

Norbert Wiener University Embraces Layered Security from Hillstone Networks

The Customer

Founded in 1996, Norbert Wiener Private University is part of a family of prestigious educational institutions based in South America. Norbert Wiener University is the first in Peru and Latin America that obtained the ISO quality certification. Focused on the training of professionals at the service of society, Wiener University currently has an enrollment of more than 10,000 students, along with faculty in the health sciences, pharmacy and biochemistry, engineering, business, as well as law and political science.

The Challenge

Nowadays, sophisticated and targeted cyber-attacks are increasingly more prevalent and highly successful against traditional perimeter security systems. Attackers typically exploit known vulnerabilities in traditional, static network security solutions and manage to compromise networks and allow malware to hibernate in internal networks until high-value targets are detected on the servers. Once valuable data is detected, they can easily exploit the data, or encrypt it for ransom. In turn, ransomware is one of the biggest threats to date, and no organization is immune to it, but those without adequate visibility and insights into their network traffic are the most vulnerable. In non-commercial sectors such as universities, it is very common to have hundreds of thousands of attacks on its networks, and approximately thousands advanced attacks, which a traditional firewall is not equipped to detect.

“Norbert Wiener University have a significant number of users including students, administrative and guest user populations that connect or access the networks from various devices, often compromising the perimeter security, and generating breaches that could put critical information at risk. Often, it impacts business continuity, halting access to University web properties. Anticipating such probable scenarios, we look for solutions that would bring visibility into potential cyber attacks,” says Manuel Taboada, IT manager of Norbert Wiener University.

Norbert Wiener University Embraces Layered Security from Hillstone Networks

The Solution

Given the security risk to the University, the IT managers decided to apply the concept of "Layered Security" and "Security That Works!" from Hillstone. They deployed T series intelligent next generation firewalls (iNGFW) to protect the perimeter network, in conjunction with the Hillstone I-Series server breach detection system (sBDS) for intranet protection.

Both platforms, iNGFW and sBDS, are products that have imbedded with intelligence security features: advanced threat detection (ATD) and abnormal behavior detection (ABD). ATD engine leverages machine learning to recognize abnormal and potentially damaging network behavior, such as malware CnC callbacks; the ABD engine monitors the network over time to build normal network behavior profiles, then subsequently monitors for any behavior abnormalities. In addition, iNGFW and sBDS are integrated to achieve detection and prevention from the perimeter to the internal network. The solutions constantly scan the internal network for lateral movements, filter suspicious and unauthorized data, with an eye on network traffic between critical servers.

Together with visibility over user and network traffic and deep threat analysis, sBDS provides security administrators with the means to detect IOC (Indicators of Compromise) events. It provides forensic analysis of threat intelligence in conjunction with the T-Series, for timely threat mitigation and resolution.



additional resources, such as local ISPs, more quickly and without service interruption. For instance, IT managers can balance network traffic by application, the more critical apps will have greater priority.

"The migration to the Hillstone solution was much simpler than expected and the results after implementation have been outstanding. Any change, typically, implies the challenge of adoption and in-depth knowledge of new features, but the Hillstone solution has been very intuitive and easy to operate, making the work of our operators easier," commented Manuel Taboada, IT manager at the University, "Hillstone has a centralized control system and also provides a granular view of our security posture, detecting advanced threats with real-time defenses."

The Conclusion

The Hillstone solution, iNGFW in conjunction with sBDS, has helped the University not only protect its critical network assets but has also helped it fulfill its service level commitments to students and staff.

In addition, the University has seen a return on investment in less than a year: A critical attack was detected by the Hillstone solution, which would have caused an enormous breach in internal services, as well as compromised data. "We are really very happy and above all else, peace of mind," concludes Manuel Taboada.