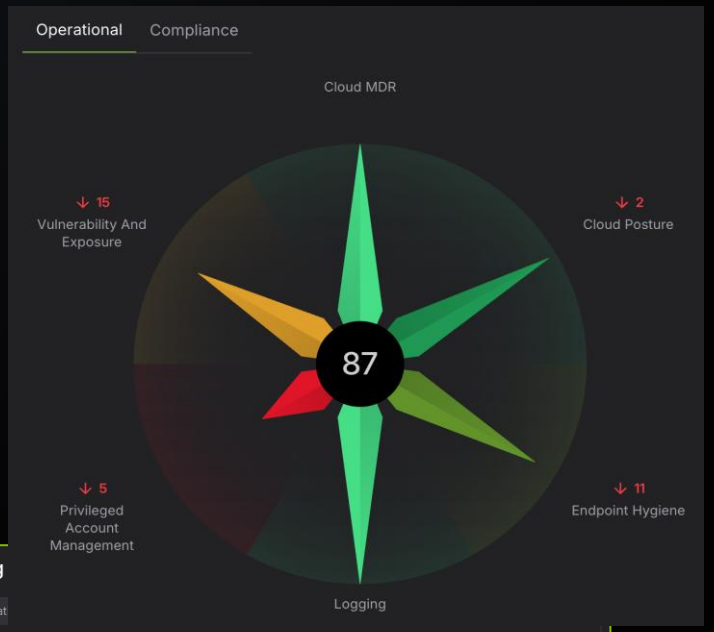


Proactive

Organizations have platforms, structures and organizational processes to proactively address current issues and challenges

Anticipatory

Organizations have platforms. structures and organizational processes to proactively address future issues and challenges

