SOPHOS
Security made simple.

CUSTOMER CASE STUDY

SAPNE AAPKE, SAATH HAMAARA

Customer-at-a-Glance

AAVAS Financiers Limited

Industry
Financial Services

Number of Staff
2,500

Website
https://www.aavas.in

Sophos Solutions
Sophos Central Endpoint Protection
Sophos XG Firewall
Synchronized Security

Sophos Customer
Since 2016

Protecting **Financial Institutions** with Next-Gen Security

AAVAS Uses Sophos to Strengthen Cybersecurity Infrastructure with Advanced Security Solutions

‘We chose Sophos because we believe that standardizing security across our organization and between the branches will provide an improved level of security, which is exactly what our customers expect.’

Mr. Yogesh Kumar Bansal
Deputy Vice President IT
AAVAS Financiers Limited

Business Challenge

- Achieving the highest level of security across the organization to protect sensitive data
- Securing data against advanced malware attacks such as ransomware
- Exercising access control for peripheral devices and removable media
- Increasing visibility into the applications, users and content moving on the network
- Improving transparency and control into website traffic, URL filtering and bandwidth optimization
- Simplifying security deployment and management and getting granular visibility into everything that’s happening on the network

AAVAS Financiers Limited is a housing finance company whose core business is providing housing loans primarily in the un-served, unreached and under-served markets across India. It is a public company and its operations have witnessed tremendous growth since the time it began operations. As a result, a significant amount of company data and PII is generated day in and out. This data is highly sensitive and needs to be secured against advanced malware attacks and zero-day threats. Their key objective was strengthening their IT security posture with next-gen security products that had the capabilities to protect data from emerging cyber threats. AAVAS identified Sophos as the security vendor best suited to deliver on its demanding security needs.

Mr. Yogesh Kumar Bansal is the Deputy Vice President IT at AAVAS Financiers Ltd. It’s his job to make sure that the company was extremely well-protected against emerging and more complex cyber attacks that had the potential to disable endpoints, adversely impact network operations, infect critical business systems and expose sensitive data to cyber attackers. “We are a financial services company and one of the key drivers of our reputation on the market is our focus on securing customer and company data. What kept me up at night was the possibility of a Zero-Day-Attack, that exploited a security vulnerability and released advanced malware, resulting in a data breach. This was a nightmarish scenario for me and my team. Such attacks could disrupt business continuity resulting in loss of productivity, and lead to tremendous monetary loss for AAVAS,” says Mr. Bansal.

The cyber threat landscape is morphing dramatically; the number of malicious apps has alone risen steadily in the last four years. In 2013, just over a half million samples were malicious. By 2015 it had risen to just under 2.5 million. For 2017, the number is up to nearly 3.5 million. (Source: SophosLabs 2018 Malware Forecast)

Mr. Bansal realized that if AAVAS was to overcome advanced threat vectors, the company had to strengthen its cybersecurity posture. He was clear that security needed to be a strategic part of AAVAS' IT infrastructure and therefore was looking to deploy next-gen security solutions that provided a comprehensive security blanket, worked together as a system and which were simple to deploy and manage. "There was no doubt in my mind that I wanted AAVAS to stay away from point products, whose deployments result in security gaps, drive up costs, increase operational complexity and deployment headaches. I and my team wanted to deploy security solutions whose approach to security spanned network and endpoints and which seamlessly worked together to defeat increasingly sophisticated cyber threats that attackers might launch against our organization," asserts Mr. Bansal.

Two key concerns of AAVAS Financiers Limited was data and productivity loss - the two factors that adversely impacted the business bottom-line. After thoroughly evaluating the choices available on the market, Mr. Bansal decided that Sophos' strong product portfolio had the necessary abilities to bring the company's cybersecurity vision to life.

'Sophos XG Firewall 17 has saved me countless hours during every work week so I can focus on other IT initiatives.'

Mr. Yogesh Kumar Bansal
Deputy Vice President IT
AAVAS Financiers Limited

What made you switch to Sophos from your existing security solutions?

Mr. Bansal and his team found that the security products they had deployed were inadequate as these products could not cope with advanced malware attacks and zero-day threats. The level of sophistication of cyber attacks and their frequency was going up and they were saddled with legacy point products. The fact that AAVAS has a distributed workforce across multiple offices complicated matters for the IT team. "I was concerned about our inability to seamlessly manage users and their access to network resources across our offices. Due to the disparate nature of our existing security products, user-based policy setting was a complex task and riddled with errors. These also offered limited device control, so there was also constant danger of compromised devices letting in malware into the network. We had a legacy on-premise solution, which had plenty of limitations when it comes to protecting against the highly organized gang of cyber criminals who wanted to get at our critical data," explains Mr. Bansal. "We were spending a lot of time in verifying user logs and cross checking the functioning of the multiple OEM security solutions we were using. Couple this with limited data control and lack of granular web protection, and we knew we had a huge problem on our hands, that needed to be sorted out quickly."

