Largest Lead Producer in India Leverages Sophos Synchronized Security to Strengthen IT Security Framework

Established in 1992, Gravita India Ltd. based in Jaipur, India, is one of the largest lead producers in the country. It has more than 500 professionals driving its transformation efforts with a single-minded focus on lead and lead products to improve productivity and efficiency through an environmentally-friendly process. Rapid growth of the company has put the spotlight on not only strengthening its manufacturing ecosystem but also bolstering its IT defenses. While next-gen firewall and endpoint security were definitely on its radar, Gravita wanted security solutions that did not exist in silos but were able to share critical security intelligence with each other. Sophos'synchronized security, where different Sophos solutions talk to one another to deliver actionable information was the perfect fit.

CUSTOMER-AT-A-GLANCE

GRAVITA

Gravita India Limited

Industry
Manufacturing

Sophos Solutions
Sophos XG Firewall (multiple)
Sophos APX Access Points
Sophos Central Intercept X Advanced
Sophos Central Intercept X Advanced for Server

"Silofication of security was our greatest worry. We were always concerned about the security of our IT ecosystem but were relying on point products that were working individually without synergy and increasingly getting difficult to manage. We decided that we had to move from a legacy security ecosystem to a more efficiently managed security approach, underpinned by advanced security solutions that talked to each other."

Prakash Saini, Deputy Manager, ITG

Challenges

- Multiple layers of security delivered by different vendors meant multiple management consoles that did not offer unified visibility into the diverse security deployments.
- Amount of time required to manage the numerous firewall installations and other security solutions was excessive due to lack of centralized management.
- Legacy endpoint meant there was a danger of advanced threats falling through the security gaps, resulting in data breaches.
- Existing security approach was unable to prevent ransomware attacks, and there was a need to focus on a security paradigm that addressed such advanced malware attacks

What were the factors that drove your efforts towards overhauling existing security framework?

"Right from the get-go, we were aware of the need for taking necessary steps to bolster our IT security framework. We went for point products from vendors specializing in specific aspects of the security landscape but started encountering problems from a management perspective and found that these products were not built to scale and couldn't address evolving security needs," says Mr Prakash Saini, Deputy Manager, ITG.

The biggest problem was the inability to get a comprehensive view of the various security implementations and the various IT assets and their security status. The IT team had to work with different management consoles to push security policies across the spectrum of security solutions and spent a lot of time to get insights into security incidents, risky user behavior, malicious traffic and the overall state of compliance.

Another concern was the lack of conjunction between endpoint and firewall security wherein they were working in silos. While they were addressing threats, they were not delivering comprehensive protection reinforced by intelligent security where threat identification at the endpoint level, could result in the firewall taking immediate measures to stop the threat at the network level, and vice versa.

Coupled with an endpoint security solution that lacked next-gen features, and the Gravita IT team had to work with a security ecosystem with limited capabilities. The danger of ransomware attacks exploiting vulnerabilities was always on the horizon and Gravita believed if it did not sort out its defenses, it would soon be of the victim of a ransomware attack. Gavita's also needed a secure wireless setup that could deliver focused visibility into threats, allow accelerated remedial action and offer clear and consistent visibility via a central platform.

How did you zero in on the security ecosystem of choice and how has it addressed the key security needs and challenges?

"The two primary requirements we had were advanced capabilities of our security solution and both the endpoint and firewall should be able to share security intelligence with one another in real time, to help us build a strong security foundation," explains Mr Saini.

He felt Sophos had the security solutions that addressed Gravita's requirements perfectly and was one of the few vendors that had powerful products for both network and endpoint. Sophos solutions not only had the advanced capabilities needed to prevent evolving attacks, but these solutions interconnect through Security Heartbeat™; and all Sophos products could be easily managed through the Sophos Central management console, which was a key point in Sophos's favor.

The superior visibility into suspicious traffic, risky activity and advanced threats provided by Sophos Firewall helps the IT team keep Gravita networks as secure as possible. With next-gen protection technologies like deep learning and intrusion prevention, Gravita is safe from even unknown threats. Additionally, automatic threat response facilitates instant threat identification and isolation of compromised systems on the Gravita network to stop threats from spreading laterally.

By delivering industry-leading performance, visibility, policy tools and built-in intelligence, the many blind spots in Gravita's network security framework have been removed and the IT team benefits from unmatched visibility and error handling. Sophos APX Access Points help Gravita leverage the benefits of cloud-managed Wi-Fi, enabling access control for managed clients and instantly identify threats on Wi-Fi networks.

Sophos Intercept X protects Gravita endpoints with next-gen capabilities including ransomware file protection, automatic file recovery and behavioral analysis to stop ransomware and other sophisticatedattacks. Gravita can also take the advantage of deep AI capabilities built into Intercept X to detect both known and unknown malware without relying on signatures. Also, active adversary mitigation and exploit prevention offer comprehensive protection to stop threats before they become a problem.

Whether it is endpoints or server, Gravita is now confident that their IT environment is safe from sophisticated threats. The integration of all Sophos products and the benefit of one console to manage all Sophos deployments, bolstered with comprehensive reporting and insights, has made life easier for the Gravita IT team.

How has the security ROI from Sophos deployment strengthened the business?

Not only is Gravita more secure, it is also saving on manpower and cost, and has seen network performance improvements. Sophos Firewall has helped save 10 man-hours per week, since firewall administration is now centralized and can be done by a small IT team. The gain in network performance is over 18%, which is a huge gain compared to the previous solution. More importantly, synchronized security has automated many security incident management tasks, which has saved more than 20 man-hours per week that were used to check and analyse every system, after every alert. Gravita has also experienced 25-30 % cost benefit purely as an outcome of Sophos deployments.

“Considering the tangible benefits experienced through the deployment of Sophos, we recommend Sophos solutions to any organization that wants security returns from day one,” signs off Mr Saini.

Learn more about
Sophos Firewall today.
www.sophos.com/firewall

2022-08-15 CCS-EN (NP)