NetworkingPS Security Management Services
Overview

ABOUT NETWORKINGPS

NetworkingPS (NPS) is a mid-sized Information Technology professional services firm based in Piscataway, NJ, specializing in a wide variety of managed security services offerings. Leveraging their highly-skilled staff of professional consultants, NPS has earned a reputation for their proficiency in planning, designing, assessing, implementing and supporting systems, applications, networks and operations activities for their nationwide, cross-industry client base.

Industry research shows that clients today want an open computing environment in conjunction with an open marketplace with alternate channels of distribution. In addition, organizations wish to integrate new technology into their existing systems, as well as have both their computing resources and user base managed and supported in a cost-effective manner that will support their business priorities.

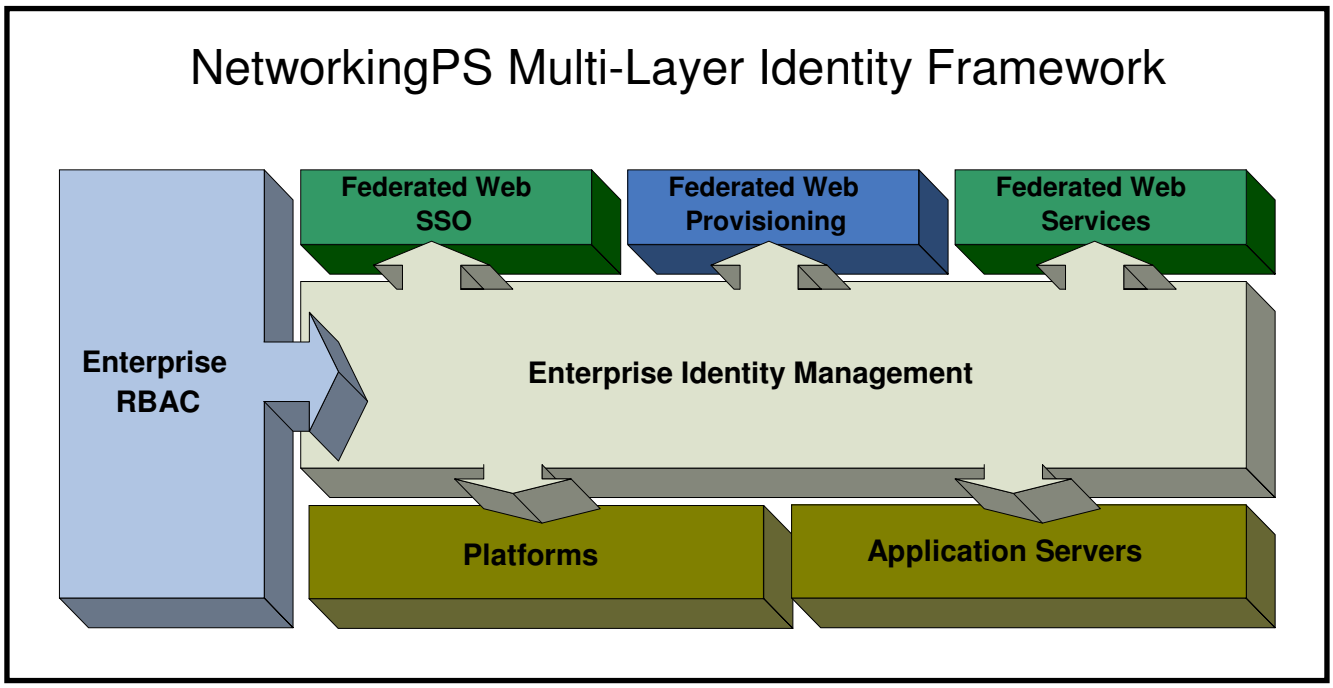
NPS is responding to these customer requirements by focusing its resources on helping customers plan, build, implement and maintain the business information systems, networks, and operations they need to compete in today's changing business environment. Building on its core competencies in software, systems, networks, and services, NetworkingPS provides a complete range of information processing solutions.

Thought leadership is critical to NPS's work as a Professional Services Firm. The ability to stay ahead of industry trends – to understand shifts in customer expectations and new technologies- is fundamental to our ability to guide our clients to the right solutions. Collaborative discussion and problem solving generates far greater results than independent, heads-down research and development. By bringing together the industry's best minds and most experienced resources, NetworkingPS and its customers have benefited from the interaction and shared experiences that occur during projects, all of which look beyond the present and beyond the technology, to create better, long-term operability for the future.

END TO END IDENTITY MANAGEMENT STRATEGY

As the global marketplace continues to expand, new and innovating ways of conducting business are becoming a necessity in order to maintain corporate security practices and remain in compliance with existing governmental regulations. In order to keep sensitive data within the hands of the right people, more and more corporations are seeking out multi-layer identity management solutions. Although the core of any robust Identity Management (IdM) architecture lies within its user provisioning capabilities, there are multiple components necessary to keep application data secure.

NPS promotes a bottoms-up approach in its product and services offerings that span every aspect of identity management, from basic to more advanced user lifecycle management activities.



NetworkingPS product and services offerings span every layer of identity management, from federated user provisioning and detailed role management activities, to basic user provisioning.

