

ForeScout Unveils New Security Solution for VMware Software-Defined Data Center Environments

- *ForeScout extends agentless visibility and control to private cloud and software-defined data centers powered by VMware NSX*
- *ForeScout expands collaboration to offer enhanced security, improved compliance and optimized data center utilization in VMware environments*
- *ForeScout enables consolidated visibility and consistent policy management infrastructure wide*

SAN JOSE, Calif., June 27, 2017 – [ForeScout Technologies, Inc.](#), a leading Internet of Things (IoT) security company, today announced its new [ForeScout data center security solution](#) for VMware environments. Expanding on its existing technology collaboration with VMware, ForeScout's data center security solution will now provide enhanced security and compliance for organizations by discovering, classifying and assessing endpoints across traditional and software-defined data centers. ForeScout will help VMware NSX® customers further improve security through consolidated visibility across virtual and physical infrastructures, reduced attack surface and enforced segmentation policies in heterogeneous environments.

“As enterprises shift from traditional to software-defined data centers, IT organizations are struggling to detect rogue, non-compliant, unmanaged virtual machines and devices,” said Michael DeCesare, president and CEO, ForeScout. “While virtualization and cloud solutions provide much needed flexibility, having comprehensive visibility in those environments is essential to preventing blind spots. ForeScout's interoperability with VMware NSX is part of our broader strategy to help provide customers with visibility and control across their network infrastructure from the campus to data center to cloud. You can only secure what you can see.”

As networks continue to evolve and organizations adopt IoT devices and virtualization, cyberattacks can take advantage of any visibility and control gaps. If rogue, non-compliant, unapproved, zombie and orphan virtual machines go undetected, they can increase an organization's attack surface and open the door for hackers to exploit weak links, access shared resources, or move laterally across a network to obtain sensitive information. As such, organizations need visibility across the network infrastructure to validate virtual machine and device properties as well as stronger security controls to prevent new attack vectors.

Security analysts leveraging ForeScout's new data center security solution for VMware will be able to maximize existing security investments to improve the following:

- **Visibility:** Improve visibility into software-defined data centers as virtual machines are created, moved, off-lined or retired. Validate virtual machine properties using a policy-based approach to help true-up asset inventories and configuration management databases (CMDB) with more up-to-date information about connected virtual machines and their associated properties.
- **Compliance:** Assist customers in adhering to security best practices and virtual machine hardening standards. Automate compliance checks to measure against standardized guidelines and initiate remediation actions to mitigate risk from non-compliant or rogue virtual machines.
- **Resource Optimization:** Help maximize capacity of virtual machine infrastructures and optimize utilization by proactively identifying zombie and orphan virtual machines to reduce virtual machine sprawl and prevent unnecessary consumption of resources.
- **Risk Mitigation and Response:** Verify security profile and posture of virtual machines and apply appropriate VMware NSX security tags to enforce segmentation policies, isolate non-compliant endpoints and facilitate remediation actions.

Earlier this year, [ForeScout announced](#) its security solution for Amazon Web Services (AWS) to enable visibility into cloud workloads. Now, working separately with both VMware and AWS, ForeScout provides consolidated visibility and consistent policy management across campus, private data center and public cloud infrastructures.

For more information on ForeScout's data center solution for VMware, please [visit here](#).

Supporting Quotes:

“We continue to work with our customers to help transform security as part of their digital transformation. Our approach with NSX is to deliver a security platform with our ecosystem where security is aligned to the application. With ForeScout and NSX we are delivering on our promise of application aligned security with agility for our joint environments.”

- *Milin Desai, vice president of products, networking and security business unit at VMware*

“Today's enterprises are modernizing their IT infrastructures and moving to hybrid and multi-cloud environments. However, security considerations continue to be a challenge as endpoints proliferate beyond laptops and physical servers to virtual machines, making it more critical than ever for enterprises to look at security solutions that can seamlessly extend from campus to data center to the cloud. A collaboration like ForeScout and VMware, which extends agentless visibility and control across traditional and software-defined data centers with the NSX technology, will be valuable to organizations looking to secure their heterogeneous infrastructures.”

- *Abhi Dugar, research director, Cloud and Enterprise Infrastructure and IoT Security, IDC*

Additional Resources:

- ForeScout's data center solution for VMware solution brief: <https://www.forescout.com/company/resources/data-center-solution-brief/>
- Video: [Redefining Visibility & Control from Campus to Cloud](#) by Rob Greer, senior vice president of products and CMO, ForeScout
- Press Release: [ForeScout Extends Agentless Visibility, Classification and Control Across Campus, Data Center and Cloud](#)
- Follow ForeScout online: [Facebook](#) | [Twitter](#) | [LinkedIn](#) | [Blog](#)
- ForeScout's corporate brochure: <https://forescout.com/forescout-company-brochure-pr/>

About ForeScout

ForeScout Technologies, Inc. helps make the invisible visible. Our company provides Global 2000 enterprises and government agencies with agentless visibility and control of traditional and IoT devices the instant they connect to the network. Our technology integrates with disparate security tools to help organizations accelerate incident response, break down silos, automate workflows and optimize existing investments. Learn more at www.forescout.com.

© 2017. ForeScout Technologies, Inc. is a privately held Delaware corporation. ForeScout, the ForeScout logo, ActiveResponse, ControlFabric, CounterACT, CounterACT Edge and SecureConnector are trademarks or registered trademarks of ForeScout. Other names mentioned may be trademarks of their respective owners.

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

ForeScout Media Relations Contact:

Katie Beck
ForeScout Technologies, Inc.
650-314-8705
katie.beck@forescout.com