CASE STUDY | **DEFENSE CONTRACTOR**

CRYPTONITE NXT

**NIST SP 800-171 defines over 110 security requirements relating to network auditing and accountability, policies and procedures, and implementation of best practices.**

## The Challenge

Cyber attacks on the aerospace and defense industries have continued unabated the past few years. The aerospace and defense industries face cyberattacks from nation states and their complicit partners in organized crime. Targets include intellectual property on defensive capabilities, military infrastructure and other available intelligence. Threat actors actively seek the ability to infiltrate, monitor and then critically compromise key military and intelligence assets.

DoD mandated that defense contractors conform to the **National Institute of Standards and Technology in Special Publication 800-171 (NIST SP 800-171)** with a deadline for implementation mandated for **December 31, 2017**. NIST SP 800-171 defines over 110 security requirements relating to network auditing and accountability, policies and procedures, and implementation of best practices. Defense contractors that must meet these requirements will need to review and update their cyber defense systems and policies. The requirements of NIST SP 800-171 places additional pressure upon defense contractors to bring in new technologies and to align best practices to defeat persistent attackers that have penetrated their networks.

## Our Case Study

Our case study focuses on the selection and installation of CryptoniteNXT Moving Target Cyber Defense (MTD) and network segmentation by a leading defense contractor and important government "Think Tank." This contractor provides vital consulting and development services to government agencies and other defense contractors. They provide technology innovation, research and development in a variety of areas to include signal processing, cybersecurity, big data, defense systems analysis, healthcare, aerospace, and other key defense technologies.

**"Moving Target Cyber Defense (MTD) is a key technology that will enable our security operations team to shut down the start of an attack by effectively making targeted systems and servers invisible. By denying reconnaissance and highly restricting lateral movement, CryptoniteNXT offers unique and highly advanced warfighting capabilities to meet and defeat the most advanced cyber threats."**

Cybersecurity Operations Program Manager

They manage contractual obligations to protect data associated with highly secure programs as well as an internal need to protect their intellectual property and trade secrets.

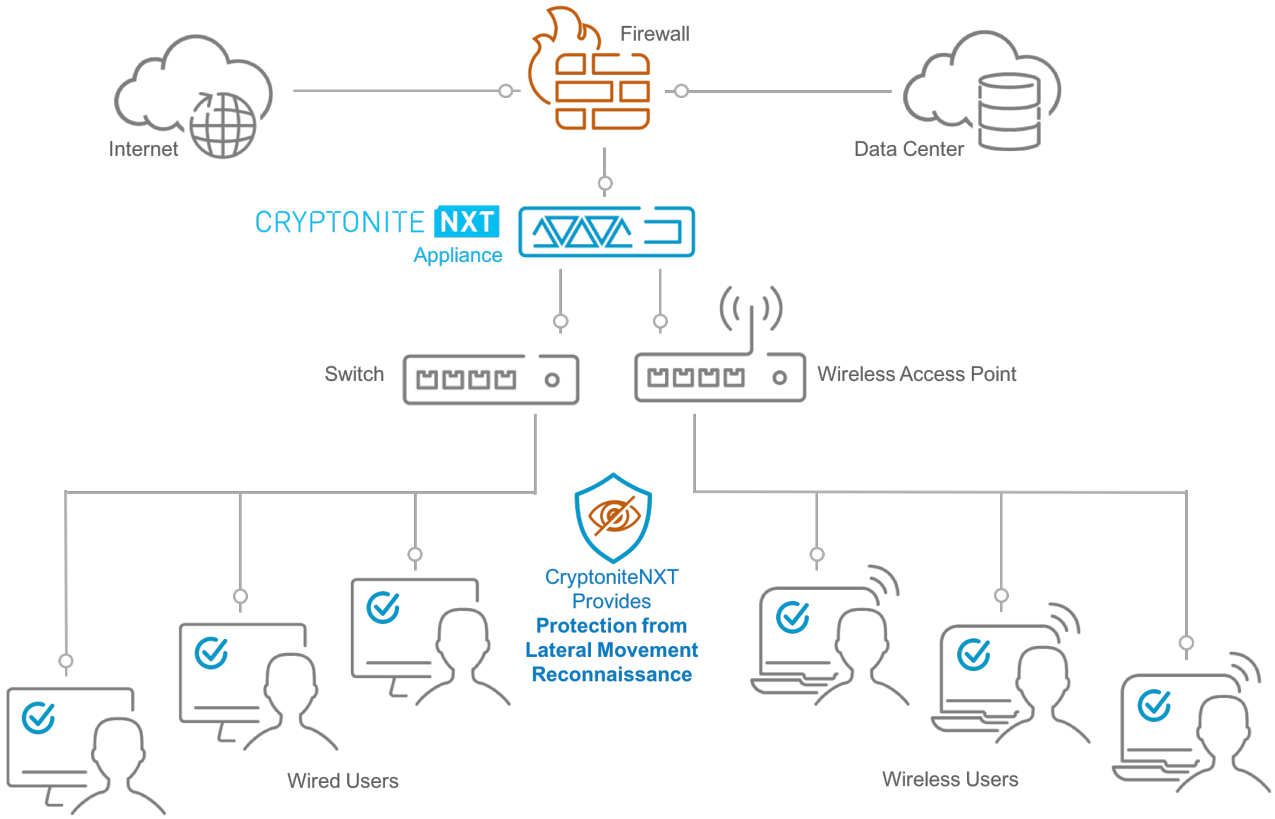
This defense conractor's existing investment in cybersecurity defense includes endpoint detection and remediation (EDR), IPS/IDS equipment, 2nd generation firewalls.

They became aware of CryptoniteNXT's customer deployments and became a participant in early testing and deployment of the product platform. Their technology teams provided an exhaustive analysis of CryptoniteNXT functionality, and documented, in detail, the capabilities and performance of the systems they tested. Their team also suggested enhancements and features that would improve the overall effectiveness and operation of the CryptoniteNXT platform.

## The Results

The CryptoniteNXT appliance protects several key networks within the company. Attackers that seek to perform reconnaissance and enumerate the network are logged and alerted, and, most importantly, they are immediately shut down and stopped. Attacker or insider threat lateral movement out of policy is logged and generates an alert, but, in a similar fashion, they are also restricted and shut down. This automation benefits the security operations team, often overloaded with alerts, many of which require investigation and manual remediation.

The CryptoniteNXT platform was then selected for internal use, on a permanent basis, and is in the process of being deployed to several enclaves within their internal networks. The continued testing of the MTD technology has gone well, and they have contracted to roll out company-wide deployment of CryptoniteNXT by the end of 2017.




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.**