White Paper

Next Generation Privilege Identity Management

Nowadays enterprise IT teams are focused on adopting and supporting newer devices, applications and platforms to address business needs and keep up pace with the changing market dynamics. Initiatives such as bring-your-own-device (BYOD), cloud deployments, mobile app connectivity are boosting costs reduction by decreasing capital expenditures and increasing productivity via ease of use and flexibility to employees. With increased complexity around IT setups, security concerns have also elevated owing to insecure channels leading to information leakage, vulnerabilities and newer threats posed by advanced cyber attacks. These growing security concerns have made it axiomatic to assert that managing authentic access to resources is vital for any organization.

Mostly all organizations enforce rules and policies on individual user logins to determine what information and services are accessible to them. Aside these individual accounts for employees, organizations have other powerful accounts on their networks with special permissions to have complete access to all the resources of target environment. These accounts, known as Privileged accounts and Identities are extremely powerful, allow users to log on anonymously and have unrestricted control of the system. It's not surprising that managing privileged identities and protecting sensitive data continues to be a primary concern for security teams.

The broad paradigm shift from closed, hierarchical and static systems to open, cloud based and dynamic systems necessitate move from traditional PIM methods around centralized, siloed, proprietary and rigid systems to next generation methods focusing on virtualized, shared, open-sourced and diversified platforms. These facets throw new challenges for organizations to effectively manage security and compliance requirements.Intent of this paper is to analyze these challenges from different factors which influence the Next Generation privilege identity management solutions.

Securing Cloud platforms

Cloud computing is rapidly transforming businesses by delivering mission critical applications at unprecedented pace and more efficiently than ever before. The shift to cloud-based (public/private/hybrid) deployments allows resources to be deployed, moved, and scaled in agile manner. But, for all its benefits these advances have created new security vulnerabilities whose full impact is yet to be assessed as it's still emerging. Next Generation PIM solutions have to be equipped with dealing with these emerging challenges and security threats and should take into consideration the below five key aspects:

- Cloud infrastructure is not constrained in any perimeter (at times their location is abstract) and thus management systems have to operate beyond the constrained environments spanning multiple technology platforms and interfaces.

- Data Breaches on cloud infrastructure can be more serious as a flaw in a single application can expose entire shared data exposing data from potentially each and every client on shared system.

- Flexibility for control structures to be extended for evolving compliance crequirements and audit mandates using established best practices.

- Cloud solutions add a new landscape for hackers and malwares to hijack accounts and services with newer advanced techniques like Cross-Site Scripting, Advanced Persistent Threat (APT), Spear fishing etc.

- Malicious insiders have greater chances to access to potentially sensitive information in an inappropriately secured cloud scenario.

Manage beyond the perimeter

Organizations are readily adopting a hybrid model owing to unprecedented flexibility gained by the rapid deployment of applications. Moving beyond the traditional perimeter based solutions has helped the IT managers to optimize costs and reduce time to market by selecting any of the various platforms available both on-premise and on cloud. Cloud adoption has led to an increase in the number of applications that now reside outside the organizations firewall and are disconnected from on premise security services. These applications are accessible to employees, customers and partners over swarm of handheld devices including smart phones and tablets which are neither connected to secure corporate network nor are under control of IT.

In this hybrid setup, organizations are finding it very challenging to secure the access beyond traditional network and company boundaries. Because no single traditional product met needs of vivid platforms, over years enterprises have created, and are now burdened with managing, multiple on premise systems which work in isolation to protect specific applications and hence lack the capability of handling multiple control points across different environments. Further, these solutions have resulted in inconsistent and redundant policies across systems and have burnt out the administrative bandwidth.

To support today's aggressive growth and given the cloud strategies are still not mature enough, it is thus essential for enterprises to think about a PIM solution which is comprehensive and can provide single management pane with ability to secure platforms across traditional, virtualized and cloud environments. This Next Generation solution is expected to allow organizations to define the policies around entire infrastructure, comprising on-premise and beyond, and enforce them seamlessly from a single control point.

Another important aspect will be to reduce complexity of audit and compliance controls and the ease to adopt any changing requirement. An ideal system will be tasked to manage the resources which can exist anywhere and everywhere on the cloud and still keep the administrative overhead to minimum.

Automating PIM in elastic environments

It's not wrong to assert that primary concern of most organizations has been around protecting the critical applications and sensitive data. Enterprises have been enthusiastically embracing newer processes and solutions to control the privileged users, protect their delicate credentials and be able to meet the compliance requirements. This has never been an easy task and with the advent of cloud-based computing infrastructure these long-standing concerns have further complicated.

Organizations now have greater flexibility over infrastructure and deployments, can now rapidly add/remove/modify any of their resources, applications and infrastructure to keep up pace with the dynamically changing business requirements and demands. In a way enterprise IT has gone elastic now which can be scaled either way to manage fluctuating workloads.

To meet the demand of new elastic setup, enterprises are seeking a holistic management product and to be effective and not just another application on the IT stack, this product has to be dynamic in essence to keep up pace with the changing requirements.

So far, we've talked about three major trends around Securing Cloud, Managing beyond Perimeter and Automating Security. Now let's explore some key capabilities that a Next Generation PIM should essentially have.

Has to be comprehensive - Should provide full featured PIM capabilities providing centralized single click provisioning, de-provisioning, securing, authenticating, monitoring and auditing.

Consistent Policy Enforcement – Ability to span multiple technology platforms, interfaces, systems and bring them under the umbrella of single policy enforcement management pane.

Extendible Control Structures - Policies and processes are constantly evolving in response to security best practices, audit and compliance requirements. Target solution should be able extend control structures and successfully move them to entire organization fabric.

Automatic discovery – It could be a potential threat if there is a time lag between when the resources are added and when they are finally secured as per company polices. Product should automatically discover and instantaneously secured them with appropriate set of polices to avoid and abuse.

Scalable & Available – The solution has to highly scalable supporting possibly millions of nodes and credentials. It should have high-availability architecture (such as fault-tolerance, clustering, failover and load balancing) to provide a reliable setup for mission critical deployments.

Flexible – These days new platforms are being added more frequently than can be imagined. PIM solution is therefore expected to provide flexibility in supporting broad range of resources including servers, databases, networks and applications which run over these platforms. It should readily integrate with industry standard third party products.

Monitor & Record – Last but not least, session monitoring and recording is expected to be the integral part of any security application and PIM is no exception. Next Generatio system has to additional provide an extension to these capabilities, to include all possible channels of access.

Conclusion

New era of virtualization and cloud environments have undoubtedly bring newer challenges and requirements for privileged identity management solutions. As described, the next generation PIM will be required to deliver additional capabilities to effectively manage privileged user and protect organizations of unfavorable conditions.

About ARCON

ARCON is a leading Information Security solutions company specializing in Privileged Identity Management and Continuous Risk Assessment solutions. With its roots strongly entrenched inidentifying business risks across industries, it is in a unique position to comprehend and identify inherent security gaps in an organizations infrastructure framework and build and deploy innovative solutions/products to significantly mitigate potential risks.