blackpoint

WHITEPAPER

Blackpoint Cyber MDR + LogIC vs. SIEM

PURPOSE

This whitepaper compares Blackpoint Cyber's 24/7, true Managed Detection and Response (MDR) technology and Logging with Integrated Compliance (LogIC) add-on with traditional Security Information and Event Management (SIEM) tools. Blackpoint partners may choose to replace an existing SIEM tool in their current security stack with Blackpoint's MDR technology and LogIC add-on solution. This replacement often occurs when there are requirements to receive around-the-clock detection and response services, support from a fully managed Security Operations Center (SOC), and hyper-efficient log collection and data storage for compliance efforts. These requirements may be heavily influenced by MSPs' clients and cybersecurity insurance agencies. Compared to a robust yet costly SIEM tool, the Blackpoint ecosystem streamlines your services, enhancing your data to prevent breaches faster than any other solution on the market today. This whitepaper defines the capabilities and benefits of Blackpoint's MDR and LogIC offerings, as well as the functionality of a SIEM, to help our partners make an informed decision as they build out an effective cybersecurity strategy and toolset.

Blackpoint Cyber’s Ecosystem

Our ecosystem of integrated solutions keeps our partners ahead of various cybersecurity challenges and requirements.

MDR

Managed Detection and Response

Blackpoint offers true, 24/7/365 MDR through SNAP-Defense, our proprietary cybersecurity operations and incident response platform. Our patented MDR solution is the first contextually aware detection and response program on the market, preventing breaches faster than any other solution. We have unparalleled visibility into suspicious events, hacker tradecraft, lateral spread, and remote privileged activity, using a lightweight software agent deployed to our partners’ endpoints.

Our SOC team takes the actionable data provided by our MDR and parses it, looking for patterns and correlations that may otherwise go unrecognized as threats to the network. With this, our team can investigate, isolate, and stop cyber threats from even the most advanced threat actors. Blackpoint’s visibility across all endpoints within an environment and active threat hunting processes close the gap between the identification of an event and the actual detection and response, which is vital in safeguarding sensitive data and thwarting lateral spread. Blackpoint acts on your behalf before the malicious actor is even aware.

Disrupting the hacker timeline early on saves our partners from missing indicators of compromise (IoC) and takes the burden of managing alerts off our partners’ shoulders. SIEMs, firewalls, endpoint protection, anti-virus (AV), and anti-malware (AM) do not provide equivalent detection and response.

Build out your offense with the following services:

- Lateral movement, tradecraft, and insider threat detection
- Continuous monitoring of privileged users, accounts, and activity
- Remote access and user behavior audits
- Mapping to MITRE ATT&CK® Framework
- Lightweight agent ensuring easy deployment
- Cloud-based, multi-tenant architecture
- Ransomware readiness assessments
- API-first architecture for ease of integration
- Automated, anti-ransomware capability
- Infrastructure enumeration and asset visibility
- Frictionless customer support

LogIC

Logging with Integrated Compliance

Blackpoint LogIC leverages our MDR technology to cover our partners' security, logging, and compliance needs in a single, hyper-efficient platform. Log entries are key to performing security audits, as they are used for the following:

- Identifying indications of unauthorized activities attempted or performed on a system, application, or device,
- Satisfying security compliance framework requirements,
- Establishing normal operational baselines and trends as well as building organizational standards, policies, and/or controls, and
- Providing evidence during investigations, audits, and forensic analysis.

Compliance audits ensure that organizations handling sensitive information are held to a standard set of rules and regulations. Should a breach occur, being compliant can shield the organization from reputational damage as well as severe legal and financial ramifications.

When partners use the Blackpoint ecosystem to handle compliance and security needs, our experienced SOC team enhances the value of the complex security logs. With this data, they can gather threat intelligence and acquire a baseline snapshot of what normal network operations look like. That way, the team can proactively search for local threats, detect malicious files, investigate changes to assets, and detain malicious activity within the network(s).

