PROACTEYE

# BUILD PRIVILEGE MANAGEMENT INFRASTRUCTURE via CLOUD ACCESS SECURITY BROKER

**WHITE PAPER**

**Today in enterprises, many times, cyber crimes happen only because enterprises do not bother to secure or monitor their applications. Application data hosted on networks, servers, and cloud environments can easily be compromised from a security standpoint if a dangerous hacker is after it.**

**In any enterprise, those who have privileged access to every application can leak any data and if their accounts are compromised by hackers, it spells bad time for the enterprise. The cyber security of the enterprise is sabotaged.**

## Risks and challenges regarding cyber security

The risks faced by organizations are fragmented and complex. Hybrid Data Locations and non-compliant use of cloud-based resources leaves the cloud networks (and data they store) prone to various kinds of cyber attacks. The cyber security of any enterprise hence remains vulnerable.

Cyber security is weak due to lack of insights, control and tools. There is limited data about how many or which cloud applications are being used. Their usage details are also sometimes unavailable.

Sometimes, users do not know how to assess the risk. Obviously those who cannot assess the risk have no way to control it and protect the privileged accounts. Traditional network and endpoint security measures are no longer effective for foolproof cyber security.

For elaborate cyber security, organizations need to be sure that access to their resources is controlled by a variety of security mechanisms that include authentication (who the user is), authorization (does user have sufficient rights to access application), privacy (confidential material accessed only by those authenticated and authorized), audit and control (monitoring of transactions).

To prevent the data leakage and cyber threats, enterprise needs to formulate a system for Privilege Management where no employee has unconditional access to every application.

Standardization in cross-domain user provisioning, strong Authentication and Authorization and centralized IAM for different purposes and populations as Access Security Broker are the key purposes served by PMI.

Hackers are growing smarter and you can beat them in their own game only if your cyber security and Privilege Management Infrastructure (PMI) is smarter than them.

Privilege Management Infrastructure is a security system that supports a strong authorization subsystem via the management and use of privileges to secure & protect IP.

Privilege Management Infrastructure safeguards applications in order to prevent data leakage and boost cyber security. The key objective of such Infrastructure is to provide secure access to any target resource that has been specified on the basis of policy to deal with next gen cyber attacks.

PMI operates on the premise of least privilege. It unifies the treatment of access Channels, Populations and hosting models. It integrates cyber security and log aggregation modules with IAM.

PMI prepares for Interactions at Internet Scale and arranges for conditional access regarding all applications and for all user accounts in cloud network via Access Security Broker.

## What is Cloud Access Security Broker

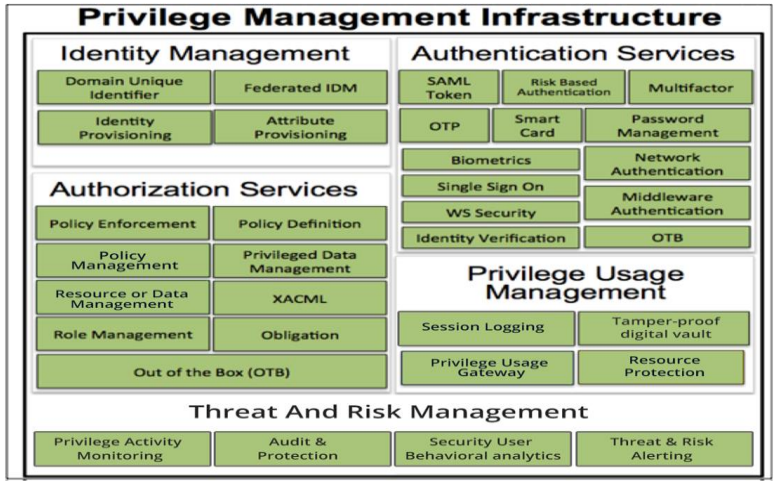
Cloud Access Security Broker is a software broker that sits between an organization's on-premises & Cloud Apps and a user who would like to access. It acts as a gatekeeper, allowing the organization to extend the reach of their security policies beyond their own infrastructure.

Along with Access Management, Cloud Access Security Broker also offers Identity Management with User Activity & Usage Monitoring .

Cloud Access Security Broker analyses all user and privilege activities to discover threats and risk in real time.

PMI provides secure access to any target resource that they specify based on policy to deal with next gen cyber attacks.

Privilege Management Infrastructure includes Identity Management, Authentication Services, Authorization Services, Privilege Usage Management, Threat and Risk Management.




Cloud Access Security Broker empowers users in multiple ways like Authentication with multi-factor support, Authorization and Support for XACML 2.

Since CASBs act as a proxy between cloud apps and users, they have the ability to see all traffic to/from those cloud apps, and to inspect and secure data. At access, CASBs provide visibility, identity, access control, and data protection.

## What are its advantages building PrivilegeManaged Infrastructure using CASB?

**Increasing Business Value**
Offers improved user experience, speed to market and Post-M&A Assimilation. It also enables E-business and Collaboration.

**Reducing Risk**
Reduces the risks regarding cyber security via Security Lifecycle Management, Security Policy Enforcement and lastly, Data Integrity & Confidentiality.

**Containing Cost**
Is cost effective. It enhances the time to productivity by doing more with fewer (or the same) resources, along with consolidation of IT Infrastructure. It also reduces Outsourced Contract Values.

**Improving Compliance**

Improves internal auditing, regulatory compliance and competitive compliance.

## ProactEye for Privilege Managed Infrastructure.

Proacteye Cloud Access Security Brokers are quickly emerging as a must-have security solution for organizations looking to adopt cloud-based applications. ProActeye fills in the gaps that cloud app vendors have left to the enterprise to solve—visibility and data security.

ProActeye can secure cloud data wherever it goes—from the cloud to the device. It builds Zero Trust Authentication, Authorization and Identity Services with Data leakage prevention.

# Summary

Enterprise can enhance security and overcome cyber threats by establishing Preveliage Managed Infrastructure.  Not only they can achieve internet of scale but also keep abreast of every activity in the organization via effective monitoring.

ProactEye, Cloud Access Security Broker sits between an organization‘s Cloud Apps and user.

ProactEye modules offer  innovative components, which instantly build Privilege managed infrastructure

PROACTEYE

## ABOUT PROACTEYE

ProactEye is the Cloud Access Security Broker with Security Behavioural Analytics Platform.

It detects & prevents fraud, data leaks and advanced inner as well as outer attacks and Big Data.

For more information, visit
www. Proacteye.com

Email : enquiry@proacteye.com