CRYPTONITE NXT

BLUEHALO

Zero Trust Network Architecture

BLUEHALO

bluehalo.com | info@bluehalo.com

Zero Trust Defined

The Zero Trust network architecture was created by Forrester Research in 2009. Since inception, Zero Trust has gained increasing acceptance and adoption across a broad mix of commercial enterprises and government organizations. Forrester's position was that the notion of treating the internal network as trusted and the external networks as untrusted was inherently flawed, and their conclusion was that every network should be considered untrusted.

BlueHalo's flagship security platform, CryptoniteNXT, is an integral component of a Zero Trust Network Architecture.

Zero Trust does not allow any access to network resources, internal IP addresses, or servers until the identity of the user is authenticated properly and their access to the specific assets is authorized. One of the underlying principles of Zero Trust is to only allow a user full access to the bare minimum they need to perform their job or least privilege. Users that seek to go outside of the policy will be stopped from this unauthorized activity. Zero Trust makes the important assumption that the system could be compromised at any time and reduces network visibility accordingly to stop adversaries.

BlueHalo's CryptoniteNXT is an integral component of a Zero Trust Network Architecture and is built on the principles of zero trust – never trust, always verify, and only provide need to know access. When installed, CryptoniteNXT removes an adversary's ability to execute entire categories of in-network attacks that are used to target high vulnerability environments.

Zero Trust is Collaborative Mix of Technologies

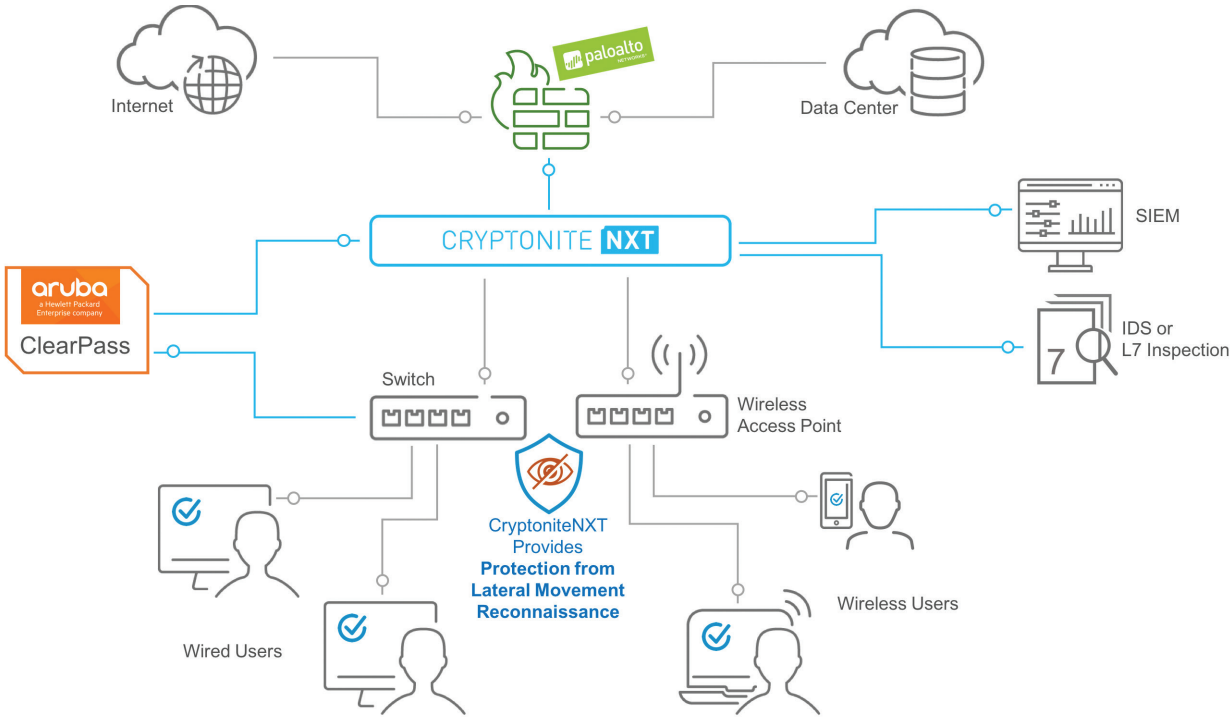
Without visibility into the network, it is impossible for cyber attackers to map the network, access unpatched vulnerabilities, and proceed with an attack.

