NEXUSGUARD

A Leading Hong Kong Bank Goes With Nexusguard To Stymie Hacker Attacks And Secure Its Key Online Services

Nexusguard's vast experience meeting the industry's strict security and privacy compliance requirements seals the deal.

A sophisticated DDoS attack leads to ransom demands.

Shortly after a top Hong Kong financial services company fell victim to a well-coordinated cyber attack, the real threat was revealed: blackmail. To stop the attacks, the hackers ordered the bank to pay a ransom within 24 hours or risk having their online services taken down again and again. The extortionists threatened to increase the ransom demands every hour until the bank paid up. And although the bank had DDoS protection provided by its ISP, it wasn't able to handle such a sophisticated attack.

The mission? To keep online banking up and running without interruption.

Of its three online platforms — banking, trading, and corporate — the hackers threatened to attack the company's most essential service: online banking. It was critical to ensure 100 percent reliability and uptime. Having lost confidence in their existing ISP's built-in DDoS protection, the bank reached out to specialized anti-DDoS firms, and began to evaluate the offerings of a number of cloud-based DDoS mitigation providers.

Compliance was the key to selecting the right provider.

When it comes to cyber security, financial institutions are required to comply with much more stringent standards than companies in other industries. Nexusguard was expressly selected for its deep experience and understanding of the stricter privacy and security protocols demanded of governmental and financial institutions. Nexusguard's PCI DSS (Payment Card Industry Data Security Standards) compliance, along with its ISO 27001:2013 certification, assured the bank that its data and sensitive information would be handled with industrial-grade security and privacy.

Why PCI compliance?

PCI compliance gives the bank ample confidence to upload their SSL private key and certificate to Nexusguard's secure scrubbing network without any worries. As soon as Nexusguard's emergency security provisioning was implemented, the bank's traffic — including HTTPS — was routed over to Nexusguard's mitigation platform. The blackmailer's extortion attempts came to a halt as their attacks failed to impact any of the bank's online services or customers.

A comprehensive and customizable solution.

Nexusguard's DDoS solution is designed to monitor and scrub traffic — even SSL-encrypted traffic — in network Layers 3, 4, and 7. In addition, since the online banking platform is comprised of many different applications (i.e. e-statement services, transfers) that were unique in terms of their coding and structure, Nexusguard made sure to tailor the protection specific to each of these applications. The network protection solution that the bank adopted protects the online network at both the front end and back end. This protection, combined with customized application support, ensures that the bank and its customers will not be affected by future malicious attacks, either application- or volumetric-based.

Maximum uptime for online banking — and much more.

Beyond critical uptime for its online banking services, Nexusguard provides the bank with cybersecurity measures that comply with the industry's most widely recognized security standards. Due to the frictionless implementation of the solution and its keen focus on compliance and data sovereignty, the bank's board is considering moving all of its existing protection solutions onto Nexusguard's world-class security platform.