Centrica protects international energy services with Blue Hexagon Multi-Cloud Deep Learning Threat Detection and Visibility

MULTI-CLOUD ENTERPRISE-WIDE SECURITY

Blue Hexagon's cloud security spans thousands of instances, networks, datastores, accounts and subscriptions in this Large Energy Company's cloud infrastructure. The nature of the IT infrastructure posed several challenges, primarily how to attain a comprehensive security posture against advanced threats in multi-cloud environments. Centrica selected Blue Hexagon Cloud Security solution for protecting their entire multi-cloud infrastructure with a single unified cloud hardening and real-time security defense platform.

SECURE ON DAY 1

"Deploying Blue Hexagon's Cloud Security solution for AWS and Azure with just a few clicks, in a matter of minutes, across multiple AWS and Azure subscriptions, was a game changer for our security team," said - Mark Wootton, Head of Threat and Vulnerability Management at Centrica. *"We have a complex environment with many controls, and Blue Hexagon team worked with us on integration with existing solutions including Secure Web Gateways and integrated SIEM. With their engineering team, together made sure all the security finds were tightly integrated with our SIEM platform. I have rarely seen this level of competency and engagement effort from a vendor"*.

AGENTLESS VISIBILITY AND DEFENSE

Blue Hexagon monitors the multi-cloud environment, providing visibility and threat defense for cloud network and workload activity in a single unified view -- all without needing any software agents to be deployed, or workloads to be disrupted or re-architected.

Cloud Inventory: Continuous visibility into all assets, in all regions, in all accounts, and in all clouds delivered in a single pane of glass. From instances in EC2 to Azure VMs, all asset information and resource metadata is collected and made available, indexed and searchable in the Blue Hexagon cloud security dashboard.

User, Entity and Resource Behavior Visibility: Every transaction made by an IAM role and user with external parties as well as with internal resources is continuously tracked, indexed and made queryable in the Blue Hexagon cloud console.

Cloud Network Visibility: Every transaction of a protected cloud asset with external parties as well as with internal resources is continuously tracked, indexed and made queryable. This information can then be correlated with the user, entity and resource visibility for incident investigation - all within the same unified platform.

About Centrica

Centrica is a leading energy services and solutions company focused on helping our customers live sustainably, simply and affordably. Our business is founded on a 200-year heritage of serving people. We supply energy and services to over 9 million residential and business customers, mainly in the UK and Ireland, through strong brands such as British Gas, Bord Gáis and Centrica Business Solutions, supported by around 7,000 engineers and technicians.

https://www.centrica.com/

NETWORK DETECTION AND RESPONSE FOR MULTI-CLOUD

Blue Hexagon provides real-time detection of threats at sub-second speed and natively works with cloud and security infrastructure for immediate visibility and enforcement. By applying Deep Learning AI to network traffic, storage activity and workloads, Blue Hexagon is able to identify both known and unknown threats with >99% accuracy in network traffic, container/K8S workloads and cloud storage, typically in less than a second.

Blue Hexagon's agentless cloud security platform connects to the cloud infrastructure within minutes using cloud-native APIs to collect data for security analysis. For example in AWS, Blue Hexagon will continuously ingest all AWS CloudTrail data, VPC Flow Log data, VPC Traffic Mirroring data and configuration data.

This raw data is enriched, aggregated and indexed in a single cloud-hosted portal to enable visibility, hunting and alerting across multiple clouds, multiple accounts and multiple regions.

