NWN

SECURITY POV

Before
Discover
Enforce
Harden

During
Detect
Block
Defend

After
Scope
Contain
Remediate
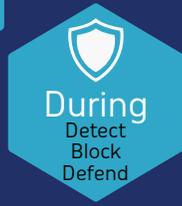
NWN SECURITY
PROOF OF VALUE ASSESSMENTS

Cisco helps customers simplify the complexity of security through a comprehensive approach that's unique in the marketplace. NWN has teamed up with Cisco to provide a best-in-class portfolio of solutions designed to span the entire security attack continuum, addressing threats before, during, and after the attack. Cisco's platform-based solutions solve customers' specific challenges, while smoothly integrating into their overall security system. The result is complete protection throughout the entire IT infrastructure.

CISCO UMBRELLA POV

Explore the capabilities of a DNS based threat detection system for on premise and off premise users. Get complete visibility into your organizations cloud usage and granular per-user access control for web content over 60+ URL categories while protecting your organization from sophisticated threats leveraging advanced evasion techniques like DGA (domain generation algorithms) and other known bad actor behaviors. More granular administrative control based on Active Directory can also be accomplished with agents and Cisco virtual machines installed into your environment to allow group-based access control and monitoring. Blacklists are automatically updated regularly from Cisco Talos, Threat Grid, and other Security Intelligence feeds to provide your organization with comprehensive protection against constantly evolving threats

CISCO SECURITY
CISCO FIREPOWER POV

Cisco helps customers simplify the complexity of security through a comprehensive approach that's unique in the marketplace. NWN has teamed up with Cisco to provide a best-in-class portfolio of solutions designed to span the entire security attack continuum, addressing threats before, during, and after the attack. Cisco's platform-based solutions solve customers' specific challenges, while smoothly integrating into their overall security system. The result is complete protection throughout the entire IT infrastructure.

CISCO AMP FOR ENDPOINTS POV

Network based Malware protection provides visibility to a portion of information in an entire attack profile. Capturing data from the network leaves a hole in the visibility of a malware attack. That's where AMP for Endpoints fills that gap. Running an agent on any Windows, Mac OSX, Android, or Linux based system, AMP provides security analysts with file execution details and threat detection. AMP is fed continuous information from a cloud security intelligence powered by Cisco Talos and ThreatGrid. AMP for endpoints provides retrospective security that can "look back in time" to detect the change in posture of any file running on a protected enpoint. This provides the ability to detect previously trusted files that later became malicious. Point in time solutions cannot provide this level of protection and visibility. Additionally, AMP for endpoints directly integrates with AMP for Networks running on FirePower sensors and appliances and AMP for Content running on Cisco Web Security and Email Security gateways providing the most up to date real-time protection for your environment across the attacke surface.