Secure Cloud Computing

Extend visibility and control from your campus to your private and public cloud environments

Supported cloud platforms:

- VMware® vSphere
- Amazon® Elastic Compute Cloud (EC2)
- Microsoft® Azure

With the widespread adoption of cloud computing, enterprise security teams must see and control cloud-based workloads—just as they do with endpoints in campus environments. At Forescout Technologies, our approach to cloud security is a logical extension of securing managed, unmanaged and Internet of Things (IoT) devices in the physical world. In fact, Forescout secures cloud deployments using the same products and architectural flexibility that made us the leader in campus cybersecurity.

The Challenge

Companies are racing to realize the benefits of private and public cloud computing. As workloads move to the cloud, basic security issues must be addressed, such as tracking virtual servers, virtual machines (VMs) and cloud instances, as well as determining their security posture. Next, it is important to understand if they are secure and are assigned to the right security or port groups to ensure separation of different trust zones. Enterprises moving to the cloud must also be able to discover, classify and monitor devices, users and applications connected to cloud resources and take into account new tools, personnel and training that will be required for the cloud-computing environment.

Challenges

- Introducing unfamiliar tools, processes and methodologies hinders new technology adoption as it requires investing time for learning and training
- New operating environments and tools increase the security team's net Capex
- Integrating new tools into existing infrastructure and workflows is complex and disruptive, and its true impact is often underestimated

Forescout Solution

- **See:** Single pane of glass to discover, classify, monitor and manage the connection, state and security posture of physical and virtual endpoints across campus and cloud environments
- **Control:** Policy-based enforcement of rules and remediation of security gaps to reduce your attack surface and help improve compliance with industry mandates and regulations
- **Orchestrate**: Unify multivendor, cross-platform network security policies across virtual and physical infrastructures and cloud-based services

Forescout Benefits

- Reduce overall IT Capex and Opex by accelerating cloud adoption
- Leverage existing SecOps team, skills and processes; no new tools to learn
- Eliminate security management silos between campus and cloud teams
- Minimize errors by automating manual processes
- Use a single pane of glass to manage campus and cloud security

The Forescout Solution

There are fundamental similarities between the security principles and processes that are used to secure campus and cloud environments. Forescout physical and virtual security appliances deliver real-time discovery, classification, monitoring and policy-based management of devices as they connect to your campus or cloud network. Moreover, unlike traditional security management solutions, Forescout does not require onboard software agents or previous knowledge of endpoints. As a result, Forescout can offer a single-pane-of-glass perspective across campus and cloud environments so that you obtain visibility and control of physical devices, virtual machines and cloud instances irrespective of where they reside.

Regardless of environment, Forescout delivers value in three distinct ways:

See Security starts with visibility. Distributed infrastructure, devices, servers, users, applications and operating systems must be discovered, classified, monitored and managed to ensure secure computing in a campus or cloud environment. Forescout provides the visibility you need to protect your physical and virtual environments. Forescout's advanced visibility capabilities let you:

- Pinpoint virtual machines that lack up-to-date versions of VM software and security applications
- Identify virtual machines or instances that are located in the wrong zone (port group or security group, for example)
- Profile the guest operating system running on virtual machines and instances
- Identify peripheral devices on VMs
- Detect unauthorized access to and from cloud instances

Control Forescout can allow, deny or limit network access based on virtual machine posture and security policies. By assessing and remediating high-risk virtual machines and cloud instances, it mitigates the threat of data breaches and malware attacks that would otherwise put your organization at risk. In addition, by continuously monitoring VMs and cloud instances and applying controls in accordance with your security policies, Forescout dramatically streamlines your ability to demonstrate compliance with industry mandates and regulations. Among other things, Forescout's policy-based controls allow you to:

- Allow, deny or block virtual machines' network access by assigning or changing VM port groups or security groups
- Identify and block rogue virtual machines
- Enforce the use of approved golden VM images
- Remediate out-of-date virtual machines (OS patches, security applications, signatures and more)
- Restrict removable storage devices

Orchestrate Forescout integrates with virtual infrastructure, leading VM hypervisor management suites as well as cloud-based services. Forescout can trigger the installation of VM-specific tools and share real-time security intelligence across systems to enforce a unified network security policy that reduces vulnerability windows by automating system-wide threat response.

Forescout Benefits

One of the biggest challenges enterprises face with cloud adoption is to ensure security. While this may seem like a daunting task—especially in a new, relatively unknown environment—Forescout's solution lets you make the most of existing personnel, processes and technology, thereby significantly reducing capital expense (Capex) and operating expense (Opex) as compared to starting from scratch and deploying new security resources for your cloud environment. Since Forescout's solution provides a simple, single pane of glass for security operations (SecOps), enterprises can dramatically minimize the expense of additional tools and training, as well as vendor lock-in.

Forescout makes it easy to leverage trusted people, proven processes and the latest technologies across campus and cloud environments

Deploying Forescout Platform for Cloud Environments

Forescout is available as physical and virtual appliances. Its heterogeneous support offers out-of-the-box integration with leading virtual switches, physical switching and wireless infrastructure. This ability to run in both physical and virtual environments helps you centrally manage and enforce consistent security policies across campus and cloud environments using the same solution and management console.

***Notes**

1. Altman Vilandrie & Co. https://enterpriseiotinsights.com/20170602/security/20170602securitystudy-iot-security-breaches-tag23
2. Forescout analysis
3. ABI Research
4. Gartner Top Strategic IoT Trends and Technologies Through 2023, September, 2018

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

Learn more at Forescout.com