Little of this occurs in a meaningful timeframe when systems are processing big data. Artificial intelligence (AI), machine learning (ML) used in SIEM and security tools are bound to what you input. They are only as good as their latest update and calibration, relying on the manual effort of an organization's cybersecurity team. Breaches are often missed or detected too late, and suspicious behavior can blend in with normal activity.

Therefore, the human-powered element for cybersecurity is a crucial factor that synchronizes collected threat intelligence, data logs, and advanced security technology, safeguarding your business. Threat hunting and analysis always get you farther since deduction, monitoring, and interpreting are done in real-time without prior instruction. Data interpretation, on top of data collection, allows for indicators of threat to be pinpointed and actioned quickly. Leverage our MDR's active threat hunting and immediate response to cover your security, logging, and compliance needs.

Not only does the Blackpoint ecosystem streamline your security and compliance measures, it also offers extreme ease of use and simple onboarding. Within LogIC's self-serve management web application, our partners can manage and customize event and log collection settings in real-time. Blackpoint's LogIC add-on offers the following capabilities:

- **Simple push-button setup** with no additional hardware, appliances, or agent rollouts required. Built directly into the Blackpoint ecosystem, setup can be done within minutes.
- **Efficient collection of key data** necessary for compliance requirements and audits (including file integrity monitoring [FIM], syslog, and device logs).
- **Intelligent and automatic mapping** of your Blackpoint services to compliance standards. The auto-answer capability provides answers and justifications to hundreds of requirements all at once based on your existing Blackpoint products and services.
- **A safe, long-term repository for log data storage** encrypted with 256-bit Advanced Encryption Standard (AES-256) and compliant with SEC rule 17a-4, PCIDSS, HIPAA/HITECH, FedRAMP, EU GDPR, and FISMA data storage regulations.
- **Compliance framework reports** for use in audits and certifications.

LogIC

LogIC currently supports compliance tracking and reporting for the following regulatory compliance frameworks:

PCI-DSS

Payment Card Industry Data Security Standard (PCI-DSS) is a set of information security standards for organizations handling credit cards. It focuses on increasing controls around cardholder data, reducing credit card fraud/theft, and improving payment account security throughout transactions.

HIPAA

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

NIST 800-171

Special Publication (SP) 800-171 was created by The National Institute of Standards and Technology (NIST) to protect Controlled Unclassified Information (CUI). It requires any non-Federal computer system to ensure the security of CUI, including its storage, processing, and distribution.

CMMC (Level 1, Level 2, Level 3)

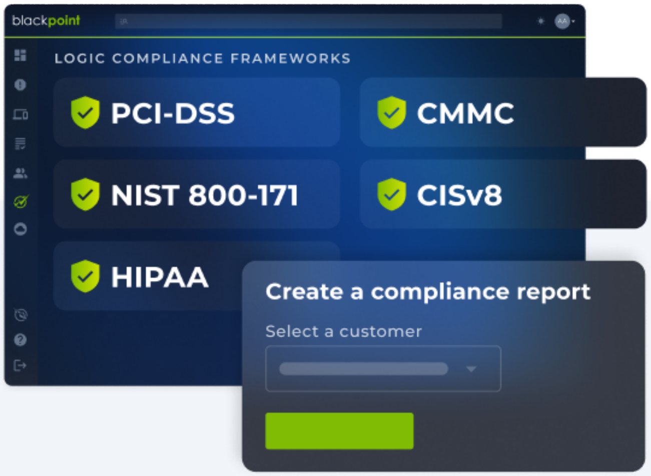
The Cybersecurity Maturity Model Certification (CMMC) verifies that defense contractors have controls in place to safeguard their IT systems. It protects any Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) that is stored on or transmitted by those systems.

