CASE STUDY | **FINANCIAL**

CRYPTONITE NXT

...credit card fraud losses topped $24.71 billion in 2016, a 12% increase over 2015. At this rate, losses are expected to exceed $31.67 billion in 2020.[1]

The Challenge

Credit card processors, similar to credit bureaus, have incredibly valuable databases and face an increasing onslaught of cyberattacks each year. These attacks impact not only the credit card processors, but the banks and the retail point of sale (POS) systems that tie to their networks.

Stolen records brought to the dark web daily include credit card magnetic-stripe account data, which is often accompanied by the CVV verification numbers. This credit card data fuels a multi-billion dollar business globally. The cyber threat to credit card processors is formidable, causing increased losses every year. It is estimated that credit card fraud losses topped $24.71 billion in 2016, a 12% increase[1] over 2015. At this rate, losses are expected to exceed $31.67 billion in 2020.The deployment of the EMV chip card standard, while beneficial in offline environments, has accelerated criminal activity online. In 2016 fraudulent card-not-present online transactions increased 40% in 2016.

Our Case Study

Our case study focuses on the selection and installation of CryptoniteNXT Moving Target Cyber Defense (MTD) and network micro-segmentation in a leading credit card processing company. Their team is highly secretive about the tactics, techniques, and procedures they use for cyber defense within the company. They currently have a strong existing investment in cybersecurity software and network security equipment, including endpoint protection, email gateways, secure web gateways, new technology for behavioral analytics, IPS/IDS equipment, and 2nd generation firewalls deployed in various locations. They have a strong security operations team - several of their team members have a deep knowledge of cybersecurity warfare operations

1 https://www.nilsonreport.com/upload/content_promo/The_Nilson_Report_10-17-2016.pdf

from recent experience working within classified government operations. They understand best practices for the deployment of classic defense-in-depth strategies to protect their enterprise-class network defense. They also understand that this is no longer good enough. Every quarter they evaluate new technologies and practice continuous threat hunting and red team activities to identify and correct any weaknesses in their networks.

The team leaders have seen both network penetrations and policy violations by internal users. In the high threat current environment, they were highly concerned that their current cybersecurity architecture would be breached and that they would be unable to detect the breach until significant harm had been done. They are also required to maintain compliance with PCI 3.1 and the pending 3.2 requirements.

Network segmentation was chosen as an important technology set for investigation. Initially, they wanted to reduce policy violations through enforcement by segmentation. They wanted to limit most internal network lateral movement and looked at various approaches to implementation. The CryptoniteNXT platform was selected, not only for the features and ease-of-use of our Micro Shield segmentation but also for the incremental capabilities offered within the same network appliance with our Net Guard MTD. The selection was also driven by our support for all of their existing switches and network components; none of these had to be replaced. Net Guard MTD offered them some very substantial advantages over the deployment of segmentation alone. MTD would enable their systems to stop cyberattackers at the start of the attack, effectively making the targets within the credit card processor's network invisible. By shutting down reconnaissance, the security operations team felt that the MTD combination with fine grained micro-segmentation offered strong advantages not available in any other network security appliance.

