

Imprivata looks to transform SSO into 'converged identity' data collector

Analyst: Steve Coplan

Sector: Networks & Media

Better known as a single sign-on (SSO) specialist, **Imprivata** is in the midst of a transition from merely easing an operational headache (minimizing the need for users to remember passwords and helpdesk resources to remind them) to compiling user profiles across physical and logical domains. Exploiting its inline appliance's position at identity checkpoints and the ability to correlate physical-access records with system logins, Imprivata can generate visibility into the correlation between multiple identities to a single user in a specific location, constructing what it calls a 'converged identity.'

The converged identity can then become the foundation for compliance monitoring and security controls. The repercussions of maintaining a 'meta' user profile with a physical context are not limited to Imprivata's top line – this also opens the door to a more flexible approach to identity management that distributes management and control.

The 451 Take

Imprivata is still in the early stages of its transition from operational tool to 'converged' identity-based monitoring, but the shift is an indication of the flux in the broader identity management landscape. The old models and technology approaches are due for a rethink. Although not all the product elements are in place, Imprivata's take on the next phase of evolution is intriguing: enterprises require more visibility hand-in-hand with more flexibility in managing access to ensure availability of applications.

Context

Imprivata is a well-established player in the SSO market, having shipped its first OneSign appliance in April 2004. In recent quarters, customer acquisition has picked up, the company claims. Imprivata says it added 200 customers in 2007, with a third of those signing up in the fourth quarter. The company has accumulated just over 500 customers in about four years, with US customers accounting for 70%. Indirect channels account for about 80% of its revenue. However, Imprivata has limited penetration of large enterprise customers.

Imprivata charges a license fee per user, either by individual module or a suite (SSO, physical/logical and authentication management).

The company's most recent funding round was in early 2006, when it raised \$12m from **General Catalyst Partners, Highland Capital Partners** and **Polaris Venture Partners**. Employee headcount is just over 100.

Technology

The technology elements to underpin the transformation to monitoring from SSO have been in place for a while: Imprivata's appliance model enables distribution of its boxes across the network (while its license model effectively subsidizes the box). The appliances

have supported the ability to capture physical-access data for about 18 months. And the appliances support SSO and authentication for access to multiple internal systems (such as email and network logins) as well as remote access via SSL and IPSec VPNs, terminal host and RADIUS server. From the perspective of network topology, its appliances sit between the user, identity stores and the target resource (workstation, server, Web or legacy application). As a result, the Imprivata appliances in aggregate become a funnel for data on who the user is in the context of multiple identities and what the user is doing, so that administrators can determine whether it conforms to a defined policy.

To build more facets of a user's converged identity, all the data captured by the appliances is fed into a standard **Oracle** 10g relational database management system, which is then correlated around a central concept, i.e., a user profile, with a physical overlay. The system serves the need to identify multiple identities with a single user, and to build a picture of where the user is, both logically and physically. The result is what Imprivata claims is the ability to identify anomalous activity – such as logging in to a system via roughly simultaneous card swipes in two different locations – as well as getting a view of the multiple identity facets of a particular user. Imprivata contends that as enterprises collect the data through their appliances, they can start to get a handle on how identities are distributed within an organization and the one-to-many relationships to users so that auditing is more automated and systematic.

The converged identity can also become the foundational element of identity management policy. The notion is useful in the context of ensuring rights and privileges but also in setting up parameters on when control of identity can be distributed to different organizational groups in order to enable dynamic changes in what users can access. Distributing control in a managed and hierarchical fashion based on visibility into all facets of user's identity allows for a flexible balance between security and availability.

Imprivata currently provides about 40 canned analysis reports for a deeper dive into monitoring statistics, and it has implemented an alerts system. This is obviously an area where further product development would reinforce the underlying value of the correlated data.

Strategy

Although the ability to assimilate data into a single repository has always been an option for Imprivata (since its appliances capture login events and identity data), it hasn't had the elements in place it needed to pursue the market opportunity. The change is a function of market conditions and the nature of the reseller and system integrator partnerships it has developed over the course of 2007.

Compliance auditing has created enormous pressure to maintain visibility into what systems users are touching and under what conditions. Physical-access controls are an important threshold control mechanism, but they (obviously) have no use in the logical realm. Logical access and authentication controls are limited to the extent that they can only know for sure that users can prove they are who they say they are. The combination of the two sets of data, which are then correlated to user-system interaction, delivers vertical and horizontal visibility. By 'horizontal,' we mean physical records can be matched to actual system logins by location, and by 'vertical,' we mean that multiple user authentication credentials are correlated to a single identity. These parameters of visibility enable both more useful

information for auditing and a baseline for policy enforcement. This is obviously a far cry from SSO implementations and has some interesting implications.

