CUSTOMER CASE STUDY

How did CSM Technologies strengthen cybersecurity and earn client trust?

Industry
IT consulting and services

Country
India

Who is CSM Technologies?

CSM Technologies is a global IT consulting and services firm with operations across Asia, Africa, and North America. The company employs more than 1,600 staff and delivers over 30 service offerings across 10 domains, serving both government and enterprise clients. To secure its environment, CSM has implemented a comprehensive suite of Sophos solutions including Sophos Firewall, Sophos Extended Detection and Response (XDR) and Sophos Endpoint Detection and Response (EDR), Endpoint, and Sophos Email.

Why is cybersecurity so critical in IT consulting and services?

For IT consulting and services firms, cybersecurity is a competitive differentiator and necessity. With government agencies and large enterprises as key clients, providers like CSM Technologies face constant pressure to protect sensitive data, maintain uptime, and prove compliance. The rise of ransomware, zero-day exploits, and targeted attacks has made traditional security approaches inadequate, requiring intelligent, and integrated protection.

What cybersecurity challenges was CSM facing?

With more than 26 years of experience, CSM Technologies has earned the trust of public sector organizations across multiple continents. But with that trust comes risk. The company was increasingly exposed to sophisticated threats such as ransomware and targeted attacks that put client services at risk. At the same time, a shortage of skilled cybersecurity professionals made it difficult to monitor and respond to every incident. On top of that, legacy defenses lacked visibility across endpoints, networks, and cloud environments.

CSM's leadership knew that a single successful attack could mean service disruption for government clients, loss of trust, and reputational damage. In 2015, CSM was hit by Cerber 3 ransomware, when two of its systems were encrypted — and it's still struggling to get the data from those systems.

> "Cybersecurity had to be one of our core strengths, not just for business continuity, but also for client trust."
>
> **Amit Kumar Das**
> Associate vice president of IT, CSM Technologies

SOPHOS

How did CSM select the right security approach?

CSM Technologies evaluated solutions that could deliver user-level monitoring, simple deployment, and reliable support. It needed tools that could scale with its global operations and unify security across multiple environments.

After evaluating the market, CSM Technologies implemented a Sophos solution portfolio that including Sophos Firewall with DDoS protection, IPS/IDS, Web Filtering, and WAF, as well as Sophos Endpoint, with XDR and EDR for advanced ransomware and exploit prevention. CSM has deployed Sophos Endpoint for 1,200 end users and 200 servers spread in multiple locations from India, Kenya, USA, Dubai, and South Africa. All of these are managed through Sophos Central, which is a centralized console that lets CSM integrate endpoint, application, email, and network protection for seamless control.

What business impact has the new security model delivered?

Since strengthening its defenses, CSM Technologies has not experienced a successful cyberattacks. Automated reporting and adaptive policies ensure defenses stay aligned with new and evolving threat.

The company also observed several immediate benefits. Threat detection became faster, and automated response features reduced the time to contain incidents by half. False positives decreased, which cut down alert fatigue for IT staff. Centralized management simplified administration and eliminated the need for multiple tools.

In the longer term, the new security approach strengthened CSM's security posture, ensuring resilience against ransomware and zero-day exploits. Staff productivity also improved, with IT teams reclaiming 120 hours per month that were previously spent on manual investigations. Most importantly, client confidence increased as CSM demonstrated strong defenses to its government partners.

"Every time we faced a roadblock, the Sophos team provided immediate solutions. That responsiveness gave us the confidence to roll out advanced protections quickly."

Amit Kumar Das
Associate VP – IT,
CSM Technologies

How has stronger security changed company culture?

Improved security hasn't just strengthened CSM's defences, it has reshaped its cybersecurity culture. Employees now receive weekly awareness emails and participate in twice-yearly cybersecurity training sessions. Security reports help reorient internal policies and procedures, and teams now view security as a shared responsibility.

"We've aligned our people, processes, and tools. Security is now embedded in our culture."
Amit Kumar Das, Associate VP - IT, CSM Technologies

What has CSM's experience with support and partnership been like?

CSM highlights the quality of support from both its local partner, Vishant Solutions, and from Sophos and its customer success team. Das explains that support and services from Sophos and its partner have been excellent, without hesitation or doubt. Whether the need involves hardware, licensing, or product guidance, the Sophos team was always quick to provide fast and effective help.

Where is CSM heading next with its security strategy?

As cyberthreats evolve, CSM is planning to enhance its defences with Network Detection and Response (NDR). Das emphasizes that intelligent automation, unified management, and advanced detection capabilities will continue to be pivotal in protecting both CSM and its clients.

To learn more visit Sophos.com

SOPHOS