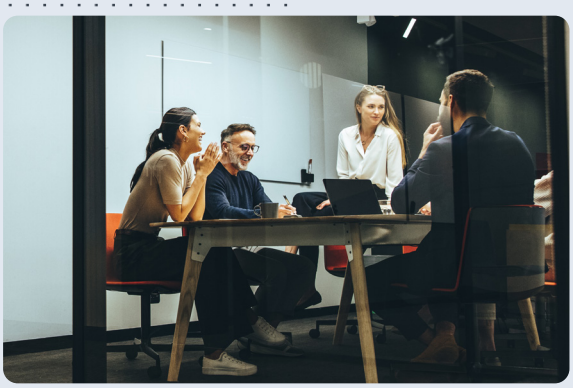
Impact

After implementing ThreatAware, Wellcome Trust experienced significant improvements in asset management and cybersecurity. The platform provided complete visibility across all devices, achieving 100% coverage for Endpoint Detection and Response (EDR).

ThreatAware's automated, real-time data collection replaced the need for intensive manual processes. This shift freed up the team to focus on more strategic tasks rather than tedious data entry. One of the most significant improvements was in the visibility of Cloud instances.The team now has 80% visibility, helping to enable them to monitor instances in real-time and quickly address any vulnerabilities.

Scheduled reports and alerts from ThreatAware ensured continuous oversight of their cybersecurity posture. Based on the Wellcome Information Security team's experience, no other tool has provided the same level of ease of use and accuracy, all from a single unified interface.

This proactive and streamlined approach has not only improved the charity's IT management but also fortified its cybersecurity, providing peace of mind and operational efficiency across the board.



"ThreatAware gives me in-depth data and has allowed me to focus on working on the data rather than trying to collect it."

"Scheduled reports help keep us at 100% coverage. I log in to ThreatAware every day. I am very confident, and I no longer rely on anything else."

"We achieved 80% visibility in Cloud instances, which was a huge improvement from before ThreatAware."

Syed Ali
Security Operations Manager, Wellcome Trust

Key Benefits

Time Savings
ThreatAware drastically reduced the time spent on manual data entry and asset management, enabling the IT team to focus on higher-priority strategic initiatives.

100% Device Coverage
With ThreatAware, Wellcome Trust achieved 100% coverage for EDR.

Efficient Cloud Monitoring
The team went to 80% visibility, significantly improving their ability to monitor and protect their cloud assets.

Real-Time Updates
The platform provided automated alerts and reports, helping the team keep all security fundamentals up to date, including patching and device tracking.