CyberOne

Luxury International Fashion Brand Case Study

Transforming endpoint protection to future-proof against the latest threats

The Client

A fashion brand renowned for timeless British luxury, including leather bags, accessories, womenswear and travel collections.

The Challenge

Following a business review by auditors, the client had received a recommendation to tighten-up their security posture and to improve the security analytics tools in use. They were still operating a largely traditional, on-premise server estate and the gaps in endpoint protection were a particular concern, with a legacy, signature based antivirus system in use across 600 Windows and Mac PCs.

The client was collecting and analysing security data in isolation, without any context or correlation. This was creating gaps in what their security team could see and detect. Their manual investigation process was slow and cumbersome, causing their security team to fall behind in containing and remediating threats.

The organisation had achieved Cyber Essentials Plus, but sought to work towards ISO27001, aligning themselves to either the CAF or NIST frameworks.

Having previously run successful penetration testing with CyberOne, the client was keen to work with us again to shore-up their endpoints.

The timescales were tight, with implementation needed prior to their next audit, just a few months away.

The Solution

The client had already taken steps towards a cloud platform with Microsoft and 365, so Microsoft's Sentinel SIEM service met the current and future requirements for security analytics integration. As a Microsoft Gold partner, Sentinel is at the heart of our Security Operations Centre offering. We recommended SentinelOne as the ideal solution to replace their legacy, signature based anti-virus system, working seamlessly within the SOC.

Working closely with the client, the CyberOne and SentinelOne consultants ensured the deployment methodology proposed was understood and appropriate. This integrated way of working enabled the key endpoints to be built and passed through our robust testing process at speed, ensuring the client had successfully replaced their legacy anti-virus on time.

With SentinelOne endpoint protection now in place, CyberOne have helped to unify and extend the client's detection and response capability across multiple security layers. Their security teams now enjoy centralised, end-to-end visibility along with powerful analytics and an automated response across their complete technology stack. Machine learning and predictive modelling techniques identity malware and malicious behaviour before they have the chance to compromise security.

With SentinelOne integrated into the SOC, CyberOne's team of highly trained SentinelOne and Sentinel experts now identify threats quickly, initiating rapid-response escalation procedures and a war room to neutralise and isolate threats at speed and before they impact the business.

The Benefits

CyberOne's endpoint specialists provide round-the-clock endpoint security management for the client, where previously they had struggled with a lack of in-house skills and resource.

Autonomous endpoint protection through SentinelOne reduces the time required by security analysts to discover and remediate threats, whether the device is on or off-line or even air-gapped.

A single platform provides comprehensive protection for Windows, Mac and Linux endpoints, plus cloud native workloads such as Kubernetes clusters and other non-standard (IoT type) devices using the SentinelOne Ranger option.

By combining Sentinel One technology with CyberOne's managed service, a comprehensive security solution is delivered without the need for costly, dedicated in-house information security staff working a 24x7 shift.

The CyberOne and SentinelOne combination ensures the client is future-proofed as our technology and processes evolve continuously in the face of continually evolving cyberthreats.

Contact us for more information on endpoint protection, EDR and how CyberOne can support your business.

Get in touch →

About CyberOne

CyberOne strives to offer the most trusted cyber experience in the digital world. Founded in 2005 and based in Milton Keynes, our assessment, detection and response services empower you to stay one step ahead of the latest cyber threats. We are trusted by leading UK and global businesses and our people provide a service that is second to none.

www.cyberone.security
+44 (0)3452 757575
enquiries@cyberone.security