portnox™
boundlessly smart

DATA SHEET

THINK THE CLOUD ISN'T PART OF YOUR NETWORK?

Think again.

Portnox for Cloud Solution

As cloud based services become growingly popular for mission-critical business applications and for handling of sensitive information, companies face a new set of security challenges:

User identification and password management

Knowing who accesses your sensitive data is as critical with cloud-based services as it is with your physical network. The challenges are practically identical; whether its password fatigue, zombie accounts or phishing attempts resulting from the use of multiple passwords for multiple applications.

Real-time device identification and control

Controlling devices (not just "users") that access your on-demand applications is critical since rogue users can gain access through any IP device.

Location monitoring and control

Knowing and controlling the source of the access is crucial since users can also gain access from any browser regardless of its physical location.

Single directory integration

A unified integration capability with a company's local directory to federate across all corporate cloud applications.

ROI Management

CIOs need a real-time and coherent understanding of the business activities of their SaaS applications.

Mobile workforce

Existing VPN solutions, which direct connections via the corporate LAN, limit the capabilities of the cloud and increase the connection complexity.

KEY FEATURES:

- Seamless and comprehensive Single Sign-On procedure.
- User, device and application profiling and identification.
- Flexible and extended authentication policies.
- Customized enforcement based on device type, health, user, time of day parameters and more.
- Complete and robust Active Directory integration.
- Behavioral analytics of individual users, including administrative changes.
- Real-time, 24/7 detailed access and usage reporting that is integrated into an internal access management dashboard.

Online services such as Sales Force or Microsoft Office365 are an integral part of your network even if they are controlled by third parties and not hosted or maintained on premise. Eventually, such services host precious information of your company, and therefore should be able to be controlled and managed when it comes to access control. CIOs, CISOs and network managers need a solution to help them address these new challenges and move services to the cloud in confidence.

Portnox Solution

Portnox for Cloud extends your access management capabilities from the standard layers of Ethernet, switch or wireless antennas, into the realm of cloud (SaaS).
Designed from the ground up, Portnox Cloud allows you to stretch the corporate access management ability over the cloud layer and maintain a single, unified access control solution through:

Single Sign-On

Provides seamless SaaS log-in and log-out, automating user and password provisioning for corporate users.

Active Directory integration

Provides a single and comprehensive Active Directory integration capability that enables a uniform access mechanism for all users, using cloud-based applications.

Multiple authentication

Leverages your two factor authentication requirements, or any other extended model in use on premise with your SaaS application provider.

Extended enforcement

Enforces your access policies on the Cloud and controls access to applications based on device type, compliance, user, time of day parameters and more.

Behavioral analytics

Identifies usage patterns and provides visibility into individual user activity, including relevant administrative changes.

Centralized and customized audit and reporting

Provides real-time, detailed 24/7 access and usage reports, that are integrated into the centralized access management dashboard.

User, device and application profiling and identification

Manages and monitors all access activities providing full visibility of usage location, operation hours and traffic levels.

How it works?

The Cloud module stretches your network access control mechanism over the cloud by using a standard federation model (supported by SaaS vendors). Each connecting user is authenticated via a corporate identity, in addition to the SaaS identity, and is validated for usage of a corporate device.

Portnox for Cloud verifies compliance levels in terms of security components, such as anti-virus, to protect your precious assets on the cloud. Using a shared device which does not comply with Portnox's security policy is not granted with access to the service. The Cloud module doesn't require the user to 're-login' for the set access to the cloud which is free and is not limited by the corporate VPN transport.

Minimum Portnox System Requirements:

SOFTWARE	HARDWARE*
Operating System: • Microsoft Windows Server 2008 R2 **Database:** • Microsoft SQL server 2005 • Microsoft SQL server 2008 R2	**1 CPUs Dual Core Xeon 3.x** • Min of 4GB RAM • 72 GB of disk space • Single network adapter 100/1000 * Available also as virtual appliance

USA tel. +1.855.4portnox | usinfo@portnox.com | 623 Eagle Rock Avenue, Suite 396, West Orange, NJ 07052
UK tel. +44.1273.256.325 | dotell@portnox.com | 5 Albourne Court, Henfield Road, Albourne, West Sussex BN6 9FF
ISRAEL tel. +972.9.957.9889 | fax.+972.9.950.9879 | tellus@portnox.com | Elbe House, 33 Ben Gurion St., Herzlia 46785