

# Cool Vendors in Identity and Access Management, 2009

Gartner RAS Core Research Note G00165391, Ray Wagner, Avivah Litan, Ant Allan, Lawrence Orans, Earl Perkins, Mark Nicolett, 17 March 2009, R3034 10012009

**Identity and access management (IAM) technologies are changing rapidly in response to evolving business needs and threat environments. Chief information security officers (CISOs) and other security decision makers need to familiarize themselves with the emerging technologies presented by Gartner's Cool Vendors and other leading-edge providers.**

## Key Findings

- Gartner's Cool Vendors in IAM offer innovative solutions for the requirements of specific use cases and market segments, including the demands of small and midsize businesses (SMBs) and distributed computing environments.
- Many of these Cool Vendors, and the emerging technologies they offer, target enterprises and other businesses that are looking for low-cost or low-entry-point solutions — a key competitive differentiator in a time of constrained IT and IT security resources.

## Recommendations

- Consider innovative products and services — including those from Gartner's 2009 Cool Vendors — when considering solutions for IAM issues.
- Don't base product or service implementation decisions for IAM or any other security-related area on technological innovation alone. Consider real-world workability in addition to vendor capability and viability as key selection criteria.

## ANALYSIS

This research does not constitute an exhaustive list of vendors in any given technology area, but rather is designed to highlight interesting, new and innovative vendors, products and services. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

### 1.0 What You Need to Know

The product and service providers that Gartner has chosen as its 2009 Cool Vendors in IAM share a commitment to leading-edge technological innovation. However, these choices are set apart by a trend toward delivering cost-effective, low-risk IAM — an understandable focus in a time of highly constrained IT, IT security budgets and personnel resources.

Most of these Cool Vendors' offerings are oriented toward delivering low-cost or low-point-of-entry IAM solutions that require limited changes in hardware and software configurations, and that integrate as unobtrusively as possible with existing computing and business environments. Gartner clients in this market segment and others are clearly more risk-averse than they have been, and are looking for IAM solutions that can be piloted or implemented as easily and inexpensively as possible.

Even in today's complex and volatile business environment, however, there is considerable room for real technological and process innovation, as these Cool Vendors show. For assessments of Cool Vendors in two other important security market segments, see "Cool Vendors in Infrastructure Protection, 2009" and "Cool Vendors in Software-as-a-Service Security, 2009."

## 2.0 AdmitOne Security

Issaquah, Washington, USA ([www.admitonesecurity.com](http://www.admitonesecurity.com))

*Analysis by Avivah Litan*

**Why Cool:** AdmitOne Security, founded in 2006, markets a comprehensive fraud-detection solution that grew out of its core biometric authentication technology, which is based on end users' keyboarding patterns. (The company changed its name from BioPassword in 2008, when it introduced additional layered security features that augment its biometric authentication.) The integrated AdmitOne solution enables a strong, additional layer of security that doesn't require changes in user behavior, or in hardware or software configurations. User keyboarding patterns can be established gradually, after only a few interactions, or can be established immediately during user enrollment in the system.

The biometric technology is surrounded by fraud-detection features that analyze device login characteristics (for example, device identification and geographical location) and user transaction behavior, as well as other fallback authentication methods (such as predetermined question-and-answer, which is invoked if keyboarding patterns aren't recognized). Keyboarding profiles or templates for an individual user — which improve over time — can typically be established after three to five samples, but up to 15 samples are required about 5% of the time.

The AdmitOne solution helps to prevent account takeover and unauthorized access to digital subscription services, content or other Web-based customer services (such as online testing). This application can be inserted or eliminated without any disruption to the user experience, and without the user's knowledge. To date, AdmitOne has acquired more than 125 customers and has established a good service record with them.

**Challenges:** AdmitOne's biometric technology is generally effective, but it isn't 100% reliable. An enterprise will sometimes find it difficult to build a template for a customer, and will need to establish a more-gradual enrollment process with that customer's template improving over time — for example, after 15 typing samples are collected. Some users will face difficulties in gaining access to their accounts — among them the elderly and infirm, whose hands may shake, thereby making their keyboarding patterns inconsistent. In cases such as these, the enterprise can choose to lower the threshold of acceptable risk and enable lower-risk transactions under specified conditions based on established business rules.

