

# PALO ALTO NETWORKS AND CRYPTONITE

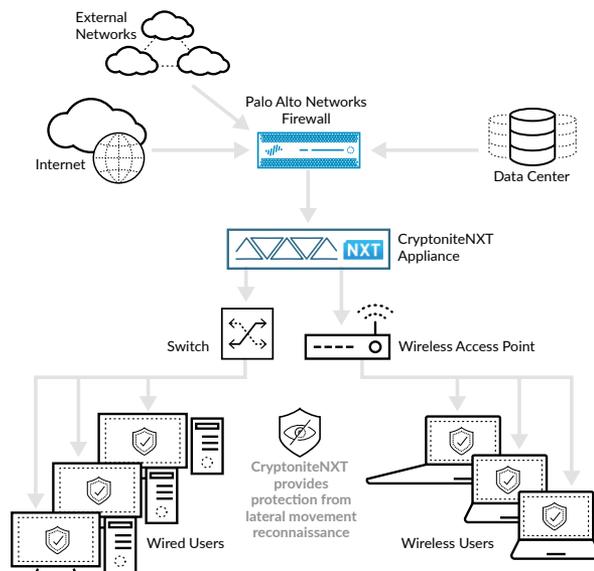
## Key Benefits of the Integration

- Palo Alto Networks Next-Generation Firewall safely enables applications, preventing known and unknown threats.
- CryptoniteNXT hides the network architecture from attackers while providing username-to-IP mappings to the next-generation firewall.
- Palo Alto Networks users benefit from the full capabilities of CryptoniteNXT MTD along with all the benefits of their existing Palo Alto Networks Next-Generation Security Platform.

Attackers are using increasingly sophisticated techniques against the most advanced networks. Once inside a network, attackers can perform additional reconnaissance, move laterally to discover and steal data, or even worse, attempt to corrupt or destroy information technology assets. Cyberattackers have the advantage today because TCP/IP networks are not designed to be secure – they are completely transparent and easy for attackers to exploit. With the integration of Palo Alto Networks® and CryptoniteNXT, customers benefit from best-in-class security with a network that's dynamic and impossible to map. Attackers' tools don't work – they cannot discover what they cannot see, and cannot attack without a target.

## An Introduction to CryptoniteNXT

CryptoniteNXT Moving Target Cyber Defense, or MTD, deceives and contains cyberattackers at the very beginning of an attack, and makes their targets invisible. Reconnaissance is completely shut down. Without visibility into the network, it is impossible for cyberattackers to map the network, access unpatched vulnerabilities and proceed with an attack.



---

CryptoniteNXT Net Guard does this by transforming the endpoint's view of the network into a dynamic, abstract structure, effectively making the once-static network into a dynamic, moving target. Net Guard MTD creates a mapping from the obfuscated network to the real one to enable flow of traffic across the traditional network infrastructure. Attackers cannot collect actionable information about the network or masquerade as another legitimate endpoint. Meanwhile, legitimate traffic is unaffected by Net Guard. All of this is done without sacrificing performance or transparency for users.

### **Palo Alto Networks Next-Generation Security Platform**

With its Next-Generation Firewall, Threat Intelligence Cloud and Advanced Endpoint Protection, Palo Alto Networks Next-Generation Security Platform protects enterprise, government and service provider networks from cyberthreats, using an innovative traffic classification engine that provides full context by identifying all traffic by application, user and content. By combining network, cloud and endpoint security with advanced threat intelligence in a natively integrated security platform, Palo Alto Networks safely enables all applications and delivers automated, preventive protection against cyberthreats at all stages in the attack lifecycle without compromising performance.

### **The Joint Offering**

CryptoniteNXT Net Guard MTD deceives and stops attackers by shutting down reconnaissance through the obfuscation and periodic rotation of visible IP addresses. The integration passes the correct, hidden IP data, along with the identifying user data, through a standard XML RESTful API into Palo Alto Networks Next-Generation Firewall. With this complete visibility inside their networks, security teams can enforce policies, such as blocking groups of users from accessing the internet, and provide other important capabilities.

### **Sample Use Case: Reducing the Risk Posed by IoT Devices**

**Challenge:** The recent proliferation of the internet of things introduces cybersecurity risk. Many devices, including security cameras, automated lighting, energy controls, thermostats and other components of IoT-connected buildings, can become pivot points for advanced cyberattacks.

**Approach:** CryptoniteNXT integration with Palo Alto Networks stops endpoint reconnaissance directed into the network that might allow compromise of an unprotected IoT device while providing Palo Alto Networks Next-Generation Firewall with the correct, hidden IP data, along with the identifying user data, through a standard XML RESTful API.

### **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](http://www.cryptonitenxt.com).

### **About Palo Alto Networks**

Palo Alto Networks is the next-generation security company, leading a new era in cybersecurity by safely enabling applications and preventing cyber breaches for tens of thousands of organizations worldwide. Built with an innovative approach and highly differentiated cyberthreat prevention capabilities, our game-changing security platform delivers security far superior to legacy or point products, safely enables daily business operations, and protects an organization's most valuable assets. Find out more at [www.paloaltonetworks.com](http://www.paloaltonetworks.com).



3000 Tannery Way  
Santa Clara, CA 95054

Main: +1.408.753.4000  
Sales: +1.866.320.4788  
Support: +1.866.898.9087

[www.paloaltonetworks.com](http://www.paloaltonetworks.com)

© 2017 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies. palo-alto-networks and cryptoniteNXT-tpsb-111717