

Affymetrix Adds Identity to IT's DNA

Biotechnology seems likely to characterize 21st century technology the way that physics, computing, and the space program characterized the 20th. The sequencing of the human genome and other biotechnological advances offer great promise for better drugs, healthier foods, and more efficient medical diagnosis. One of the key enabling technologies for biotech is the Affymetrix gene-chip. But with breakthrough technology comes the need to protect intellectual property, and there is also the issue of regulatory compliance. Identity contributes to managing both.

In 1989 Affymetrix CEO Stephen Fodor led a scientific team that invented a new way to ask questions of DNA and get rapid answers – a gene chip that can rapidly detect the presence of a gene, or slice of genetic code, in a sample of blood or tis-



Affymetrix
production
operator inspects
a mounted wafer.

Photos Courtesy of Affymetrix

sue. In 1992 Affymetrix was created as an independent company. Development of its gene chip technology advanced rapidly over the years, and in 1996 it became a NASDAQ listed public company. Today Affymetrix is the recognized leader in gene chip technology.

As was true in semiconductor development, gene chips are following something like a Moore's Law curve, becoming

able to pack more genes into smaller spaces every year. In 1994 a gene chip contained about 16,000 DNA probes. Today's chips hold up to 2,500,000 DNA probes. Researchers are now using gene chips to test patients for susceptibility to drug reactions, and specialized gene chips can even test food samples for purity. For example, one Affymetrix chip, called the FoodExpert, rapidly tests for the presence of 33 different species of animal in any food product by detecting DNA sequences specific to those animal species.

Protecting Intellectual Property

Given the promise of biotechnology this is a highly competitive field. Affymetrix has over 200 patents relating to gene chip technology, and over 400 patents pending. So it is no surprise that Affymetrix must focus on protecting its intellectual property. "Affymetrix has a large intellectual property portfolio," said CIO Moses Cesario. "So security around data stores that reside on the network in some way, shape or form is of high importance to us. Likewise the applications that overlay those data stores and how we manage that data are important."

bioMérieux
FoodExpert-ID Array.

"We liked the architecture, although it wasn't broadly proven – reference the big players and what they're doing, which is quite different fundamentally."

In 2003, Cesario realized that Affymetrix needed to take steps to better control and manage access to the company's data. "Over time we had built an infrastructure that had many different password protected applications that [interacted with] various data bases and we ended up with a pretty complex mix – kind of a mess really – of different password based accesses. So we started thinking 'how do we lock this down and start to control it in a manageable, but scaleable way?'"

The proliferation of passwords was creating security issues, "so Single Sign On became a pretty important aspect," said Cesario. "In addition we wanted to add not just the typical kind of Windows based security layer that exists with the network, we wanted to go a bit beyond that, or to have the option to do that. So that started us looking."

Looking for an Answer

Cesario looked into identity management solutions from the larger suite vendors, but cost was a barrier. "I was looking at doing this security infrastructure proactively," said Cesario. "We hadn't had a situation where intellectual property was lost or where we had a significant event, and business wasn't demanding it. But I wanted to address it proactively. I didn't have broad support for a significant infrastructure investment in security, so a half million dollar purchase was not going to happen for us."

In his search he discovered Encenatue, an identity management product with a different approach. "What they offered was fundamentally a different approach



to the architecture,” said Cesario. “An approach to Single Sign On that we felt would be empowering to us in terms of managing an infrastructure environment. We liked the architecture, although it wasn’t broadly proven – reference the big players and what they’re doing, which is quite different fundamentally. But there was also another factor and that was the cost. It afforded me the opportunity to get the levels of security that I wanted at the right price. I knew I was taking a calculated risk by going with Encentuate but the dollar amounts were low enough that if it just didn’t work I could write it off and move on.”

Testing it Out

Affymetrix started testing and piloting in late 2003. “We took some time to sort it out,” said Cesario. Affymetrix was an early adopter of the technology. “What we were doing in my mind had the flavor of beta test. We were helping them work out configurations of their software. What we worked through is to the benefit of Encentuate in terms of maturation, and working with them through those challenges that we had for full configuration in the installation and environment they handled incredibly well. They have a strong team, and they are extremely customer service oriented.”

After solving the product issues during the pilot, Affymetrix took the deployment live in early 2004. “We are a true enterprise implementation, and we are successful in that,” said Cesario. “It’s functioning well for us and it’s been almost problem free. Our users have gained good benefit from it because they’re not struggling with multiple passwords now. We have close to thirty apps loaded into Encentuate today, and that covers ninety percent of the employees within Affymetrix and their password needs. So the perception of most of the company is that they need one password to function around here.”

