



Sophos Delivers Synchronized Defence Against Advanced Cyber Threats to a Top Hotel Brand

Serena Hotels is one of the world's leading hospitality brands, with a collection of 23 unique hotels, resorts, safari lodges and camps located across Africa. Focusing on meeting the most demanding customer requirements, each and every Serena property offers a unique hospitality experience that is purely customer focused. The brand has experienced tremendous growth over the years resulting in a rapidly growing IT infrastructure spread across distributed locations. This means Serena has to address a continuously expanding attack surface and traditional security solutions were proving to be incapable of doing so. The brand was therefore looking to move to a single vendor approach towards securing its IT infrastructure and protecting its assets with a proactive approach to security. Sophos and its powerful portfolio of security solutions perfectly fit its needs.

CUSTOMER-AT-A-GLANCE



SERENA HOTELS
KENYA • TANZANIA • ZANZIBAR • UGANDA • MOZAMBIQUE • RWANDA

Serena Hotels
Kenya

Industry
Hospitality

Website
www.serenahotels.com

Sophos Solutions
Sophos XG Firewall
Sophos Intercept X Advanced
- 1050 Licenses
Sophos Intercept X Advanced
for Servers - 151 Licenses

“Rapid growth of our business meant an equally rapid increase of attack surface. In order to address modern day threats, we wanted to build an integrated cybersecurity infrastructure, that increased our ability to stop cyberthreats, from device to cloud and in the present and future.”

Chispine Mboga, Country IT Manager, Kenya

Challenges

- › Lack of a robust UTM technology with flexible and simple configuration interface, sold at a good price point.
- › Risk to global rampant ransomware prevalence in the absence of a security solution that focuses on dealing with ransomware attacks.
- › Lack of synchronized defense in a multi-layer security implementation. Existing solutions were acting alone without the synchronization of threat intelligence and unified protection.
- › Lack of central management of configurable security policies across multiple sites/locations and countries, within a single management portal.
- › Limited visibility of threat and protection data and that too available through a complex, difficult-to-use portal.

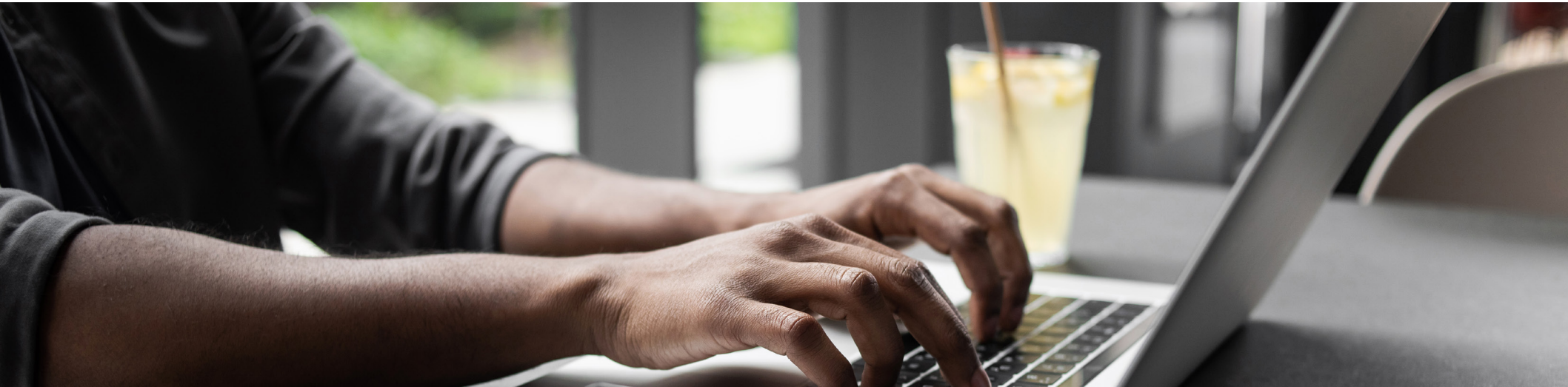
Serena Hotels was using a range of different UTM appliances and endpoint solutions before moving to Sophos. Security solutions from different vendors resulted in disparate data coming from different installations. It was becoming difficult to keep track of all security statistics coming the IT Team’s way and quickly pushing policies that kept the network and endpoint safe and secure. The team was also disappointed with their rigidity, complex configurations and limited administrative/troubleshoot tool sets.

“Limited features, yet a high cost of purchase and subscription of our threat management appliances was a cause of concern for us. A quickly evolving cyber threat landscape highlighted by rampant prevalence of ransomware made us realize that a layered security architecture made up of security solutions from different security vendors was not the way ahead. We needed to move to a more advanced security paradigm,” explains Mr. Chispine.

The IT team felt their endpoint security was the last point of defense, yet the most vulnerable as their existing endpoint solutions were not evolving fast enough to catch up with newer threats. Also, their existing security solutions did not focus on detecting and stopping ransomware attacks while in the process also decrypting any files that get hijacked.

Moreover, these had a heavy computing resource footprint therefore becoming a bottleneck to efficient computing both at the server and workstation level.

Another problem area was the on-prem deployment of management console for end point solutions, which required regular upgrades and higher administrative overheads for the IT Team.



