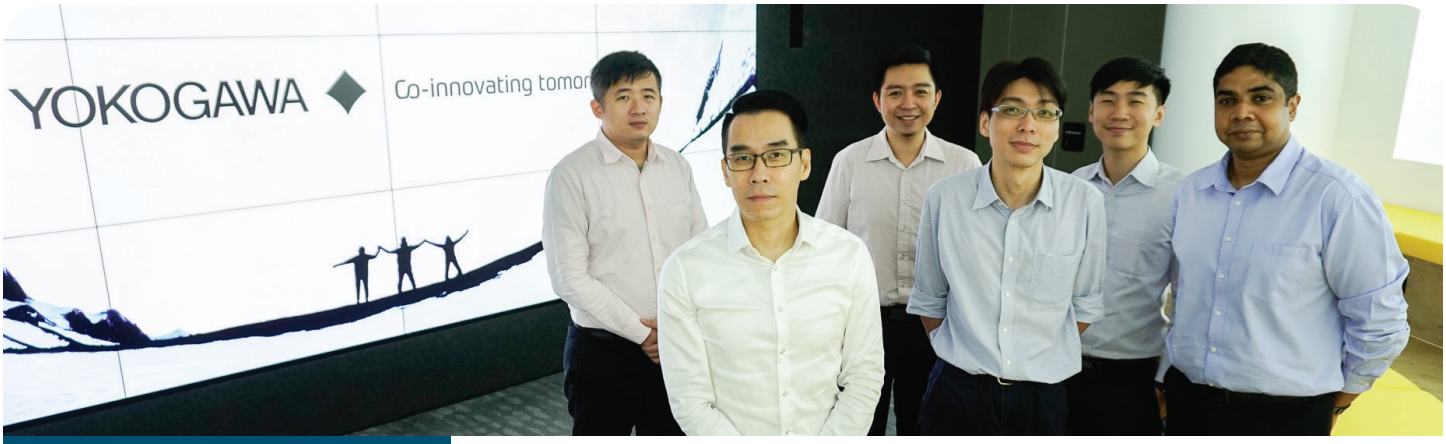
Staying One Step Ahead In Cybersecurity

While the WannaCry ransomware attack cost potentially billions of dollars to companies around the world, Yokogawa was shielded from it.

Yokogawa Engineering Asia is a leading provider of industrial automation, test & measurement, aviation and digital automation solutions. Given an increasingly challenging cybersecurity threat environment, Yokogawa sought to fortify its cybersecurity framework. To do this, the company implemented the Cisco Advanced Malware Protection (AMP) solution across the ASEAN, Oceania and Taiwan regions.



Yokogawa Engineering Asia

Industry:

Industrial Automation, Test & Measurement, Aviation, Digital Automation Technology

Location:

ASEAN, Oceania & Taiwan

Size:

2000+ employees

Website:

www.yokogawa.com/sg

Challenges

- Increasing sophistication of malware attacks and advanced persistent threats
- Lack of timely threat intelligence
- Maintaining security at the endpoints and on network devices
- Geographic diversity with thousands of users, each of which a potential entry point for cyberattack
- Need for a standardized approach to combating cybersecurity threats

Solution

- Cisco Advanced Malware Protection (AMP)

Results

- Improved visibility and control over endpoints and network security
- Consistent cybersecurity standards across the region
- Centralized management and monitoring – ‘a single view to the truth’
- Ability to pre-empt malware behavior
- Successful identification and mitigation of attacks including the WannaCry ransomware attack in 2017

Challenge: Implement a comprehensive cybersecurity framework to combat increasingly sophisticated attacks

The breadth of intellectual property at Yokogawa is very wide. The company, which has been in existence for more than a century, has a foothold in a range of industries – aviation, marine, oil, gas, chemicals, power, iron & steel, pulp & paper, pharmaceuticals and food. Yokogawa is at the forefront of innovation in these sectors.

The increasing sophistication of cyberattacks meant that Yokogawa had to take a hard look at its cybersecurity framework. "Our biggest asset is our reputation," Alvin Joseph, Senior IT Manager at Yokogawa Engineering Asia, said. "How effective we are in combating cyberattacks – that has a bearing on the confidence that our customers have in us."

