SWAN™ *IT Solutions Management Company*

July 2020
Casestudy

Swan provides complete protection to critical assets of a banking and financial institution.

Industry: Banking & Finance

Head Quarter: Mumbai, India

Client: (Provided on request)

Objective

- Protection of Linux and AIX Servers from Cyber threats.
- Deployment of Centralized Server Protection Solution.

Solution

- Behaviour Analysis/HIPS
- Web Security
- Download Reputation
- Web Control, Peripheral Control
- Application Control
- Data Loss Prevention
- Patch Assessment
- Malware Removal
- Endpoint Exploit Protection Crypto-Guard Anti-Ransomware
- Live Protection

All above Sophos is powered by a state of the art Deep learning engine which is subset of machine learning.

Introduction

The pace of digitization of financial transactions in India continues to gather pace. It is estimated that the total payments conducted via digital payment instruments will be in the range of USD 500 billion by 2020, which is approximately 10 times of current levels.

Cybercrime has jumped to the second position as the most reported economic crime and financial institutions are prime targets. As cybercriminals find new ways to attack, breach, and exploit Banks, threat patterns such as phishing, spear-phishing, and social engineering evolve and become more sophisticated. The recent episodes of malware attacks, viz. WannaCry and Petya, brought Banks the rising menace of ransomware. As more Banks recognize the risks of ransomware attack via email, criminals are exploring other vectors.

Ransomware authors are also starting to use techniques other than encryption, for example deleting or corrupting file headers. With the advent of IoT-powered botnets, destructive DDoS attacks are inevitable and have intensified in volume and frequency.

Swan provided a better security option with Sophos Protection Enterprise edition on Linux and Aix servers to protect their data from Ransomware.

Challenge

Banks in India need to improve their response capability to mitigate DDoS risks. As BFSI is a highly regulated sector, banks invest time, money and effort in deploying best-in-breed technology, which unfortunately end up running in silos and are

difficult to manage together. Traditional signature based solutions are no longer enough on their own and are prone to zero-day attacks. it.

Approach

- **Deep Learning** : The artificial intelligence built into **Intercept X** Advanced for Server is a deep learning neural network, an advanced form of machine learning, that detects both known and unknown malware without relying on signatures.
- **Exploit Protection** : Denies attackers by blocking the exploits and techniques used to distribute malware, steal credentials, and escape detection. This allows Sophos to ward off evasive hackers and zero-day attacks in your network.
- **Active Adversary Protection** : Protects against advanced hacking techniques performed by attackers to establish their presence on a device, steal credentials, escalate privileges, or gain more enduring access, including Code Cave mitigation and credential theft protection.
- **Root Cause Analysis** : Detailed, forensic-level analysis illuminates the root causes of attacks and their infection paths, and offers guidance to help remediate infections today and bolster your security posture.
- **Server Lockdown/Application Whitelisting** : With a single click, we scan and inventory applications – only allowing those to run, and also to update without manual intervention.
- **Application Aware**: On a server it's critical that specific server applications run, and we know that repeating inspecting databases just slows them down, so we treat them specially, to reduce False Positives.

Business Benefits

Full breadth of security capabilities to prevent, detect & respond to today's threats.

- Higher cost to business when servers are held hostage but now banks servers are protected by Sophos anti-ransomware.
- Servers are protected from credential theft, privilege escalation, or code cave.
- Block the latest threats, including ransomware, exploit-based attacks, and server-specific malware with powerful deep learning technology.
- Stop real-world hacking techniques used for credential harvesting, lateral movement, and privilege escalation.
- Prevent unauthorized applications from running on servers by whitelisting permitted applications.
- Anti-exploit technology denies attackers by preventing the tools and techniques they rely on in the attack chain.
- It gives power to proactively hunt down evasive threats and deep-dive into security incidents to understand their scope and impact.
- Machine learning is that it can detect malware that has never been seen before, ideally increasing the overall malware detection rate.
- Provide insight into what has occurred to help avoid future security incidents.
- Protect critical system files and data from any unintentional changes, and optionally monitor key application locations. Sophos Server Protection continuously monitors and tracks unplanned and unexpected changes to help identify potential PCI DSS security breaches.
- Sophos console enables easy management and visibility of mixed server environments – for example, alerts, events, and reports all filtering through into one easy-to-access and easily understood view.

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