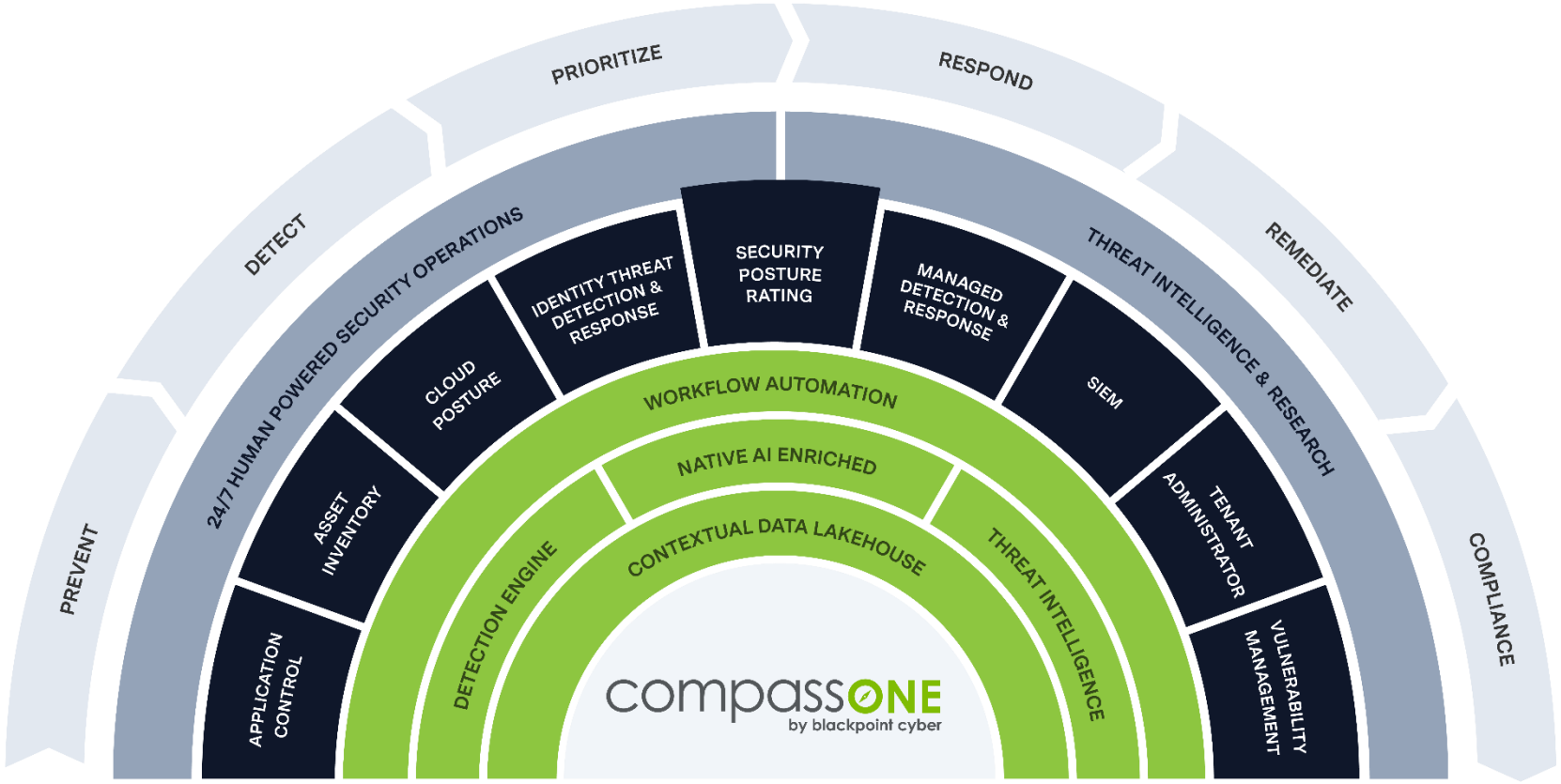


Factors Impacting Your Rating

Posture Metric	Rat			
All monitored endpoints should have a backup solution in place	1	Endpoint Hygiene	Recover	Ensure a backup system is in place for monitored endpoints
Prioritized Known Exploited Vulnerabilities (KEV) on devices should be remediated within an appropriate timeframe	10	Vulnerability And Exposure	Protect	Ensure that Prioritized KEV on devices are remediated
External Attack Surface scans should be conducted at a frequent interval such as daily or weekly	5	Vulnerability And Exposure	Identify	Configure scheduled External scans
Are there too many privileged M365 cloud accounts compared to total user accounts	5	Privileged Account Management	Identify	Review privileged M365 cloud accounts are limited to only those needing privileges
Are there any Windows or Mac assets within the environment that are running End of Life Operating Systems	2	Endpoint Hygiene	Identify	All End of Life Operating systems should be updated
Managed Application Control should be in Blocking Mode	3	Endpoint Hygiene	Detect	Enable Managed Application Control in Blocking mode

blackpoint

ONE PLATFORM. ONE AGENT.
UNIFIED SECURITY POSTURE & RESPONSE.



Blackpoint Data Collection

Blackpoint Agent

Devices

Identity

Applications

Network

Syslog

Scans

API

THIRD PARTY INTEGRATIONS

Endpoint Security: SentinelOne, CROWDSTRIKE, Malwarebytes, Windows Defender, Bitdefender, WEBROOT by opentext, SOPHOS, Microsoft Defender for Endpoint

Identity: Microsoft 365, Google Workspace, DUO, Microsoft Azure

Vulnerability Management: CONNECTSECURE, tenable, Qualys, RAPID7

Firewall: SONICWALL, WatchGuard, CISCO, FORTINET, UBIQUITI, SOPHOS, paloalto

STATS FROM OUR

Security Operations Center

~700

Responses per week

20%

of organizations find a Business Email Compromise upon onboarding Blackpoint Cyber

30:1

Cloud to On-Prem Response Ration

72%

of the time EDR is missing the attack where Blackpoint patented technology detects and responds

SOC Monthly Snap-shot

AVERAGE MONTHLY NUMBERS

1 Billion+

Total Events in Action Engine

10+ Million+

Cloud Events in Action Engine

4 Million+

EDR/AV Events in Action Engine

2,000+

Disabled cloud accounts for suspicious activity

blackpoint

BLACKPOINT SECURITY OPERATIONS

REAL PEOPLE SOLVING REAL PROBLEMS

Real Experts, Real Action

Staffed by elite analysts—former nation-state cyber operatives—who don't just monitor threats, they actively work and stop them in real time.

Instant Threat Response, Not Just Alerts

When a threat emerges, our SOC takes immediate action to neutralize it—no tickets, no delays, just real-time protection.

Full-Service SOC—You're Never Alone

We don't just notify you; we guide you. With 35,000+ direct SOC calls last year, we walk partners through incidents and remediation, day or night.

Human Expertise, Enhanced by Engineering

Our SOC works seamlessly with APG, detection engineers, and automation to focus on what matters—stopping one BEC attempt every 30 minutes, 24/7/365.

blackpoint

YouTube

MEET BLACKPOINT SOC LEADERS







Blackpoint vs. Other Solutions

The Blackpoint Difference:

1. **Advanced Threats:** Focus on tradecraft behaviors not just tools, stopping threats at the front of the attack life cycle
2. **Resource Constraint:** Extension of your team monitoring and managing on your behalf
3. **Alert Fatigue**: Uses context across your attack surface to detect and respond, increasing efficacy

Managed EDR

Focus on malware

Executes at end of attack cycle

Relies on endpoint data

Blackpoint Cyber

Monitors both malware & tradecraft

Isolates at the first sign of attack

Uses context to protect

Managed SIEM

Requires significant operational overhead

Delayed detection due to post-ingestion processing

High cost

Alert fatigue

Blackpoint Cyber

Expert teams managing for you

At the earliest stage of the attack cycle

Flexible pricing

Isolation happens on your behalf

Looking at The Threat Landscape



Surge in Critical Vulnerability Exploits

Over 30+ major threat notices from BP highlight ongoing exploitation of critical vulnerabilities.

Cybercriminals are using these vulnerabilities to gain persistence, move laterally, and exfiltrate data before launching destructive attacks.



Rising Pre-Ransomware Activity

Ransomware operators are evolving, focusing on maximizing disruption and financial gain.

