blackpoint

LogIC

INTELLIGENT LOGGING AND COMPLIANCE

The future of true security + compliance is here

## Combine the power of MDR with intelligent logging

During a security event, cutting down on response times is crucial to safeguarding sensitive data. While logging is a start to collecting data and ensuring visibility across an IT environment, true value is in real-time data interpretation allowing for immediate action.

True, 24/7 Managed Detection and Response (MDR) *enhances* the value of security logging. Maximize the power of integrated logging and compliance by pairing it with active threat hunting and immediate response.

Streamlined, hyper-efficient compliance is finally here

To help MSPs meet the growing demand for both compliance and robust cybersecurity, we designed Blackpoint LogIC – our newest MDR add-on focused on logging with integrated compliance. LogIC is built to be hyper-efficient and provide real-time data collection, helping MSPs collect the data needed for future audits while keeping you and your clients secure.

With LogIC, auto-map against hundreds of compliance requirements all at once, so you can understand where your current security products and services are covering you in terms of compliance. Trust LogIC to make your journey towards regulatory compliance easier.
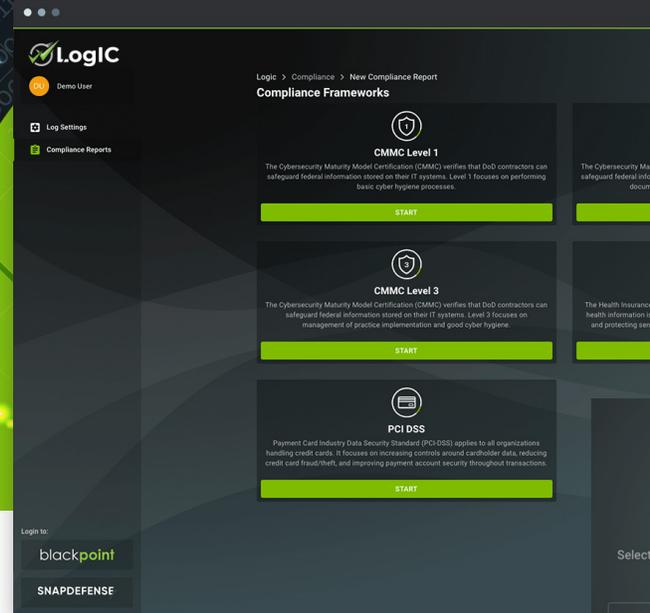
66%
Of companies see compliance mandates driving spending. (CSO Online)

45%
Increase in the cost of non-compliance since 2011. (Diligent Compliance)

31%
Of security leaders say lack of visibility of sensitive data is a compliance concern. (Censuswide for Panaseer)

Building a streamlined, end-to-end stack? Blackpoint can help.

Simple Logging Setup and Configuration

Log collection setup is usually complicated, often requiring additional hardware, appliances, and agent rollouts. LogIC leverages our existing nation-state grade MDR technology for an easy, push-button setup. Adding LogIC to your existing MDR service is as simple as clicking a few buttons. Use our self-service web application to manage and customize all aspects of event and log collection.

Robust Compliance Framework Support

LogIC's hyper-efficient logging architecture supports real-time collection of device logs, file integrity monitoring (FIM) events, and any other application or system that supports syslog*. It currently supports and maps to PCI-DSS, HIPAA, NIST 800-171, CMMC, and CISv8 security frameworks while storing your log data as read-only in 3 different zones with standard AES-265 encryption. Additional compliance standards are to come, ensuring that LogIC will continue to help you collect valuable data.

*Syslog source data will allow 100GB of event data per month. Utilization above this will be charged in $25 increments per 100GB.

Intelligent Mapping to Compliance Standards

Compliance requirements include complicated levels of processes, practices, and qualifiers. Based on the products and services you have with Blackpoint, LogIC's auto-answer capability does the heavy lifting for you by mapping against hundreds of compliance requirements all at once. Then, use our self-service, guided web application to answer any remaining controls. With LogIC, streamline how you prepare for future audits and assessments.

WHY LOGIC?

- ✓ Leverages Blackpoint's proprietary MDR technology for easy, push-button setup.

- ✓ Customize and manage log collection in LogIC's Compliance Report web application.

- ✓ Collected logs are stored in compliance with SEC rule 17a-4, PCIDSS, HIPAA/HITECH, FedRAMP, EU GDPR, and FISMA data storage regulations.

- ✓ Includes 365 days of hyper-optimized, complimentary log storage with options for additional log retention durations.

- ✓ Automatically maps hundreds of compliance controls to Blackpoint technology and services, reducing reporting and assessment efforts.

- ✓ Embeds LogIC information to Blackpoint's monthly MDR reports.

Ready to streamline your compliance and cybersecurity?

Request Demo

For more information, or to read our Frequently Asked Questions, refer to our LogIC page at **blackpointcyber.com/logic**.

Blackpoint LogIC's logging architecture bolsters your cybersecurity posture by supporting real-time collection of file integrity monitoring (FIM) events, device logs, and any other application or system that supports syslog. While LogIC collects key data to assist users in understanding where they are covered in terms of compliance, users must consult with a regulatory compliance authority and/or compliance auditor to guide them through the official assessment.

blackpoint

1.410.203.1604
blackpointcyber.com