



First Micro-Segmentation Benchmark Report Validates VMware NSX Capabilities Enable a Zero-Trust Model

Westminster, Colo. – September 21, 2016 – Coalfire, an independent cyber risk management advisor and assessor, is today publishing an industry-first [Micro-segmentation Cybersecurity Benchmark Report](#) sponsored by VMware that evaluates the security efficacy of VMware NSX®. Coalfire found that VMware NSX, which enables the creation, management, deployment and operationalization of security policy and controls at a granular level to applications, workloads and users enables a Zero-Trust model independent of network topology, preventing unauthorized access through least-privilege policy.

The VMware NSX network virtualization platform enables micro-segmentation that bridges differing architecture and deployment methods to more effectively manage security policy across mix-mode environments where workloads of different security levels are hosted on the same physical infrastructure. Coalfire's benchmark report concluded that the VMware NSX product:

- was validated to map to the NIST Special Publication 800-125B "Secure Network Virtual Configuration for Virtual Machine (VM) Protection" recommendations for protecting virtual environments;
- provides granular level security policy control and traffic visibility that operationalizes security and enables clients to meet regulatory compliance requirements such as PCI DSS;
- meets the definition of micro-segmentation by enabling the combination of multiple capabilities (further listed below).

As a finding in the benchmark report, VMware NSX meets the definition for micro-segmentation which reduces risk and increases security posture by delivering these capabilities:

- 1) Distributed stateful firewalling for topology agnostic segmentation,
- 2) Centralized ubiquitous policy control of distributed services,
- 3) Granular unit-level controls implemented by high-level policy objects,
- 4) Network overlay-based isolation and segmentation and
- 5) Policy-driven unit-level service insertion and traffic steering.

In addition to these validations, it was found that when deployed, the VMware NSX platform can prevent lateral movement within the network from insider threats and prevent the spread of malware within the environment due to security policy implementation at the application level.

"VMware NSX meets the rigorous requirements for security in regulated industries, bringing a new level of risk reduction by building security controls aligned to the application," said Milin Desai, vice president, products, networking and security business unit, VMware. "Micro-segmentation has been a critical driver in the adoption and production deployments of VMware NSX, and validation of these capabilities by Coalfire means customers can virtualize the network even more confidently with NSX."

"Armor deployed NSX micro-segmentation to better manage security policy across its environments. By leveraging the distributed firewall capabilities, Armor is able to meet the requirements of the PCI DSS for their annual assessments, as audited by Coalfire," said Jason Rieger, Principal Cloud Architect, Armor. "The distributed, stateful firewall capabilities that VMware NSX was able to provide through micro-segmentation, along with a robust API, gives us greater control and flexibility in implementing security policy to meet our needs. These micro-segmentation capabilities make recurring PCI assessments easier to manage, resulting in faster audits."



Click the link to go to the VMware website to learn more about the [micro-segmentation capabilities of VMware NSX](#). Visit the [Coalfire website](#) for more information on Coalfire's cloud and virtualization validation services, cyber risk management, assessment and advisory services.

About Coalfire

Coalfire is the trusted leader in cybersecurity risk management and compliance services. Coalfire integrates advisory and technical assessments and recommendations to the corporate directors, executives, boards, and IT organizations for global brands and organizations in the technology, cloud, healthcare, retail, payments, and financial industries. Coalfire's approach addresses each businesses' specific vulnerability challenges, developing a long-term strategy to prevent security breaches and data theft. Coalfire has offices throughout the United States and Europe. www.coalfire.com

#

VMware and NSX are registered trademarks or trademarks of VMware, Inc. in the United States and other jurisdictions.

Press Contacts:

Adam Cormier
Racepoint Global
+1 617 624 3218

Coalfire@racepointglobal.com