Strengthening Your IAM Program with Identity Governance Administration by : Garret Grajek, CEO of YouAttest

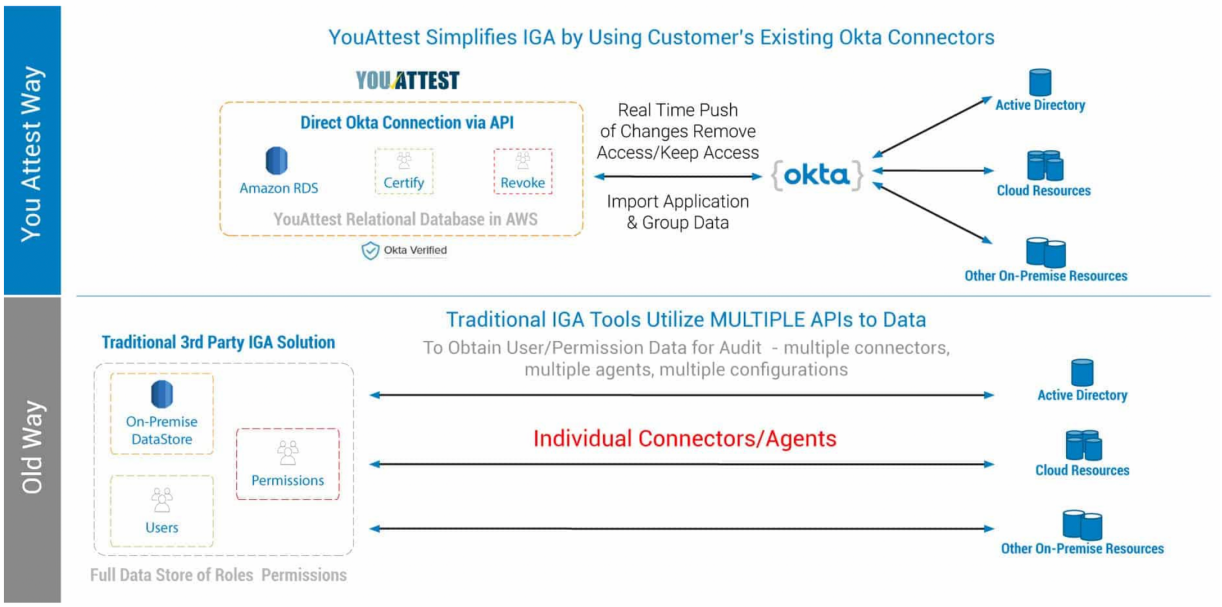

Image source: https://youattest.com/

Access Request Approval

The access request approval should be able to meet the government compliances like NIST, CCPA, GDPR etc. This is important because enterprises require an auditable process that quantifies when a user requests and receives new access right.

Escalation Triggers

Escalation triggers works on the principle of least privilege which allows authorize access to the users who need to have the necessary accesses. This process alerts the whole system when a change auto permission is executed.

User Access Review

Reviewing what permissions have been given and documenting those permissions is the most important part of an organization . Therefore YouAttest creates reports, documents approvals and delegation of authority when reviewing access of groups users or applications.

THE TALK

The biggest problem is the bad relationship between process (access management) and function-oriented people. the talk I attended was focused on Identity Aovernance Administration and the threats detectable via IGA incompliance with Identity and Access Management (IAM). There has to be a complete transparency in the processes while implementing the actions. So, whenever somebody come to the enterprise the administration should be able to show and explain all the processes along with the documentations. although IGA is a security tool but the question is does it prevent cyber-attacks and the attacks related to PCI DSS, HIPPA etc. The solution is YouAttest, the disruptive IGA solution that enables simple IT Access Reviews and IT Credential Review and Change Control relevant to HIPPA, SOX, PCI-DSS, SoC Type 2 etc. To solve the gap YouAttest integrates into the process the following three approaches.

1. request occurs
2. approvals
3. documentations of Vienna damages occurred.

The benefit of real time attestation is to meet the compliance and to run the reports so that everything is more secure and recognized. The CEO also mentioned that the access reviews occur like 12 times a year. We all know that IT people or IT Directors perform all the functions, but it is the basic right of the external auditors do know what changes in the recent days (say last 90 days).

So, the most important piece of advice is identity governance is a part and parcel in today's era and processes should be functional.