**ForeScout Extends Agentless Visibility, Classification and Control
Across Campus, Data Center and Cloud**

- *Expanded collaboration with VMware offers agentless visibility and control in software-defined data centers*
- *Advanced out-of-the-box device classification with new taxonomy for IoT and OT devices*
- *Enhanced scale, resiliency and a redesigned user interface to manage over one million devices per deployment in multi-vendor environments*

SAN JOSE, Calif., June 27, 2017 – ForeScout Technologies, Inc., a leading Internet of Things (IoT) security company, today announced that ForeScout CounterACT® is redefining agentless visibility and control across the campus, data center and cloud to help keep evolving enterprise infrastructures secure. To support the exponential growth of IoT and operational technology (OT) on enterprise networks, CounterACT now features new advancements including out-of-the-box device classification and taxonomy, enhanced scale and resiliency to manage more than one million devices within a single deployment, and a redesigned user interface to implement consistent policies across multi-vendor and hybrid-cloud environments.

Today ForeScout also introduced its ForeScout Data Center Solution for VMware, which allows enterprises to discover, classify and assess virtual endpoints within private clouds and software-defined data centers (SDDC). Earlier this year, ForeScout announced its new solution for Amazon Web Services (AWS) to help enable agentless visibility and control into cloud workloads on the world's most comprehensive and broadly adopted cloud platform. Being able to leverage both VMware and AWS, in combination with the latest enhancements to CounterACT, allows ForeScout to help enterprises improve their security posture across heterogeneous environments.

"At ForeScout, we are redefining what visibility means to the enterprise and stretching our value proposition to help organizations secure their network as they modernize their infrastructures for greater innovation and business efficiency," said Michael DeCesare, president and CEO, ForeScout. "Whether moving from a physical campus and data center to a software-defined, multi-vendor environment or adopting IoT devices, our customers rely on ForeScout to see and control the devices connecting to their network through our agentless approach to security."

With the rapid influx and diversity of devices connecting to enterprise networks and the ever-evolving cybersecurity threat landscape, organizations are struggling to keep their physical and virtual environments secure while embracing IoT and OT. Simultaneously, they are trying to manage resource and budget constraints as well as siloed security solutions. ForeScout is helping customers tackle these challenges by delivering a single solution that quickly discovers, classifies and assesses devices across an organization's infrastructure – from the campus to the data center and cloud.

News Highlights:
- **Out-of-the-Box Classification:** Device profiling and classification with an extensible taxonomy that automatically identifies and categorizes traditional devices as well as IoT, OT, mobile, and virtual endpoints. Organizations can use configurable profiling methods and out-of-the-box, or customized, rules to classify devices and apply context-based compliance, segmentation and control policies. A crowdsourcing model allows customers to opt in and share new IoT device fingerprints that can contribute to CounterACT's device profile library, enabling IoT adoption while preserving security.
- **Enterprise Scale and Resiliency:** To keep pace with the rapid increase in IoT devices, ForeScout's Enterprise Manager can now manage deployments of over one million devices to provide centralized monitoring, policy management and administration capabilities. New resiliency options help enable

customers to deploy a cluster of CounterACT appliances in a failover configuration to provide redundancy and service continuity without the need for idle standby appliances. Failover clusters can be deployed in single or multi-site environments and are managed via the ForeScout Enterprise Manager to provide resiliency and load redistribution in case of single or multiple points of failure.

- **Enhanced User Interface:** A redesigned and improved CounterACT console provides consolidated visibility, consistent policy management and customizable control actions across heterogeneous environments. With an enhanced device view, customers can quickly drill-down, filter and search through hundreds of device attributes for physical and virtual endpoints across campus, data center and cloud infrastructures, including IPv6 environments. CounterACT's easy-to-use policy engine with an innovative policy graph feature enables customers to create unified compliance, segmentation and remediation policies, as well as review the policy actions applied across their entire infrastructure.

Additional Resources:
- ForeScout CounterACT: https://www.forescout.com/products/counteract/
- Video: Redefining Visibility & Control from Campus to Cloud by Rob Greer, senior vice president of products and CMO, ForeScout
- 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.

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