Attackers are spending more time in networks before deploying ransomware, increasing the damage potential.



Identity as a Primary Target

AI-powered phishing makes social engineering harder to detect.

Obfuscation & tailored payloads bypass traditional defenses.

Fileless malware runs in memory, evading detection.

Cloud exploitation rises as many migrate operations.

blackpoint

MEET

compassONE

by blackpoint cyber

CompassOne is Blackpoint Cyber's unified security posture and response platform, purpose-built to integrate prevention, detection, response, and recovery.

CompassOne Modules

ASSET INVENTORY

Eliminate Blind Spots.
Level-Up Security.

TENANT ADMINISTRATOR

Risks Identified.
Tenants Secured.

MANAGED DETECTION & RESPONSE

Integrated Intelligence.
Accelerated Response.

APPLICATION CONTROL

Expert Curated.
Proactive Protection.

VULNERABILITY MANAGEMENT

Prioritize Vulnerabilities.
Elevate Security.

CLOUD POSTURE

Protect your users.
Secure your cloud.

STREAMLINED SIEM

Modern Logging.
Simplified Compliance.

SECURITY POSTURE RATING

Measure Risk.
Improve Defenses.

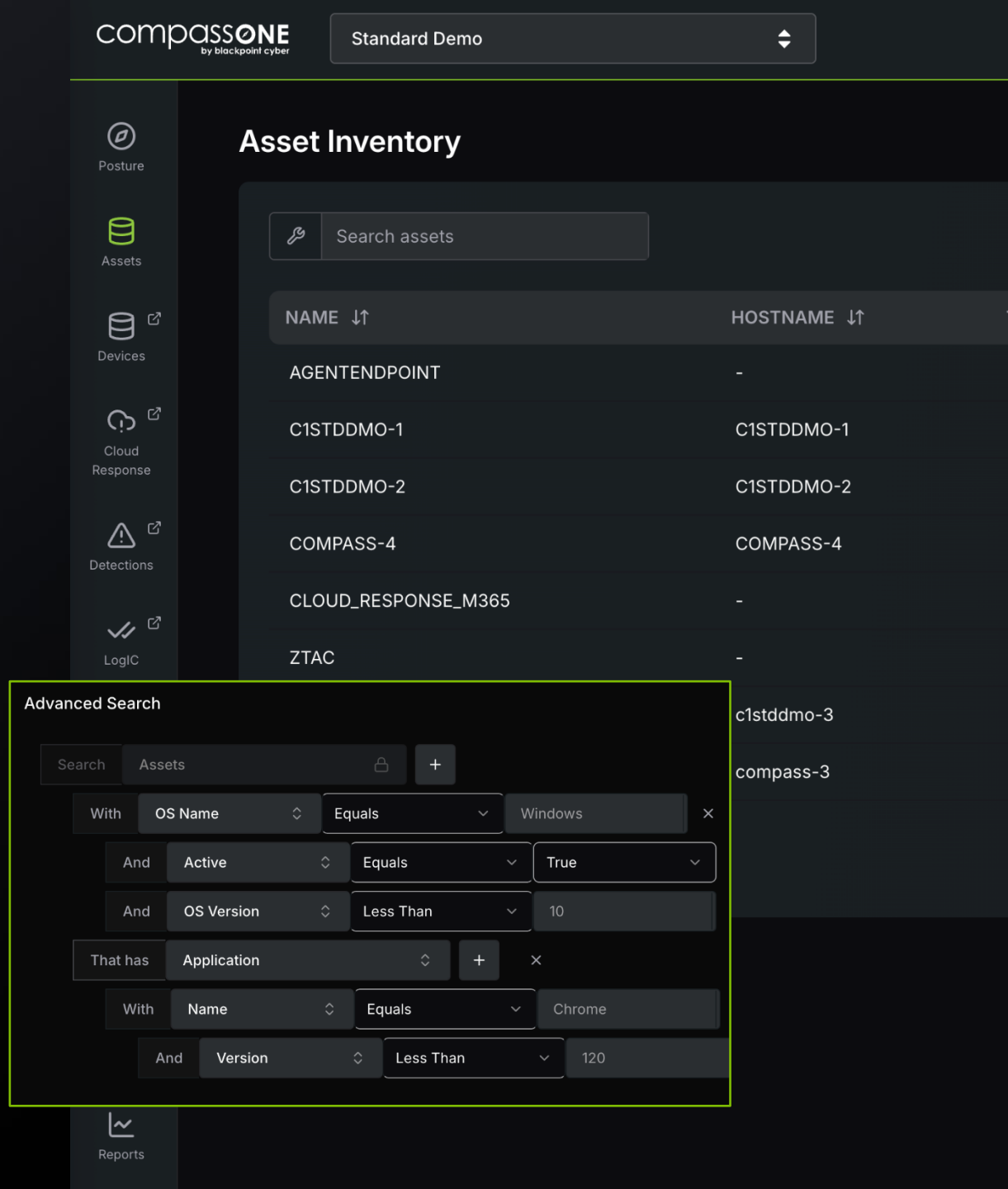
Asset Inventory

Eliminate Blind Spots. Level-Up Security.