AdmitOne has acquired more than 125 customers and established a good service record, but remains a small "startup" and hasn't yet achieved profitability. For this reason, the company may continue to encounter resistance from prospective customers that would prefer to engage with a larger vendor that's perceived as more stable. AdmitOne's newer fraud-detection solution should provide sufficient backup and fallback methods for cases where user keyboarding patterns aren't recognized, but the complete solution is relatively new and hasn't been proved in production environments.

**Who Should Care:** IT and e-commerce personnel who are involved in user authentication and fraud-detection strategies and projects should familiarize themselves with AdmitOne's offering. Managers who wish to regulate the use of digital subscription or content services and distribution should consider AdmitOne Security for transparent user authentication, especially when they want a solution that doesn't require changes to end-user behavior or to hardware or software configurations.

## 3.0 Apere

San Jose, California, USA ([www.apere.com](http://www.apere.com))

*Analysis by Earl Perkins*

**Why Cool:** Apere, founded in 2004, is trying to change the rules regarding how an IAM product should be delivered and function, via an IAM appliance that provides access management and user provisioning functionality to targeted markets. The company is funded by its management team, which has worked together for more than 15 years and has been instrumental in two other startups. Apere introduced its Identity Managed Access Gateway (IMAG) in 2007. The appliance is based on x86 hardware running the open-source Red Hat Enterprise Linux operating system (OS), and is structured on the concept of a "rapid connector framework." This framework provides a broker layer for integrating IMAG functions with key infrastructure and application types. A series of modules uses the framework to deliver services, including:

- Basic user provisioning, password management and self-service
- A workflow for role and profile management, including recertification
- Agentless single sign-on (SSO)

Apere also offers modules for interfacing with Secure Sockets Layer virtual private network (VPN) and Network Access Protection (NAP)/network access control (NAC) services. A series of modules uses this framework to deliver services, including:

- IMAG-True SSO
- IMAG-Guest Server (authentication server)
- IMAG-IdM (user provisioning)
- IMAG-AD Virtualization (Active Directory authentication)
- IMAG-Privileged Account Management

Apere applies an architectural approach, similar to one used for multifunction security devices (for example, unified threat management), to IAM. The available modules can be deployed one at a time as “module purchases,” with a per-module pricing model that offers targeted small and midsize businesses (SMBs) — typically those with 2,000 to 10,000 users — a low-cost and distributed means of delivering basic IAM functionality in the \$25,000 to \$100,000 range, depending on the configuration. Setup and configuration times average one application (for example, collaboration or human resources) per day, and don’t require the construction of application programming interfaces, thereby presenting opportunities for service providers. Apere is currently targeting the healthcare, financial services and education markets. By focusing on specific markets and segment sizes, Apere is attempting to avoid overextending its delivery model. The company’s key technology partners are predominantly infrastructure providers (for example, Cisco, Citrix, F5 and Juniper Networks).

**Challenges:** Apere, which has more than 50 employees in India and in the corporate headquarters in San Jose, California, is in a market dominated by large vendors (among them CA, IBM Tivoli, Novell, Oracle and Sun Microsystems) that are characterized by varying degrees of maturity in the products and services they offer. Some of those services (for example, user provisioning) are still widely perceived by customers as highly customized, and are increasingly influenced by access administration activities, such as role life cycle management and identity analytics. These products provide basic functionality; however, some more-complex features involving process workflow, compliance audit reporting and granular application authorization aren’t yet available. This may not be a significant challenge in the SMB market, but enterprises seeking to use Apere’s product to extend existing IAM services, or to create a “tiered” basic service, may find that some of the features they need aren’t yet available. However, this doesn’t necessarily preclude the use of Apere’s solutions in large enterprises (for example, as an “extension” option for larger systems).