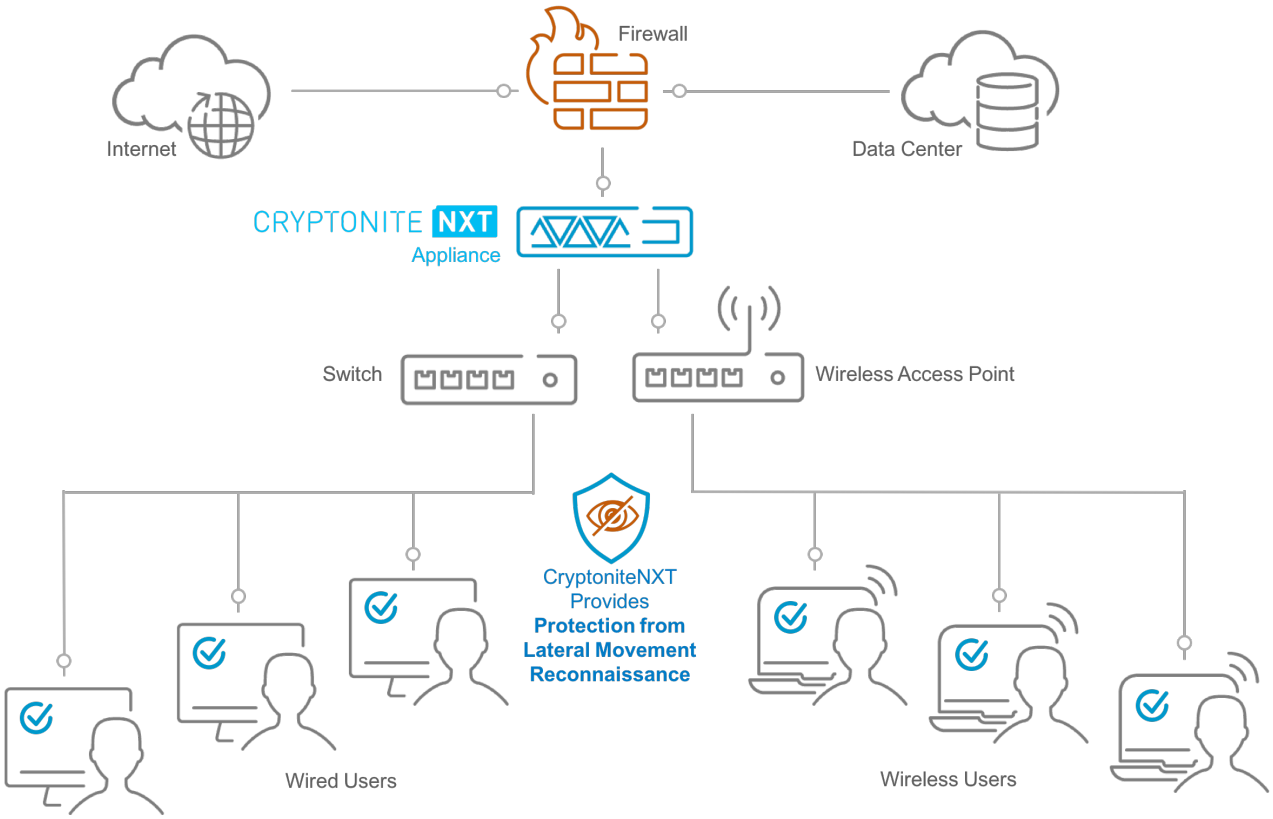
"CryptoniteNXT is agentless and at all times has been transparent to users. The users cannot tell they are in a highly protected and secure environment. There is no performance impact to the users or system operations and this is very important to us."

Security Operations Center Team Leader

The Results

The CryptoniteNXT appliances have successfully been in operation for months, protecting a very important network within the credit card processor's core operations. The team has validated the performance and protection offered by the system using their internal threat hunting teams.

They have also been positive about the automation and speed of containment. There are no alerts to resolve to action - CryptoniteNXT does that automatically. Attackers that seek to perform reconnaissance and enumerate the network are logged and alerted, and, most importantly, they are immediately stopped and shut down. Attacker or insider threat lateral movement outside of policy is logged and generates an alert, but in a similar fashion they are restricted and shut down. This automation is very important to the security operations team as they have been overloaded with many thousands of alerts which, in some cases, require investigation and manual remediation. They have acknowledged this speed of containment and remediation is key to preventing a future data breach. The deployment of the CryptoniteNXT network security appliances into all of their back-office operations is planned for 2018.



CryptoniteNXT Architecture

Prevent Reconnaissance and Stop Lateral Movement

Contain attackers and make their targets invisible. An attacker can't discover what they can't see, and likewise can't attack without a target. CryptoniteNXT eliminates an adversary's network visibility and reduces their attack surface, without sacrificing performance or transparency to your users.

About Cryptonite, LLC

Cryptonite is a leader in moving target cyber defense. CryptoniteNXT enables any network to actively shield itself from cyber-attacks by preventing all attacker reconnaissance and lateral movement. Patent pending moving target cyber defense and micro-segmentation technologies protect enterprise networks from an advanced cyber attacker, insider threats and ransomware. The Cryptonite customer base includes leading commercial and government customers around the world. Learn more at **www.cryptonitenxt.com.**