Sophos Addresses the Holistic Security Needs of a Leader in Chemicals & Textiles

Incorporated in 1983, GHCL Limited, a diversified group active in the chemicals, textiles and consumer Products segments has a marketing capitalization of around Rs. 3000 crores. In the chemicals sector, the company manufactures Soda Ash. Its end-to-end textile operations include weaving, dyeing, printing and processing right up until the finished product is delivered in the form of sheets and duvets, which are exported across the world. The company's consumer product division manufactures and sells edible and industrial grade salt. Its manufacturing facilities are located across distributed locations, and from a security prerogative, this presented plenty of challenges. GHCL's primary objective was to build an integrated cybersecurity infrastructure that delivered extensive security cover across its locations, and which could also be easily managed from a single location through a unified console.

CUSTOMER-AT-A-GLANCE

GHCL Limited

Industry
Manufacturing (Chemicals and Textiles)

Sophos Customer
Since 2015

Website
www.ghcl.co.in

Sophos Solutions
Sophos XG Firewall – 330 - Appliance in high availability
Sophos XG Firewall - 210 - Appliance in high availability
Sophos XG Firewall – Four 135 Appliances
Sophos XG Firewall – Three 125 Appliances
Sophos Intercept X Advanced for 800 endpoints
Sophos Intercept X Advanced for Server for 88 servers
Sophos Central Device Encryption – 25 licenses
Sophos Intercept X Advanced for Mobile – 25 licenses

"The overarching challenge was that we did not have complete visibility and control of our existing cybersecurity infrastructure and were trying to address sophisticated threats with legacy OEM solutions. Our core objective was to deploy only the most advanced security solutions, which offered a single pane of glass for all security appliances guarding our network and endpoints."

Vinod Pandey, Head - IT, GHCL

Challenges

- Lack of comprehensive protection against a growing threat landscape
- The ever-increasing risk of falling pretty to cyberattacks
- Data breaches at the network perimeter
- Inability to mitigate risks on external devices like laptops and desktops especially at a time when employees are working from home
- Absence of visibility into user activities and other information along the same lines that would help the IT team make proactive security decisions
- Incapacity to meet demanding compliance requirements with respect to end user activity and trace/log
- Inconsistency in access control on critical IT systems
- Inefficient process of critical server updates which meant servers were not updated on time

A Limiting Cybersecurity Posture before Sophos

The IT Team at GHCL led by Mr. Pandey was experiencing challenges associated with legacy security solutions. The existing OEM solutions had management complexities which were consuming the already stretched resources of the IT team. More importantly, irregular technological upgrades and unreliable software updates were proving to a be a major headache. "We realized our existing security solutions did not have the capability of safeguarding mission critical assets spread across our distributed network. Attacks are getting more sophisticated by the day. We couldn't afford to leave our endpoints unprotected and therefore wanted to move to a more cutting-edge and layered approach to security," explains Mr. Pandey.

The IT team wanted to speed up threat identification and remediation and wanted a security solution to immediately flag malicious activities on the network and deliver reliable protection against threats, both known and unknown. Mr. Pandey wanted a 360-degree approach to security bolstered with actionable intelligence shared between network and endpoint, to automate threat identification and response.

Moving to a More Integrated Security Approach

A thorough research of the security solutions available on the market made it very clear that Sophos' powerful product portfolio exhibited extremely high standards of performance, deployment, simplicity, usability and advanced security features.

Sophos also satisfied the IT team's need for a centralized and secured Control Center for managing all security appliances. GHCL were also impressed by Sophos' next-generation of cybersecurity which gave them confidence against the most advanced threats in the present and also the future.

Another important factor which helped the team decided in Sophos' favor was the prospect of securing both their network and endpoints under a common umbrella.

The team at GHCL worked with Sophos partner M/s Allot System Integration, who started by designing the entire security landscape for the company. M/s Allot System Integration followed up with a proof of concept. This left no room for doubt in the IT Team's mind that Sophos was best to handle all manner of security challenges.

GHCL were confident that Sophos Professional Services would ensure meaningful consultation, speedier implementation, and a threat landscape-driven configuration of Sophos solutions. The customer believed all their security needs would be addressed with security best practices from Sophos Professional Services.

Future Proofing Cybersecurity Posture with Advanced Security Deployments

After evaluating GHCL's existing cybersecurity infrastructure and assessing its cybersecurity requirements, Sophos surmised that the protective cover the organization needed could be accomplished using the full spectrum of Sophos solutions. Sophos XG Firewall, Sophos Central Intercept X Advanced, Sophos Central Intercept X Advanced for Server, Sophos Central Device Encryption and Sophos Intercept X Advanced for Mobile were identified as the solutions needed to strengthen GHCL's security posture.

