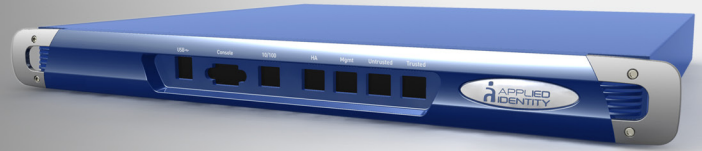


Identisphere™

Compliance and Protection for Critical Applications



Solutions

- Fastest Time-to-Value for Application Compliance**
 Cost-effectively meet your compliance-related requirements to protect sensitive data and legacy applications, with no application reengineering required.
- Beyond Guest Networks: Segregating Users and Resources**
 NAC solutions can provide guest access. Identisphere goes beyond this and helps protect against insider threats by regulating internal access to resources by groups such as employees, contractors, offshore development teams, and system administrators.
- Protecting Critical Applications**
 Improve business efficiencies by safely extending your enterprise network to remote sites, foreign offices or semi-public locations.

Benefits

- Saves Time**
 Deploys rapidly into your existing infrastructure
- Saves Money**
 Reduces administrative overhead and eases compliance burdens
- Saves Your Network**
 Applies the power of identity aware networking to protect your network from the inside

Controlling Access to Networked Applications

Today's enterprises are increasingly faced with the conflicting objectives of opening their network borders to diverse users (employees, guest, contractors, etc.) and endpoint devices (laptops, PDAs, etc.), and the need to ensure that critical applications and data are protected from unauthorized access. Added to these challenges are the various government and industry regulatory compliance mandates, many of which include the requirement to control access to sensitive data and require auditing of access to those resources by individual user identity.

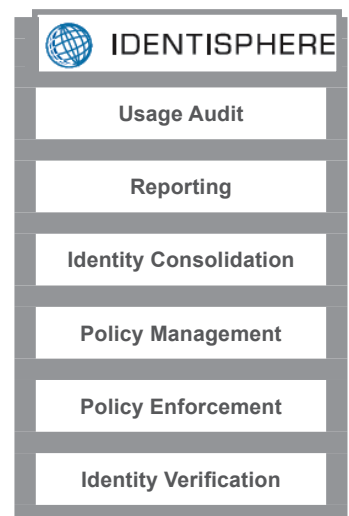
Current solutions used to control access to networked resources are insufficient as policies are based on access rights that apply to individual network IP addresses, physical network subnets, or Virtual Private Network (VPN) connections – all of which are at best, loosely tied to individual user identity. Further complicating the situation, user activity audit trails are often maintained in cumbersome log files and activity is tracked merely by IP address. Analyzing these log files and attributing activity to specific users or user groups is time consuming, costly and often impossible to do as many companies use dynamic IP address assignment each time a user accesses the network.

Building Policy into the Network

Applied Identity's Identisphere uniquely addresses these challenges by ensuring only authorized users and client applications can gain access to specific network resources. It does this by delivering network-level access policy management, enforcement, and auditing based on users' enterprise identities and on run-time validation of users' client applications. Identisphere deploys quickly into existing network infrastructures with no need for "rip-and-replace" upgrades and supports both wired and wireless networks. Since enforcement takes place at the network level, it delivers access control and accountability without the need for application integration or systems reengineering.

Applied Identity's Identisphere enables:

- Auditing of user access activity which can be used to quickly define access policies and generate user-based compliance reports
- Centralized network policy administration and monitoring, greatly reducing administration time
- Consistent enforcement of policies for any user accessing the network from any location, reducing the risk of security breaches
- Real-time consolidation of user identities across multiple identity stores without the need to deploy directory synchronization or metadirectory solutions
- Transparent integration with virtualized application and desktop delivery infrastructures to protect backend resources from unauthorized user access and enforce user-based resource segregation
- Easy integration into enterprise network environments leveraging existing identity stores



Identisphere Components

Identisphere Manager

Is the central interface for the creation and management of access policies. It integrates with LDAP directories to leverage enterprise user identities, roles and access policies.

ID-Audit

Provides a central repository of audit data on user behavior and resource usage. Enables the creation of real-time views and historical reports that can be used to create policy via a "one-click" Global, User or Exception policy implementation.

ID-Unify

Consolidates user identities between multiple and disparate identity stores, creating a virtual mapping and normalization of user information.

ID-Enforce

ID-Enforce is an identity aware network enforcement solution that enables enterprises to embed identity and access policy control into the network, reducing operating costs and complexity.

ID-Enforce VA

ID-Enforce VA delivers the functionality of ID-Enforce and the convenience of a virtual appliance, allowing you to deploy Identisphere network policy enforcement and control points rapidly anywhere you need them.

ID-Mark

In environments that require an increased level of accountability and non-repudiation of events, an optional ID-Mark™ client agent can be installed on the client workstation to further enhance security.

Identisphere Enables Access Policy Lifecycle Management

Controlling access to the network should be viewed as a lifecycle as it requires careful ongoing assessment and management to accommodate changes. Identisphere uniquely meets these challenges by providing solutions that fully address all stages of creating, maintaining and enforcing the Access Policy Lifecycle process.

Audit

The initial step in the process is to establish a baseline by identifying current network resource activity to gain visibility into which users are accessing the network resources, when they are being used and how those users are granted access. Identisphere's ID-Enforce solution is deployed inline and can be placed in front of a data center, at the entry point of a network segment, or at a remote location. There is virtually no setup required to deploy ID-Enforce in "Audit Mode" – which baselines user activity and creates a log of resource usage. The information collected forms the basis of reports used to create network access policies for enforcement.



Unify

Identisphere provides the solution for quickly consolidating identities across multiple user identity stores to support enterprise and cross-agency deployments. Identisphere's ID-Unify creates a virtual identity mapping or normalization of user identities between identity stores – without duplication of identity objects and attributes and without changes to existing identity stores - dramatically reducing operational costs and complexity.

Define and Simulate

Authorization policies are created leveraging data from generated Network Activity Assessment reports and are based on roles or individual identities defined within the existing directory services. Identisphere Manager, Identisphere's centralized management console, automates the process with "one-click" policy creation and easy client application whitelist management. Once policies are defined, Identisphere's exclusive simulation capability allows them to be evaluated in real time against live traffic, avoiding potential service disruptions from inappropriate policy changes.

Enforce

Users are either granted or denied access based on the policies assigned to their identity, as well as on run time validation of their client applications. ID-Enforce obtains access policies for each user after they have been authenticated to the network, and applies these consistently regardless of endpoint device or how (LAN, WAN, remote/VPN, wireless) they are attaching to the network. Identisphere reduces the risk of unauthorized access to applications and data by providing each user with visibility only to the networked resources for which they are granted access.

Audit

Assessment of user activity must be ongoing – for refinement of access policies, behavioral analysis, forensic analysis, as well as for audit of regulatory compliance related to control of user access to confidential data. ID-Enforce creates a log of each user's network activity by user ID, IP address, network resources accessed, client application and a time stamp. Reports are available via Identisphere Manager and log data can be sent to third party applications for further analysis.



188 South Murphy Avenue
Sunnyvale, CA 94086
Phone: 888.286.7336
Fax: 415.593.2101
www.appliedidentity.com



Arrange a FREE network audit that will tell you who is accessing what resources and when on your network.
Call 888.286.7336 - Email: sales@appliedidentity.com