Asset Inventory provides complete visibility across your organization's attack surface, including devices, identities, applications, and SaaS accounts— all in one place.

Solves for:

- Manual asset tracking or spreadsheet sprawl
- Delayed visibility into new or changing devices
- Fragmentation across tools with no shared context



blackpoint

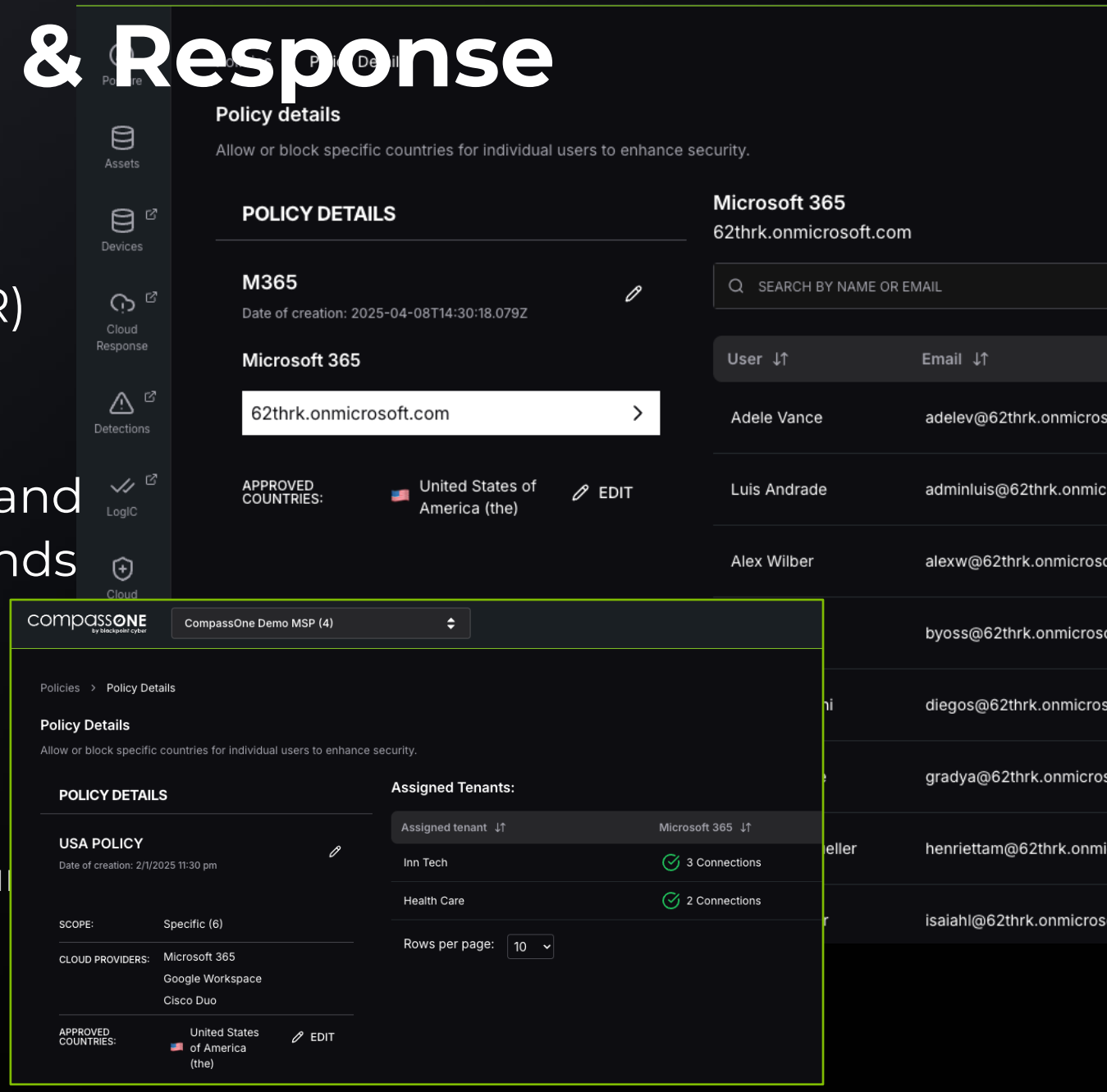
Managed Detection & Response

Integrated Intelligence. Accelerated Response.

Managed Detection & Response (MDR) delivers 24/7 protection from Blackpoint's human-led SOC. By monitoring across identity, endpoint, and cloud, MDR rapidly detects and responds to threats before they can escalate.

