

Closing the Cloud Security Gap with Privileged Access Governance

ISSA-LA Chapter Dinner Meeting

Presenter: Art Poghosyan, CEO, Britive Inc.

October 16, 2019

Why is Cloud So Difficult to Secure?

- ☁ It's dynamic and high-volume
- ☁ There is a learning curve
- ☁ You don't have a complete control over it
- ☁ Cloud-native security tools are still maturing
- ☁ Wrong approach (and tools) is used

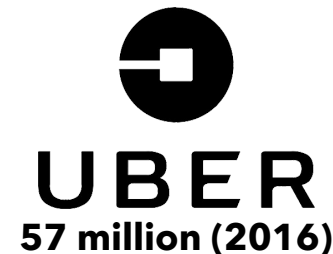


Bad Guys Relentlessly Target Privileged Access

As evidenced by research surveys:

- ☁ 2019 Verizon DBIR
- ☁ Forrester & Gartner Reports
- ☁ McAfee Report

And data breaches:



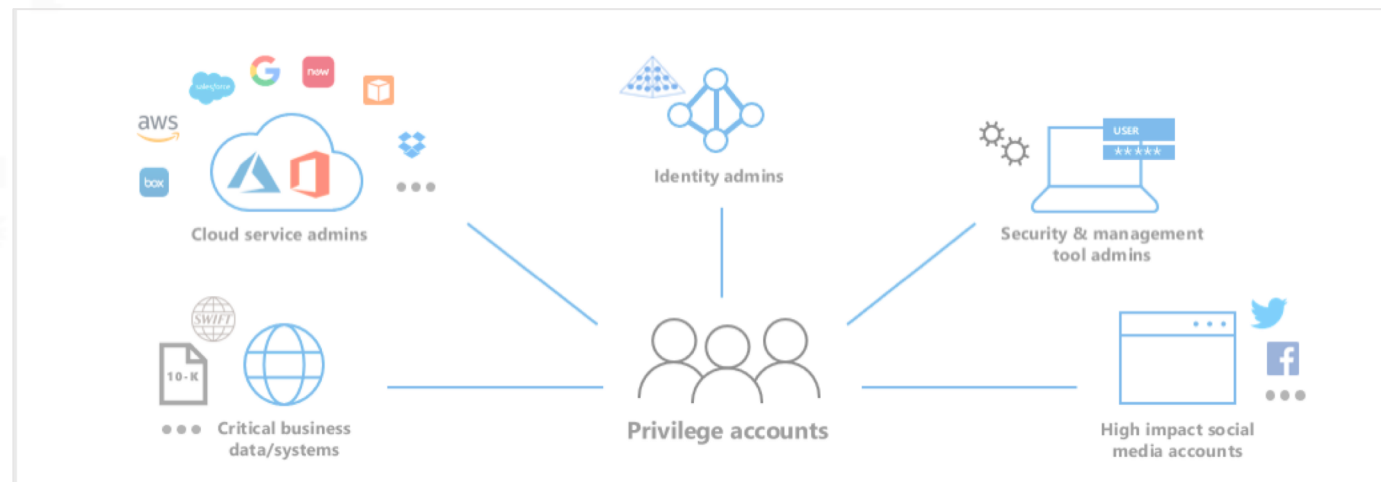
Privileged Access is More than “r00t” Accounts

Cloud components that require privileged access

- ☁ Management Consoles
- ☁ CLIs
- ☁ APIs
- ☁ Resources
- ☁ Workloads
- ☁ Administrative functions
- ☁ Data level access

