

## WHITE PAPER

---

# Pushing Security to the Perimeter: Trusted Computing Technology Adapts to Changing Enterprise Needs

Sponsored by: ProCurve Networking by HP

---

Sally Hudson  
February 2006

## IDC OPINION

Today, enterprise organizations are laden with the burden of ever-increasing security threats. IT professionals must continuously strive to keep both malicious users and software away from the network, while allowing the approved users access to the right resources at the right times. Identity and access management has risen to assist the IT organization in regaining and maintaining control over the users on their network.

Complicating the access challenge is increasing user mobility, combined with new and different device types capable of accessing network resources. Today's enterprise requires a network that can be controlled centrally, but capable of pushing access and administrative policies to the amorphous edge. Here, at the edge, properly configured and deployed physical network connection devices can quickly approve or deny access of users and/or devices — effectively stopping potential threats before they enter the network.

ProCurve's Identity Driven Manager 2.0 (IDM) is designed to provide this type of intelligent security for IT organizations. As part of ProCurve's Adaptive EDGE Architecture and based on Trusted Network Connect architecture open standards, ProCurve's IDM provides the IT organization with the ability to manage access to their network resources in a highly flexible, scalable and reliable manner. IDC believes a solution such as ProCurve's IDM, when properly implemented, can significantly reduce bandwidth and administration costs, while increasing security and providing reporting capabilities for regulatory requirements.

## METHODOLOGY

IDC wrote this white paper in Fall 2005. It is based on historical and current primary research.

The IDC software market sizing and forecasts are presented in terms of "packaged software revenue." Packaged software is defined as programs or codesets of any type commercially available through sale, lease, or rental, or as a service. Packaged software revenue typically includes fees for initial and continued right-to-use packaged software licenses. These fees may include, as part of the license contract, access to product support and/or other services that are inseparable from the right-to-use license fee structure, or this support may be priced separately as software maintenance. Upgrades may be included in the continuing right of use or may be priced separately.

Packaged software revenue excludes service revenue derived from training, consulting, and system integration that is separate (or unbundled) from the right-to-use license, but includes the implicit value of software included in a service that offers software functionality by a different pricing scheme (e.g., the implicit or stated value of software included in an application service provider's (ASP's) or other hosted software arrangement). It is the total packaged software revenue that is further allocated to markets, geographic areas, and operating environments. The software revenue forecasts presented in this study represent IDC's best estimates and projections based on the following:

- ☒ Reported and observed trends and financial activity in 2004 as of the end of January 2005, including reported revenue data for public companies trading on North American stock exchanges (1Q04–3Q04 in nearly all cases, plus 4Q04 where available).
- ☒ Additional modeling to fill in any information gaps using a top-down/market-level approach to estimate overall 2004 market sizing.
- ☒ Bottom-up regional forecast growth rates provided by IDC analysts in each geographic region.
- ☒ Bottom-up/company-level data collection began in March 2005, with in-depth vendor surveys and analysis to develop detailed 2004 company models by market, geographic region, and operating environment. This activity will form the basis of vendor share, updated forecast, and competitive analysis studies that will appear later in the year.

In addition, please note the following:

- ☒ The information contained in this study was derived from the IDC Software Market Forecaster database as of March 15, 2005.
- ☒ All numbers in this document may not be exact due to rounding.
- ☒ For more information on IDC's software definitions and methodology, see *IDC's Software Taxonomy, 2005* (IDC #32884, February 2005).

Augmenting this research, IDC talked to customers and vendors affected by the challenges of deploying and maintaining an effective identity and access management (IAM) system.

## **IN THIS WHITE PAPER**

This IDC white paper reviews the growing need for network-based security as a fundamental component in the IAM market. Security concerns, identity theft and regulatory compliance requirements are converging to drive the need for strong IAM solutions within the enterprise. IDC defines IAM solutions as a comprehensive set of technologies used to identify users in a system by associating user rights and restrictions with the established identity. These solutions can include enterprise single sign-on (SSO), legacy authorization, user provisioning, advanced authentication hardware and software, and other endpoint security solutions. We also profile the ProCurve Identity Driven Manager 2.0 with Adaptive EDGE Architecture to illustrate a cost-effective IAM solution that can help enterprises address their concerns while adding value to their networks.

