A leading publisher keeps its network protected with an intelligence-driven early warning system that prevents cyber attacks.

**BUSINESS NEED**
A leading publisher in the U.K. wanted to strengthen network security, allowing its small security team to leverage expert security analysts without having to increase staff numbers.

**SOLUTION**
The publisher engaged SecureWorks and its Counter Threat Platform service to deliver round-the-clock defence.

**BENEFITS**
- Intelligence-driven protection from data centre to desktop
- An early warning system that operates 24x7
- Simplified security to see more, know more and do more

**PRODUCTS** SecureWorks Counter Threat Platform
Cyber threats against businesses are increasing. Overcoming these threats is challenging for companies without the expertise or resources to keep up. This was the situation at a leading publisher in the U.K. While the company had security experts in-house, the team was too small and ill equipped to combat the level of cyber threats it was experiencing.

**THE NEED FOR COMPREHENSIVE SECURITY**
A well-known organisation, the publisher saw its network was increasingly becoming a target for hackers. Its digitalisation strategy, which aimed to boost online revenues, was making it vulnerable to attack. But with just four staff focused on security, it was challenging to keep up with the output of the network’s security tools and maintain a 24x7 safeguard. In addition, the team had poor visibility of the threat landscape. And with the number of threats multiplying, plus those threats becoming more complex, the situation was likely to deteriorate.

**AN EARLY WARNING SYSTEM THAT DELIVERS**
After a successful proof of concept, the publisher engaged with SecureWorks. From this point, SecureWorks analysts started assessing the customer’s data network around the clock. They also began correlating output across multiple products to identify more threats, even those that do not use malware. The publisher adopted the SecureWorks Counter Threat Platform (CTP), a software-as-a-service (SaaS) solution providing security monitoring and management capabilities. As part of the CTP solution, the publisher also deployed SecureWorks Counter Threat Appliance (CTA) technology. The CTA collects network data and filters out the false positives. The filtered data is then passed up to the SecureWorks Counter Threat Operations Center (CTOC), where analysts assess the information, and, if they have concerns, raise tickets for the publisher’s security team.

**INTELLIGENCE-DRIVEN PROTECTION END-TO-END**
The publisher has clear visibility into threats on the network by working with SecureWorks. It has the Advanced Malware Protection and Detection (AMPD) service, which continuously monitors and inspects email and web traffic on the company’s network using next-generation network sandbox technology powered by Lastline. This technology helps defeat advanced persistent threats, including those from evasive malware designed to bypass traditional sandboxes.

**TRUSTED SECURITY THAT NEVER SLEEPS**
The security team can work safe in the knowledge that the network is protected 24x7. SecureWorks managed solutions are delivered from five resilient CTOCs around the world, which are fully staffed and functional at all times. This means SecureWorks’ Senior Intrusion Analysts and Counter Threat Unit Researchers are always on hand to review threat data from the publisher’s network to determine if any potential threats should be escalated to the security team.

**A LONG-TERM SOLUTION TO A LONG-TERM PROBLEM**
The publisher has peace of mind that the security of the organisation will be fit-for-purpose today and tomorrow. Based on the success of the engagement, the publisher has also extended the service to one of its major subsidiaries. As threats evolve, even the best technology must be coupled with expert analysis to identify the complex behaviours of threat actors. The SecureWorks CTP SaaS solution offers the advanced data analytics needed to combat the latest malware that threatens businesses everywhere.

**PART OF A PROTECTED COMMUNITY**
To strengthen the network’s defences, the publisher also gains intelligence on threat levels from the SecureWorks community. This community comprises thousands of SecureWorks clients around the world. Newly identified threats at one organisation will be quickly shared with SecureWorks staff protecting other client networks. This ensures everyone in the community stays well-guarded.