A new kind of giant SCUID: Identropy offers its own ID management as a service

Analyst: Wendy Nather

25 Feb, 2013

Where there's a need, there's a market, and this has been especially true with identity and access management governance. Who gets access to what – and most importantly, why – is an ongoing question that the business needs to answer, but often ends up delegating to the IT department, or creating shortcuts that can turn into entitlement nightmares ('Oh, just give her whatever Joe used to have').

All these chickens come home to roost when an auditor asks for an explanation; or worse yet, when there's been a breach and the organization resolves to clean up its act. No matter how much automation it's had in place, the enterprise must create an overview that makes sense, and takes into account all the different platforms and applications that it's managing. This is where provisioning and governance strut into the barnyard, spoiling for a fight.

Identropy has been offering identity management as a service through its Secure Cloud-based Unified Identity (SCUID) platform, to corral enterprise IAM systems such as those from IBM, Oracle, Sun, Novell and others. It has helped customers over the years as they went through what Identropy describes as a common progression: the enterprise buys one of these large systems; it hires a contracting company with IAM expertise to help set it up; the project drags on longer than anticipated; the hard-to-find experienced IAM engineers come and go.

Identropy thinks it has the answer to the complicated legacy IAM lifecycle, in the form of its own – one specifically designed for the hybrid enterprise and for easy administration by nontechnical customers. SCUID Lifecycle, offered as a SaaS, was announced in January 2013 to take over the 'last mile' of ID management.

The 451 Take

Identropy is now offering its own provisioning and governance for both enterprise- and cloud-based IDs. This could further lure into the net some of its current customers, who have been using the SCUID platform to manage legacy IAM systems. It also makes a compelling argument for greenfield customers (such as energy and manufacturing) that want a quick and easy deployment. The Identropy advantage is that with SCUID Lifecycle, it has doubled down on usability without losing functional flexibility: contextual workflows and UI displays, along with the ability to create templates, actually make the idea of putting ID management in the hands of the business a reasonable proposition. However, Identropy has focused only on provisioning and governance. This makes it a good partner (or potential acquisition) for authentication and SSO vendors, but it could be viewed as only a partial solution in contrast to the many competitors that are trying to do it all.

Context

Founded in 2006 by Victor Barris, now CEO, and CTO Ashraf Motiwala, Identropy is based in New York. It acquired the assets of consulting company Earthling Security in 2007, which netted Identropy some subcontracting vehicles for what it described as a very low deal price. The company raised $4m in series A funding from Milestone Venture Partners and Osage Partners, announced in December 2011. It is now up to 55 employees, with roughly 150 customer accounts in North America.

Technology and services

The SCUID Platform straddles the on-premises and cloud worlds, offering unified management. Its Identity Connector for the Enterprise is an appliance for the customer's datacenter to bridge the management portal in Identropy's cloud with the enterprise systems. On the cloud side, the Identity Connector for Cloud (IC2) uses the third-party SaaS providers' Web service APIs (such as those for Box, salesforce.com, Microsoft Office 365, Google and Workday).

SCUID Operations is a managed service that can monitor, report on and remediate problems in the customer's ID management system, even if it's using a legacy, on-premises identity management system product. SCUID Lifecycle, the most recently announced addition, provides self-service account requesting and provisioning for both types of accounts (enterprise and external SaaS), along with recertification and automated de-provisioning.

The company also offers services advising on and implementing a wide range of functionality, in such areas as automated provisioning, attestation and compliance management, role-based and privileged access management, enterprise SSO, Unix system authentication, and meta-directory administration. One of the great conundrums of identity and access management is that it has to be both flexible in configuration and strict in enforcement; it has to support very complex roles and policies, while hiding the complexity from the user when it's not needed.

Identropy has managed both through the use of what it calls data intelligence, bubbling up the most common actions that the particular user carries out (such as approving access for one department to a set of three applications). It also allows the user to create task templates, so that what would normally take five minutes of answering questions or specifying settings for each account can be grouped and executed almost as a macro.

