Mitigate Risk in SDDC Environments

with Rapid7 Nexpose and VMware NSX

Integration Brief

INTEGRATION BENEFITS

- Real-time dynamic discovery
- Comprehensive risk visibility
- Automatically mitigate risk
- Increase scanning performance
- Credential-less deep scanning
- Reduced setup and management

Solution Overview

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 microsegmentation in an operationally sustainable and smart way.

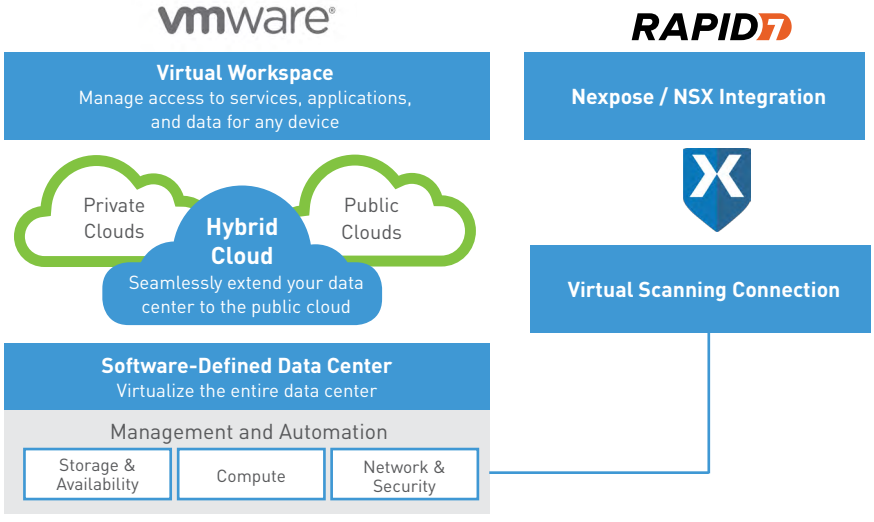
Rapid7 Nexpose is the industry-first integration with VMware NSX to provide an innovative way to scan for vulnerabilities and mitigate associated risk in SDDC environments.

How it Works

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 to perform vulnerability assessments directly through the hypervisor, without requiring traditional network or operating system access. This reduces administration effort and gives comprehensive visibility into risk.

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 microsegment where a compensating control such as Intrusion Prevention System (IPS) or firewall is applied.

This 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. Cloud architects can 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.



120715

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 firewalling capabilities 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 microsegmentation

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 to a dynamic application-specific zone, you can use microsegmentation 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 they 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.

GAIN GREATER INSIGHT WITH REAL RISK™

"Understanding risk across virtual and physical environments can quickly become a daunting task if a complete view of assets and related exposures most vulnerable to an attack are not readily available. Companies have long needed a way to make smarter choices when managing their infrastructure and vendors like Rapid7 are helping to provide insight into actual and validated risks."

-The 451 Group

About Rapid7

Rapid7 is a leading provider of security data and analytics solutions that enable organizations to implement an active, analytics-driven approach to cyber security. We combine our extensive experience in security data and analytics and deep insight into attacker behaviors and techniques to make sense of the wealth of data available to organizations about their IT environments and users. Our solutions empower organizations to prevent attacks by providing visibility into vulnerabilities and to rapidly detect compromises, respond to breaches, and correct the underlying causes of attacks. Rapid7 is trusted by more than 4,150 organizations across 90 countries, including 34% of the Fortune 1000. To learn more about Rapid7 or get involved in our threat research, visit www.rapid7.com.