DATA SHEET

CRYPTONITE NXT

Key Benefits of CryptoniteNXT

- Eliminate cyber attacker reconnaissance which shuts down the attack at the earliest possible time, reducing the time to breach detection and reducing the risk of loss and damage to critical assets by a cyber attacker or an insider threat.
- Minimizes or stops lateral movement by unauthorized parties similarly reducing the risk of loss and damage to critical assets.
- Enables broad protection for devices with embedded processors (e.g. automated teller machines (ATMs), medical devices, security equipment, internet of things (IoT) devices and manufacturing industrial control systems) reducing the risk of loss and allowing the delay for investment in expensive equipment upgrades.
- Reduce the risk of delays associated with the installation of critical security software patches and updates. Attackers cannot find, identify and leverage vulnerabilities if they cannot find or see the systems, map the network and research available exploits.
- Enables a true "zero trust environment" which substantially reduces the probability of a successful cyber-attack from sophisticated outside attackers or malicious insiders.
- Stops the propagation of specialized attacker tools such as ransomware.

Deploying a Zero Trust Environment

The Challenge

Attackers are using increasingly sophisticated techniques to penetrate the best-defended network architectures. The question isn't whether attackers will penetrate your networks, but when and how often. Attackers can be active within your networks for many months prior to detection, which can result in disaster for the targeted resources.

Once attackers are inside of your networks, they have almost unrestricted access to perform additional reconnaissance, move laterally through your networks discovering and stealing data, or even worse, attempting to corrupt or destroy your information technology assets.

The reason that cyber attackers have the advantage today is that TCP/IP networks are completely transparent, not designed to be secure, and easily exploited by attackers once they breach the perimeter. Once inside the network – everyone is generally given access as a trusted entity. Until now, there has not been a straightforward way to deploy a "zero trust environment" that can more quickly stop and identify active attackers and malicious insiders.

CryptoniteNXT Net Guard Moving Target Cyber Defense (MTD)

CryptoniteNXT Net Guard moving target cyber defense (MTD) deceives and contains cyber attackers at the very beginning of the attack and makes their targets invisible. Reconnaissance is completely shut down. Without visibility into the network, it is impossible for cyber attackers to map the network, access unpatched vulnerabilities, and proceed with an attack. Attacker tools don't work - they cannot discover what they cannot see, and cannot attack without a target.

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

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

CryptoniteNXT Net Guard also protects against attackers or insiders that have been in your network prior to installation. Network mapping done prior to the installation of Net Guard is not actionable. All of this existing sensitive information is rendered useless for continued cyber attacker planning.

CryptoniteNXT Micro Shield Segmentation

CryptoniteNXT Micro Shield Segmentation significantly reduces attack surfaces accessible via lateral movement. Users only have visibility to the servers and other devices necessary to support their daily work. Attackers and malicious insiders are denied access to lateral movement beyond a very narrowly defined set of resources. CryptoniteNXT automation identifies every specific device, the approved access to resources, and the user authenticated and authorized to use it.

Our automation allows you to configure and deploy CryptoniteNXT in the largest commercial and government enterprise networks. IT staff can easily define policies within the CryptoniteNXT platform to control network access based on device types, user profiles, applications or numerous role-based characteristics shared via Active Directory or a Lightweight Directory Access Protocol (LDAP)-based directory service. Micro Shield is also highly flexible. Micro Shield supports all your existing routers, switches and network infrastructure.

CryptoniteNXT Protects IoT and Embedded Processors

Attackers and their tools seek out vulnerabilities at the earliest opportunity. There will always be systems and servers that are behind on software updates. This will never change. Out of date endpoint and server software presents an almost perfect target. Add to this legacy unpatched operating systems, internet of things (IoT) devices, point of sale terminals, embedded processors in manufacturing industrial control systems (PLM, SCADA, etc.), medical devices, automated teller machines, specialized telecommunications controllers and much more. The attackers are both denied access to finding these on the network, and if they find access, severely limited in terms of lateral movement within the network. If you cannot find these targets, see the network, nor move laterally within it, the attack is effectively over.

