Identity Management: A Landscape That Tries to Fix Square Pegs into Round Holes

Ever tried to fix a square peg into a round hole? Doesn't work, does it? It is stupid to try, it is a logical fallacy. When something is made for one thing, and is tried to fit to another, confusion and time wastage ensues. Such is the state of Identity Management today.

The problem begins at the very root stage of intent. Cybersecurity, of which IAM is a component, has traditionally been treated as a luxury rather than a necessity, and this attitude continues today. When you realize the critical barrier that IAM provides against data breaches and cybercrime, how can you create solutions that are meant to sell, rather than those that are meant to work for their purpose? Yet this is the attitude with which solutions are created today.

The entire landscape of internet related business has been a rich opportunity to make big bucks. It can be likened to the California Gold Rush in the 1950s; everyone wants a piece. But this has brought all kinds of people into the foray of business activity, most with a single intent: monetization. But this can't be the goal of the cybersecurity industry, not the primary goal at any rate.

Firstly, cybersecurity is a business opportunity made possible by cybercriminals. Strange as it may sound, those that profit from it must acknowledge that there is something unclean at the core of it all. The prime incentive of profiteering from something that is meant to protect innocent citizens is just in bad taste. The industry must first aim to provide solutions that work, at affordable prices, and that provide a sufficient barrier against cyberattacks. Then and only then can one look at the profit motive. But the landscape is in reverse.

IAM has all kinds of products and vendors that try to create things that sell, not things that work. To sell the same product to as many possible companies is the singular goal. But, companies vary in size, segment and scope. How can a product meant to cater to the common bottomline fully protect a mid-sized business in the manufacturing industry equally? The midmarket and manufacturing industry has very specific and unique needs. For one, they have shop floor machines which typically utilize thick-client, on-premise software. These need password management and single sign-on as much as a corporate business requires them for their daily IT activity. But, only one vendor currently offers thick-client SSO. And the midmarket demands high ROI, short implementation times, and economical costs. Most IAM products cost an arm and a leg.

Smaller businesses also need to save on license costs. But nobody has developed a single sign-on feature that allows a single license to be used by different users. The reason is a lack of vision. Content with providing common features that customers have grown to expect, nobody is innovating on a level that provides features that customers **NEED**, only what they think they **want**.

When it comes to Identity Governance, a lot of time and confusion can be saved if Access Requests are handled in an intelligent manner. Businesses know they need this feature, and the market only offers it at its most basic, as this is enough to sell the product. But, for instance, a solution which enables employees to see the risk score of a requested access; ie.,the likelihood of getting it approved by someone in their role and position, would save the business a lot of confusion and save employees frustration of unapproved accesses. Only one vendor currently offers such a feature.

The approval side of access requests can also be improved upon when it comes to the industry standard. Currently, most solutions offer manager level approvals. But, what happens when a manager is not confident of approving a certain access for a role? What if they are simply too overburdened with access requests to ensure proper allocation? A delegation feature is required. Again, only one vendor currently offers such a feature.

The bottomline is that IAM vendors can provide far better features than they currently do. Blindsided by ‘what sells’ rather than ‘what's best for the customer’, they create products that do what the customer expects. But customers only know what to expect from the common bottomline of what vendors offer. It is a vicious cycle. IAM customers need to be told what they need, vendors need to preemptively solve their challenges, not just engineer products based on what the latest and greatest features are. This is sorely lacking.

One vendor stands out against this landscape. Ilantus Technologies, an IAM vendor that has been around for over 20 years, is painstakingly offering solutions that customers truly need, not just what they expect. They offer thick-client SSO, SSO for multiple users with a single license, risk guided access requests, and delegated approvals, amongst other features that are uncommon but vital to solving **REAL** business challenges. To top it all off, their products are typically offered at a cost that suits most midmarket budgets, something that should be typical in an industry like cybersecurity. They even offer multiple payment models such as perpetual licensing, subscription, and even the industry’s first true pay-as-you-consume model. This company is really looking out for its customers and not just for itself. It is time other vendors started adopting a similar approach for the betterment of the industry. Customers should be able to choose between multiple vendors to match their exact needs, and each vendor’s product should reflect the pinnacle of their capability in understanding and catering to customer needs. **Square pegs should not be tried to be fitted into round holes.**