Solves for:

- Alert fatigue and missed signals across disconnected tools
- In-house resource constraints or lack of arou the-clock coverage
- Slow or reactive incident response



blackpoint

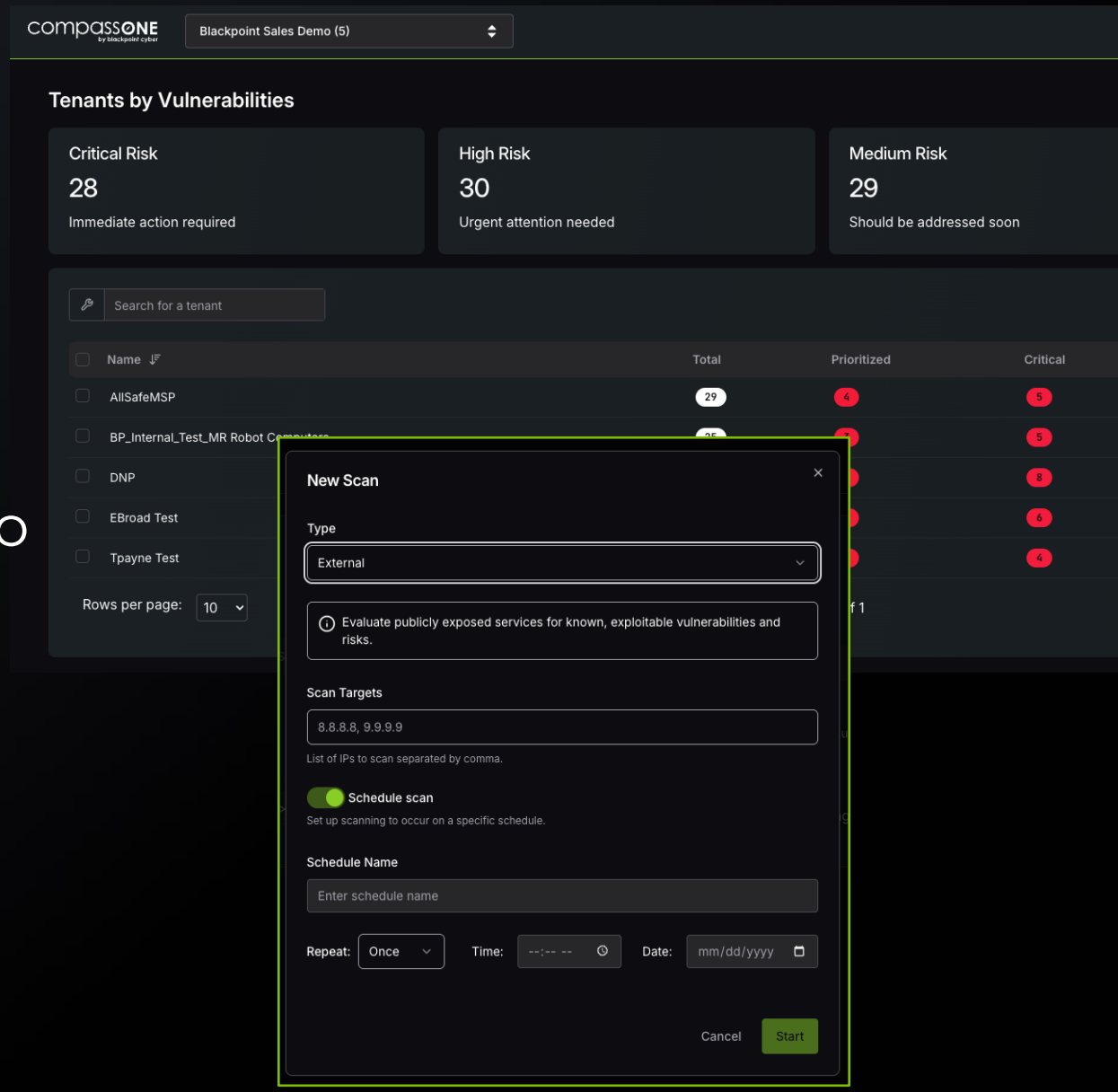
Vulnerability Management

Prioritize Vulnerabilities. Elevate Security.

Vulnerability Management continuously scans and prioritizes vulnerabilities across your endpoints and systems. It gives MSPs the ability to focus on exploitable, high-impact threats: turning endless patch lists into actionable plans.

Solves for:

- Overwhelming patch queues with no prioritization
- Reactive security posture driven by CVE volume
- Lack of context between vulnerabilities and active threats



