FORESCOUT

See

- Profile and classify VMs, physical servers, applications and operating systems
- Improve visibility into SDDCs as VMs are created, moved, or retired
- Proactively identify zombie and orphan VMs to reduce risk and optimize resource usage

Control

- Allow, deny or restrict network access by assigning or changing VM port groups or NSX tags.
- Help ensure ESXi hosts and VMs adhere to best practices and hardening guidelines
- Remediate non-compliant VMs as it pertains to OS patches, security applications, signatures and more

Orchestrate

- True-up asset inventories and CMDBs with up-to-date VM information
- Facilitate on-connect vulnerability scans and reduce the attack surface on connected VMs
- Monitor VMs for Indicators of Compromise (IOCs) to mitigate threats

Securing Software-Defined Data Centers

Extend visibility and control to your private cloud and software-defined data centers

As shown by a recent survey, virtualization continues to increase[1] with 75 percent of organizations using private clouds. Private clouds increase flexibility, improve service levels, reduce operating costs and alleviate multi-tenancy concerns. While the dynamic aspect of virtualization in private clouds provides speed and agility, it also creates inherent challenges for the security teams leveraging siloed tools, and allows adversaries to take advantage of noncompliant and vulnerable servers—virtual as well as physical. ForeScout's data center security solution can help you meet these challenges with unified visibility and automated, policy-based controls across your physical and virtual infrastructure.

The widespread adoption of private clouds has allowed organizations to leverage virtual computing to speed application deployment, simplify data center operations and increase business agility. Many enterprises are further evolving their virtualized data centers to adopt the Software Defined Data Center (SDDC) approach. One popular solution for doing just that is provided by VMware® with the vSphere and NSX solution, which allows administrators to decouple network resources from underlying hardware and optimize resources within an SDDC.

So what about security? IT security teams continue to be responsible for protecting the entire enterprise, including virtualized data centers, where not only servers are virtualized but networks as well. New security solutions are needed. Traditional products protect north-south traffic or the traffic flowing through the data center perimeter, and leverage user identity and granular contextual information to allow or deny traffic. With approximately 85 percent of traffic likely to flow in an east-west direction in private data centers by 2021,[2] the rules governing private cloud environments are more challenging than physical environments.

Protecting data in your modern SDDC requires new security methodologies. Security best practices necessitate that applications and resources be separated and allowed access on an as-needed basis. In addition, security policies and control must extend beyond north-south traffic to include east-west traffic as well.

The Challenge

Visibility. Serious attempts to manage security risk must start with knowing who and what is on your network, including visibility into whether the connected devices and virtual machines (VMs) comply with your security standards. Many organizations are in the dark regarding a significant percentage of VMs in their software-defined data centers because they are:

- Orphan or zombie VMs
- VMs with disabled or non-compliant agents
- Transient VMs undetected by periodic scans

This can lead to incomplete data in asset inventories and out-of-date information in configuration management databases (CMDBs). As a result, organizations may also be unaware of the additional attack surface and elevated risks from these VMs.

Within the private cloud, workloads are deployed in VMs. Network traffic can be between VMs on the same hypervisor, between VMs on different hypervisors, or between a VM and a physical device. Maintaining visibility into all network traffic through continuous monitoring is an important aspect of comprehensive security for your data center and private clouds.

Threat Landscape. Private cloud adoption continues to grow, and while the benefits of virtualization and SDDCs are undeniable, so are the inherent security challenges:

- Numerous blind spots can be created due to lack of visibility into VMs
- Knowledge of device hygiene is incomplete even for known devices
- The presence of unused or orphan VMs expands the attack surface

These challenges create wide-open opportunities for attackers to exploit vulnerabilities, access shared resources and move laterally across a network to obtain sensitive information. This can lead to data breaches, reputation loss and costly investigations—erasing any cost savings associated with virtual infrastructure.

Compliance. Unlike physical environments, virtual computing allows you to spin up a new server in a few seconds with little or no training. Consequently, well-meaning employees who aren't qualified to maintain and patch servers can install new servers or revive offline ones that may not be compliant with the organization's security policies. Since VMs share physical resources, a misconfiguration or vulnerability in one VM can potentially compromise other VMs and lead to increased risk.

Inefficient Resource Utilization. Approximately one-third of the VMs occupying server resources in sampled organizations were found to be zombies, according to a recent research study.[3] These zombie VMs are unlikely to have the latest security patches or comply with security policies, making them a higher security risk. Additionally, in many virtual environments, VMs are created, cloned and migrated based on cyclic organizational needs or seasonal business demands. This flexibility can lead to VM sprawl—out-of-control proliferation of VMs or orphan VMs that have no parent-child linkages—resulting in unused and locked resources, reduction in data center capacity and a large exposed attack surface.

The ForeScout Solution

By deploying ForeScout's data center security solution, you can achieve your critical security goals. ForeScout CounterACT® learns contextual information about the SDDC infrastructure, including virtual and physical servers. The solution provides:

Visibility and Asset Management
The ForeScout platform discovers and classifies rogue, unmanaged or unapproved VMs, as well as VMware ESXi hosts and their associated properties, to let you can gain vastly improved visibility into your SDDC and private cloud. Your security operations team can stay apprised of changes in VMs as they are created, moved, off-lined or retired, and can take automated, policy-based actions to verify configured properties on existing VMs. In addition, this improved visibility lets you true-up existing asset inventory tools such as CMDBs with up-to-date information about connected VMs and their associated properties.

Compliance
With ForeScout CounterACT, you can create automated policies to help ensure VMs adhere to VM hardening standards or security benchmarks. For non-compliant VMs, you can take corrective actions based on threat severity or risk level, including isolating them in pre-defined port/security groups or requiring the presence of functional security agents.

Resource Optimization
ForeScout can help you proactively identify and manage under-utilized or shadow VMs and help ensure that they comply with your security policies. This lets you optimize data center resources, boost infrastructure capacity and improve overall security posture.

Segmentation and Risk Mitigation
The ForeScout platform, along with solutions like VMware NSX, help you protect data in your modern SDDC. You can adopt mechanisms to govern lateral movement of traffic with disparate trust levels. VMware NSX enables micro-segmentation, which allows you to divide your data center into distinct security segments down to the individual workload level, and then define security controls and deliver services for each unique segment.

With ForeScout, you can validate if all the VMs and hosts deployed have the right security posture, are placed in the right security zones, and enforce security tags/groups based on security posture. As a result, you can fortify your defenses and enforce the Zero-Trust model for your SDDC.

Supported Data Center Products

- VMware vSphere
- VMware NSX

Unified Visibility from Campus to Private Cloud

Security starts with visibility. At ForeScout, our approach to private cloud security is a logical extension of securing managed and unmanaged devices in a physical network. The ForeScout platform provides an accurate and consolidated view of your physical and virtual devices—a view that spans campus, data center and cloud. You can leverage this consolidated visibility to ensure unified compliance; implement segmentation and control policies across physical and virtual infrastructure; and take automated, policy-based actions to reduce risk and mitigate threats throughout the enterprise network.

[1] RightScale 2018 State of the Cloud Report.
[2] https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html
[3] https://www.computerworld.com/article/3196355/servers/a-third-of-virtual-servers-are-zombies.html

Learn more at
www.ForeScout.com

FORESCOUT

ForeScout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591