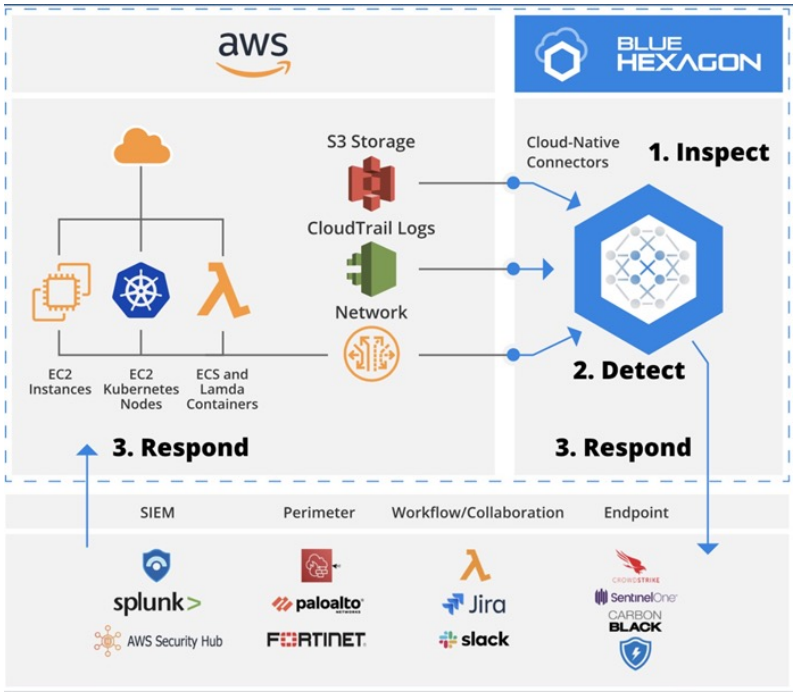
Output from the system, such as misconfigurations and security findings, can then be routed to a variety of response tools.

SIEM: Security findings and associated raw metadata can be sent to platforms like Azure Sentinel, Splunk or AWS Security Hub for further analysis or correlated with other tools.

Perimeter: IOCs derived from security findings like malicious IPs, domains or hashes can be provided as rules to perimeter security tools.

Workflow/Collaboration: Security findings can be added to ticketing systems such as Jira for further investigation or remediation or to collaboration systems like Slack. Cloud-native response automation is also possible by sending security findings to a serverless function and taking action in the function based on the findings.

Endpoint: Security findings around infected assets, malicious or network entities can be shared with EDR or EPP tools for prevention.



> **"We selected Blue Hexagon because of their forward-looking approach to securing multi-cloud environments with unparalleled threat detection capabilities based on their advanced deep learning AI technology."**
>
> **Mark Wootton** | Head of Threat and Vulnerability Management at Centrica

About Blue Hexagon

Founded in 2017, Blue Hexagon is a deep learning AI innovator of Cloud Threat Detection and Response (CNAPP) enabling enterprises to adopt the public cloud securely, reduce risk and detect & resolve threats faster. Its real-time deep learning AI delivers the world's highest detection efficacy for 0-day & known threats. Blue Hexagon helps customers Harden & Defend their public cloud through an agentless cloud-native security platform for AWS, GCP, Azure & OCI, powered by Deep Learning. It's the only AI-powered solution that enables CSPM, CWPP, and CDR in a unified platform for comprehensive protection of public cloud - IaaS and PaaS. Customers can now uniquely prioritize risk, combining both threat detection and misconfigurations, including at pre-deployment and at runtime.

Blue Hexagon is the world's most recognized AI cybersecurity company and has been widely adopted by leading technology, healthcare and financial organizations. Blue Hexagon helps these customers protect their business and brand against known and unknown threats including zero-day ransomware and malware, C2, cryptomining and insecure apps/code. The multi-cloud agentless solution deploys in minutes and integrates with cloud-native stack to help reduce DevSecOps friction and triage delays for faster remediation.

Blue Hexagon is headquartered in Sunnyvale, CA, and backed by Benchmark and Altimeter Capital. Follow us on Twitter @ bluehexagonai or on the Web at bluehexagon.ai.

Headquarters
150 W Iowa Avenue #103
Sunnyvale, CA 94086
https://bluehexagon.ai
inquiries@bluehexagon.ai

BLUE HEXAGON