blackpoint

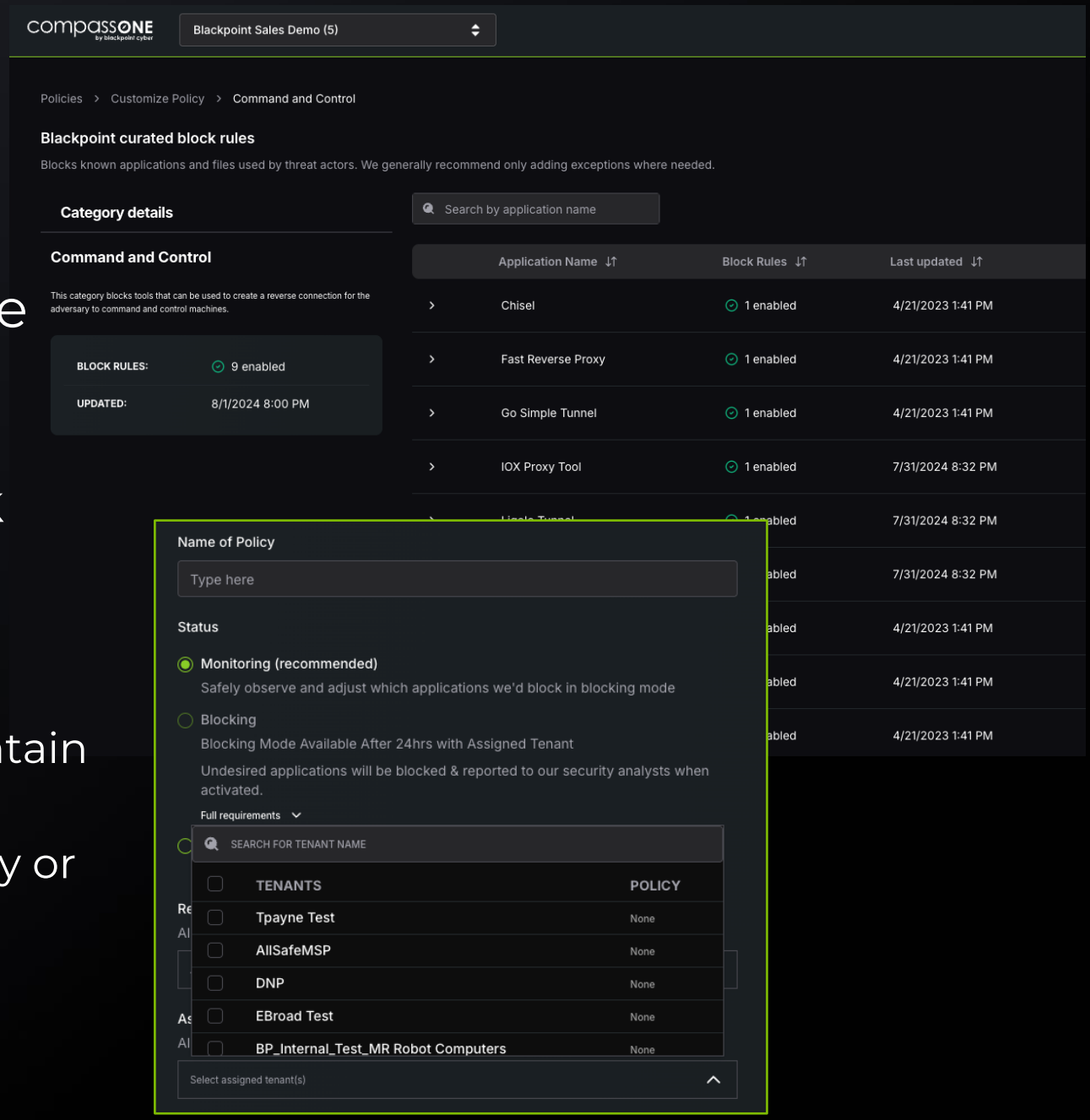
Application Control

Expert Curated.
Proactive Protection.

Application Control delivers proactive protection against malicious applications through an expert curated block list based on real work threat events.

Solves for:

- The need for resources to manage and maintain allow/deny lists
- Alleviates blind spots quickly identifying risky or unauthorized apps
- Enforcing security policies at scale



