

CUSTOMER CASE STUDY

A Market Research Institution (Confidential)

About the Client

The client, operating in the Market Research Domain, runs a human-driven aggregate technology platform that connects enterprises with the most relevant professionals, thought leaders, and domain specialists across industries worldwide.

Global Reach:

Access to 100,000+ experts, KOLs, and business leaders across 50+ industry verticals.

2 Operational Model:

Teams working 24/7 as an extension of clients' own teams.



Core Value:

Delivering secure, confidential, and reliable knowledge-sharing sessions through customized expert engagement services.





Strengthening Cybersecurity for a Market Research Leader with Sophos EndPoint Protection

Background

The client manages large volumes of sensitive business and market research data daily. With a distributed workforce and heavy reliance on digital platforms, the risk of cyberattacks, such as ransomware, phishing, or malware infiltration, was increasing. They needed a comprehensive security solution to protect research data and ensure compliance without hampering productivity.

Given the sensitivity of the market intelligence they handle, maintaining data confidentiality, compliance, and uninterrupted operations is critical to their success.



The Challenge

The client identified several security gaps in their existing setup:

- Lack of real-time threat intelligence to prevent modern attacks.
- Limited visibility and centralized control across 60+ systems.
- Concerns over data confidentiality during international research projects.
- Need for minimal downtime, as disruptions directly impact ongoing client engagements.

Cybersecurity threats were not only a technical risk but also a reputational risk, any data breach could jeopardize global trust in their platform.



Solution DTF Provided:

Sophos EndPoint Protection



The client selected SOPHOS Central Intercept X Advanced after evaluating multiple vendors. The solution provided the scalability, advanced defense, and centralized control they needed.

- Al-Powered Threat Prevention Blocks ransomware, malware, and exploits proactively.
- Sophos Central Management Unified visibility and policy enforcement across all endpoints.
- Web & Application Control Restricts unauthorized applications and malicious websites.
- Device Control Prevents risks from USBs and removable media.
- Optimized Performance Protects systems without impacting research workflows.

Implementation

Deployment Size:

60+ client systems, including analyst and research workstations.

Timeframe:

Full deployment completed within 48 hours.

Integration:

Centralized policies applied seamlessly through Sophos Central.

Training:

IT team trained on monitoring, reporting, and proactive defense actions.

The transition was smooth, with zero downtime reported during deployment.



Results & Benefits

The adoption of SOPHOS Central Intercept X Advanced delivered measurable improvements:

- 100% Endpoint Coverage: All 60+ systems fully secured and policy-compliant.
- 75% Faster Incident Response: Centralized monitoring reduced threat investigation time.
- Zero Security Breaches Post-Deployment: Strengthened resilience against ransomware and phishing attacks.
- Enhanced Productivity: Research teams continued operations without slowdown or disruption.
- Improved Compliance: Aligned with global data protection and client confidentiality standards.

Testimonial

As a company that deals with highly sensitive research data, we were looking for a security solution that could balance advanced protection with system performance. After evaluating multiple vendors, we found that only Sophos offered a truly Al-backed security solution that not only safeguarded us from evolving threats but also ensured our systems continued to perform seamlessly. The ability to have a solution that was centrally managed and easy to monitor was a critical factor for us, and in the end, the only solution that truly qualified our requirements was Sophos.

Ms. Tajwar A.

