VMware® NSX with Rapid7 Nexpose®

A revolutionary approach to vulnerability management

Security teams are constantly challenged to deploy best practices such as isolation and segmentation, which are required to protect against today's threats. With VMware NSX, the network virtualization component of the software-defined data center (SDDC), teams can adopt these practices including micro-segmentation in an operationally sustainable and smart way.

Nexpose is the industry-first integration with VMware NSX to provide an innovative way to scan for vulnerabilities and mitigate associated risk in SDDC environments.

The VMware NSX distributed service platform allows best-of-breed security solutions, like Nexpose, to be dynamically inserted as a security service to improve operational efficiency and improve security. Nexpose integrates with VMware NSX platform to perform vulnerability assessment directly through the hypervisor, without requiring traditional network or operating system access to perform a vulnerability assessment. This reduces administration effort to deploy and maintain the service and gives comprehensive visibility into risk.

To take vulnerability management a step further, VMware NSX allows Nexpose to be included as part of a security policy comprising one or more services including NSX Distributed Firewall, NSX Data Security, and NSX Server Activity Monitoring. This enables Nexpose to tag virtual machines based on vulnerability posture, allowing administrators to quarantine risky virtual machines by placing them into a micro-segment where a compensating control such as Intrusion Prevention System (IPS) or firewall is applied.

This new approach to vulnerability management enables Nexpose to assess true vulnerability risk, restrict access to risky assets, and maintain complete visibility of risk posture, all within the SDDC. This approach also enables cloud architects to define application templates using pre-defined NSX security policies in a self-service IT model, where users simply request workloads, and the infrastructure automatically delivers the intended security policy. This automation enables micro-segmentation at scale without continuous oversight from IT departments.

Key Benefits

- **Real-time dynamic discovery**
  Nexpose provides continuous visibility into online and offline virtual machines, ensuring there are no gaps in your risk visibility.

- **Comprehensive risk visibility**
  Scans directly through hypervisor including virtual network topologies like isolation, segmentation, and micro-segmentation giving a complete picture.

- **Automatically mitigate risk**
  Nexpose security data is exposed through NSX, allowing for workload provisioning and automation to micro-segment, tag and quarantine virtual machines, or apply stricter policies to proactively block potential attacks until remediation is completed without service interruption.

- **Increase scanning performance**
  Due to scanning directly through the hypervisor, network bandwidth and resource utilization is minimized as local scan engines are automatically deployed to every host and impact on each virtual machine is reduced.

- **Credential-less deep scanning**
  Using NSX Guest Introspection, Nexpose is inserted as a trusted security service, eliminating the need to setup and maintain credentials to perform deep vulnerability scans against virtual machines.

- **Reduced setup and management**
  Nexpose is easily set up in VMware NSX, and automated continuous deployment removes dependency on security teams for ensuring vulnerability assessment is configured correctly.
**Vulnerability assessment in the SDDC**

The SDDC brings a paradigm shift for security in the data center architecture by virtualizing compute, network, and storage. This has enabled logical management of the network and for new security services to be inserted into the layers.

VMware NSX with Nexpose takes advantages of these advances in data center architecture to give fast and accurate visibility into risk posture without the extra effort of setting up and managing a vulnerability management program.

**Isolation and segmentation as a security best practice**

Network segmentation is a security best practice by SANS, PCI, and NIST. When attackers get unauthorized access into the network, segmentation can prevent the next step of network intrusion by limiting further movement. More layers of segmentation typically increase security but are burdensome to maintain and ensure configuration accuracy.

NSX network virtualization and firewalls provide isolation, segmentation, and micro-segmentation by default. The NSX platform can be extended through advanced security services like Nexpose, and be inserted dynamically into the logical service pipeline. When Nexpose identifies a risky virtual machine, a stricter policy can be applied or it can be quarantined until remediation is completed.

**Movement towards application-specific micro-segmentation**

Traditional isolation and segmentation is achieved through static security zones that prevent or limit network traffic to the zone. This approach prevents propagation of threats between zones. However, there is still east-west traffic within the zone that can allow propagation of a threat.

By shifting towards a dynamic application-specific zone, you can use micro-segmentation to control east-west traffic to increase security. Nexpose and other advanced security services that perform service orchestration not only make this operationally feasible, but a reality.

**Prioritize risk that matters, quickly and efficiently**

Not every virtual machine is the same and shouldn’t be treated the same from a security perspective. Different virtual machines have different data and their importance to the business varies. Security administrators need to know the context of the risk to ensure they are prioritizing and remediating risk that matters to their business.

Nexpose is the only vulnerability management solution that prioritizes vulnerabilities, controls, and configurations across the modern network to make better risk management decisions, faster. Nexpose leverages RealContext™, RealRisk™, and critical threat awareness from Metasploit® to prioritize and validate your risk, so you can focus on fixing the issues that have impact.