Increasing interest in service-based IAM improves Apere’s opportunities with service providers, but heightens larger competitors’ focus on the same opportunity. Apere’s market penetration is improving in Central Asia and the Middle East, but the company still faces challenges in raising its visibility in other parts of the world, including North America. There’s a continuing debate among customers and industry observers about the feature sets that can or should be combined in an IAM appliance, and about which feature sets should be administered with which appropriate skill sets (for example, user provisioning vs. identity analytics), or be delivered with the appropriate technical and business standards.

**Who Should Care:** Apere’s immediate appeal is to SMBs seeking to quickly deploy and deliver access management and identity administration services in relatively simple environments. Larger businesses (with more than 10,000 employees) will wish to evaluate Apere’s functionality as a low-cost and distributed extension to existing, software-based IAM solutions. Service providers considering the delivery of IAM as a service will wish to evaluate Apere’s rapid change/configuration capabilities and hardware footprint for basic IAM service offerings to future clients.

## 4.0 Napera Networks

Mercer Island, Washington, USA ([www.napera.com](http://www.napera.com))

*Analysis by Lawrence Orans*

**Why Cool:** Napera simplifies the deployment of Microsoft NAP (MNAP), which is Microsoft’s version of NAC. Napera sells an Ethernet switch that includes embedded support for MNAP. Enterprises that build LANs with Napera switches won’t need to purchase add-on appliances or additional software to implement MNAP, provided that their endpoints are MNAP-ready. (Microsoft Vista and XP SP3 include support for MNAP, but other OSs will need an MNAP-compatible agent.) Napera switches embed a policy server, which is used to establish endpoint and/or user-based policies, and to decide the appropriate level of network access. MNAP, like all NAC implementations, requires a policy server component. By embedding its own internally developed policy server, Napera eliminates the need for enterprises to deploy Microsoft’s Network Policy Server (which requires Windows Server 2008), or a separate MNAP-compatible policy server. Napera also provides an in-the-cloud portal that enables users to access a management dashboard and configure their switches (configurations can also be backed up in the cloud).

In addition, Napera switches can enable a basic form of identity-aware networking, because its policy server integrates with Microsoft’s Active Directory to determine a user’s role. Napera’s switches enforce policies (via access control lists and virtual LANs) that control a user’s access, based on his or her role, to critical resources. Napera also embeds a Remote Authentication Dial-In User Service (RADIUS) server (the open-source FreeRADIUS) in its switch, and this server can be used to implement guest networking across wired and wireless environments.

Napera’s solution is targeted at SMB environments. Its switches are 24-port stackable devices — the form factor that’s most popular with SMBs. Its N24 switch, with the embedded policy and RADIUS servers, lists at \$3,495, and its N24S lists at \$995 (up to seven N24S switches can be stacked with an N24). These price points are competitive with similar Ethernet switches from competitors, but those switches can’t match Napera’s embedded security functions.

**Challenges:** Napera’s value proposition is strongest in environments where Windows PCs are MNAP-ready. The slow uptake of Vista presents a challenge for Napera, although this effect will be offset as enterprises that currently favor XP upgrade to SP3.

Napera’s Ethernet switches lack support for Power Over Ethernet (PoE, which powers IP telephony handsets), which is an important feature for organizations deploying IP telephony. The lack of PoE support will be an obstacle for Napera as more SMBs adopt IP telephony. Many similarly priced switches from other SMB switch vendors already support PoE.

Napera, founded in 2006, is a new entrant in the mature market for SMB switches. The market is dominated by 3Com, Cisco, HP, and several other established vendors that have strong worldwide sales as well as distribution channels and support programs.

**Who Should Care:** Network managers who need to protect security “pain points” (for example, conference rooms and visitors’ cubicles or offices) should consider adding Napera switches to their existing infrastructures. SMBs that need to upgrade their LAN infrastructures and implement NAC also should consider Napera. The company’s capability to integrate with Active Directory and MNAP, and its embedded RADIUS server, makes Napera a good solution for multiple NAC use cases, including guest networking, endpoint baselining and identity-aware networking.