Mr. Bansal and his team wanted to move from traditional security solutions to cloud managed security solutions and adopt a unified approach towards security. They wanted to team up with a single vendor who was a leader in both next-gen endpoint security and network security that could better address evolving threats. They were essentially looking for a complete security solution that was easy to manage and offered far greater simplicity and scalability than their current security products. Their search for this vendor ended at Sophos.

'We loved Sophos' approach of providing a solution rather than a product.'

Mr. Yogesh Kumar Bansal
Deputy Vice President IT
AAVAS Financiers Limited

How did Sophos emerge as your security vendor of choice?

Mr. Bansal is an IT security veteran, and keeps in touch with all the latest cybersecurity trends and therefore knew exactly the kind of security solutions that would bolster AAVAS' cybersecurity environment. "The scale and complexity of cyber threats is increasing day-by-day and I wanted to deploy security solutions that stopped threats at my network's edge, offered advanced malware protection on the device itself and where threat intelligence was shared between network and endpoint to identify and respond to a compromised system on my network," describes Mr. Bansal.

Mr. Bansal started looking for a vendor whose portfolio consisted of powerful security products and whose technological innovation kept pace with the rapidly changing threat landscape. "We worked with a channel partner with a proven track record of successful implementation behind them and they recommended Sophos as a vendor whose solutions could help us build an amazing IT security infrastructure. While we evaluated other security vendors as well, it was Sophos Central Endpoint, Sophos XG Firewall and Sophos Firewall Manager that met our expectations, especially those pertaining to web control, user management, policy control, data security, peripheral and application control, centralized user management and next-gen security against advanced malware like ransomware, phishing attacks and zero-day attacks," discloses Mr. Bansal.

Mr. Bansal and his team thoroughly evaluated the vendors on the market and were impressed with the preparedness of Sophos' products to address the latest cyber threats. They loved the fact that Sophos product portfolio offered next-gen security, but extremely simplified management. "We wanted to deploy solutions that made sure we could serve our customer in a hassle free and timely manner. Also, it was important that advanced security did not come at the cost of complexity. Sophos delivered on these expectations, perfectly," pronounces Mr. Bansal.

How did Sophos's Endpoint Protection secure your organization from advanced malware and infections?

With Sophos Central Endpoint Advanced, AAVAS has brought sophisticated yet simple security to their desktop environment helping Mr. Bansal and his team secure the company's primarily Windows systems against malware and advanced threats such as targeted attacks. "Malicious traffic detection backed by real-time threat intelligence from SophosLabs helps us prevent, detect and remediate threats with ease. Where earlier we were pouring a lot of time into remediation, Sophos Central Endpoint Protection removes detected malware automatically or isolates compromised devices in order to prevent damage. This saves a lot of time that can be better spent elsewhere," expresses Mr. Bansal.

Sophos' endpoint protection solution also delivers on AAVAS' key requirements of better web, application and peripheral control. By enforcing category-based web filtering on and off the corporate network, Mr. Bansal gets more control over the content employees can access over the net. With application control, Mr. Bansal can block application by category or name, thus reducing risks posed by employees accessing malicious, illegal or unauthorized software. He also has better control over removable media and mobile devices with Peripheral Control. Also, the Data Loss Prevention capability allows him to restrict unauthorized data flow with the use of prebuilt or custom rules.

"We are benefiting from Sophos' new approach to protection and its ability to catch zero-day threats without adversely impacting device performance. This means the Sophos Central Endpoint Protection is doing its job transparently, without impacting employee productivity. This is a huge plus," declares Mr. Bansal. "Sophos truly delivers next-gen protection and this is illustrated by its 'Behavioral Analytics' feature that determines suspicious behaviors; malware specially designed to dodge legacy solutions can be easily detected by Sophos Endpoint Protection."

Mr. Bansal and his team also value the simplicity of log management and the user-friendly interface, which allows them to maximize the potential of this security solution. "To put it simply, Sophos Central Endpoint Advanced has made our lives a whole lot easier. It offers granular visibility into the security status of my workforce and makes it easy to extend protection to all user devices on and off the network," he adds.

How did XG Firewall secure the network perimeter defenses of AAVAS?

AAVAS has deployed 220 XG Firewall's out of which 218 have been deployed on MPLS and VPN to secure the network of branch offices and remote offices. "Our branch and remote offices offer the same services as our corporate office and therefore demand the same level of security. We had no doubt Sophos XG Firewall, with its ability to offer unprecedented visibility into our network, users, and applications was best suited for our needs," reveals Mr. Bansal.

Mr. Bansal and his team used firewall security policy to implement zone based policies, wherein they could restrict access to certain zones. This meant they ensured only a certain number of users could authenticate from certain zones, e.g. the LAN zone or they could restrict zone access to a limited number of users. Another XG firewall capability that helped AAVAS drive business continuity was multiple ISP management that allowed them to configure failover and load balancing. This helped achieve constant and secure availability to the internet and avoid network vulnerability.