## SITUATION OVERVIEW

The IAM market is a comprehensive set of solutions used to identify users (such as employees, customers, or contractors) in a system. These solutions control the users' access to resources within that system by associating rights and restrictions with the established identity. In general, this is accomplished through the use of some or a combination of the following: Web SSO, host SSO, user provisioning, advanced authentication, legacy authorization, and directory services. Each of these services can be critical components of IAM. IDC defines each of these components as:

- ☒ **Advanced Authentication:** This software includes tokens and it is designed to support hardware authentication solutions such as smart cards or biometrics. It also covers many services associated with the creation, dissemination, validation, and protection of digital certificates.
- ☒ **Web Single Sign-On:** This software enables the enterprise to administer and consistently enforce user access to Web applications and provides SSO services to users. Web SSO provides Web application security and identity management to employees, customers, partners, and contractors.
- ☒ **Host Single Sign-On:** This software enables users to log in to internal applications, databases and other corporate systems with just one identity. This solution enforces password policies and eliminates the need for employees to remember multiple passwords.
- ☒ **Legacy Authorization:** This software includes mainframe access control products. Access control is primarily used on large computers such as services and mainframes, and very rarely on personal workstations.
- ☒ **User Provisioning:** This software automates the process of granting access rights, automates the changing of those rights, and, in some cases, audits the appearance of inappropriate rights in users' profiles.

With increasing threats of viruses, fraud and identity theft complicated by constricting regulations, enterprises are throttling their networks in an attempt to gain control over what touches and, thus, impacts their networks. From new policies and software to new appliances, enterprises are experimenting with a wide range of solutions trying to stay ahead of potential security breaches while meeting increasing regulatory requirements. Given the depth and breadth of many organizations, finding the right well-integrated solution capable of meeting the majority of needs, from both a business benefits and security perspective, is challenging.

Out of sheer frustration, some enterprises have resorted to simply turning off everything and only allowing certain trusted sources to interact with the network. This is neither a foolproof nor a completely secure method. Common complaints with this approach center on the fact that it often makes access more difficult for users and chokes the actual business processes as well as the threats.

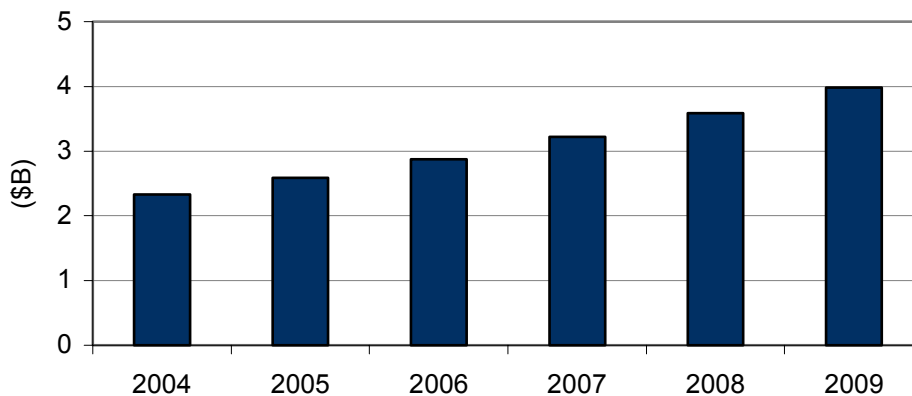
The constantly rising tide of threats has resulted in government reaction not just in the United States, but also on a worldwide basis. New legislation and regulations seem to be appearing on an almost daily basis. Unfortunately, much of this legislation is ambiguous in nature and actual recommendations to address these issues and solve these problems are vague at best. This has not prevented the addition of rather stiff penalties and fines for those individuals and corporations who willingly or neglectfully choose non-compliance. To ensure the avoidance of penalties, many enterprises and their management are sharply attentive and concerned for their need to comply appropriately in a timely manner, and, therefore, are evaluating a wide range of IAM solutions.