CISv8 (Implementation Group 1, Group 2, and Group 3)

The Center for Internet Security (CIS) created Critical Security Controls Version 8 to mitigate prevalent attacks against modern day systems and networks including the increasing shift towards cloud-based computing, virtualization, mobility, outsourcing, and remote working conditions.

Additional compliance standards are to come, ensuring that LogIC will continue to help you collect valuable data.

SIGN UP FOR A DEMO



Security Information and Event Management (SIEM)

What is SIEM?

SIEM is a fused approach to security management that combines SIM (security information management) and SEM (security event management). A SIEM tool is used to collect and sift through copious amounts of raw data and logs within a centralized platform, utilizing behavioral logic, rules, algorithms, and ML to trigger notifications identifying IoCs. These notifications may be based on deviations from a predetermined normal state, possible security events, anomalous behavior, or opportunities vulnerable to threat actors. An organization's cybersecurity team is then prompted to analyze the alert and take appropriate action as they see fit.

How does SIEM fit into satisfying compliance requirements?

A SIEM tool is designed to discover and aggregate logs of relevant system and user event data from multiple sources for compliance purposes, ensuring necessary controls and regulations are met. They help stop unknown malicious activity as well as reduce the likelihood of 'low hanging fruit' attacks. Additionally, a SIEM tool houses substantial amounts of data beneficial to building monitoring controls based on suspicious behavior and aids in investigative/forensic efforts and audits.

Why is SIEM ineffective?

Most SIEMs are expensive to operate, dependent upon extensive upkeep to achieve security value, and cannot stop advanced cyber threats, such as tradecraft or insider threats, independently. Further, they are not designed to provide the necessary context for qualified analysts to detain cyberattacks. The the log aggregation approach inhibits the quality and speed of security response and overloads the analyst with a high quantity of 'noise': data that is unnecessary to the specific threat at hand. Typically, SIEM log correlation only runs every 60 minutes.

In short, relying on SIEMs for threat detection is inefficient and requires constant manual upkeep from a dedicated cybersecurity team. Additionally, storage for SIEM is usually priced by total number of events per second, so if customers are collecting logs from systems that generate a higher-than-average number of events per second, then storage costs increase quickly. Designed initially for enterprise-level environments, experienced in-house cybersecurity teams are required to perform continual manual effort to help the SIEM differentiate between normal activity and anomalous behavior. If reliant on a SIEM tool, a cybersecurity team is responsible for manually:

- Creating rules and tuning alerts,
- Reviewing logs, reports, and configuration,
- Keeping rules and software up to date,
- Calibrating evolving types of networks regularly,
- Parsing, filtering, and re-evaluating alert validity, and
- Responding to true cyber threat alarms.

