CASE STUDY

BLOCKAPT™

Self-Defending Autonomous Platform

KSG Catering

CLIENT:

Kylemore Services Group (KSG):

Industry: Food Services &Hospitality

Locations: 120+ across Ireland

Employees: 1,300+

Overview:

Kylemore Services Group (KSG) is a leading provider of restaurant and hospitality services, delivering high-quality food experiences across five key sectors: Professional Offices, Travel & Leisure, Retail, Higher Education, and Healthcare. With over 1,300 employees operating across 120 sites in Ireland, KSG is deeply committed to innovation - not only in service delivery but also in safeguarding its digital infrastructure from evolving cyber threats.

Key Cybersecurity Pain Points - Hybrid MSP Environments:

- **Complex Infrastructure:** Disparate security tools with limited integration across multiple MSP's, resulting in poor visibility and inefficient monitoring capability.
- **Lack of Unified Visibility:** No single source of truth across systems, applications, networks, and endpoints, hindering threat detection and response.
- **Toolset Incompatibility & Integration Challenges:** Varied security tools and platforms used by internal teams and MSPs hinder integration, reducing operational cohesion and efficiency.
- **Siloed Threat Monitoring:** Isolated monitoring processes impair timely threat detection and cohesive incident response across the entire IT landscape.
- **Change Coordination Risks:** Cross-team change management, divergent escalation paths and inconsistent incident response protocols increase the risk of errors, slow resolution times and complicate crisis management.
- **Regulatory Compliance Pressure:** Manual processes made it difficult to meet evolving compliance mandates and respond to audits efficiently. Blurred accountability across shared control environments makes it difficult to manage audits, evidence gathering, and regulatory compliance.

The Challenge:

KSG faced growing cybersecurity and compliance demands across a complex and fragmented IT environment. With numerous IoT and OT devices, distributed systems, and siloed technologies, they lacked:

- Unified visibility across their IT and OT landscape
- Centralised security control and management
- Efficient, automated compliance and governance workflows

This fragmentation increased risks to customer data, hindered incident response times, and made quarterly internal and external regulatory audits resource and time intensive. KSG needed a scalable, intelligent platform to streamline operations, reinforce data protection, and improve their Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

The Solution: BlockAPT Platform:

The BlockAPT Platform delivered a unified, intelligent cybersecurity solution that provided end-to-end visibility, control, and compliance management through a single interface.

Business Outcomes & Impact:

- **Centralised Management & Control:** KSG gained full-spectrum oversight and real-time control of their IT environment. BlockAPT's orchestration streamlined threat monitoring, automated response actions, and eliminated tool silos.
- **Unified Visibility & Threat Intelligence:** A "single pane of glass" provided real-time analytics, anomaly detection, and access governance across digital assets and environments - reducing risk and improving operational clarity.
- **Automated Compliance & Governance:** The BlockAPT Platform supported KSG's quarterly audit readiness, access reviews, and policy enforcement - saving significant time and resources.
- **Role-Based Access Management:** Secure access control based on user roles improved accountability and reduced risk exposure across business-critical systems.

BlockAPT Unify: Unified Visibility and Strategic Insight

- **Comprehensive Visibility & Faster Incident Detection:** Offers a single source of truth that eliminates monitoring silos and enhances both manual and automated threat detection, significantly reducing time to respond.
- **Improved Stakeholder Collaboration:** Facilitates seamless communication and coordination with internal teams and external MSP partners, enabling better workload allocation and faster incident resolution.
- **Standardised Integration & Data Access:** Delivers a consistent and simplified framework for integrating systems and accessing key data points across the organisation.
- **Enhanced Change Tracking & Configuration Management:** Enables proactive identification of configuration changes and potential risks through a unified view.
- **Streamlined Incident Response Protocols:** Reduces complexity in response workflows by standardising escalation paths and event handling processes.
- **Improved Dependency Mapping & Impact Analysis:** Advanced observability tools with simplified queries allow teams to map dependencies and assess business impacts more effectively.
- **Remediation Planning Through Gap Identification:** Helps security teams identify security control gaps and formulate effective remediation strategies using actionable insights.
- **Policy & Compliance Oversight:** Quickly surfaces policy misalignments and compliance issues across the ecosystem through simplified dashboards and real-time reporting.
- **Enhanced Misconfiguration Detection:** Automatically identifies misconfigurations to reduce exposure and improve security posture.
- **Central Log Repository:** Acts as a unified platform for log storage, incident review, and audit readiness.
- **Cross-Team Collaboration Enablement:** Customisable dashboards and reporting foster improved communication and shared situational awareness across internal and external teams.

CASE STUDY

Kylemore Services Group (KSG)

BLOCKAPT™

Self-Defending Autonomous Platform

BlockAPT Control: Centralised Action and Operational Agility

- **Automated & Manual Remediation:** Enhances incident response with both automated and manual remediation capabilities, enabling faster and more accurate threat mitigation.
- **Cross-Vendor Collaboration Enablement:** Supports integration across vendors and technologies, enabling broad interoperability and improving response coordination.
- **Centralised Change Management:** Simplifies configuration and change tracking, improving auditability and proactive change governance.
- **Accelerated Incident Resolution:** Streamlines incident handling workflows, reducing downtime and improving service continuity.
- **Gap Remediation Through Central Control:** Empowers security teams to identify and address gaps proactively, with automated notifications and actions to reduce risk.
- **Risk Mitigation Through Automated Actions:** Detects and resolves misconfigurations automatically to reduce risk and improve security consistency across environments.

Client Testimonial:

> “*The challenge for modern IT Departments with multiple Managed Service Providers and their disparate technology stacks is to achieve the single pane of glass across the entire IT infrastructure both on premise and in the cloud. KSG opted for the BlockAPT Platform because it goes beyond a mere glimpse into our IT systems. Their centralised management, customisable dashboards, real-time analytics, and automated workflows—all under one roof—have strengthened our security and data protection. From PCI-DSS to GDPR compliance, the BlockAPT Platform gives us a unified view and has enriched our RPO and RTO parameters. I'd highly recommend it.*
>
> — **Stephen Daly**, Group Head of IT, KSG

BLOCKAPT™

Alpha House, 100 Borough
High Street, London, SE1 1LB
Tel: +44 203 608 6177
Email: info@blockapt.com
Website: www.blockapt.com

BlockAPT was created in 2019, is venture backed and has been recognised for its disruptive technology which unifies disparate end point solutions into a centralised management platform enabling vendor agnostic control with a single pane of glass view across IT ecosystems.