"XG Firewall version 17 uses the latest advanced technology including ATP, Dual AV, top-rated IPS, web and application control and full featured Web Application Firewall to protect our network perimeter from ransomware and advanced threats. We benefit from exceptional visibility into the risky users in the network, unknown and potentially dangerous apps, and suspicious payloads. XG's rich on-box reporting enables my team to look at a comprehensive set of reports, organized by type. We can change or refine our policy setting as per the risk insights we get," expresses Mr. Bansal. "We also appreciate the risk assessment provided by Sophos User Threat Quotient (UTQ) that delivers actionable user intelligence based on a user's surfing habits. This enables us to identify which user needs more training on security best practices and digital hygiene. What also works for us big time is the unified view for firewall rules and policies, which allows us to deploy new configurations easily and quickly," articulates Mr. Bansal.

The team is extremely impressed with the latest version of XG Firewall, version 17; they have a high word of praise for the management and troubleshooting tools in the new version and make good use of the policy tester tool. They also have good things to say about the new web content filtering tools in XG Firewall v17. "The new and improved web filtering tools now enable us to block Potentially Unwanted Applications from being downloaded, enabling us to address a problem before it becomes a crisis," verbalizes Mr. Bansal.

> *'Sophos Security Heartbeat™ is cutting-edge technology. We are excited that we can link our Sophos protected endpoints and our XG Firewall together in order to have real-time communication and complete visibility into our entire network.'*
>
> Mr. Yogesh Kumar Bansal
> Deputy Vice President IT
> AAVAS Financiers Limited

The Sophos Firewall Manager gives Mr. Bansal and his team the benefit of centralized management for all the XG Firewalls deployed across corporate HQ, branch and remote offices. "With over 200 Firewall units, we wanted a single plane of glass, which allowed us to easily monitor the health of our managed devices and ensure consistent policy deployment across our offices. The SFM made this possible allowing us to manage all policies and settings across all deployed firewalls from a single console," says Mr. Bansal.

How has Synchronized Security benefited AAVAS?

AAVAS is using Synchronized Security at its Head Office and believes it is an extremely innovative approach in security and the ease with which this concept was rolled out across Sophos products was impressive. "With Sophos

Security Heartbeat™ we can ensure only the cleanest traffic moves from our HO LAN to Server farms because the endpoint knows exactly what applications are running and this data is shared with the XG Firewall," explains Mr. Bansal. "With Synchronized Security, we know our next-gen endpoint security and firewall protection are talking to one another, sharing threat updates, and talking to one another to deliver the best protection possible. Sophos has definitely added another feather in the cap with Synchronized Security and its truly a revolution in threat protection," affirms Mr. Bansal.

How did deployment results wow AAVAS?

Mr. Bansal and his team were especially confident they had made the right decision to trust Sophos to protect their business. Right from the word go it was incredibly clear that Sophos was improving business continuity, employee productivity and keeping AAVAS secure from the evolving threat landscape. "Cyber attacks have wreaked havoc on some of the world's largest financial services organizations. These threats continue to increase in scale and complexity at an alarming rate. With Sophos, we are confident of addressing these security challenges," states Mr. Bansal. "Sophos has brought an immense range of benefits to the table, that spans business continuity, employee productivity, and security. After deploying XG Firewall v17, we have experienced a marked reduction in the downtime of IT infrastructure across multiple locations, resulting in significant time and cost savings. The enhanced web filtering offering on XG Firewall and Synchronized App Control have not only given us more control of the apps being used on our network, but also resulted in maintaining and achieving productivity targets of our employees."

Post Sophos deployment, Mr. Bansal and his team have breathed a sigh of collective relief because fewer people are calling IT to sort out a security issue. Sophos XG Firewall v17 offers better networking and VPN with IKEv2 Support, VPN UI Enhancements, Wildcard Support for Domain Name Host Objects and NAT Rule Enhancements. This has enabled Mr. Bansal to extend network with secure communication and also extend network with protection for branch offices. These features have made sure that irrespective of where the employees access corporate resources from, the data is safe and the traffic remains private.

"It's not only XG Firewall that impresses us. We are happy with the performance of Sophos Central Endpoint Advanced with its signature-less approach to malware detection. One of its key features that has benefitted us immensely is web filtering which can be enforced off the network as well. This has enabled us to deny access to unproductive web resources, which has dramatically brought down our internet bill," declares Mr. Bansal. "When we deployed Sophos, we expected it to deliver tangible ROI after 3 years. But, the Sophos solutions have been so successful that the deployment started delivering ROI straightaway. AAVAS started experiencing better employee productivity almost immediately and at the same time the exposure to sensitive data was kept to an absolute minimum."

Sophos' focus on ease of use was of great benefit to the IT team. "The ease of keeping threats at bay and automated incident response courtesy Synchronized Security helped the IT team maintain SLAs," asserts Mr. Bansal.

AAVAS also singled out SophosLabs for praise and the work it does to process millions of suspicious emails, URLs, files, and other data points at light speed to deliver comprehensive threat and malware analysis. "All Sophos solutions are backed by the excellent work done by SophosLabs providing 24x7 security research and analysis. This gave us confidence in the ability of Sophos products to quickly respond to threats targeting our ever-expanding IT infrastructure. All the Sophos products have delivered on the confidence reposed in them," concludes Mr. Bansal.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2018-05-02 NA (NP)

SOPHOS