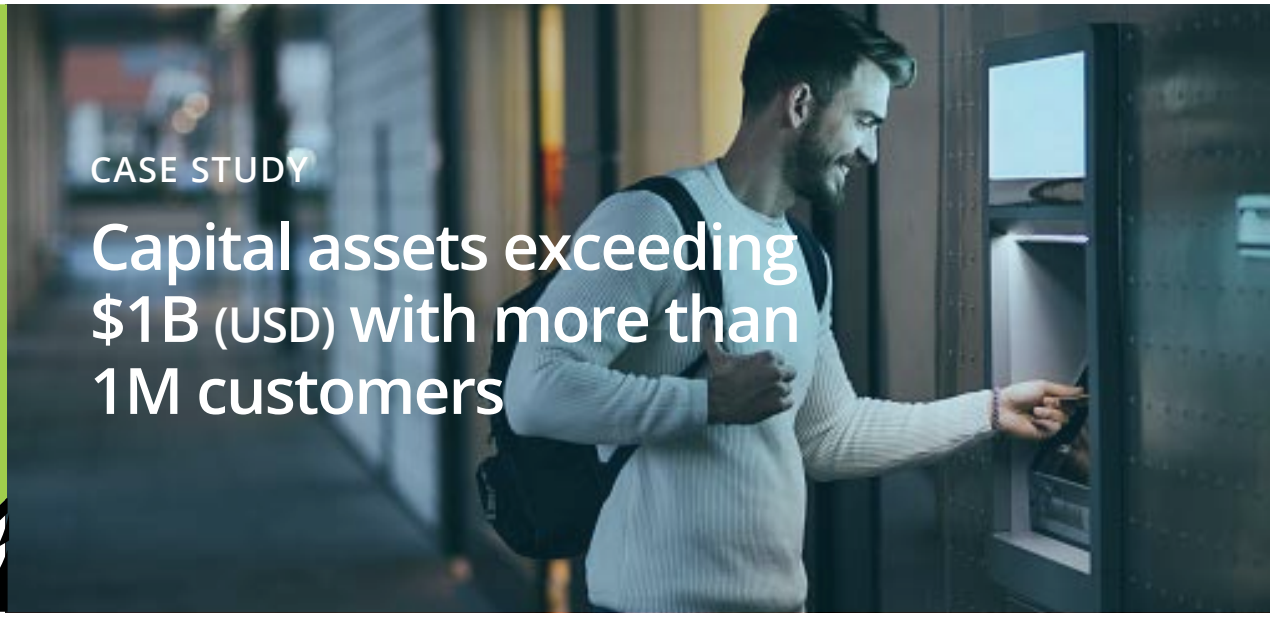
RIDGE SECURITY



CASE STUDY

Capital assets exceeding $1B (USD) with more than 1M customers

A commercial bank serving the ASEAN countries, with capital assets over $1B in USD and over one million clients had an IT infrastructure consisting of mainly Window® Servers in a virtualized environment, hosting several external websites that they secured with an Intrusion Prevention Solution (IPS) and firewalls in High Availability (HA) mode. As with all organizations in the financial sector, the Bank must comply with specific regulations: PCI DSS, ISO 270001. The Bank's current security team is small but mighty, consisting of five administrators, organized as such: one individual on a red team, two on a blue team, and the remaining two admins handling general issues.

Challenge

The Bank's security strategy included running quarterly pen-testing, primarily since they were under-resourced, and pen-testing can typically be a cumbersome, manual task.

Their IT infrastructure included Windows® 2008 Servers, as well as other outdated systems and therefore was increasingly vulnerable to external threats. The fact that one ransomware attack had already targeted them prompted the IT team to seek a testing platform that provided continuous testing, risk-based vulnerability findings and ransomware simulation to augment their existing infrastructure solution, as they built out and implemented a more robust security strategy.

Request a demonstration of RidgeBot today!
ridgesecurity.ai/demo

We are truly impressed by the simplicity and efficacy of RidgeBot. We didn't realize that pen-testing can be done so efficiently—automatically detecting vulnerabilities in our system and helping us maintain regulatory compliance through effective risk management.

—CISO of the Bank

Solution

The IT Team at the Bank deployed RidgeBot from Ridge Security and created the "Attack VLAN" to reach the test targets—internal servers and external websites—mainly using three predefined scenarios available in RidgeBot: Full penetration, Web Penetration and Ransomware Prevention.

Results

RidgeBot discovered several validated vulnerabilities through the tests, allowing the IT Team to witness RidgeBot exploiting the dated Windows® 7 Eternal Blue vulnerabilities exploited in front of their eyes. Eternal Blue was responsible for enabling the notorious ransomware attack, WannaCry, in 2017. Their Blue team followed RidgeBot's recommendation to quickly remediate the risks; after which they were able to export the data to feed into PCI DSS compliance requirements.

RidgeBots are intelligent, enterprise-class, automated, penetration-testing robots

RidgeBot helped save time and resources for the Bank, allowing them to spend less time on tedious, but critical tasks. The IT Team was particularly impressed with the AI Engine (the intensive threat intelligence that RidgeBot has built into its database), RidgeBot's ability to automatically draw "attack topology," and its advanced post-exploitation techniques.

Among multiple competing vendors, the Bank selected RidgeBot as their pen-testing solution of choice. As part of the testing, they look for additional security defense systems to deploy, such as APT Sandbox, patch management, and SIEM to strengthen their overall cybersecurity posture.

RidgeBot Benefits

- Automated, user-friendly tasks
- Fast learning curve and ramp-up on solution
- No need for specialists or expertise