This optimization makes life easier for, say, an application owner who has to process dozens of requests per week. But it also makes it easier to transfer knowledge from one user of the platform to another, so that one who takes over that provisioning or approval task can do it just the way the first user did it. It allows the enterprise to codify its processes without embedding them in a way that's going to cause trouble later when the business

requirements change. Adding support for business processes, along with business rules, turns IAM from an annoyingly arcane IT system into just another utility that the business uses every day alongside its enterprise resource management, email and office applications. In other words, it becomes a business tool, not a security tool.

Another main marketing point from Identropy is that it's easy to deploy: its example scenario describes three weeks of assessment, one month for the setup (at a one-time price of $50,000), and then it's off to the races. The mileage will undoubtedly vary, particularly where a company doesn't understand its own processes, or where much institutional knowledge is needed during the assessment as well as in the rollout. All SaaS-based IAM systems will be easier to deploy by their nature, of course, so the differentiation will be in whether the enterprise can use it out-of-the-box for its most complex requirements, or whether it will have to spend months and consulting dollars beating the app into submission.

Strategy

The company says its customers span many verticals: banking, healthcare, telecom, government, biotech and higher education. The list also includes energy and manufacturing, which were early adopters of SCUID Lifecycle. This makes sense, since these industries are less likely to have been entrenched within another commercial IAM system.

Identropy isn't trying to tackle the single sign-on market; it says it sees higher ROI in provisioning and governance. This leaves plenty of openings to continue partnering with vendors that are primarily on the SSO side, rather than competing with the entire IAM field. But it also keeps Identropy's technology poised to become an addition to a more holistic offering, or the match that completes one of its partners. By focusing on one of the parts that's so hard to get right – usability – the company can fit in just about anywhere.

In the meantime, Identropy can capture the consulting dollars that would have gone to one of the Big Four; SCUID may be relatively easy to deploy, but there's never going to be a silver bullet for IAM in general, since its requirements stem from the business and its organizational processes.

Competition

The company is swimming with the groups of hungry sharks that want to nibble away the legacy IAM market from the industry whales: IBM, Oracle, NetIQ/Novell and CA Technologies. Identropy can start out by overlaying and managing what the enterprise currently has installed, with the hope that if the customer grows tired of on-premises infrastructure and software, it can easily abandon ship to use the rest of the SCUID.

The feeding areas are crowded, however. BMC, Symantec, McAfee, RSA, Dell/Quest and BeyondTrust are circling, as are SafeNet, Imprivata, Okta, OneLogin, SaaSID, Ping Identity, Symplified, Centrify, CertiVox, Stormpath, Lieberman Software, Cyber-Ark, Microsoft (PhoneFactor), Duo Security, SecureAuth, Courion, UnboundID, Avecto, SailPoint Technologies, Thycotic, Axiomatics, CloudLock, Aveksa, Xceedium,WiKID, IronStratus, SyferLock and Covertix.

Many of the above are more on the authentication and SSO sides, and some focus on governance and IAM auditing. There are also the open source players: ForgeRock, Shibboleth and Gluu. And we can't forget managed IAM providers such as Mycroft and Lighthouse Security Group, which can also sit on top of Identropy's partners.

But we think the advantage is still going to lie with the vendors that offer a shiny new SaaS – a clean break from the past – without a walled garden or long-term consulting contract dragging it down. And Identropy intends to sell the easiest and quickest deployment. The deployment race is already on with some rivals, but it will really depend on the age, size and complexity of each customer's environment, so it's not fair to track times on different obstacle courses.

SWOT Analysis

Strengths	Weaknesses

Easy to deploy and easy to use, without limiting any choices, Identropy makes a concerted play for the overloaded IT department and the business users.

Opportunities

With its use of open standards, Identropy can grease the skids for a customer with legacy IAM to grow into the use of SCUID Lifecycle. Since it's not trying to provide authentication or SSO, it could be a good tuck-in for one of those partners. We can also see Identropy fitting into a large hosting provider environment.

By focusing only on provisioning and governance, Identropy is missing pieces that some of its rivals already incorporate (authentication and SSO). Where a potential customer is in the IAM deployment process may greatly influence whether it will reach for a partial offering.

Threats

The IAM ocean is teeming with competitors, most of which are focusing on SaaS account management today. Because of Identropy's focus on governance and provisioning, it could lose out to a more complete package from another vendor.