### **The Need for Identity and Access Management in Enterprise IT**

IDC forecasts the IAM market to grow from US\$2.3 billion in 2003 to almost US\$4 billion in 2009 (Figure 1). The IT environment will continue gaining in complexity as the enterprise increases the resources (both people and electronic) upon which it is reliant. The IT organization requires proper IAM solutions to maintain control of the IT environment. IDC advocates a standards-based approach as key to long-term success in this effort. By utilizing a standards-based approach to managing identity and access (such as the Trusted Computing Group's Trusted Network Connect standard), the enterprise will be positioned to provide greater interoperability with new services and requirements. ProCurve's Adaptive EDGE Architecture with Identity Driven Manager 2.0 is an example of an IAM solution that provides a standards-based approach.

**FIGURE 1**

Worldwide Identity and Access Management Revenue, 2004-2009



Source: IDC, 2005

Research shows that IAM is growing significantly in the enterprise IT environment. Unfortunately for IT organizations, complexity is growing at the same rate. No longer is the IT organization dealing with users sitting at desktops or logging into mainframes. Now, they are dealing with wireless networks, remote home offices, guests, visitors, customers, partners, vendors and more all wanting access to the enterprise's network resources. The possible access permutations are truly endless, and the IT organization is tasked with the extremely difficult job of providing the right access to the right users and at the right time in a 24/7 environment.

This complexity essentially requires most organizations to adopt a SSO solution to assist their users with password management, and to increase the security of their networks by increasing the amount of control the IT organization has, and how the end user manages his or her passwords. It gives the user easier methods of password management, and can be configured to force regular password changes — a policy that reduces the chance of a security breach through carelessness.

IT organizations are also shifting toward more centralized, IT-driven provisioning systems as they recognize the inherent security benefits. A more centralized provisioning system allows the IT organization, and thus the broader enterprise, greater control over who has access to which corporate resources and when. A contractor might have access to certain resources from within the building and during regular business hours. Once outside the building, in an unauthorized part of the campus, or after business hours, that contractor's rights would be restricted. With centralized IT services, it becomes much easier to record, track and audit the identity and access of users. This assists the enterprise in complying with the many layers and levels of governmental regulations.

Additionally, the enterprise seeks to push much of the intelligence of their network to the edge, where the user and the application really connect. Moving the authorization process out to the edge provides the enterprise with a number of benefits, such as:

- Reduced bandwidth requirements
- Administrative time savings via dynamically provided access
- Increased security by providing the correct rights to the users from the moment they touch the network

---

## **ProCurve Networking**

As enterprises struggle with the increasing need for mobility, security and flexibility in their networks, vendors work to provide answers to those challenges. Networks are becoming less centralized and more distributed as the intelligence is pushed away from the core and closer to the user. Vendors such as ProCurve are working to develop new, flexible architectures to help their customers push the intelligence of the network from the core to the edge. In the case of ProCurve, the solution is called the "ProCurve Adaptive EDGE Architecture."

Since users and their access to applications connect at the edge, this is the first point of entry and an ideal place for the network to determine how to handle the traffic. Certain security policies should be enforced from the perimeter inward, since topologies that require decisions be made from the core of the system often impede the process and negatively impact the performance and scalability of the network. This "core-approach" also requires much greater demand on network bandwidth.

When security access is enforced at the edge, the opportunity for attacks is minimized — providing that the location where access is physically attained and where authorization is granted are closely linked.

By utilizing architecture such as Adaptive EDGE, access decisions can be made automatically. Known users can be immediately granted their previously assigned services, and unknown users may be provided with guest access, or no access at all. With the increasing security threats from every direction, it becomes imperative for security to be controlled at the center and enforced at the edge. Adaptive EDGE has been designed to allow the IT organization to accomplish this, as it supports both centralized and distributed network cores.

A fundamental benefit derived from architecture such as ProCurve's Adaptive EDGE is that it is built upon the policies of broad interoperability. ProCurve is a member of the not-for-profit Trusted Computing Group (TCG) organization. TCG was initiated to develop open specifications for trusted computing and security technologies for both hardware and software. Membership includes leading component manufacturers, and a large number of PC manufacturers, as well as a host of other companies. TCG's goal is to provide protection from software and network attacks available across a broad range of computing devices with common software interfaces. Within TCG, the Trusted Network Connect Sub-Group (TNC-SG) is tasked with defining and promoting an open solution architecture enabling network operators to enforce policies at the network edge to determine whether to allow access to a requested network resources.