Zero Trust draws from a wide range of technologies designed to integrate with your existing cyber ecosystem and network defenses to better secure and harden standard TCP/IP networks. New technologies such as next-generation firewalls, moving target cyber defense (MTD), micro-segmentation, deception technology, 802.1x compliant 2-factor user and device authentication, and more may be combined to enable a Zero Trust environment. Absolutely nothing should be allowed network or resource access until they have proven that they should be trusted. The goal of this empowered cyber ecosystem is to authorize, validate, manage, and enforce the identity of the system and users throughout the network.

Critical Vulnerability Use Cases Protected by Zero Trust Networks

Legacy Systems. Legacy systems present a challenging environment to cybersecurity tool sets that are not part of a Zero Trust ecosystem. These older systems are typically void of the protection from security tools such as endpoint protection and are operating on unsupported software platforms. The vulnerabilities that exist within legacy environments are often available and waiting for cyberattackers to exploit them.

Overdue Software Updates and Security Patches. Unpatched software is the primary source of exploits for cyberattackers. The sheer quantity and timing of updates and patches to test and then install in an enterprise is overwhelming and unmanageable for most IT staffs. Cyberattackers will take advantage of this challenge and find entry points into networks and then perform reconnaissance, enumerate the network, move laterally to identify potential target resources, determine the versions of software you are running, and then map and target the exploits to move laterally. Insider threat by rogue employee's, partners, and connected compromised systems may also be introduced to the network.



Embedded Processors and IoT Devices. Many networks contain various difficult to defend embedded processors and internet of things (IoT) devices. In the finance and banking industry, these include point-of-sale systems and automated teller machines (ATMs). In health care, these include a broad diversity of medical devices and patient monitoring devices. In manufacturing, these include industrial control systems components of many types. These embedded processors and IoT devices typically do not have the access or resources to apply security updates, cannot be protected by standard endpoint security, and require the manufacturer's personnel on-site to do basic updates.

Connected Mobile Devices. Smartphones and tablet computing devices add to the risk of networks being targeted by cyberattackers. Mobile devices are particularly attractive to cyberattackers because of their high volumes of use and because they present a wealth of attack vectors. Browser-based attacks, targeted use of buffer overflow, and SMS/MMS are a few of the many ways basic mobile device security can be compromised and defeated. Once compromised, these devices can be used to gain access to enterprise networks.

CryptoniteNXT's role is to eliminate an attacker's visibility and stop unauthorized lateral or east-west movement.

Building a Zero Trust Architecture

A Zero Trust environment may be constructed by combining cyber defense technologies such as moving target cyber defense (MTD), network micro-segmentation, deception technology, and 802.1x compliant user and device authentication. These can enable defenders to leapfrog the tactics of cyberattacker tools.

MTD reduces the attacker's visibility within the network to the point where they can no longer conduct reconnaissance. In fact, using both MTD and micro-

segmentation to build out a Zero Trust environment renders most classic attacker tools inoperable. Lateral east-west movement in the network is similarly restricted and limited by role and policy. Cyberattackers cannot target specific servers and applications that they cannot see, and they cannot attack without a target. MTD and network micro-segmentation technologies may also include integration with identity management technologies such as RADIUS, LDAP, and Active Directory.

Deception technology adds additional layers of protection to build out a resilient Zero Trust environment. Deception technology creates a virtual deployment of fake devices which look like standard IT infrastructure and, in some cases, actual IoT devices. This deceives and attracts the attackers, enabling their potential detection early in the attack.

802.1x compliant user and device authentication allows for the very strong authentication of users, computers, and mobile devices within the network.

Deny, Deceive and Defeat Cyberattackers

DENY. The first step in a Zero Trust ecosystem is to deny entry into the network with a NGFW, to deny unauthorized user access, and to deny access to any unauthorized systems.Network segmentation then allows users to access what is required per policy to perform their job. Everything else is blocked.

DECEIVE. Zero Trust then deceives attackers by controlling network visibility utilizing MTD. Attackers are unable to successfully navigate the network. The deception may be deeper as network resources may appear legitimate, but may instead be decoys or traps.

DEFEAT. Eliminating an adversaries' ability to perform reconnaissance and limiting their movement defeats attackers' intended activity. This will generally frustrate a cyberattacker to the point of stopping the attack or forcing them to attempt higher risk behavior which would make it easier to identify them.

In summary, a Zero Trust network is a powerful collaborative ecosystem. Zero Trust supplements, strengthens, and realigns your existing cyber ecosystem such that attackers are kept out of the network to the greatest extent possible. In the event of a data breach, cyberattackers are promptly identified and stopped from movement or acquiring resources. All of this reduces your risk of a data breach, reduces the risk of malicious damage to your ongoing operations, and protects the private and sensitive data within your information technology infrastructure.

About CryptoniteNXT

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

CRYPTONITE NXT
BLUEHALO