wavex

Strengthening **Cyber Resilience**

Enabling Cyber Essentials Plus compliance
through proactive device management

Microsoft Tier-1 Cloud Solutions Provider

Microsoft Partner — Gold Security, Gold Cloud Productivity, Gold Collaboration and Content, Gold Data Analytics, Gold Datacenter, Gold Cloud Platform

Cyber Security Excellence Awards Finalist 2018

ISO 27001 Certification Europe

intl Winner Azure Partner of the Year 2018

Cyber Essentials Plus

IT Europa Finalist 2019

01

The **BUSINESS**

A leading independent research firm specialising in global macro and investment strategy, the company provides in-depth analysis and market insights to institutional investors across more than 30 countries.

With a reputation built on data accuracy, confidentiality, and analytical excellence, the firm's operations depend heavily on secure digital collaboration between its London headquarters and remote analysts around the world. Ensuring the protection of client data, proprietary models, and financial forecasts is a top business priority, making cybersecurity and compliance central to its continued growth and credibility.

02

The CHALLENGE

The firm needed to obtain Cyber Essentials Plus accreditation to qualify for a major client contract, requiring robust controls across its IT estate to demonstrate cybersecurity resilience.

However, the company's hybrid work model introduced several challenges. Employees using personal devices (BYOD) to access corporate data posed security risks, as there was no central mechanism to monitor or enforce security patching. Additionally, the internal IT team was stretched thin, leaving little capacity to prepare for the upcoming audit. The tight deadline for certification added an extra layer of challenge during an already busy period.

In this context, the client turned to Wavex for support. As an ISO 27001:2022 certified organisation, we applied our proven information security practices to help ensure audit readiness, strengthen endpoint governance, and accelerate compliance, all without disrupting day-to-day operations.

03

The Wavex **SOLUTION**

We began with a comprehensive pre-audit review of all devices connected to the company's environment. This assessment helped us identify vulnerabilities, configuration gaps, and policy deviations that could affect Cyber Essentials certification.

Working closely with the client's IT and compliance teams, we then:

- **Implemented remote monitoring and management (RMM)** agents across all corporate and BYOD systems, ensuring every endpoint could be tracked and patched in real time.
- **Established automated patch management** workflows to deliver OS and application updates seamlessly, reducing the risk of human error.
- **Remediated non-compliant configurations,** including user privilege controls, firewall policies, and antivirus deployment.

> **Empowering secure, compliant environments with proactive solutions and tailored support.**

- **Aligned configurations with Cyber Essentials requirements**, such as MFA enforcement, secure baseline policies, and incident logging.
- **Deployed a comprehensive security dashboard,** enabling the client to monitor and review multiple aspects of their security and risk profile in real-time.
- **Provided flexibility** in scheduling the audit, accommodating the client's internal timelines and annual leave schedules to ensure full readiness.

This end-to-end engagement not only addressed immediate audit requirements but also built a foundation for ongoing compliance management.

04

the RESULT

Through Wavex's proactive engagement, the firm successfully achieved Cyber Essentials Plus certification ahead of schedule, positioning itself to secure the high-value contract.

Key outcomes included:

Enhanced device visibility and control: With RMM agents deployed across all devices, IT administrators gained centralised oversight of patch status, compliance posture, and endpoint health.

Improved security hygiene: Automated patching reduced the window of exposure for known vulnerabilities, which is a critical factor as 57% of data breaches stem from unpatched systems[1].

Audit success and client confidence: The firm demonstrated full compliance with the UK's National Cyber Security Centre (NCSC) standards, reinforcing client trust and eligibility for future tenders.

Operational flexibility: Wavex's adaptive scheduling ensured zero disruption to business operations during the audit preparation phase.

> **Wavex made a complex process simple. Their expertise, flexibility, and proactive communication gave us complete confidence heading into the audit.**

The engagement not only secured certification but also equipped the organisation with a repeatable compliance framework, empowering them to maintain Cyber Essentials standards as their business and IT landscape evolve.

[1]Storeware