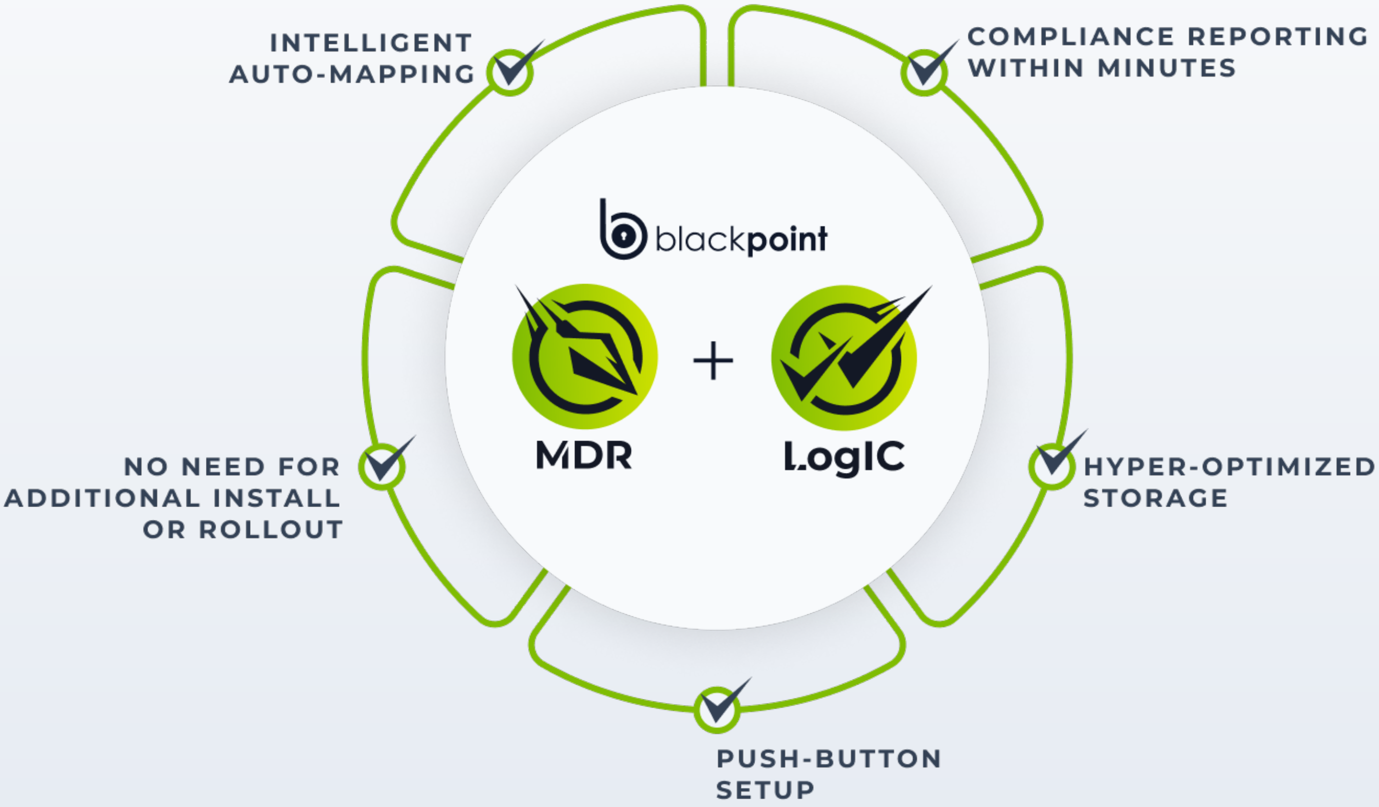
COMPARISON

Blackpoint Cyber MDR & LogIC	VS.	General SIEM Tool
LogIC uses the existing Blackpoint MDR agent, eliminating the need to deploy additional software or provision servers. Setup can be done from the LogIC user interface within minutes of service activation.	**Deployment & Onboarding**	SIEM tools require provisioning of multiple servers, installation of software, and configuration by an cybersecurity team which can take weeks or months to complete.
Since LogIC operates within the MDR ecosystem, no additional purchases of hardware or appliances are needed. This allows the add-on to be affordable.	**Pricing**	SIEM solutions can be a hefty investment. A recent report by IDG found that large businesses pay around $607,000 a year to manage theirs.
The Blackpoint ecosystem is SMB-friendly due to the fully managed, 24/7 nature of its operation, saving you both time and money. While you run your business, we will manage your cybersecurity, respond to all risks, and optimize log collection.	**SMB-Friendly**	SIEMs generally aren't SMB friendly because they require an experienced, in-house cybersecurity team able to support infrastructure and applications, implement the SIEM, and perform ongoing maintenance. If such a team doesn't exist, hiring necessary cybersecurity staff can be costly and/or the SIEM will not be utilized to its fullest capability.
Designed from the ground up, Blackpoint supports MDR objectives, including all features and capabilities out-of-the-box such as arming security analysts to perform effective threat hunting. Our SOC team has a deep understanding of threats and abnormal behavior that usually get past systems such as AV or AM.	**Threat Detection**	Once the SIEM has collected log files from devices and apps, they are repurposed to perform security analytics, resulting in threat detection at a slow rate. The amount of data the cybersecurity team must sift through for threat hunting can be cumbersome. Overall, the SIEM-based log collection approach has too many dependencies.
On top of log collection, our MDR analysts organize, interpret, and detect cyber threats.	**Log Collection**	SIEMs are designed to house copious amounts of data from all events within the network and systems.
Our SOC team actively investigates risks and threats across the full spectrum of attacker activity. They provide active, immediate response to threats using our lightweight endpoint agent with built-in response capabilities.	**Active Response**	SIEMs do not use an endpoint agent and are reliant on remote log collection. Therefore, the cybersecurity team is responsible for immediate mitigation. They must sift through false positives, verify real threats, comprehend the data sources, and resolve the threat independently.
Blackpoint LogIC offers 365 days of hyper-optimized, complimentary log storage. Additionally, LogIC has a fixed cost per device so the total number of events per second is not a cost factor.	**Complimentary Cloud Storage**	Depending on the carrier, you may be able to utilize a free trial and/or complimentary storage, but it is not guaranteed across all SIEM solutions. After that, cost is dependent on the number of events per second.