## 5.0 PacketMotion

San Jose, California, USA ([www.packetmotion.com](http://www.packetmotion.com))

*Analysis by Mark Nicolett*

**Why Cool:** PacketMotion provides user activity and resource access monitoring through an out-of-band (OOB) appliance that analyzes network packets, and can also be used to terminate abnormal session activity. PacketMotion’s solution is unique in providing broad-scope user activity and resource access monitoring from the network, without any dependence on application or system logging. This capability is important for internal threat management, and can also be used to satisfy some compliance reporting requirements. Gartner has spoken with a reference that said the technology has the capability to report on broad user, application and resource access with very little configuration or customization.

Security information and event management (SIEM) vendors provide user and resource access monitoring, but SIEM depends on log or event data generated by the monitored applications, and the technology is difficult to deploy for application-layer monitoring. Database activity monitoring technology uses a network monitor, but its scope is limited to database access. Data loss prevention technology also uses a network monitor, but is data-centric and currently provides only limited-scope user context. Some fraud-detection technologies also implement a network monitor for user and application activity, but the technology providers focus on that specific use case.

**Challenges:** PacketMotion’s primary challenge is to gain access to monitoring technology implementation projects that are funded with the objective of solving compliance issues. Many enterprises, for example, can obtain funding for a log management technology deployment to resolve compliance-related user and resource access monitoring issues, because auditors expect log management technology to be deployed to resolve the issues, and because some regulations (for example, Payment Card Industry) specify log management technology. PacketMotion’s technology can provide user and resource access monitoring in a way that isn’t dependent on log management functions, but PacketMotion is seldom considered for compliance use cases that are typically resolved with log management. Other challenges are that the technology can’t sense the activity of a user who accesses a system via its local console (this is a superuser monitoring requirement for many compliance-driven initiatives), and that there may be deployment issues related to highly segmented networks and encrypted network data streams. PacketMotion indicates that it plans to address local access visibility and decryption of traffic in future releases.

**Who Should Care:** Chief information security officers (CISOs) and security operations managers seeking to improve internal threat management and compliance reporting capabilities should consider the PacketMotion solution.

## 6.0 PhoneFactor

Overland Park, Kansas, USA ([www.phonefactor.com](http://www.phonefactor.com))

*Analysis by Ant Allan*

**Why Cool:** PhoneFactor, which changed its name from Positive Networks after the sale of its VPN line of business in late 2008, offers an eponymous OOB authentication method. More than 30 vendors offer OOB authentication methods using Short Message Service (SMS) to deliver one-time passwords (OTPs) to users’ mobile phones or other mobile devices, and nearly 10 vendors use voice telephony to deliver (or capture) the OTPs. PhoneFactor is one of only a handful of solutions that provides response-only OOB authentication. In this mode, the user only needs to answer a voice call to his or her registered number and press a specified key, and then the dual-tone multifrequency signal confirms that he or she is holding the phone. There’s no OTP to transcribe from phone to PC, although the method can also prompt for a personal identification number (PIN) response directly on the phone for additional verification. PhoneFactor’s service is distinguished from other vendors’ offerings because it’s offered free for up to 25 users. This option enables SMBs to deploy two-factor authentication with a very low total cost of ownership (due to limited internal-support costs and other associated costs). An enterprise can use the free version in a low-cost, low-risk pilot before deciding whether to deploy the solution to larger groups of users. The premium editions of PhoneFactor offer advanced features, such as a PIN response option, operational enhancements, user enrollment and self-service tools, technical support, Active Directory and LDAP integration. Many Gartner clients report that they have started with the free service and quickly switched to a premium service.

**Challenges:** PhoneFactor faces the challenge of differentiating itself from the crowd of OOB authentication vendors, which includes well-established authentication vendors such as ActivIdentity, CryptoCard and EMC/RSA. PhoneFactor offers better reliability and ease of use than the popular SMS OOB authentication method, but the company lacks the market credibility of other players. Like many new authentication vendors that only focus on one or a limited number of authentication methods, PhoneFactor provides solutions for a very limited set of enterprise authentication use cases. For this reason, PhoneFactor should seek partnerships with broad-portfolio authentication vendors or other vendors that offer a versatile authentication server and a single infrastructure that can support multiple authentication methods.

**Who Should Care:** The PhoneFactor offering should interest CISOs and other security managers who are seeking a lower-cost alternative to traditional OTP authentication methods for remote access to enterprise networks and Web applications.