Sophos XG Firewall offers excellent visibility and protection with Xstream Deep-Packet Inspection (DPI) engine that scans traffic for IPS, AV, Web Protection and App Control in a unified streaming engine. With Xstream TLS inspection, the firewall removes security blind spots by delivering visibility and comprehensive policy tools all backed by built-in intelligence. GHCL also receives protection from zero-day threats with industry-leading machine learning technology. The IT team can also configure user identity-based policies and benefit from unique user risk analysis to control users. With application control, web protection and advanced threat protection, GHCL now has a comprehensive network security cover.

"With XG Firewall, our cybersecurity infrastructure is empowered by a firewall that seamlessly adapts to our network, and the IT Team is not pressurized into adapting the network to the firewall. We gain the advantage of a huge list of rich features and amazing versatility that secures our environment," explains Mr. Pandey.

Mr. Pandey can now ensure that this secure network can be extended anywhere, with seamless ease with the firewall's VPN secure access solutions.

With Sophos Intercept X Advanced for endpoint and server, GHCL obtains signatureless malware detection backed by deep learning, an advanced form of machine learning. With this technology, the customer earns true scalability and increased effectiveness against unanticipated threats.

Intercept X Advanced allows for cutting-edge ransomware functionality which ensures GHCL is able to safeguard against the malicious encryption processes used in ransomware attacks. Add in exploit prevention, application lockdown, web control, and data loss prevention and the IT team know GHCL endpoints and servers are protected against all types of threats.

Synchronized Security ensures Sophos solutions like Intercept X Advanced and Sophos XG Firewall share data in real-time while responding automatically to incidents. This helps the IT team save significant time, resources, and effort.

With Sophos Intercept X Advanced for Mobile, GHCL benefits from secure Unified Endpoint Management (UEM) solutions which help the IT Team spend less time and effort otherwise spent in managing and securing traditional and mobile endpoints.

The GHCL team can ensure uniform security policies are pushed across multiple endpoints and both users and the organization at large benefit from consistent polies. Intercept X Advanced for Mobile delivers a superior level of protection that secures mobile devices against ransomware, network attacks and exploits.

"We are able to leverage the powerful set of security tools offered by Intercept X for Mobile to protect our employees' mobile devices from malicious websites, phishing text messages, and unsafe downloads and links. Today our employees are more reliant on their mobile devices than ever before and comprehensive mobile security allows them to use these devices with confidence," explains Mr. Pandey.

Integrated into Sophos Central, Sophos Central Device Encryption, helps the IT team manage Windows BitLocker and macOS FileVault native device encryption. The customer can deploy and start protecting valuable data in quick time. Encryption policies can be pushed with just a few clicks and the GHCL team can now easily secure data on laptops of employees that are working from home.

The additional benefit is that all Sophos security solutions can be managed from a unified console – Sophos Central.

A Robust and Business-Centric Cybersecurity Infrastructure

GHCL has experienced tangible business benefits following the deployment of Sophos security solutions. The return on investment (ROI) on security appliances has increased by 50%. The IT team is saving 90% on man hours, which were previously spent responding to security incidents. The threats to servers and endpoints have also seen 90-100% reduction, which has proved that the layered approach to security has delivered immense security value.

"We have reduced the capital expenses on security appliances by 50% since deploying Sophos solutions. We no longer have to spend a substantial portion of our time resolving security incidents. This allows our IT Team to invest time and resources in other activities which can further maximize the potential of our IT infrastructure," shares Mr. Pandey.

Furthermore, GHCL is now saving on the cost of replacing security appliances every 3 years and supplementary security infrastructure. With Sophos now firmly in place, the customer experiences low impact on PC performance. Currently real time threat alerts have ensured the IT team is more proactive than reactive to cyber threats and security incidents. The company has benefited immensely from the availability of comprehensive logs from Sophos Central, which allows GHCL to meet all compliance regulations. With GHCL's move towards next generation security solutions, there is now a concrete incident response plan in place backed by the expertise of highly trained IT-engineers from Sophos.

"Sophos is simple, affordable, scalable and easy to manage. With the security ROI delivered by our existing Sophos solutions, we are planning to extend our protection with Sophos EDR, Sophos Network Access Control (NAC) and benefit from its next-gen AI/ML powered product suite. Based on our experience on Sophos products so far, we can strongly recommend Sophos to all organizations who want to build a strong and extendable cybersecurity infrastructure," concludes Mr. Pandey.

(Optional) Insert Sophos CTA.

SOPHOS

2022-01-12 CCS-EN (NP)