The key focus of their search for a new security partner was to deploy solutions from a single vendor, but also benefit from the firewall and endpoint talking to each other, sharing threat intelligence; and building a cybersecurity infrastructure wherein security incidents are remediated with automated response.

How Did Sophos Deliver All-Encompassing Security, Managed Simply and Effectively?

Serena Hotels worked with Microskills Information Technologies (Kenya) Limited, a Sophos Partner who coordinated Proof of Concept testing. After thorough pre-sales discussions and product functionalities review and facilitation of product

demos, the IT Team was convinced Sophos products perfectly addressed their security challenges.

With XG Firewall, Serena Hotels gets the best protection to stop advanced threats before they have a chance to cause havoc on the network. Features like Deep Packet Inspection, Encrypted Traffic, Web Protection, Zero-Day and ML Protection, Advanced Threat Protection, Cloud Sandbox and more, protect Serena's network from the latest hacks. The Secure Sophos VPN Client enables the IT Team to conform with social distance norms as the majority of their staff work from home. The staff can securely access critical business applications at a time when it is imperative to maintain productivity, but still not expose the staff to the threat of infection.

With Sophos Intercept X Advanced for Endpoint and Server, the IT Team benefits from rich and powerful features that reduce the attack surface such as web security, peripheral control, web control, application control, and download reputation. Also, malware threats are stopped before they run on the device with security features such as anti-malware file scanning, deep learning malware detection, pre-execution behavioral analysis (HIPS) and more.

"Sophos Intercept X delivers specialized layered protection for our endpoints that predictively prevents ransomware attacks, and with CryptoGuard, we know that any changes to the files will be rolled back in real time. This has definitely given us peace of mind knowing Intercept X is protecting our endpoints and servers in real time, from ransomware attacks," says Mr. Chrispine.



A key area of concern for the IT team was the inability of the disparate security installations to work in deep synergy and Synchronized Security had solved this problem for them. "With Security Heartbeat™ linking our Sophos Endpoint with the Sophos XG Firewall, threat intelligence is now shared in real time enabling multi-layered automated coordinated response to isolate threats and prevent the spread of malware activity across the network," explains Mr. Chrispine.

Sophos Central delivers multi tenancy sub-estates on a single management portal. Previously, the IT team was saddled with an exclusive standalone management console with different sets of security policies configured on each instance for each site/location. With Sophos Central, the IT Team has overcome this challenge as a uniform approach can be leveraged to push the same set of policies across different sites and installations.

"Apart from the deep and detailed, yet simple reporting and Threat Analysis that the IT Team gets visibility into, we are also pleased with the diverse UTM subscription offerings, which allows us to choose a subscription that perfectly addresses our needs. Also, on-premise security solutions have given way to solutions hosted on the cloud, all managed with a single pane of glass delivered by Sophos Central. This has improved the efficiency of the IT Team and brought down the IT-centric costs," says Mr. Chrispine.

Sophos also made specific customized configurations on the Sophos Central to ensure Serena Hotels can effectively use a multi-tenancy Sun-Estate to group and manage their devices according to custom policies for their different sites (27 branches) in the 6 different countries they operate in.

What were the business results of Sophos Deployment?

The Sophos solutions were deployed over a period of 2 months with the help of a Sophos Sales Engineer for Kenya. This was in line with Serena's approach to deploying new IT assets. Any new deployment for Serena Hotels involves initial proof of concept testing, followed by a one-month in-product pilot at one site and thereafter concurrent deployment across the rest of the sites over the ensuing month.

The IT Team also attended Sophos Administrator Certification Training that gave them a deeper understanding of the technologies and configuration for the solutions.

CUSTOMER CASE STUDY **SERENA HOTELS**

“Our experience of using Sophos Professional Services was excellent. The Sophos Technical Engineer helped ensure a quicker deployment, while guiding us to tailor the solutions to our preferred security architecture, in the process helping us to efficiently troubleshoot any emergent “teething” issues,” says Mr. Chrispine.

From the cybersecurity standpoint Serena Hotels experienced enhanced cybersecurity and improved security and threat visibility. They also benefited from significant costs savings by deploying secure multi-country VPN connections to replace expensive point-to-point data connectivity through connectivity providers/carriers.

The IT team finds it simpler to manage all Sophos solutions compared to the previous solutions they used. This saves time, improves efficiency, and increases confidence in the cybersecurity infrastructure.

With Sophos, the team’s multi-level layered approach to security remains the same, but changes have been made around proactive and reactive security administrative action courtesy the simplicity of Sophos Central reporting and reliability of the deployed Sophos solutions.

“We plan to progressively scale up Sophos solutions across all the layers of security architecture, deepening our uptake of the whole spectrum of available Sophos cybersecurity solutions, especially where consolidation of protection management and further opportunities for heartbeat synchronization can be leveraged. Sophos offers value for money, and works seamlessly, leaving more time for Information Technology personnel to focus on business innovation and the core business applications. We recommend it to any organization that wants a proactive approach to security, that can be managed easily and effectively,” signs off Mr. Chrispine.

For more information on
how Sophos can help you,
please visit sophos.com