SWAN™ *IT Solutions Management Company*

May 2020
Casestudy

Swan Strengthens Cyber Security with Sophos Synchronized Security for a Leading E-learning Service Provider.

Industry: E-learning

Head Quarter: Mumbai, India

Client: (Provided on request)

Objective

- Simple, more manageable security that also offers protection for non-technical users and their devices on-site and on the go from zero-day attacks, advanced threats, and ransomware.
- Smooth acceleration and automation of incident response processes to reduce the workload in this area.
- Single pane of glass solution which gives layered synchronised security for End points, Servers, Email , Mobile.

Solution

- Sophos Central Intercept X Advanced with Managed EDR for 450 Users.
- Sophos Central Intercept X Advanced for Server with EDR for 25
- Sophos Mobile Advance for 450 Mobiles - Customers will manage & Monitor their users' Mobile devices with the help of Sophos MDM solution.
- Sophos Phish Threat – 50 License
- Customers will educate their users for Phishing attacks with the help of Sophos Phishing simulation solution.
- Sophos Central

All above Sophos solutions are managed and administered from Sophos Cloud platform.

Introduction

More and more sophisticated and targeted attacks made it necessary for our E-learning customers to replace their existing, outdated infrastructure and start looking for a more modern network security solution that would grow with the business and its requirements. Our customers scanned the market for IT security solutions, but were dissatisfied with the existing silo solutions. The IT managers of our E-learning service providers, explained that the point products available worked in isolation and required them to juggle multiple administrative consoles. They approached Swan to achieve their requirements.

As a result, they were difficult to manage and unable to quickly and effectively counter today's coordinated attacks. Additionally, these tools were not all-inclusive and required expensive add-ons and upgrades.

Swan provided a better security option with Sophos Synchronized Security for the E-learning service providers to protect their data from Ransomware.

Challenges

- As cyber threats become ever more complex, the pressure to have the right endpoint solution in place has also grown.
- Having a shortage of internal security expertise- Usability is also essential if hard-pressed IT teams are to make best use of the protection capabilities.
- Primary concern- Malware includes both known as well as never -seen-before malware. Often, solutions struggle to detect the unknown malware.
- Rise of crypto mining programs used in crypto jacking attacks.
- Protection from Ransomware.
- Preventing malicious behaviours of applications, like a weaponized Office document that installs another application and runs it.

Approach

- **Anti-malware/antivirus:** Signature-based detection of known malware. Malware engines should have the ability to inspect not just executable but also other code such as malicious JavaScript found on websites.
- **Application lockdown:** Preventing malicious behaviours of applications, like a weaponized Office document that installs another application and runs it.
- **Behavioural monitoring/Host Intrusion Prevention Systems (HIPS):** This foundational technology protects computers from unidentified viruses and suspicious behaviour. It should include both pre-execution and runtime behaviour analysis.
- **Web protection:** URL lookup and blocking of known malicious websites. Blocked sites should include those that may run JavaScript to perform crypto-mining, and sites that harvest user authentication credentials and other sensitive data.
- **Web control:** Endpoint web filtering allows administrators to define which file types a user can download from the internet.
- **Data loss prevention (DLP):** If an adversary is able to go unnoticed, DLP capabilities would be able to detect and prevent the last stage of some attacks, when the attacker is attempting to exfiltration data. This is achieved by monitoring a variety of sensitive data types.
- **Machine learning:** There are multiple types of machine learning methods, including deep learning neural networks, random forest, bayesian, and clustering. Regardless of the methodology, machine learning malware detection engines should be built to detect both known and unknown malware without relying on signatures. The advantage of machine learning is that it can detect malware that has never been seen before, ideally increasing the overall malware detection rate.
- **Anti-exploit:** Anti-exploit technology is designed to deny attackers by preventing the tools and techniques they rely on in the attack chain.
- **Credential theft protection:** Technology designed to prevent the theft of authentication passwords and hash information from memory, registry, and off the hard disk.
- **Endpoint detection and response (EDR)/root cause analysis:** EDR analyze and respond to previously detected incidents. Offer hunting capabilities to discover attacks that previous went unnoticed.
- Sophos Synchronized Security connects Sophos Email to Phish Threat, the Sophos phishing simulation and training platform. Identifying users who have been warned or blocked from visiting a website due to its risk profile, or replying to a spear phishing email. Seamlessly enrolling them into targeted phishing simulations and training to improve awareness.

Business Benefits

- Comprehensive security for the entire organization from advanced cyber threats. Sophos Complete Security integrates endpoint, web, mobile, email and data security.
- Simplify management, Everything in one intuitive console, Same usability and same simplicity.
- Reduce complexity: One vendor, one interface, one console
- Complete control on End points, Mobiles and Emails.
- Easiest way to extend protection: Add additional security layers quickly and easily get started with a couple of clicks
- Protection from ransomware which is the most prevalent malware attack affecting today's organizations.
- Protect sensitive data while staying safe from spam, phishing attacks and malware, including the latest ransomware

Swan Solutions & Services Pvt. Ltd
404 T-Square, 4th Floor, Saki Vihar Road, Andheri East, Mumbai 400 072 INDIA.
EMAIL: enquiry@swansol.com | WEBSITE: www.swansol.com

Celebrating 30 1989 - 2019 years