Yokogawa's existing infrastructure across the ASEAN, Oceania and Taiwan regions provided basic protection at the endpoints – against virus attacks on emails and surfing. They were not designed to respond to more sophisticated attacks such as advanced malware and spoof emails. The company was yet to devise a strategy for sandboxing as well.

Key considerations in choosing a solution

Several key factors were considered in deciding upon a solution to confront the growing cybersecurity threats that Yokogawa faced:

- **Geographic diversity:** Yokogawa had more than 2000 employees spread out across nine countries in the ASEAN, Oceania and Taiwan regions. Cybersecurity standards and policies varied tremendously across these countries, hampering management and mitigation of cybersecurity risks.
- **Threats on multiple fronts:** Yokogawa needed a solution that could holistically address threats at various areas – at the endpoints, the network layer as well as at the firewall layer. Head of Infrastructure at Yokogawa Engineering Asia, Daniel Tan said: "Today, when an attack happens, it happens on multiple fronts simultaneously. Hackers are ingenious in their attempts, adopting diversionary tactics to make us focus on one area, while a more serious attack is launched on another front."
- **Ease of administration:** While the option of going with different 'best-of-breed solutions' was on the table, the company decided against it. Daniel explained: "That would have significantly added to our administrative overheads, meaning training and certifications by multiple vendors. But most importantly, it would also have slowed us down, and made us more inefficient, requiring us to monitor the environment through multiple user interfaces."

"Cisco AMP was able to give us insights into how the malware travels from one endpoint to another, allowing us to pre-empt and mitigate further damage. This was perhaps its biggest difference versus other solutions."

Daniel Tan
Head of Infrastructure at Yokogawa Engineering Asia

- **Ability to project malware trajectory:** The Cisco AMP solution that the company implemented was able to chart the entire life cycle of a malware. Daniel said: "Cisco AMP was able to give us insights into how the malware travels from one endpoint to another, allowing us to pre-empt and mitigate further damage. This was perhaps its biggest difference versus other solutions."
- **Cloud-based solution:** "Cisco AMP was the first cloud-based security platform we implemented," Alvin said. "Being a cloud-based solution brought many advantages – it was easier to deploy across the countries and elevate our level of cybersecurity to the same standard everywhere. Everything is done centrally from Singapore, and we didn't need to have expertise in each of those countries."

Proof of reliability

The proof of Cisco AMP's reliability came during the WannaCry ransomware attack that happened in May 2017. The damage from the attack, which affected around 200,000 computers across 150 countries, is estimated to be between hundreds of millions and billions of dollars to multiple companies worldwide.

However, Yokogawa managed to thwart the attack. As Cisco's Talos Intelligence Group was already on the lookout for suspicious patterns relating to WannaCry, it was able to spot it before it launched an attack on the user endpoints.

The Cisco Talos Intelligence Group is one of the world's largest commercial threat intelligence teams, consisting

"When an attack happens, it happens on multiple fronts simultaneously."

Daniel Tan
Head of Infrastructure at
Yokogawa Engineering Asia

"How effective we are in combating cyberattacks – that has a bearing on the confidence that our customers have in us."

Alvin Joseph
Senior IT Manager at
Yokogawa Engineering Asia

"We control all our endpoints across our regions, from one centralized location. A single view to the truth – that's the benefit of the cloud."

Alvin Joseph
Senior IT Manager at
Yokogawa Engineering Asia

of world-class researchers, analysts and engineers. They use sophisticated systems and telemetry to create accurate and actionable threat intelligence for Cisco customers, products and services. Talos defends Cisco customers against known and emerging threats, discovers new vulnerabilities in common software and interdicts threats before they can do harm.

"While many companies were affected by WannaCry, we were successfully shielded by Cisco AMP," Daniel added. "The WannaCry attack happened during the night, on a weekend. We heard it on the news in the morning. Our first instinct was to rush to the office. However, because Cisco AMP is a cloud-based system, we were able to remotely monitor that it had successfully obstructed the attack."

"In the last few years, we have really fortified ourselves," Alvin said. "And now we control all our endpoints across our regions, from one centralized location. A single view to the truth – that's the benefit of the cloud."

Daniel added: "When it comes to cybersecurity, there's really no substitute for eternal vigilance. Cisco AMP has solidified all our endpoints."