The ultimate aim of the TNC-SG is to provide a framework and architecture that can be developed to achieve a vendor neutral and interoperable network standard with the following features (source: Trusted Computing Group):

- ☒ **Platform Authentication:** The verification of a network access requestor's proof of identity of their platform and the integrity-status of that platform.
- ☒ **Endpoint Policy Compliance (Authorization):** Establishing a level of 'trust' in the state of an endpoint, such as ensuring the presence, status, and upgrade level of mandated applications, revisions of signature libraries for antivirus and intrusion detection and prevention system applications, and the patch level of the endpoint's operating system and applications. Note that policy compliance can also be viewed as authorization, in which endpoint compliance to a given policy set results in the endpoint being authorized to gain access to the network.
- ☒ **Access Policy:** Ensuring the endpoint machine and/or its user authenticates and establishes their level of trust before connecting to the network, leveraging a number of existing and emerging standards, products, or techniques.
- ☒ **Assessment, Isolation and Remediation:** Ensuring that endpoint machines that do not meet the security policy requirements for "trust" can be isolated or quarantined from the rest of the network, and, if possible, an appropriate remediation applied, such as upgrading software or virus signature libraries to enable the endpoint to comply with security policy and become eligible for connection to the rest of the network.

By adhering to TNC specifications and architecture, enterprises ensure hosts are interoperable with their network while providing a minimum level of compliance to organizational policies for network access. Policies can include services such as firewalls, antivirus checkers, application patches and intrusion detection systems. IDC believes enterprises can achieve stronger security, higher network efficiencies and greater flexibility by deploying an architecture based on open standards and interoperability. An example could be illustrated using ProCurve's Adaptive EDGE Architecture. Using this framework, an enterprise could elect to add modules to further increase certain aspects of the network's robustness, and an important element of this type of security could be derived from a product such as ProCurve's Identity Driven Manager 2.0.

---

## **ProCurve's Identity Driven Manager 2.0**

Released in the fall of 2005, ProCurve's Identity Driven Manager 2.0 (IDM) was created to help enterprises decrease operations costs, improve productivity and reliability, and protect their technology and business investments. Faced with the onslaught of viruses and other security threats, enterprises are looking for new ways to manage a wide variety of users accessing the network from a wide variety of places, and looking to utilize a wide variety of resources. Based on the philosophies espoused by TCG, the IDM has two key principles: placing control out at the edge of the network, and providing command from the center. IDM dovetails neatly into ProCurve's Adaptive EDGE architecture and provides the IAM that enterprises need to help make their organizations more efficient, and their network more reliable and secure.

ProCurve's IDM dynamically assigns access rights to users (identities) on the network based on the user, their location and the time of day. It allows for easy creation and management of user policy groups. IDM's management policies set network parameters to provide desired network functionality. This allows the administrator to set parameters on bandwidth limits, or quality of service based on user/group, time, location, device ID and client integrity status. IDM allows the enterprise to centrally control and manage all users touching the network regardless of time and place. User access is controlled at the edge, where end-user devices physically touch the network. This approach can reduce the security exposure incurred by having all authentication architected to reside centrally in the network core.

### ***Features of IDM 2.0***

#### **Command From the Center**

- Centrally manage which users are members of which access policy groups, and what network access rights are given to that group.
- Access policy information is distributed to IDM "Agents" integrated on RADIUS authentication servers in the network.
- IDM is designed to integrate easily with ProCurve Manager Plus, which can be integrated with OpenView's Network Node Manager.

#### **Control at the EDGE**

- Triggered by a secure user login, IDM dynamically sets parameters in ProCurve edge devices, enforcing the centrally defined policies (access rights, priority and bandwidth).
- At logoff or disconnect, the policies are discarded and the port blocked until a new user authenticates and new policies are loaded.

#### **Synchronization of Information From the Enterprise Directory**

- The enterprise can import user and group data from Active Directory, other LDAP directories or via XML, as well as defining the Default Access Policy for users who are not yet assigned to a Policy Group.

#### **Endpoint Integrity Checking as Part of the Policy Decision**

- IDM integrates with the Trusted Network Connect Architecture.

