

Globe Telecom Simplifies Endpoint Security

**Profile:**

Globe Telecom, or Globe, is a major provider of telecommunications services in the Philippines. Operating one of the largest mobile, fixed-line, and broadband networks in the country, it has about 65.8 million mobile, 3.5 million broadband, and 859,000 landline subscribers.

Location:

Headquartered at Bonifacio Globe City, Taguig, Metro Manila, Philippines

Industry:

Telecom

Website:

www.globe.com.ph

Solutions:

- Ivanti Endpoint Security

Benefits:

- Centralized patch management and application control to 10,000 workstations
- Efficiency in patching critical zero-day vulnerabilities
- Ransomware containment
- Automatic deployment of other security solutions such as NAC agents, AV, and anti-APT agents to all workstations

The Search for Centrally Managed IT Security

Globe Telecom is a national telco company with over 7,000 employees spread across multiple offices in the Philippines. It needed to centrally manage automated IT security capabilities, which includes patching, application control, and asset management.

Without centralized management, the IT team faced many challenges. For example, when new work tools were assigned to all the company's users, there was no mechanism to properly account for and tag each asset, no visibility into complete inventory, no proper tracking, and most important, no way to ensure that each workstation was properly patched and applications were blocked from running.

Globe's team used data from Ivanti to build their own asset tracking for better security management.

The Right Solution

As an interim fix, the telco's IT team deployed Microsoft System Center Configuration Manager (SCCM). Ultimately though, Globe needed a permanent solution—one that could be deployed across all systems and provide visibility into all assets from a central location.

To find the right solution, the telco conducted extensive research into the endpoint security products space. They finally settled on Ivanti® Endpoint Security, which provides fast, effective, and scalable protection from sophisticated malware and targeted attacks. It allows organizations to quickly identify and patch vulnerable workstations and servers, and helps prevent unauthorized applications from executing (and the unauthorized use of removable devices and ports).

“The final deciding factor was actually the proof of concept I conducted for each solution,” said Jake Kashina-milunda, head of Information Security Assurance & Compliance, Globe Telecom. “Ivanti’s solution came up on top in delivering my primary requirements, which were ease of use, ease of deployment, and cost efficiency.”

Deployment of the Ivanti Solution

With Ivanti Endpoint Security, the telco team set out to provide defense-in-depth protection for targeted threats, combining operational and security capabilities to effectively reduce the attackable surface area. The product enabled them to cater to robust centralized patch management, application control, and device control.

With Altair as Expert Solution Provider, Globe Telecom deployed Ivanti Endpoint Security across 10,000 nodes—desktops, laptops, and servers—across six major corporate sites, three data centers, and several hundred regional offices.

Better Overall Security

With the implementation of Ivanti Endpoint Security, the overall security posture of Globe Telecom’s corporate environment has improved dramatically.

“We have seen an exponential increase in overall workstation patch compliance over the past two years,” Kashina-milunda said. “In addition to providing centralized patch management and application control, Ivanti Endpoint Security helped us contain ransomware and deploy other security solutions such as NAC agents, AV, and anti-APT agents to all workstations with minimal need for manual or onsite intervention.”

Another key benefit of the deployment was efficiency in patching critical zero-day vulnerabilities.

To combat WannaCry during the outbreak, anti-WannaCry scripts and detection tools were deployed. Kashina-milunda’s team created custom patch jobs to perform very specific, tactical tasks such as:

- detection and modification of registry keys to disable SMBv1 and enable/update SMBv2,
- trigger immediate forced reboots to update registries of all vulnerable workstations,

- deploy special files to prevent and negate the execution of the ransomware on an infected workstation,
- deploy McAfee and update the McAfee AV to catch the ransomware entering the environment, and
- force patching of all outdated workstations.

“We had ZERO ransomware executions despite several hundred infections,” Kashina-milunda said.

With Ivanti Endpoint Security, Globe’s IT team was also able to define and enforce trusted application usage through whitelist policies to ensure only applications explicitly authorized or trusted can execute.

“We used application control to block certain applications from running, such as torrents, internet downloaders, and games. We are currently working with the IT team to fully implement application whitelisting across the enterprise,” Kashina-milunda said.

Globe was able to solve its discovery and inventory control issues with Ivanti Endpoint Security’s enhanced asset discovery and agent deployment functionality. IT can scan the environment for endpoints to gain visibility of managed and unmanaged systems and deploy agents to unmanaged systems automatically or on a scheduled basis.

Better Customer Service

Beyond a winning feature set, Ivanti provided the level of service Globe sought. “One of the more important deciding factors for me when choosing a solution is not the brand name nor the positioning of the solution on some ‘magic quadrant,’ but more the quality of support and ease of delivery,” Kashina-milunda added. “Altair and Ivanti have worked hand-in-hand to ensure my team and I get the most relevant and efficient support when needed, and the ease of commercial fulfilment when it counts.”

Learn More



[ivanti.com/contact](https://www.ivanti.com/contact)



epg@ivanti.com