



Why Compliance Will Change IDENTITY MANAGEMENT

The need for compliance has created the first universal application of identity infrastructure – the first task that every business has to address that requires identity infrastructure to automate. Initially this need is accelerating the deployment of existing identity management solutions, but over time it will inevitably alter what we see as identity infrastructure and what we expect it to do.

Automating compliance is certainly driving sales of identity products, with most vendors reporting sales increases of 100% or more in the past six months. But over time, compliance will also force significant changes to the identity software and products themselves – because it alters the mission assumptions they were designed with.

The first ways in which those changes will occur can already be seen in added reporting and auditing capability to nearly all identity management products, and in new products such as those from Courion and Sun that integrate compliance verification and auditing policy enforcement into identity life cycle management. But ultimately identity technology changes will be far more significant than most now anticipate.

Automating compliance places demands on identity software that are both different and far more rigorous than the demands of abstracting authentication, access control, and password management. The requirements of compliance automation also frustrate many of the simplifying assumptions and problem segmentation approaches much by today's identity management solutions. For these reasons, the emergence of compliance as the primary driver of identity management sales will inevitably force the technology to change.

Will Compliance Remain an Agent of Change?

Before we look into why the nature of compliance automation will force evolution, and in what directions, lets look at the reality of compliance itself as a long term driver of identity tech-



nology. Is it here to stay, or, as some assert, is it something that will create a brief burst of sales and then fade out? To find the answer, we must look at how compliance requirements affect



80% of the companies surveyed were affected by two or more regulations, with 41% having to comply with four or more regulations simultaneously.

companies, and whether those stresses will cause the compliance requirements to be relaxed over time.

Depending on its nature, compliance produces two types of stress on a company. The first is the most obvious, compliance can be a cost that must be borne just to do business. Regulations such as Sarbanes-Oxley certainly fall into this category. Once the money is spent, the business doesn't seem to have gained much competitive advantage, they just have the ability to keep the auditors satisfied.

The other stress is the competitive disadvantage that occurs when competitors comply and you don't. Some regulations, Basel II in financial services for example, offer potentially significant

business rewards for implementing tighter levels of compliance. If a bank can that automating compliance has sufficiently reduced its risks, regulators will lower the reserve requirements for loans, allowing more business to be done with the same resources. One international bank used identity based compliance software to improve its compliance to Basel II enough that it was allowed to lower its reserve requirements by over \$2 billion. That \$2 billion then became available to make money for the company with no further investment or financing on the bank's part.

The End of a Golden Age

High technology has lived through a golden age in which it was essentially free of regulation. We are in the early days of regulation impacting IT infrastructure, and as was true at the end of all such "golden ages" of unregulated business practices, there are many people hoping that this type of regulation will be reduced or go away. This is extremely unlikely despite the very real hardships added compliance initially creates. This debate – and its accompanying lobbying efforts to ease regulation – will go on for some time. But ultimately lawmakers will not feel comfortable lowering the requirement for businesses to demonstrate control of their key procedures. In fact, as technology starts to provide automation for compliance at a reasonable price, these regulations are likely to continue to tighten up.

Meanwhile, the burden of compliance will continue to rise with time. This year the Sarbanes-Oxley deadline will occur for smaller public companies. These companies will be hard hit as they try to comply. A December 9, 2004 USA Today article reported on some smaller public companies that have spent nearly \$1 million thus far to reach SOX compliance. These are companies for whom that might represent 10% or

This type of technology will never translate to the needs of the smaller companies who must have compliance automation solutions.

more of their top line revenue. These costs simply must be reduced as a recurring burden on such companies, or they will be unable to continue in business. Some companies are even going private to avoid the public company compliance costs.

Manual Compliance Cannot Continue

There's an old saying that a trend which cannot continue, won't continue. Something will happen to change it. The cost of manual compliance is unreasonable, and will always stay that way. The regulations that require it, however, are not going away. There might be some temporary relaxation of compliance deadlines in certain cases, but long term regulators and lawmakers are likely to require even tighter compliance as years go by. Thus the trend of trying to comply manually can't, and won't continue. The answer is obvious, it is that technology will move in to automate compliance, largely eliminating the recurring costs – there is no other possible outcome.

