



Automated Detection: How Sophos helped **MYDIN** manage 3,000 connected devices

Mydin Mohamed Holdings Bhd (MYDIN) is one of the largest retail and wholesale grocery chains in Malaysia. The company operates 73 outlets nationwide including a chain of premium stores called Sam's Groceria. Due to its widespread network and offices nationwide, maintaining a complex information technology architecture has been a challenge for MYDIN. As the company grew, it moved from a manual to a digital framework in 2002 when Malik Murad Ali, MYDIN's chief information officer, established its IT department. Malik's main goal was to centralize MYDIN's systems and management for a better information system. Currently backed by a team of 70 IT employees, MYDIN has centralized all servers and systems including finance, enterprise resource planning/supply chain, and risk management, and has also virtualized all its servers and desktops.

CUSTOMER-AT-A-GLANCE

MYDIN

Mydin Mohamed Holdings Bhd

Industry

Wholesale and retail

Website

www.mydin.com.my

Number of Users

10,000 employees nationwide

Sophos Solutions

Sophos Central Endpoint Advanced

Sophos Intercept X

Challenges

- High staff turnover causing time-consuming desktop updates
- Lack of visibility over all platforms and devices
- Constant security threats and concerns regarding customer database theft and ransomware
- Need for scalable system to match growing business

Is it possible to keep a tangled web of systems in check?

As part of MYDIN's IT maturity journey, one crucial component was to improve the organization's IT security posture. The company started with a different cybersecurity vendor before opting to work with Sophos more than seven years ago. At that time, MYDIN's high staff turnover, coupled with the difficulty of tracking and updating antivirus solutions on each desktop, meant a heavy backlog of work for the IT department. This led to security issues and the need for manual troubleshooting.

MYDIN found the previous Sophos next-generation endpoint security solution performed well, but the organization decided to improve its security posture even more. IT wanted its security to scale to keep one step ahead of the evolving threat landscape. As a result, the IT team explored options for a cloud-based cybersecurity partner. After a thorough search, MYDIN again chose Sophos.

Why are cloud security solutions better for large enterprises?

As its IT infrastructure became more complicated, one of the key challenges MYDIN's IT team faced was addressing the need for continuous monitoring and responding to advanced threats. Security analysts required the right endpoint visibility and insights to discover, investigate, and respond to threats and broader attacks across multiple endpoints.

Sophos Central Endpoint Advanced and Sophos Intercept X offered the perfect combination for MYDIN's need to protect its 3,000-plus devices. The comprehensive defense-in-depth approach to endpoint protection Intercept X provides integrated with deep learning to detect known and unknown malware without relying on signatures was perfect for the job.

"The quality and effectiveness of Sophos' solutions have made us a loyal customer for many years. Thanks to the presence of cloud, we now have a more up-to-date central system that automatically patches and updates when required. This makes our work easier and helps us monitor our network without worrying about missing any threats," said Malik.

The Sophos solution not only helps MYDIN save on costly individual licenses for each desktop, it also allows the team to troubleshoot faster than ever before. The reports provided by Sophos mean the team can make better decisions based on real-time data.

'The quality and effectiveness of Sophos' solutions have made us a loyal customer for many years. Thanks to the presence of cloud, we now have a more up-to-date central system that automatically patches and updates when required.'

Malik Murad Ali
Chief Information Officer
Mydin Mohamed Holdings Bhd



"We have more transparency over our networks and can scale quickly as the business requires," said Malik. "Being able to manage all updates centrally and on virtual desktops means we can perform patches on all devices simultaneously. Previously, this was a huge problem for us as we relied on employees to manually update their machines and many employees, however, ignored warnings and crucial update pop-ups."

Why is it important to have a seamless and quick solution?

With 10,000 employees nationwide, MYDIN finds it difficult to educate all its employees about the company's policies on cybersecurity threats such as malware and ransomware. As a result, it was susceptible to cyberthreats brought into its network via infected documents employees opened via email.

"In the first month after implementing Sophos Central Endpoint Advanced, there was a case where one of our servers detected ransomware. However, thanks to Intercept X's comprehensive defense-in-depth approach to endpoint protection, we detected and quarantined it immediately. We avoided a major catastrophe in minutes," Malik added.

MYDIN believes that machine learning and artificial intelligence (AI) will thwart cybersecurity threats more independently in the future. With the use of AI, suspicious files and malware can be detected and blocked before they take hold.

How can cloud and on-premise solutions bring the best of both worlds?

"Hybrid implementation such as Sophos Central Endpoint Advanced is a huge advantage for businesses. Not only do you get the power, speed, agility, and scale of the cloud, but also on-premise control. It works very well and I recommend businesses to consider it," concludes Malik.

'Our adoption of Sophos Central Endpoint Advanced is a blessing in terms of efficiency, productivity, and the amount of time saved when it comes to labor.'

Malik Murad Ali
Chief Information Officer
Mydin Mohamed Holdings Bhd

Start your free trial of Sophos Central today to get started with Synchronized Security.