IT Solutions Disruptor Builds a More Efficient Cybersecurity Framework with Sophos Synchronized Security

CloudFactory is a global leader in delivering workforce solutions for machine learning and business process optimization. Since its inception, it has earned a reputation for building innovative and cutting-edge solutions, which has enabled the company to build solutions for some of the most reputed companies in the tech world and beyond. They are making a mark in a fast-paced environment wherein tech evolves continuously, and therefore were also aware of the risks posed by cybercriminals, sophisticated cyberattacks and a growing attack surface. An innovation-focused company cannot depend on an outdated approach towards securing its network and endpoint. CloudFactory wanted to transition to a more consolidated and synergistic approach to security, and Sophos Synchronized Security emerged as the best option for their needs.

CUSTOMER-AT-A-GLANCE

CloudFactory

Industry
IT Services and Consulting

Sophos Solutions
Sophos XG Firewall
Sophos Intercept XDR
Sophos Encryption
Phish Threat

"Transitioning to a more integrated security framework was par for the course because we were using a mix of legacy security solutions and a manual approach towards managing these. This was neither delivering security value nor addressing evolving security concerns. This prompted our move to Sophos network and endpoint protection and its cybersecurity system – Synchronized Security."

Sumesh Karki, Security Operations: EUC Specialist

Challenges

- Managing and controlling the security of peripheral devices manually, which was time taking and prone to errors.
- Lack of a centrally managed endpoint and network solution.
- Inability of existing security solutions to detect viruses and worms in user devices.
- Security solutions working independently from one another resulting in intelligence gaps and no synchronization between them.
- Inability to address phishing attempts.
- Complex network management resulting in a low-performance network and ineffective network security.

What were your minimum requirements for security and the key challenges your organization was facing?

A key requirement was building a new and improved security ecosystem with reliable centralized management and reporting. The IT team had also identified certain security lacunae that needed to be plugged. "Our existing solutions did not receive frequent updates and sporadic signature updates meant there was a danger of viruses falling through security gaps and distributing malware," explains Mr. Karki.

The IT team was unable to enforce role-based control which resulted in a cross-section of personnel being able to access software, applications and data that weren't relevant for them or did not fall under their profile of responsibilities. This meant there was an increased danger of critical information falling into the wrong hands, if employees fell prey to phishing attacks.

Log collection of all security incidents which helps zero in on operational trends, investigation and analysis, is a security imperative. CloudFactory lacked proper log keeping and a process for incident analysis and investigation. This meant the organization couldn't take the necessary regular steps to build a robust security fabric.

Mr. Karki and his team were also concerned about the lack of security awareness, specifically about phishing attacks and they were always a worry that a phishing attempt would result in a data breach. Something else that was worrying them was compliance and the demands of multiple regulations that needed implementation of comprehensive security protocols. The need of

the hour was deploying the right security solutions, and being able to manage them effectively to ensure the CloudFactory security framework was compliant with different regulations. One of the key requirements of most regulations is encryption and this was a critical challenge CloudFactory wanted to address.

A lean IT team coupled with a need for an extensive security framework across the endpoint and network, meant they needed both network and endpoint to talk to each other, share intelligence, managed from a single management console.

How does an extremely agile company protect its network and endpoints with a next-gen approach to cybersecurity?

With Sophos XG Firewall, CloudFactory benefits from high-performance traffic scanning for IPS, AV, Web Protection and App Control. This network solution delivers improved visibility, policy tools and built-in intelligence to strengthen security across the network. The team is now confident that the latest ransomware and unknown threats are kept away from the network backed by industry-leading machine learning technology, powered by SophosLabs Intelix.

Other features like Web Protection, Advanced Threat Protection, user identity-based policies, web control, application control and content control ensure that the CloudFactory network is protected from threats that continuously evolving. Traffic shaping policies and bandwidth allocation makes for an optimally performing network that is further strengthened by high performance core networking including enterprise-grade network technology, routing and bridging.