The Nature of the Changes

Identity management has thus far been primarily a technology designed for, and adopted by, very large enterprises. As a result, it has presumed a heavy professional services component, and significant customization to each deployment. This type of technology will never translate to the needs of the smaller companies who must have compliance automation solutions. So one of the changes we should expect is the emergence of identity management for smaller companies, packaged in more off-the-shelf ways and with much lower price points. If the history of the com-

puter industry is any guide, we would expect to see some new companies appear in this space with innovative solutions and have great success. The new, lighter weight techniques developed for smaller businesses are then likely to be adopted in the larger enterprise class solutions over time.

As large and expensive as they might be, many of today's identity management solutions nevertheless address only segments of the heavily siloed IT infrastructure and applications in large enterprises. Web access, legacy system access, Web services, network access, ERP access, CRM access, etc. tend to be tackled as separate projects, meaning there is no unified identity or identity-based activity view across the entire enterprise. But compliance requires an integrated, application wide identity based view of an enterprise's IT infrastructure, so another of the changes we can expect is ways that today's solutions can flexibly integrate to provide such a unified view. This seems likely to drive technologies such as virtualization and federation which link identity systems, and perhaps create new technologies to integrate identity solutions in a more loosely coupled fashion.

Increased Agility

Courion recently took a survey of its Fortune 500 user base to learn the impact of compliance on their IT systems. Among their sample they found fourteen regulations that impacted 11% or more of those customers' IT systems. They found that 80% of the companies surveyed were affected by two or more regulations, with 41% having to comply with four or more regulations simultaneously.

Compliance is not a one-time event, it must be continuous. This means that as a company goes about developing its business, finding new ways to sell products, developing new products to sell and new markets to sell them into, compliance automation must not impair the agility of a business or its IT systems to adapt to changing business conditions. And acquisitions must be integrated rapidly to assure compliance across the resulting enterprise. Current identity management technology simply cannot remain agile while handling compliance with multiple regulations across an entire enterprise's IT infrastructure.

Centralized Policy and Management

Compliance requires a centralized view of identity and its use, and should have a central location where policy is specified, approved, and implemented. In order to allow an IT infrastructure to remain agile in the face of this type of policy and identity based management, one of the changes we should expect to see is that this type of centralized management will become largely decoupled from the systems that implement that policy, monitor its adherence, and report on its status for auditing and forensic purposes. This is a trend that has already begun, but it has much farther to go.

With Loosely Coupled Integration

In order to gain the agility that compliance automation requires as well as the scope of coverage to follow transactions through whatever applications paths they take, will require that systems have a number of standardized, interoperable interface options. Protocols such as

SAML, WS-*, and a number of the JAVA protocols are providing ever more flexible XML based interface options for identity and management. But this is an area that will be forced to evolve sig-

the expression and transmission of policy. Today, policy must be expressed in a variety of locations in an identity infrastructure, and it is largely a manual effort to take the corporate policies and turn them into policies that various bits of management software can act upon. Role and rule engineering must become far more simplified that it is today, and that will require new paradigms for expressing policy and relating it to distributed identity stores.

Identity management is already limited by the ability to express policy with a reasonable effort. How will we express policy from a central management point and then distribute it to the various application and enforcement points in the network across legacy, web, Web service, mobile and other network architectures, having it adapt to its context at each location? Only by significant innovation and change in how policy is viewed, expressed, and used.

There are early signs that methods to make policy easier to express in a dynamic integrated infrastructure are occurring. Such things as the contextual approach pioneered by TruLogica (now part of HP) and things like Dynamic Groups from Courion. This is a journey that has just begun, but it is one that automating compliance will accelerate significantly. Systems like those from Prodigen and Eurekaify that “learn” policy by observing applications in use may also indicate a direction policy expression may go.

What is certain is that in a relatively short time identity technology will evolve significantly because of the needs of compliance. The results will be identity infrastructure that is easier to deploy, more agile in use with changing business needs, and which finally begins forming the basis for a universal identity infrastructure. ■



So one of the changes we should expect is the emergence of identity management for smaller companies, packaged in more off-the-shelf ways and with much lower price points.

nificantly by compliance. Since every part of an IT infrastructure and application must ultimately be integrated across many administrative domains, the coupling must become loose enough that each part can be upgraded, modified, or changed without affecting the rest of the system.

It's All About Policy

Perhaps the area where the most revolutionary advances remain to be discovered and implemented are in the area of