#### **Increased Fine-grained Access to Network Resources**

- The enterprise will set user-based access control lists (ACLs) as part of the network policy, and IDM provides an easy-to-use ACL builder based on network resources (such as servers and services).

#### **Automated and Enhanced Reporting Capabilities**

- IDM is able to track detailed network usage by user or policy group, and provides alerts for access setting that cannot be implemented by access devices. Also, detailed session reports provide ability to audit network access. IDM allows for 30 days of user-selectable history, and reports can be scheduled to run at regular intervals.

The latest version of the product supports a range of industry leading RADIUS servers, including Funk Steel-Belted RADIUS on Windows and support for freeRADIUS on Linux platforms is planned for the first half of 2006. The product also provides integration with ProCurve Secure Access 700wl series products. Initial access deny decisions made by IDM will be honored by Access Control Server, and IDM will pass on the user's group membership for the Access Control Server to use.

## **FUTURE OUTLOOK**

IDC believes the IAM market will grow (11.3 %) from 2004 through 2009. Given the current market conditions of rampant viruses, security threats and still growing regulatory requirements, it is no surprise that enterprises want strong, yet efficient and easily managed IAM technologies to help them face their challenges. ProCurve continues to participate in standards efforts within the Trusted Computing Group and other standards bodies, in order to standardize the technologies around security network access.

By focusing on an open standards-based solution such as ProCurve Adaptive EDGE Architecture with Identity Driven Manager 2.0, the enterprise will gain the many benefits of utilizing an architecture based on open standards, including product interoperability, network flexibility, and strong security reliability.

## **CHALLENGES**

The addition of IDM 2.0 to the ProCurve Adaptive EDGE architecture can provide the enterprise with several key benefits drawn from its ability to dynamically assign the appropriate access rights to users from policies based on the identity of the user, his or her location, and the time they are trying to access network resources. These abilities can help prevent over-provisioning, save administration time, protect existing business assets, and preserve investments in technology through the utilization of open standards.

The challenge for ProCurve in this area is to educate the IT organization as to the value of endpoint, or perimeter-focused security beyond the aspect of the firewall/VPN devices. This can be accomplished by demonstrating the value of this approach through proof of concept resulting in decreased network bandwidth consumption, the benefits of central administration, and the true viability of intelligent access controls at the perimeter points of an organization.

## **CONCLUSION**

The IT enterprise today is engaged in ongoing battles against an onslaught of existing and emerging security threats to the network infrastructure. This effort takes its toll in terms of resources, draining the IT organization and complicating the enterprise's ability to do business. Increasingly, regulations are requiring enterprises to protect and monitor who has access to the most sensitive of data that the corporation holds — whether it is the accuracy of its financial data, or the private data of employees and customers.

An IAM solution that is incorporated into the infrastructure of an organization is crucial to the enterprise's ability to protect its important data and resources. As users become more mobile and diverse, the challenge of managing who is on the network and when has increased dramatically. By selecting a flexible, open-standards network architecture, such as that outlined by the Trusted Network Connect standards, the enterprise can more efficiently centralize its policies and commands, while pushing the enforcement of those policies out to the edge.

ProCurve's Identity Driven Manager, coupled with the Adaptive EDGE Architecture, can offer a solution that allows the IT manager to centralize policies, user groups and access rights, and then push those policies to edge devices for automatic provisioning of users with the appropriate rights and privileges. This approach can help the IT organization to prevent over-provisioning, save administration time, and protect business assets through better and more efficient user identification and access management.

---

## **ABOUT THIS PUBLICATION**

This publication was produced by IDC Go-to-Market Services. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Go-to-Market Services makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of nor opinion on the licensee.

---

## **Copyright AND RESTRICTIONS**

External Publication of IDC Information and Data — Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason. Translation and/or localization of this document require an additional license from IDC.

For permission requests contact the GMS Asia/Pacific team at +65.6228.7749 or [gmsap@idc.com](mailto:gmsap@idc.com). For more information on IDC visit [www.idc.com.sg](http://www.idc.com.sg). For more information on IDC GMS visit [www.idc.com.sg/gms](http://www.idc.com.sg/gms)

Copyright 2006 IDC. Reproduction is forbidden unless authorized. All rights reserved.