Forcepoint

Customer Story

This National Investigation Bureau Trusts Forcepoint to Protect Millions of Citizens—And Its Own Agents

While this national law enforcement agency delivers government identification to citizens and protects the country against high-profile crime, Forcepoint blocks 10,000 cyberattacks per day to make sure the required sensitive data stays secure.

This national investigation bureau's focus on solving high-profile crimes paints a target on the backs of its agents. At the same time, the agency provides a critical service to citizens in the form of government-issued identification that allows them to work, sign contracts, and more. Both require sensitive data that has to be protected—and is, by Forcepoint Next Generation Firewall (NGFW).

CUSTOMER PROFILE:
An agency of the Philippine government responsible for handling and solving major high-profile cases that are in the interest of the nation.

INDUSTRY:
Government

HQ COUNTRY:
Philippines

PRODUCT:
Forcepoint NGFW

This national investigation bureau is responsible for handling and solving major high-profile cases that are in the interest of the nation. The agency handles investigation and intelligence, and reports to the department of justice. Its agents investigate major crimes, including organized crime and drug syndicates. The agency stores sensitive personal data about the agents, such as their date and location of birth and other information that would make undercover agents identifiable. The agency has to fiercely protect this data since a breach would put agents' lives at risk.

In addition, the bureau manages a countrywide clearance process via 60-plus local branches across the country and the website. The clearance is a form of ID that job applicants are required to have by many companies in the country since it proves someone has no record of committing a serious crime or violation. It's equivalent to a background check and a government-issued ID in one, and the agency has amassed an enormous amount of personally identifiable information on millions of citizens that must be kept out of the hands of cybercriminals. To help secure both the process and the data, the agency looked for a cybersecurity vendor that could provide end-to-end encryption from local branches to servers at the head office. This encryption was also required by the country's privacy act, which is similar to Europe's GDPR.

A 'human-centric' strategy and an endorsement from the FBI make the difference

After evaluating multiple vendors in the RFP process, the bureau selected Forcepoint. The agency was swayed by Forcepoint's "human-centric" approach to cybersecurity, focusing on the interaction between humans and data wherever it occurs.

This convinced the bureau that Forcepoint was a forward-looking company that could be a strategic partner over time by providing an integrated set of solutions. Also influential in the agency's decision was the announcement that the United States Federal Bureau of Investigation had entered into a five-year partnership with Forcepoint for an estimated $23M.

The agency sees the value in and is excited about the potential of the entire Forcepoint platform, but budget limitations required a phased approach. Forcepoint and the agency ran proofs of concept (POCs) on both Forcepoint Next Generation Firewall (NGFW) and Data Loss Prevention (DLP), but in order to comply with the requirements of the country's privacy act, the agency decided to focus on implementing Forcepoint NGFW as phase one.

Forcepoint NGFW's ease of management of multiple firewalls via the Security Management Center impressed the agency. It decided to purchase 90 Forcepoint NGFWs to protect its perimeter, perform deep packet inspection of web traffic, and to encrypt communications via VPN between each of its branch offices and headquarters.

10,000
attacks prevented per day

$10,000
saved per day

Challenges

Protect sensitive personal data of agency agents.

Safeguard the national clearance process for citizens.

Approach

Rollout 90 Forcepoint NGFWs to protect the perimeter, perform deep packet inspection of web traffic, and encrypt communications via VPN between each branch office and HQ.

Preventing 10,000 attacks a day saves $10,000 a day

The results of the Forcepoint NGFW implementation have been stunning: the agency has seen 10,000 new attacks prevented every day due to the NGFW Intrusion Prevention System. Forcepoint NGFW offers the industry's most secure Intrusion Prevention System as rated by independent testers such as NSS Labs. Its dynamic stream-based inspection looks beyond simple packets in order to catch attacks that might slip through other firewalls. It reconstructs and examines the actual messages, defeating evasion techniques that camouflage exploits and malware. The bureau equates each attack prevented to one dollar, so the agency sees this as saving $10,000 per day, although truly the cost would be higher if a breach were successful.

A centralized view enables day-to-day security adjustments

The agency also utilizes the NGFW Security Management Center (SMC) to determine the source of an attack (internal or external), which attack vector is being utilized, what is being targeted, and the classification of malware. Forcepoint SMC gives the staff a holistic view of the network, including configuration, monitoring, logging, alerts, reports, updates, and upgrades. This enables a daily audit report that allows the agency to adjust its security posture on a day-to-day basis. The centralized visibility and control delivered by NGFW SMC provides value to two different groups at the agency: the Security Operations Center (SOC), which focuses on analyzing, containing, and remediating threats, and the Network Operations Center (NOC), which utilizes the metrics provided by SMC to optimize network performance.

Expanding the perimeter of the network to include the people using it

The partnership has been so successful the agency made a trip to Forcepoint's Cyber Experience Center in Boston to discuss how the bureau could next leverage Forcepoint's vision for the future of cybersecurity. The agency has requested a memorandum of agreement with Forcepoint, similar to one it has in place with the FBI, in order to share cybercriminal threat intelligence including techniques, tactics, procedures, and more, to make its strategies more effective.

The agency also re-iterated that the security Forcepoint provides is not just protecting data, but actually saving lives. To expand that protection, the agency wants to take the next step in human-centric cybersecurity by adding Forcepoint Dynamic Data Protection to automate DLP policy enforcement and Insider Threat to gather evidence of risky behavior in real-time.

The agency not only considers the perimeter to be the network but also its people, according to Gelo Castro, Forcepoint Sales Engineer. He explained that the agency's philosophy is "Trust no one and inspect all."

Results

- **Prevent** 10,000 attacks a day to save $10,000 a day.
- **Protecting** data and saving lives.

The agency has requested a memorandum of agreement with Forcepoint, similar to one it has in place with the FBI, in order to share cybercriminal threat intelligence including techniques, tactics, procedures, and more, to make its strategies more effective.