Client Success Story

UK Digital Payments & Wealth Management Firm

How Altumind Strengthened a UK-based FinTech Company's Cybersecurity, Data Protection, and Compliance Operations

Industry:
FinTech

Solution:
Co-Managed Cybersecurity Operations

Client Overview

A fast-growing UK-based FinTech company partnered with Altumind to strengthen Cybersecurity, data protection, and compliance operations. The company operates across digital payments, open banking, and wealth management platforms, handling sensitive financial data for millions of end-users across multiple regions.

Facing mounting regulatory pressure and an increasingly complex threat landscape, the company sought a trusted partner to overhaul its security posture. Through Altumind's co-managed Cybersecurity operations, the company achieved a 75% reduction in security incidents and a 90% improvement in compliance scores against UK GDPR standards.

Quick Facts

- **75%** Reduction in Security Incidents
- **90%** Improvement in Compliance Scores.
- **24/7** Co-managed Security Operations.

Tools and Technologies

- Splunk for 24/7 SIEM Monitoring and Threat Detection
- CrowdStrike for Endpoint Detection and Response (EDR)
- MetricStream for Compliance Management
- Okta for Identity and Access Management (IAM)
- PagerDuty for Incident Response Automation
- Qualys for vulnerability management

Engagement Model

Co-managed Cybersecurity operations with 24/7 monitoring, rapid response, and governance support.

Challenges

The UK-based FinTech company's existing security infrastructure was struggling to keep pace with rapid business growth. Their legacy perimeter-based model was not built for a cloud-first, distributed workforce, leaving critical gaps across endpoints, cloud workloads, and third-party integrations.

Frequent data exposure and leakage incidents increased the risk of financial and reputational damage. Internal IT teams were overwhelmed by alert fatigue and growing security complexity, while a lack of specialised expertise for enteprise-grade data protection and compliance management left the organization exposed. Growing concerns around insurability, operational resilience, and customer trust made it clear that a comprehensive overhaul was necessary.

Solution: A Comprehensive Cybersecurity Transformation

Recognizing these challenges, Team Altumind embarked on a holistic Cybersecurity transformation, integrating industry-leading tools with a co-managed operations model to deliver proactive, around-the-clock protection and compliance assurance. Our goal was to build a security posture that not only addressed immediate risks but also positioned the company for long-term operational resilience.

Key Enhancements:

- 24/7 Follow-the-Sun MDR deployed for continuous threat monitoring and proactive response.
- Security Operations Centre (SOC) established with real-time threat hunting capabilities.
- Splunk SIEM integrated for centralized log management and threat correlation.
- CrowdStrike EDR rolled out across all endpoints for detection and response.
- Okta IAM implemented with MFA and privileged access controls.
- ServiceNow and MetricStream onboarded for compliance management and GRC automation.
- PagerDuty and ServiceNow integrated for automated incident response and triage.
- Compliance management and data protection services aligned to UK GDPR standards.

Implementation: Putting Security at the Centre

At Altumind, we believe in designing security solutions that align with business operations rather than disrupting them. Our approach was structured around four key phases.

We began with a thorough Security Posture Assessment, benchmarking existing controls against NIST CSF, UK GDPR, FCA and PCI-DSS frameworks to identify critical gaps and prioritise remediation.

Conducted Risk assessment on the inventory to prioritise critical assets based on business value and threat exposure.

To address the top-identified risks, we established a 24/7 SOC threat detection and response platform, implemented proactive vulnerability management by deploying Qualys, Splunk, and CrowdStrike, and integrated telemetry from endpoints, cloud workloads, and network devices.

In the third phase, compliance automation was embedded through MetricStream GRC, enabling continuous regulatory monitoring and audit-ready reporting. Cloud environments were hardened using CSPM tooling aligned to CIS benchmarks.

Finally, Altumind delivered a security awareness training programme across the organization, reducing phishing susceptibility significantly within the first 90 days of deployment.

Results: Transforming Security and Compliance

The co-managed Cybersecurity transformation delivered by Altumind produced measurable results across all key metrics. The 24/7 SOC and SIEM deployment reduced security incidents by 75% within the first six months, with proactive threat response replacing a previously reactive posture.

Compliance scores improved by 90%, enabling the company to meet UK GDPR and requirements and pass PCI-DSS and ISO 27001 audits with confidence. Centralized IAM and secure access controls significantly reduced unauthorised access attempts. Internal IT teams reported a substantial reduction in alert fatigue, with Altumind's co-managed model handling day-to-day security operations. Business resilience, stakeholder confidence, and overall cyber risk management were all measurably improved.

Testimonial

Working with Altumind has given our organization complete confidence in our security posture. Their co-managed approach means our internal team is no longer stretched, and we can focus on growth knowing our data and customers are protected.

— Chief Information Security Officer,
UK Digital Payments & Wealth Management Firm

Here's Why Altumind is a Perfect Fit for You Too

- Comprehensive Cybersecurity solutions spanning SOC, MDR, IAM, compliance, and cloud security
- Cloud-native security architectures designed for hybrid and multi-cloud environments
- Expert-led implementation and 24/7 post-deployment SOC support for continuous protection
- Seamless integrations with SIEM, EDR, GRC, and ITSM enterprise platforms.
- Adaptive talent solutions with Altumind Agiliti to access specialized security expertise on demand.

Key Transformative Solutions Delivered by Altumind

- 24/7 SOC with follow-the-sun managed detection and response
- Splunk SIEM for real-time threat monitoring and correlation
- CrowdStrike EDR across all endpoints for proactive threat hunting
- Okta IAM with MFA and privileged access management
- Compliance management and data rotection aligned to UK GDPR, FCA regulations.
- MetricStream GRC for continuous regulatory monitoring
- Cloud security posture management for multi-cloud environments
- Incident detection, response, and remediation via automation

Accelerate your Cybersecurity transformation with expert-led innovation and next-gen technology.

Get Started →