blackpoint

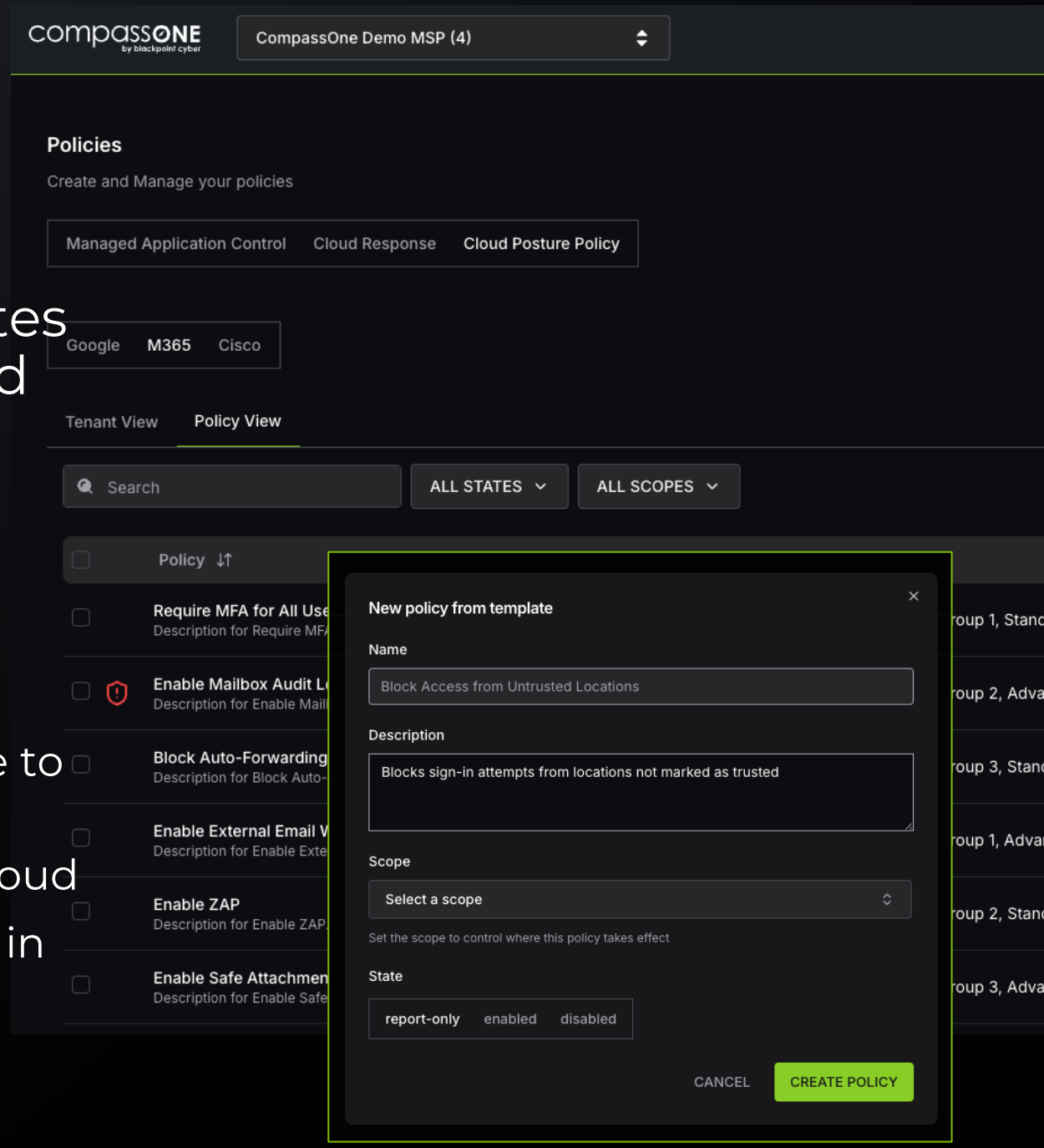
Cloud Posture

Protect your users.
Secure your cloud.

Cloud Posture identifies and remediates misconfigurations in Microsoft 365 and Azure environments, before they're exploited. It helps MSPs maintain continuous compliance and secure access settings across cloud tenants.

Solves for:

- Misconfigured cloud environments vulnerable to attack
- Manual, ad hoc security checks in Microsoft cloud
- Compliance gaps and lack of change visibility in tenant settings



blackpoint

Streamlined SIEM

Modern Logging. Simplified Compliance.

Streamlined SIEM delivers centralized, correlated logging across endpoint, identity, and cloud, without the noise, overhead or cost of traditional SIEMs.

Solves for:

- Misconfigured cloud environments vulnerable to attack
- Manual, ad hoc security checks in Microsoft cloud
- Compliance gaps and lack of change visibility in tenant settings



CIS Controls® v8 Im

The CIS Critical Security Controls® (CIS Contr
the most prevalent cyber-attacks against s
Implementation Group 1 (IG1) as essentia
minimum standard of inform

Select R

S Controls®

rity Controls® (CI
ent cyber-attack
ds and builds up
can help securit

CIS Controls® v8 Implementation Group 3

The CIS Critical Security Controls® (CIS Controls) are a prioritized set of Safeguards to mitigate the most prevalent cyber-attacks against systems and networks. IG3 is comprised of an additional 23 Safeguards. It builds upon the Safeguards identified in IG1 (56) and IG2 (74) totalling the 153 Safeguards in CIS Controls v8.

Select Report Type

The Cybersecurity Maturity Model
safeguard federal information storec
cyl

CMMC Level 2

The Cybersecurity Maturity Model Certification (CMMC) verifies that DoD contractors can safeguard federal information stored on their IT systems. Level 2 focuses on establishing documentation standards and intermediate cyber hygiene.

Select Report Type

The Cybersecurity Maturity Model
safeguard federal information storec
practice impler

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) controls how personal health information is managed by healthcare providers. It focuses on preventing fraud and protecting sensitive patient information from being disclosed without consent.

Select Report Type

Payment Card Industry Data Security
credit cards. It focuses on increasing
fraud/theft, and improving pa

