ForeScout

Solution Brief

See

- Profile and classify VMs, servers, applications and operating systems
- Improve visibility into software-defined data centers as VMs are created, moved, off-lined or retired
- Proactively identify zombie and orphan VMs to optimize resource utilization and reduce risk

Control

- Allow, deny or restrict network access by assigning or changing VM port groups or security groups
- Help ensure ESXi hosts and VMs adhere to best practices and hardening guidelines
- Remediate non-compliant virtual machines (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 virtual servers 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.

Increasing numbers of organizations are embracing virtualization for its fast build-to-run and scale architecture. While this dynamic aspect of virtualization provides speed and agility, it also creates inherent challenges for the security teams leveraging unfamiliar and siloed tools, and allows attackers to take advantage of non-compliant and vulnerable endpoints. ForeScout's data center solution can help you meet these challenges with unified visibility and automated, policy-based controls across your physical and virtual infrastructure.

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 endpoints comply with your security standards. Most organizations are in the dark regarding a significant percentage of endpoints in their virtual data centers because they are:

- Orphan or zombie virtual machines (VMs)
- Endpoints with disabled or broken 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This can lead to incomplete data in asset inventories and out-of-date information in configuration management databases (CMDBs).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 endpoints.

Threat Landscape. A recent Verizon study[1] noted that private cloud adoption is accelerating due to advances in technology and declining costs. While the benefits of virtualization and software-defined data centers (SDDCs) are undeniable, so are the inherent security challenges. The numerous blind spots that can be created due to lack of visibility into virtual machines, incomplete knowledge of endpoint hygiene and the presence of unused or orphan VMs create wide-open opportunities for attackers to exploit vulnerabilities, access shared resources or 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.

The ForeScout Solution

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. The VMware® vSphere platform allows you to decouple network resources from underlying hardware, optimizing resources within an SDDC. While server virtualization has powered rapid application deployment, these elastic workloads also need fast provisioning of networking and security services to operate without compromising security. Therefore, the rapid abstraction and flexibility provided by virtualization requires advanced security to protect virtual machines against emerging threats. By implementing ForeScout's data center solution, you can achieve your critical security goals, including:

Visibility and Asset Management

By discovering and classifying rogue, unmanaged or unapproved VMs, as well as VMware ESXi hosts and their associated properties, you can gain vastly improved visibility into your software-defined data center and private cloud. Your security operations team can stay apprised of when virtual machines are created, moved, off-lined or retired, and 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

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

Resource Optimization

According to a recent research study[2], approximately one-third of the virtual machines occupying server resources in sampled organizations were found to be zombies. These zombie VMs are unlikely to have the latest security patches or comply with security policies, making them a 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-scale shadow attack surface. 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.

Segmentation and Risk Mitigation

Security best practices require that applications and resources be separated and allowed access on an as-needed basis. With approximately 86 percent of traffic flowing in an east-west direction in private data centers by 2020[3], the rules governing private cloud environments are more challenging than physical environments, where traditional products protect north-south traffic or the traffic flowing through your perimeter, and leverage user identity and granular contextual information to allow or deny traffic. To protect data in your modern data center, you can adopt mechanisms to govern lateral movement of traffic with disparate trust levels. VMware NSX 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 virtual machines 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, unmanaged and Internet of Things (IoT) devices in the physical world. ForeScout CounterACT® provides an accurate and consolidated view of your physical and virtual endpoints from campus to cloud. You can leverage this consolidated visibility to create unified compliance, segmentation and control policies across physical and virtual infrastructure, and take automated, policy-based actions to reduce risk and mitigate threats across your campus and cloud environments.

ForeScout

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

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

[1] http://www.verizonenterprise.com/resources/reports/rp_state-of-the-market-enterprise-cloud-2016_en_xg.pdf
[2] http://anthesisgroup.com/wp-content/uploads/2017/03/Comatsoe-Servers-Redux-2017.pdf
[3] http://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.pdf