NPS product and services offerings all correspond to this multi-layer model of identity management, from fundamental user provisioning and administrative capabilities to fine-grained application role management. The NPS end-to-end identity management strategy consists of the following elements:

- **USER PROVISIONING**
  - Automated Account Management
  - User Lifecycle Management
  - Real-time Administration of User Privileges and Attributes
  - User Event Logging
  - Password Management
  - Reporting

- **ROLE MANAGEMENT**
  - Discovery, Definition and Cleanup of Existing Roles through Automated Role Mining
  - Real-time Enforcement of User Roles
  - Enterprise-wide management of formal and informal business-level roles
  - Linkage between business roles and IT roles
  - Lifecycle Management of Roles: role owner, role changes, role review, role assignment and role retirement
  - Creating a consistent development process for new roles and tying those roles into an automated role management solution

- **ACCESS MANAGEMENT**
  - Single Sign On for Web-based Applications and Web Services-Enabled Applications
  - Token Exchange between Federated and Enterprise Applications
  - Single Sign On for Federated Applications/Cross-Domain SSO
  - Defined user access controls based on minimum required necessary to perform job functions

IDENTITY MANAGEMENT SERVICES

The Challenge:

Managing your environment with respect to Security can be a time consuming endeavor. Some of the typical day-to-day issues facing IT Security Managers are:

- Identity lifecycle management (user self-care, enrollment and provisioning)
- Identity control (access and privacy control, single sign-on and auditing)
- Identity federation (sharing user authentication and attribute information between trusted Web services applications)
- Identity foundation (directory, directory integration and workflow)
- Strong Audit Control (purge of invalid accounts)
- Password Reset Automation and Self-Service
- Automated starter/leaver process

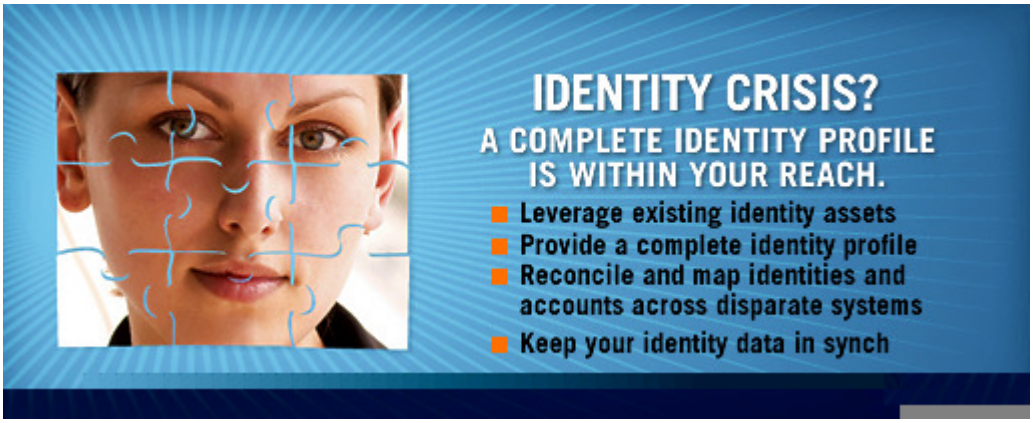
The Solution:

NPS can help you determine and implement the optimum management infrastructure for your Security Environment. We can provide:

Current Environment Assessment – While clients are preparing to move into the Identity Management arena, gaining a detailed understanding of the current environment is critical to moving into the design phase. At NetworkingPS we have broad based experience in performing detailed assessments which include documentation of current state user management, current state use cases, and recommendations to move to a proper IdM solution.

Requirements Gathering – Many clients have vision of what they want from an Identity Management solution, but are not totally clear on all of their requirements. In order to properly develop a detailed solution design, having a solid set of requirements for each of the areas to be addressed ensures that project objectives are understood and designed accordingly. We have worked with clients in great detail to extract requirements that will help them achieve their goals, while at the same time recognize value at each stage of the deployment.

Detailed Solution Design – At NetworkingPS we believe that the solution design is the apex of a successful deployment. Taking into account the information obtained from the assessment and requirements gathering activities, we develop a detailed solution design that becomes the blueprint for all deployment activity. This solution design includes:



- Identity Management Architecture
- Technical Design
- Hardware Specifications
- Operational Model
- Workflow Design
- Process Re-engineering
- Role Based Engineering (RBAC)
- System Support Model
- System Test Cases
- Future State Use Cases
- Implementation Project Plan Detail through Platform Deployment and Application Integration
- Knowledge Transfer Plan
- Business Continuity Review
- IdM Configuration Parameters
- Provisioning Policies
- Customization Specifications

Implementation Services – We employ highly trained, detail oriented, seasoned individuals. Our staff is well versed in utilization of best practices and driving value at each stage of the implementation. We work as a unified team with the client to ensure that knowledge transfer is taking place throughout the engagement, enabling self sufficiency at the conclusion of the engagement.

Performance Tuning and High Availability Consulting- Over time, as you add features and functionality to your Identity Management environment, you may be impacting the overall performance of your system. Through proven methodologies and procedures, NetworkingPS can increase the performance of your ITIM configuration to obtain the best results possible. These results are recognized in the form of improved response time, increased user concurrency, and decreased cost from not purchasing additional hardware until absolutely necessary. Understanding and correct execution of configuration of the software, application and operating system dependencies is a task best left for experts with experience. At NetworkingPS we have the experience to perform these tasks.

PROJECT EXPERIENCE

NPS has experience in a number of projects in Identity Management and Role Based Engineering, including the following:

- Performed an assessment, solution design, and implementation for a 1 million + user environment in support of an IBM Tivoli Identity Manager deployment
- Defined the roles, associated provisioning policies, and entitlements to support the aforementioned project
- Established a $5M+ Enterprise wide Identity and Access Management (EIAM) reference architecture for the Enterprise
- Created full life-cycle technical engagements for multiple Security Management solutions
- Helped clients understand key security and privacy issues, risks, exposures and vulnerabilities.
- Recommended Identity, Access Management and RBAC (Role Based Access Control) solutions to address those issues.