"We were well aware of our industry being on the radar of cybercriminals waiting to exploit a security weakness and launch a ransomware attack. We were therefore looking for an endpoint solution that delivered extensive ransomware protection," says Mr. Karki, underlining a key reason why they were searching for an extensive endpoint security solution.

Sophos Intercept X Advanced with XDR monitors and secures the whole attack chain and disrupts it using deep learning to predictively prevent advanced threats like ransomware attacks. Features such as ransomware file protection, behavioral analysis and automatic file recovery stop ransomware and boot record attacks. Deep learning, an advanced form of machine learning enables the IT team to adopt a predictive approach to protect endpoints from known and never-seen-before threats.

XDR synchronizes native endpoint and firewall deployments to offer a holistic view of their organization's environment with a rich and constantly enriching data set and deep analysis for threat detection, investigation and response, that helps them focus attention on items that need immediate attention.

More importantly, all their Sophos solutions can be effectively managed from Sophos Central, a cloud-based management platform, that helps them investigate potential threats, create and deploy policies, manage their expanding estate and do a lot more. One of the team's key pain points was peripheral control that was being exercised manually. But peripheral control is now a breeze with Sophos Central which allows the team to control access to peripherals and removable media.

Another challenge was irregular signature updates, but the regular updates across all Sophos deployments now gives the team the confidence that its cybersecurity infrastructure is perfectly positioned to keep the latest malware threats away.

With Sophos Phish Threat, the IT team now has the capabilities to improve employee awareness around phishing through numerous exercises. The modules keep updating giving them the ability of choosing different variations for user training.

The encryption worry has been addressed with Sophos Central Device Encryption that leverages Windows BitLocker and macOS FileVault to secure devices and data. As it's a part of the Sophos Central unified security console, Mr. Karki and team can manage Central Device Encryption from alongside their entire range of Sophos protection.

One of the biggest advantages of using Sophos Firewall and endpoint protection is Synchronized Security, a cybersecurity system wherein revolutionary Security Heartbeat links Sophos managed endpoint with firewall to share health and other valuable information. This drives incident response that is automated and coordinated to isolate threats and prevent lateral movement.

How was the Sophos implementation and what are the benefits of transitioning to a highly evolved security framework?

The purchase and implementation happened through Cloud Tech Solution, a reputed Sophos partner who took the CloudFactory team through the various Sophos security solutions their features to help the evaluation process and arrive at a decision. The partner also provided training and continues to provide all necessary support to help CloudFactory optimally leverage the potential of their security framework empowered with multiple Sophos products.

From the security ROI perspective, the organization has benefited in different ways. Earlier, their dependency was on manual tweaks to individual devices for machine hardening purposes. As this was a manual process, it couldn't be tracked, and it took weeks for the IT team to enforce new hardening policies. With Sophos Endpoint, all they need to do is create a policy, test it and deploy it, within a span of a few days. This has resulted in 300% time saving every time a new machine hardening policy is deployed across CloudFactory endpoints. Couple this with the man hours saved due to centralized reporting and the IT team has valuable time on its hands that it can invest in other critical activities that strengthen their IT framework.

The Sophos Firewall deployment, has reduced spam and phishing attempts by more than 70% on the CloudFactory network, which illustrates how this solution has strengthened the CloudFactory security framework.

Sophos CloudFactory also benefits from a single multi-solution vendor that addresses all of the organization's security needs. A single-vendor approach to building security ecosystem is so much better than a multi-vendor approach, in which the management of different security solutions from different vendors is a complex, time taking, costly and error prone exercise.

Sophos has helped CloudFactory meet its compliance requirements, especially through the DLP functionality. The features and functionality that Sophos brings to the network and endpoint has helped CloudFactory comply with different regulations such as ISO 27001, ISO 9001, SOC II etc.

"We recommend Sophos as a vendor to all organizations that want to leverage a consolidated and cohesive approach to security with products from a single vendor and wherein the firewall and endpoint share intelligence, proactively and deliver automated response to keep the network and endpoints safe," signs off Mr. Karki.

Visit sophos.com/firewall

© Copyright 2021 Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is a registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

SOPHOS

22-11-10 CCS-EN (NP)