Compliance Needs Arise

Affymetrix began looking at identity for security – to protect intellectual property. But along the way Sarbanes Oxley compliance became an issue. Having an identity infrastructure in place made compliance much easier to deal with. “I would have had to implement SOX based controls by application,” said Cesario, “and that would be unique for that application to control accesses. But what I had in Encentuate was a control point with which to put accesses out there. So it greatly simplified my chal-

“It greatly simplified my challenges to become SOX compliant. We were able to put in the requisite controls and respond to the business need because of the infrastructure we had put in place.”

lenges to become SOX compliant. On the IT side we were able to put in the requisite controls and respond to the business need in a very quick way because of the infrastructure we had put in place.”

The Compliance Process

“I had to define my procedures per SOX requirements,” said Cesario. “I have fifteen applications that were specified as needing to follow the SOX controls. It turned out that all but two were



Affymetrix GeneChip® probe array.

Photos Courtesy of Affymetrix

[already] in Encentuate. So from the standpoint of access controls for SOX, as long as the processes I had around managing IDs through Encentuate complied, I nailed thirteen of the fifteen right there. I had to change [some] procedures to comply with SOX standards as given to me by the audit firms that were executing our SOX audit, however I only had to do it once for all the applications that were covered by SOX. Then if my app was loaded into Encentuate I complied. I did not encounter the challenges that I think a lot of companies probably did in terms of giving access to applications and managing access to IDs.”

“From a compliance standpoint for SOX, adding individuals and giving them the requisite access and getting the approvals can now be managed from an infrastructure standpoint in a centralized and controllable way,” said Cesario. “And if you’ve got a termination I flip a switch and network access and all passwords can be abolished and eliminate the risk of exposure of data to somebody that shouldn’t have it.”

Approval Workflow

The workflow for identity life cycle management is currently being handled manually outside of the identity man-



agement system. "In terms of acquiring access to any given set of applications you get a network password set up and then request access to X, Y, and Z systems," said Cesario. "That request comes in, and we make sure centrally, through IT, that we gain the requisite approvals to get the access. If it's somebody working in finance that wants access to X, Y, and Z capabilities within the ERP, for example, we have a matrix that specifies the name of an individual in the organization who has the authorization to allow that access. We make sure that happens and document that it did happen."

"A manager can send us an email saying 'I'd like this individual's network and applications accesses to be terminated at this date,' or that can come from HR or legal or whomever," said Cesario. "We have a Departmental Operating Procedure, which specifies how that works as far as the individual in the support center who does it. Once we have that [documentation] we make the changes in Encentuate to give appropriate accesses. At that point it now self manages, so we don't have to worry about the application level synching, keeping the ID the same, updating the password at the application level, etc."

Recurring Audits

Compliance is not a one time event. "You've got to comply on an ongoing basis," said Cesario. "The Sarbanes requirement is that we will be subjected to an external audit to check for compliance on a yearly basis. But there is also a requirement that we self audit and that we be able to produce records for the self audits. With an infrastructure like Encentuate that's easier to do,

"From a compliance standpoint, adding individuals, giving them the requisite access and getting the approvals can now be managed from an infrastructure standpoint in a centralized and controllable way,"

It allows me to do audits. I can go into it and see active passwords, I can see which apps are associated with a particular ID, and I can see changes."

Moving to Strong Authentication

Another option of the Encentuate identity system is that you can mix types of authentication from passwords to strong authentication. "We have the option to move to stronger security," said Cesario. "Our intent is to move to encryption so all password activity will be encrypted. You can have two key identifications, and for some activities we will have that set up so that whether

"You've got to comply on an ongoing basis. We will be subjected to an external audit to check for compliance on a yearly basis, but there is also a requirement that we self audit and be able to produce records for the self audits."

using a tower or notebook you could use a USB key that you plug in to log into the environment, You have the key and you have the password layer, and those two things come together. Today what we've implemented is those keys actually exist on the various PCs out there. We're looking at going to true two factor identification for some activities within the business. Encentuate

has that functionality, and you configure it to suit the level of security that you desire."

Adding Applications

When asked about the impact of rolling an application into the system, and how developers responded to it, Cesario said, "Beyond some grumbling this was very painless. If you have a custom app you may need to do development within that custom application – it's like a set of API's. But Encentuate has done a good job of partnering with us to help us where we have needed it to get applications online. The thing is you do this once, and it's not that expensive. And once it's there, it's just part of the infrastructure."

Because they were an early adopter, Affymetrix had some growing pains that Cesario feels newer Encentuate customers would not have. But he is quite happy he chose this path for identity management. "Given the dollar investment that I made, my ROI is already met," said Cesario. "And how do you put a price tag on protecting information? Somebody can breach your firewall through a [stolen] password and what have you, but the real threats most typically happen from within in some way shape or form. Having a Single Sign On infrastructure that manages password and accesses that's consolidated, provides a level of control that you otherwise would not have with regard to access to information in the company. It empowers me in that regard, and puts me in a position where I know what's going on in my environment with regard to access." ■