SOPHOS
Security made simple.

CUSTOMER CASE STUDY

Trio of Sophos Products Protects **Government Agency** Against Advanced Malware

Customer-at-a-Glance

Roads and Highways Department, Bangladesh

Industry
Government

Number of Staff
400

Website
http://rhd.portal.gov.bd/

Sophos Solutions
Central Endpoint Advanced (previously Sophos Cloud Endpoint)

Central Endpoint Intercept X

XG 430 FullGuard

Sophos Customer
Since 2015

'As the head of IT security, I was very clear in my mind that I did not want to deploy end user protection and network security from different vendors. I was looking for a single security vendor who had the expertise to deliver next-gen endpoint protection and network security. Sophos met these needs perfectly.'

Kazi Sayeda Momtaz
Senior System Analyst
Roads and Highways Department

'The threat landscape is getting increasingly complicated and made worse by the infusion of point products that don't talk to each other. With Sophos and its unique Synchronized Security, endpoint protection is talking to the firewall and vice versa to work as an integrated security system automating incident response and offering better and more cohesive security.'

Kazi Sayeda Momtaz
Senior System Analyst
Roads and Highways Department

Business Challenge

- Prevent disruption of regular operations and organization processes as well as reduce threat to employee productivity
- Secure the organization from advanced malware threats and ransomware attacks, which could result in extensive financial losses to the government
- Ensure the highest level of security to the agency's network perimeter and enduser devices to guard against rapidly evolving cyber threats
- Provide a comprehensive yet simple security deployment that was easy to manage

The Roads and Highways Department (RHD) is a government department responsible for the construction and maintenance of highways and bridges in Bangladesh, as well as major road and bridge networks of the country. It prides itself on the level of accountability it brings to its activities. Its head office is in Dhaka, Bangladesh.

Since its inception, RHD's activities have led to the creation of massive amounts of critical data that enables them to streamline their activities, optimize resources, and overall deliver the kind of services that go a long way to help create the road and highway infrastructure that drives the economic growth of the country. The sensitivity of the data and the fact that this data is constantly growing in volume means RHD needs to put in place advanced IT security measures on the network and endpoint to defend against advanced malware and other cyber threats.

One of RHD's key security goals is that critical government data does not fall into the hands of rogue state or non-state actors. After conducting a thorough analysis and evaluation of the IT security vendors on the market, RHD had no doubts that Sophos' strong portfolio of powerful security solutions was best placed to cater to their cybersecurity needs.

Ms. Kazi Sayeda Momtaz, is the senior system analyst at RHD. She and her team are in charge of making sure that RHD's network perimeter and endpoints are secure against cyber attackers who want to get their hands on sensitive information that can be used to disrupt key infrastructure projects. Her primary goal was to strengthen the organization's cyber attack readiness, especially against advanced malware attacks like ransomware. Such attacks have the potential to disrupt business processes, hamper productivity, destroy the agency's reputation, and lead to financial losses. Considering RHD is a government organization, Ms. Kazi wanted to categorically ensure a robust IT security infrastructure, empowered with next-gen security solutions that worked as a system, weren't needlessly complex, and were easy to manage.

"I did not want RHD to confront a scenario wherein the company experiences a ransomware attack and suffered from its catastrophic consequences. My job is to make sure that the organization's systems are operating as they should, securely and seamlessly. I was therefore looking for reliable security solutions that offer protection against the rapidly evolving threat landscape," explains Ms. Kazi.

Unfortunately, cyber attacks, especially those leveled at government agencies, are a sad reality in today's world. These attacks not only cause great harm to the reputation of the organization, but also impact the many projects that the agency is involved with.

"I was always concerned about newer and more complex attacks being able to get into our network and causing havoc in the system. We manage immense data volumes and must meet a range of internal compliance requirements that help keep our network perimeter and endpoint safe from targeted attacks. I and my team envisioned a comprehensive framework that integrated best-of-breed security solutions and offered real-time protection. Sophos, as a leader in both endpoint and network security was best placed to bring this vision to life," says Ms. Kazi.

What is the impact of malware and targeted attacks on a government agency like RHD?

The digitization of information and increasing numbers of threat vectors presents new challenges to securing data, especially when employees are accessing corporate resources from outside the network perimeter. This leaves government agencies like RHD vulnerable to malware and targeted attacks. When this happens, the result is disastrous and organizations are left picking up the pieces for a very long time. Such attacks result in highly sensitive information being compromised, paralyzation of essential services, and loss in productivity leading to escalating overhead costs.

"As a government organization, we need to remain extremely vigilant in protecting our data from malicious attacks and ensuring our vulnerabilities aren't exploited by cyber attackers. For this reason, it was imperative that we deployed security solutions that offered only the most advanced protection. Sophos offers the latest in anti-ransomware, anti-exploit, anti-malware, and APT protection across our devices and data," explains Ms. Kazi.

How did Sophos solutions help protect against evolving threats?

