

GSIS Simplifies Security Monitoring to Stay Resilient During the Pandemic

Key Challenges

Running several security tools simultaneously to keep the organization secure was a big challenge for a small team at GSIS — especially when the pandemic required an immediate shift to remote work.

Key Results

GSIS's security operations team of four effectively manages around 20 security systems with centralized visibility into the whole company's security posture while maintaining successful operations in the mandatory teleworking mode.



Maaasahan ng Lingkod-Bayan

Industry: Public Sector

Solutions: Security, Platform

Managing distributed security systems can be complex for any team — especially a small one.

Government Service Insurance System (GSIS) is a corporation run by the Philippine government that offers social security, insurance and financial benefits such as pension funds, retirement schemes and loans to 3 million active and retired government personnel and their dependents. With a very small staff, GSIS broke down technological silos and integrated security resources from end to end — all while carrying out new initiatives like a security orchestration, automation and response project.

“To address information security, cybersecurity and data protection simultaneously, we need to deploy more than 20 independent security solutions managed by a staff of only four SOC personnel,” says Jonathan Pineda, vice president, chief information security officer and data protection officer at GSIS. He wondered, “Instead of overseeing the systems individually, could we monitor everything on a unified, intuitive platform with a one-shot view of the security status across the organization?”

The answer was yes, with the Splunk Data-to-Everything Platform.

Organizational Security at One Glance

No longer toggling between more than 20 different security applications, the GSIS security team can now monitor them all through a single, central Splunk dashboard.

“After integrating all security tools and data sources into the Splunk platform, we can analyze data across the whole organization in one shot,” says Pineda. “We now get real-time, actionable insights into the health status of every tool and the security posture of all operations, digging out the root cause of every problem in no time. Managing and monitoring information security with

Data-Driven Outcomes

20+

systems easily and effectively monitored by a limited staff

Full-stack

visibility and security for teleworkers during the coronavirus lockdown

Extended

use from security to IT monitoring and actively exploring other use cases for the business

a small team is made possible and easier with the right tools such as Splunk. Splunk shields the integration complexity and delivers full-stack visibility into all critical applications in a single pane of glass.”

Splunk not only offers end-to-end visibility, but also enables GSIS to implement a data security strategy that provides government employees with their benefits securely.

“With Splunk, we uncover the power of analytics, which allows us to turn data into timely decisions and smart actions to minimize risks and prevent threats. For instance, we can proactively notify users of phishing emails in real time, ensuring adherence to security standards,” Pineda adds.

Monitoring From Anywhere

With COVID-19 impacting so many aspects of life, the national government of the Philippines encourages local companies to implement flexible work arrangements and keep the economy alive. “But while everybody is working from home, we need to ensure that we can still monitor our applications and processes wherever we are,” says Pineda.

Thanks to the Splunk Mobile app, the team can monitor all systems around the clock through a virtual private network. With the remote application, this can be done as easily at home as it would be in the office. “Right now, we are using Splunk as our single source of truth for all our security tools, making sure the company is safe from attacks and remaining flexible in the new normal,” Pineda says.

Going Beyond Security for a Smarter Business

While it initially used Splunk solely for security, GSIS plans to maximize the platform’s full potential by bringing data to more questions across the business.

“Although we are currently using Splunk 95% for security, we also share it with the IT team for capacity monitoring,” says Pineda. And other departments across the business are following suit. The insurance team, for example, is exploring how to handle claims better and conduct essential processes with the Splunk dashboard. The operations team is also exploring how Splunk can help in monitoring member data so they can easily identify and correct mistakes that arise during data entry or data processing.

“Moving forward, we’re also looking into the possibility of automating security monitoring with Splunk,” says Pineda. “If we can have specific incidents automatically detected and sent to the appropriate team for further handling, it will simplify life for the small team while improving efficiency and productivity.” Pineda adds.

With the pandemic shaping the future, Splunk is also heralding a new paradigm in business analytics, one that helps GSIS keep up with changing market dynamics while maintaining organizational agility in the new normal.



Splunk lets us oversee everything at one stroke and keep the company safe from any attack, wherever we’re working and under any circumstances.”

Jonathan Pineda, Vice President, Chief Information Security Officer and Data Protection Officer, GSIS

[Download Splunk for free](#) or get started with the [free cloud trial](#). Whether cloud, on-premises, or for large or small teams, Splunk has a deployment model that will fit your needs.



Learn more: www.splunk.com/asksales

www.splunk.com