blackpoint

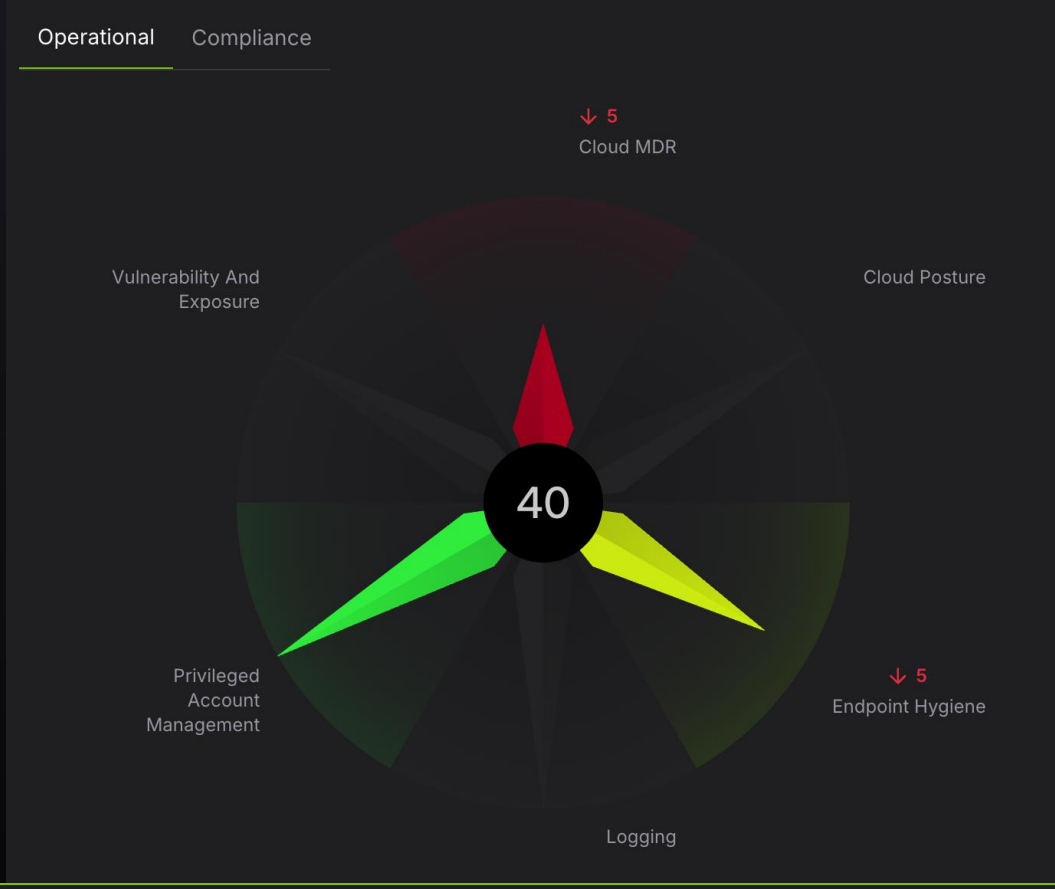
Security Posture Rating

Measure Risk.
Improve Defenses.

Security Posture Rating (SPR) gives MSPs a living, evolving view of client security health. It correlates data from all modules into a single, standardized score aligned with the NIST Cybersecurity Framework

Solves for:

- Static, manual security assessments that quickly go stale
- Difficulty proving ROI or communicating maturity to clients
- Fragmented security insights with no actionable summary



Factors Impacting Your Rating

Posture Metric	Rating Reduction	Operational	NIST Function	Action
Is Windows Defender or Microsoft Defender configured with CompassOne	5	Endpoint Hygiene	Protect	Enroll in Wind Microsoft Def integration
Is Cloud Response enabled to protect your Identity platform	5	Cloud MDR	Respond	Enable Cloud your Identity
Total Reduction	10			

blackpoint

compass ONE by blackpoint cyber

ONE platform.

COMPLETE context.

Protection you can **PROVE**.

		Essentials	Core	Standard
24/7 SOC	Block threats and prevent cyberattacks across endpoints, users, and/or identities.	✓	✓	✓
Security Posture Rating	Benchmark security posture based on NIST scoring and demonstrate ROI.	✓	✓	✓
Asset Inventory	Improve visibility of devices, users, and applications.	✓	✓	✓
Tenant Administrator	Efficiently manage multiple tenants in a single view.	✓	✓	✓
Vulnerability Management	Quickly identify, prioritize, and remediate critical security risks.		✓	✓
Application Control	Block unauthorized and risky applications from being used.		✓	✓
Cloud Posture	Automate and manage your cloud policies.		✓	✓
SIEM	Satisfy compliance requirements with log collection and automated reporting.			✓
Integrations	CompassOne integrates with over 40 technologies.*	*Partial*	*Partial*	✓

** Some integrations have an additional fee per source and availability varies between Essentials, Core, and Standard.*

blackpoint

Microsoft Intune Abuse and Cloud to On-Prem Compromise

Cloud Administration Command – MITRE ATT&CK ID: T1651



INITIAL ACCESS

TA performs credential compromise for Azure cloud environment.

EXECUTION

In MS Intune Admin Center, TA creates a custom script written in PS, instructed to download payload, and set to run w/ SYSTEM privileges.

TA runs script on demand. Further analysis shows the process was calling out to a Russian IP and attempted to download RedLine Stealer.

Upon execution, the SOC receives alerts for the attempted PS script and **isolates in under one minute**.

LEFT OF BOOM

RIGHT OF BOOM

IS THERE A BOOM?

NO

blackpoint

Questions & Discussion

CompassOne Demo

blackpoint