Sophos Solutions Protect **Colombo Dockyard PLC** from Advanced Threats

Established in 1974, Colombo Dockyard PLC (CDPLC) is a 1400+ strong organization located in Colombo, Sri Lanka within the port of Colombo, the hub of all major shipping lanes connecting the West, the Middle East, the Far East, as well as Africa and Australia. It conducts both dry dock and afloat operations and is actively involved in ship building, ship repairing and heavy engineering activities. It uses state-of-the-art machinery and equipment to service more than 200 ships annually and builds highly sophisticated complex vessels for a clientele worldwide, where the detailed design engineering is developed in house using high-end 3D modelling software operating from various remote locations. As is the case with any organization that belongs to a strategic domain, Colombo Dockyard experienced numerous malware and ransomware attacks and realized that its CDPLC ICT systems and overall IT infrastructure needed cutting-edge protection from advanced and ever-evolving threats.

CUSTOMER-AT-A-GLANCE

Colombo Dockyard PLC

Industry
Ship building, ship repairing and heavy engineering

Sophos Customer
Since 2017

Website
www.cdl.lk

Number of Users
1400+

Sophos Solutions
XG Firewall
Sophos Sandstorm
Sophos Email
Intercept X Endpoint
Sophos Wireless
Sophos Mobile
Sophos Home

> *“The search for a security solution that was a marked improvement over the solution we were using until then, ended at Sophos. With Sophos’ powerful portfolio of next-gen security solutions, we achieved comprehensive security cover that can be managed easily and seamlessly. We are suitably impressed with its dashboard that uses a single pane of glass approach to keep us on top of all the information we need to keep our network and endpoints more secure.“*
>
> P.H.S. Daminda, Chief Information Officer (CIO), Colombo Dockyard PLC

Challenges

- Controlling inappropriate web access and controlling/managing/monitoring network access privileges
- Prioritizing bandwidth allocation to critical web applications and limiting bandwidth for non-critical websites
- Absence of secured VPN connectivity
- Lack of peripheral control policy to manage and control the use of DVD ROMs and USB drives
- Protecting users’ laptops, mobile devices for secure CDPLC systems connectivity
- Securing inboxes of users to protect users from phishing attacks and fraudulent emails
- Ensuring employees working from home or outside the network perimeter are secured
- Managing both network and endpoint from one common place, easily and conveniently without spending too much time in evaluation and analysis

What did Colombo Dockyard’s cybersecurity posture look like before Sophos?

Colombo Dockyard was always aware that threats rapidly evolve and the organization’s mission critical systems like CDPLC ICT are always in the crosshairs of attackers. CDPLC ICT is critical for the functioning of CDPLC’s business. It is used for all day-to-day activities and therefore needs to be always available. As CDPLC’s existing security solution was unable to prevent malware and ransomware attacks, CDPLC decided it needed an easy to manage and deploy cutting-edge solution to help keep advanced threats at bay.

Why did the dockyards choose Sophos?

Colombo Dockyard zeroed in on Sophos after carefully considering other options. Sophos stood out from its competitors due to its use of a deep learning neural network that memorizes attack patterns and can therefore identify and prevent threats in an accelerated manner. Another benefit was Sophos’ behavior-based CryptoGuard technology that stops never-before-seen ransomware and boot-record attacks and the inherent capability of automatically rolling back affected files to their safe state in seconds. The IT

> *"Apart from a vulnerable security solution, we were also experiencing of lack of after sales support and a dawning realization that our staff lacked proper security awareness. We were also missing technical support related to the latest technology and were not secure against wireless traffic. Our core objective from an IT security perspective was to look for a bundled solution wherein it uses an integrated approach towards security."*
>
> P.H.S. Daminda – CIO, Colombo Dockyard PLC

team also went through a series of third-party test results such as Sophos' AV-TEST rankings and the Gartner Magic Quadrant to justify its selection of Sophos as its security vendor of choice.

What Sophos solutions did they chose?

The IT team identified Sophos XG cloud-based firewall, Sophos Intercept X Endpoint, Sophos Wireless, Sophos Mobile, Sophos Email, Sophos Sandstorm and Sophos Home as the best fit for its needs. A huge benefit that Sophos also brings to the table is synchronized security whereby the different security components share information in real time and automatically and quickly respond to security incidents.

With Intercept X, Colombo Dockyards knows the company's workstations have comprehensive protection. The endpoint and firewall combination blocks ransomware, bots, worms, hacks, and APTs at the gates. The IT team can now block unnecessary sites including social media and streaming sites and has the confidence to use web-based storage knowing that they have full visibility and control over users, web traffic and application and content usage.

The IT team was also concerned about the security of the CDPLC Wi-Fi network. Sophos Wireless helps administrators monitor and secure wireless traffic. Additionally, remote workers are connected to CDPLC systems via SSL secured VPN connections with two-factor authentication.

For users with no VPN connection, the company protects these devices with Sophos Home.
With Sophos Sandstorm, potentially malicious/suspicious email messages are scrutinized and quarantined if infected. This ensures a more secure inbox.

Sophos Mobile is used to secure company provided mobile phones and iPads.

How has CDPLC's cybersecurity posture improved since implementing Sophos?

The CDPLC IT team has witnessed quick and tangible benefits from its Sophos deployment. With traffic shaping policies they can control the bandwidth to less than 40 Mbps and for around 90% of operating hours the bandwidth is less than 30 Mbps. The pandemic meant that many employees are working from home, and the SSL-secured VPN with two-factor authentication has made this transition easier and more secure. CDPLC has also witnessed improved network performance since the Sophos deployment, and this has resulted in an increase in productivity and a speeding up of system-related activities.

www.sophos.com

SOPHOS

2022-07-01 CCS-EN (NP)