The most obvious answer to the need for control and visibility is to consolidate all identity data in a single repository and manage identities from a centralized point of control. But just because it's the most obvious answer does not mean it's necessarily the best one. The approach can create enormous complexity and is difficult to implement in the context of the proliferation of identities – which usually translates into cost and the creation of vulnerability. Centralized control also quickly starts impinging on the ability to provision applications and engineer flexible business processes. Imprivata's approach enables enterprises to distribute management of application access but still implement controls on who, how and when resources are accessed, thanks to greater visibility into the totality of the user activity correlated to identity. The next step in the strategy, from our perspective, is to move up the stack to find policy-enforcement partners.

Partners

A good deal of the shift in Imprivata's potential value proposition is driven by the quality of its partnerships with physical-access card vendors and the system integrators that implement physical-access control systems such as **Lenel Systems International**, **Honeywell** and **Tyco International's** Software House. As a small, privately held company, Imprivata doesn't have the firepower and resources to penetrate large accounts on its own. On the other hand, the physical-access system integrators are looking for a hook to raise their visibility into the IT side, so that they are relegated to a security niche, albeit a lucrative one.

So even if Imprivata's products may not significantly pump up the overall value of the deal, OneSign's ability to tie together physical- and logical-access data with converged user profiles security allows physical-access system integrators to advance up the corporate food chain and grab the CIO's attention with a more comprehensive security story.

Competition

The SSO – or enterprise single sign-on (ESSO) – space is congested, with some degree of pricing pressure. Competitors fall into two general categories (leaving aside for the moment open source alternatives such as the Shibboleth project): suite vendors and pure-play vendors focused on authentication and access control. **Citrix's** Password Manager is sold both as an add-on to its Presentation Server and as a stand-alone product. Although in many instances the functionality is based on an OEM, suite vendors offer SSO as an integral element in an overall implementation rather than a stand-alone product. **IBM** and Oracle resell **Passlogix's** v-GO SSO, while **Novell** resells **ActivIdentity's** ESSO. Imprivata reports that while the suite vendors generally shut out the pure-plays, the company has signed some customers that found the suite vendor's SSO functionality inadequate or too difficult to implement.

Pure-play vendors include **MetaPass**, **Encentuate**, **Bull Evidian** and **Sentillion**, which has a strong healthcare vertical focus. **Ping Identity** delivers SSO functionality as part of its federation product.

Strengths	Weaknesses
Its partnerships with physical-access vendors and system integrators are bearing fruit, and Imprivata has a pragmatic view on the evolution of identity management.	Imprivata will have to shake the perception that is only an SSO vendor and dispel the contention that there are scalability issues with its architecture to effectively penetrate larger accounts.
Opportunities	Threats
There is a set of concentric market opportunities: correlating physical-access data with system data in a repository, leveraging the repository to construct and maintain converged identities and to become the enabling platform for distributed management of application access.	In a crowded market where competitors have comparable functionality (but not the physical-access feature), other vendors will be sure to jump on the converged identity bandwagon and confuse the situation.

About The 451 Group

The 451 Group is a technology industry analyst company focused on the business of enterprise IT innovation. The company’s analysts provide critical and timely emerging-technology insight to clients at vendor, investor, services and end-user organizations – insight that aids both strategic and tactical decision making for competitive advantage.

The company’s services include the 451 Market Insight Service, which delivers daily insight into emerging enterprise IT markets; 451 TechDealmaker, a weekly analysis service focused on forward-looking M&A within the enterprise IT business; 451 Special Reports, which are produced on a periodic basis to analyze key emerging enterprise IT markets in greater depth; and 451 Strategic Counsel, the company’s analyst-inquiry program, which provides clients with direct access to 451 analysts. The company also produces via 451 Events periodic industry summits and investor conferences that address opportunities and obstacles facing emerging enterprise IT markets.

The 451 Group is headquartered in New York, with offices in key locations, including San Francisco, London and Boston. The company also operates Tier 1 Research – an independent division of The 451 Group, headquartered in Minneapolis – which analyzes the financial and industry implications of developments impacting public and private companies within the IT, communications and Internet sectors.

For additional information on the company or to apply for trial access to its services, go to: www.the451group.com