As part of our 24/7/365, fully managed ecosystem, Blackpoint manages log collection, data optimization, threat detection, and immediate response.	**Fully Managed Service**	Rules, customization, and configuration must be handled by the in-house cybersecurity team manually. This occurs both upon installation, as well as throughout its usage, requiring more ongoing maintenance than most technology tools.
Involving no additional setup, compliance reports can be generated within the user interface, and easily exported for assessment.	**Compliance Framework Reporting (Out of the Box)**	Most SIEM solutions do not include compliance framework reporting out of the box. Reporting dashboards need to be set up by the cybersecurity team after a SIEM is fully deployed.

SUMMARY

A SIEM tool collects and aggregates log data which is generated throughout the organization's technology infrastructure. While it is valuable in discovering raw data and housing large amounts of data for post-threat investigations and lessons learned exercises, a SIEM solution may take weeks or months to fully implement, is slow at detecting active cyber threats, and can rack up high storage costs. For internet-connected businesses, you must go further than AV, endpoint detection and response (EDR), or SIEM. Blackpoint Cyber does not offer a SIEM solution, but rather, a far more efficient combination: true 24/7 MDR plus LogIC.

As both services are powered by our SNAP-Defense platform, MDR and LogIC can replace legacy systems that overwhelm businesses with unnecessary data and alerts and place the burden of response on their shoulders. Blackpoint's MDR offers nation state-grade, real-time cybersecurity detection and response while LogIC delivers a hyper-efficient log collection and storage solution. When used in tandem, our technology creates a more robust cybersecurity solution that can leverage the value of security logs and telemetry. Overall, partners benefit from a managed security and compliance resource that is far more efficient and proactive than a traditional SIEM.



blackpoint

About Us

Blackpoint Cyber is the forerunner in the managed detection and response space, leveraging our proprietary ecosystem to help our partners triumphantly fight back against cyber threats. We have served organizations of all sizes around the world since 2014 and proudly continue to expand our ecosystem to meet evolving needs. No one should navigate the cyber threat landscape alone. At Blackpoint, our team strives to provide unified, 24/7 detection on your behalf to take out adversaries before they even see us coming.

Why Blackpoint?

- Enhance your security posture with compliance
- Obtain the insurance coverage your business needs
- Grow your brand and business with Blackpoint
- Trust a fully managed team of experts working for you
- True 24/7 monitoring and detection
- Unrivaled human analysis and response
- Focus on your business' growth
- Pedigree-informed operations

Interested in streamlining your compliance and cybersecurity?

SIGN UP FOR A DEMO

You can also check out our Frequently Asked Questions.

CONTACT US

info@blackpointcyber.com
blackpointcyber.com