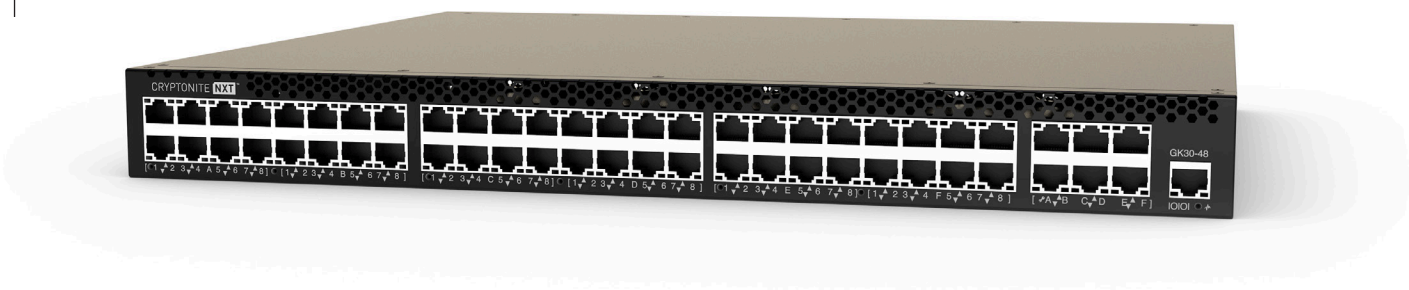
24 x 7 Zero Trust Environment

Net Guard and Micro Shield combined present a comprehensive "zero trust environment." Together, CryptoniteNXT Net Guard and Micro Shield substantially reduce exposure and contain attacks while allowing legitimate communications to take place. CryptoniteNXT cryptographically verifies the sender's identity and the legitimacy of the requested connection. This check prevents MAC and IP address forgery and renders misuse of application or operating system credentials ineffective.

CryptoniteNXT's protection is always on for all traffic. Every packet flowing through the network is controlled. Every endpoint even within the same segment. Your TCP/IP networks are no longer transparent. There is no assumption of trust and open access. However, we know attackers eventually will compromise an endpoint, IoT device, or embedded processor. Human attackers, malware tools and ransomware cannot navigate or move from that entry point. Open hunting season is permanently over.

IP addresses that worked an hour ago no longer work. Reconnaissance tools don't work. Stolen authentications, spoofing and other attempts to transverse systems and applications stall. All of these attacks hit the wall. The attacker is decisively shut down. High probability alerts detailing the violation, detection and containment of the attack are passed to your SIEM and security operations center (SOC) team for further analysis and reporting.

CryptoniteNXT is a network appliance that supplements existing network infrastructure to improve security. A unique combination of technologies effectively alters network behavior in real time with no human intervention. CryptoniteNXT blocks malicious activities while at the same time preserving performance and usability for legitimate purposes.



Compliance Ready

We are ready to help you support many compliance driven environments from including PCI DSS, SOX, HIPAA, FISMA as well as guidelines provided by the National Institute of Standards and Technology (NIST 800-53, NIST 800-171), the Department of Homeland Security and the Department of Defense (DoD DISA) and the pending European Union General Data Protection Regulation (GDPR). Federal and industry regulations, as well as various privacy acts require implementing both audit and security controls to protect and secure the regulated data.

Performance / Capacity (per appliance)	Value
Total throughput	30 Gbps
Per-port throughput	1 Gbps
Latency (typical)	50 µs
Protected endpoints	500 (recommended)
Unique MACs	1500 (maximum)
Endpoint ingress ports	Up to 42

Networking	Value
Interface modes	L3
IPv6 support	Yes
VLANs	Yes, automatic
NAT	Yes, optional distinct IPs
DHCP server	Yes

Capabilities	Value
Domain filtering	Yes
Network access control	Yes
Captive portal	Yes
Two-factor authentication	Yes
Rapid endpoint and user on-boarding	Yes
IP topology discovery prevention	Yes
Peer discovery prevention	Yes
Role-based policy enforcement	Yes
GUI interface	Yes
API	JSON / REST

Integration	Value
PaloAlto	Yes
Aruba Networks (Clearpass)	Yes
Splunk dashboard	Yes
Active Directory user/endpoint import	Yes
Active Directory DNS synchronization	Yes
Packet Mirroring (sanitized)	Yes

Hardware	Value
Management	RJ45 serial console, in band
Ports	48 10/100/1000 Ethernet
Power	Redundant 150W, 113W avg, 133W max
Max BTU/hr	454
Input voltage	100-240VAC (50-60Hz)
Max current consumption	24A@120VAC, 11A@12VDC
Max inrush current	30A@115VAC, 50A@230VAC
Rack mountable	1U, 19" standard rack, 14.5" depth
Weight	11 lbs
Safety	UL/cUL/CB; IEC 60950-1:2005 (2nd Edition); Am 1:2009
EMI	FCC Class A, CE Class A, VCCI Class A, EN55022:2010, CISPR 22:2008, AS/NZS CISPR 22:2009 +A1:2010, TCVN 7189:2009, EN6100-3-2:2006+A1:2009+A2:2009. EN61000-3-3:2008, EN 300 386 V1.6.1 (2012-09), EN55024:2010; CISPR 24:2010+A1:2015
Fans	Redundant
Shipping box dimensions	23"w X 20"d X 7"h
Rack mount included	Yes
USB to RJ45 serial cable included	Yes
Airflow	Front of chassis to rear of chassis

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.**