Ms. Kazi brings to her job her many years of expertise in IT security, and therefore was very clear that she wanted to deploy solutions that offer comprehensive security, work as a system, and are simple to use. She started looking for a security vendor that had a lineup of products that offered protection for RHD's networks and endpoints and which are easy to manage after initial deployment.

"Our overarching goal was to deploy products that have the necessary capability to address sophisticated and increasingly complex cyber threats, and at the same time have an inherent simplicity that allows my team to maximize their potential. We worked with the Sophos channel partner in the region, who had many successful implementations behind them, and are very happy they asked us to look at Sophos. Both my team and I were impressed with the ability displayed by Sophos products during the evaluation stage, and its large installed base gave us added confidence in the ability of the vendor to come good on our expectations," said Ms. Kazi.

After a thorough analysis of the IT security challenges faced by RHD, Ms. Kazi signed on for 400 user licenses of Sophos Central Endpoint Advanced, 400 user licenses of Sophos Intercept X, and 2 units of XG 430 with FullGuard subscription.

"While we evaluated plenty of security vendors on the market, we felt none of the vendors even came close to the kind of capabilities Sophos' products offered. Sophos' solutions are truly next-gen, innovative and perfectly aligned with emerging technology trends," asserts Ms. Kazi.

The IT team at RHD trusted Sophos' ability to deliver the next level of security to protect against the latest threats.

How did XG Firewall, Central Endpoint Advanced, and Intercept X benefit a government agency like RHD?

Sophos XG Firewall delivers comprehensive next-gen firewall protection to RHD and blocks unknown threats, automatically responds to incidents, and exposes hidden risks. For Ms. Kazi and her team, XG Firewall's advanced technology, including advanced threat protection, dual antivirus, web and app control, email protection, and full-featured web application firewall, offered the next level of protection against ransomware and other advanced threats they wanted.

"We were mightily impressed by XG Firewall's capability to identify the source of infection on our network and immediately limit access to other network resources in response. This made our life a whole lot easier as this automatic incident response saved us a lot of time and effort. We also knew that the unique Sophos Security Heartbeat™ was sharing the health status of endpoints and firewall to secure our organization from complex and coordinated threats," says Ms. Kazi.

The IT team also wanted more visibility into unknown apps, risky users, suspicious payloads, and much more. Not only did XG Firewall deliver on those requirements – it also made this information easy to consume with the help of rich on-box reporting.

"One of the biggest benefits of XG Firewall is that patented layer-8 identity control helps me and my team exercise user-level control over applications, bandwidth, and other network resources. This has enabled me to optimize bandwidth and ensure only the right people have access to key network resources," explains Ms. Kazi.

RHD primarily uses Windows systems and Sophos Central Endpoint Advanced made it simple to secure their systems against malware and advanced threats such as targeted attacks.

"With next-gen Endpoint Protection from Sophos, we can now detect malicious traffic with real-time threat intelligence from SophosLabs. This not only helps us prevent and detect threats but also remediate them with ease," says Ms. Kazi. Sophos Central Endpoint Advanced offers a slew of innovative features including anti-malware, Host Intrusion Prevention System (HIPS), and gave Ms. Kazi and her team granular web, application, device, and data control for enforcing comprehensive policy across endpoints. "Web filtering is enforced on the endpoint even when users are off the corporate network, which is of immense benefit. It enabled us to limit internet access of users or groups of users even when they were using their devices outside of the network. This level of control is important for a government organization like RHD," Ms. Kazi explains.

With Intercept X, RHD boosted its next-gen endpoint protection with the benefits of deep learning malware detection, anti-ransomware, exploit prevention, root cause analysis and Sophos Clean remediation.

"Intercept X protects RHD from advanced malware attacks like ransomware by detecting new and unseen malware files accurately and without signatures. CryptoGuard technology stops ransomware by identifying spontaneous malicious data encryption. The great part is that it works at the file system level and integrates seamlessly with Sophos Endpoint Protection giving RHD an additional layer of security on the endpoint," asserts Ms. Kazi.

How did the deployment of Sophos wow RHD?

RHD had tremendous expectations from the various Sophos products it deployed, and these delivered on the organization's expectations and then some more.

"With Synchronized Security, I know RHD's network and endpoint protection is working together to deliver better security against advanced threats and spends less time responding to incidents – and it handles them automatically. Before, we used to spend an immense amount of time responding to such incidents, which impacted our business continuity, and which in turn led to cost overruns in projects. This has stopped with the deployment of Sophos XG Firewall, Endpoint Protection and Intercept X," states Ms. Kazi.

Intercept X's ability to block all known ransomware also impressed the executives at RHD.

"The fact that it stops never-before-seen ransomware and boot-record attacks is of huge benefit to RHD. Data is one of our prized possessions and Sophos Intercept X ensures that no unauthorized user is able to access this data," says Ms. Kazi.

Overall the ability of Sophos deployments to offer next-gen security, simplicity of deployments, ease of management and their ancillary capabilities helped RHD save a lot of man hours, improve productivity, and control costs.

Learn more about the Sophos Partner Program

Visit www.sophos.com/partners

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

2018/05/18 CSNA (NP)

SOPHOS