How is privileged access defined

- ☁ Roles
- ☁ Policies
- ☁ Groups
- ☁ Profiles
- ☁ Permissions
- ☁ Keys



Privileged Access is a Major Challenge

☁️ Difficult to get visibility into existing access

☁️ **who** has
















☁️ **what** access

☁️ in **what** platform



☁️ Each cloud platform has it's proprietary privilege model

Cloud Privileges - Granular But Complex

Filter policies ▼ <input type="text" value="Search"/>					Showing 558 results
	Policy name ▼	Type	Used as	Description	
<input type="radio"/>	 AmazonDocDBReadOnlyAcc...	AWS managed	None	Provides read-only access to Amazon DocumentDB with MongoDB co...	^
<input type="radio"/>	 AmazonDRSVPCManagement	AWS managed	None	Provides access to manage VPC settings for Amazon managed custo...	
<input type="radio"/>	 AmazonDynamoDBFullAccess	AWS managed	None	Provides full access to Amazon DynamoDB via the AWS Management...	
<input type="radio"/>	 AmazonDynamoDBFullAcces...	AWS managed	None	Provides full access to Amazon DynamoDB including Export/Import us...	
<input type="radio"/>	 AmazonDynamoDBReadOnly...	AWS managed	None	Provides read only access to Amazon DynamoDB via the AWS Manag...	
<input type="radio"/>	 AmazonEC2ContainerRegistr...	AWS managed	None	Provides administrative access to Amazon ECR resources	
<input type="radio"/>	 AmazonEC2ContainerRegistr...	AWS managed	None	Provides full access to Amazon EC2 Container Registry repositories, b...	
<input type="radio"/>	 AmazonEC2ContainerRegistr...	AWS managed	None	Provides read-only access to Amazon EC2 Container Registry reposi...	
<input type="radio"/>	 AmazonEC2ContainerService...	AWS managed	None	Policy to enable Task Autoscaling for Amazon EC2 Container Service	
<input type="radio"/>	 AmazonEC2ContainerService...	AWS managed	None	Policy to enable CloudWatch Events for EC2 Container Service	
<input type="radio"/>	 AmazonEC2ContainerService...	AWS managed	None	Default policy for the Amazon EC2 Role for Amazon EC2 Container S...	
<input type="radio"/>	 AmazonEC2ContainerService...	AWS managed	None	Provides administrative access to Amazon ECS resources.	
<input type="radio"/>	 AmazonEC2ContainerService...	AWS managed	None	Default policy for Amazon ECS service role.	
<input type="radio"/>	 AmazonEC2FullAccess	AWS managed	None	Provides full access to Amazon EC2 via the AWS Management Console.	
<input type="radio"/>	 AmazonEC2ReadOnlyAccess	AWS managed	None	Provides read only access to Amazon EC2 via the AWS Management ...	▼

Microsoft Azure

Search resources, services, and docs (G+Y)

alex.gudanis@DefaultDi...
DEFAULT DIRECTORY
























Home > Default Directory - Roles and administrators

Default Directory - Roles and administrators

Search (Cmd+Y)

New custom role Refresh Got feedback?

Get just-in-time access to a role when you need it using PIM. Learn more about PIM →

	External Identity Provider administrator	Can configure identity providers for use in direct federation.	Built-in	...
	Global administrator	Can manage all aspects of Azure AD and Microsoft services that use Azure AD identities.	Built-in	...
	Global reader	Can read everything that a global administrator can, but not update anything.	Built-in	...
	Guest inviter	Can invite guest users independent of the 'members can invite guests' setting.	Built-in	...
	Helpdesk administrator	Can reset passwords for non-administrators and Helpdesk administrators.	Built-in	...
	Intune administrator	Can manage all aspects of the Intune product.	Built-in	...
	Kaizala administrator	Can manage settings for Microsoft Kaizala.	Built-in	...
	License administrator	Ability to assign, remove and update license assignments.	Built-in	...
	Message center privacy reader	Can read Message Center posts, data privacy messages, groups, domains and subscriptions.	Built-in	...
	Message center reader	Can read messages and updates for their organization in Office 365 Message Center only.	Built-in	...
	Password administrator	Can reset passwords for non-administrators and Password administrators.	Built-in	...
	Power BI administrator	Can manage all aspects of the Power BI product.	Built-in	...
	Privileged authentication administrator	Allowed to view, set and reset authentication method information for any user (admin or n...	Built-in	...
	Privileged role administrator	Can manage role assignments in Azure AD, and all aspects of Privileged Identity Managem...	Built-in	...
	Reports reader	Can read sign-in and audit reports.	Built-in	...
	Search administrator	Can create and manage all aspects of Microsoft Search settings.	Built-in	...
	Search editor	Can create and manage the editorial content such as bookmarks, Q and As, locations, floor...	Built-in	...
	Security administrator	Can read security information and reports, and manage configuration in Azure AD and Offi...	Built-in	...
	Security operator	Can create and manage security events.	Built-in	...
	Security reader	Can read security information and reports in Azure AD and Office 365.	Built-in	...
	Service administrator	Can read service health information and manage support tickets.	Built-in	...
	SharePoint administrator	Can manage all aspects of the SharePoint service.	Built-in	...
	Skype for Business administrator	Can manage all aspects of the Skype for Business product.	Built-in	...
	Teams Communications Administrator	Can manage calling and meetings features within the Microsoft Teams service.	Built-in	...
	Teams Communications Support Engineer	Can troubleshoot communications issues within Teams using advanced tools.	Built-in	...
	Teams Communications Support Specialist	Can troubleshoot communications issues within Teams using basic tools.	Built-in	...
	Teams Service Administrator	Can manage the Microsoft Teams service.	Built-in	...
	User administrator	Can manage all aspects of users and groups, including resetting passwords for limited adm...	Built-in	...

Cloud Privileges - Granular But Complex

Google Cloud Platform		britive-gdev.net		🔍							
IAM & admin		Roles		+ CREATE ROLE		📄 CREATE ROLE FROM SELECTION		DISABLE		🗑️ DELETE	
<div><div></div><div>IAM</div><div></div><div>Identity & Organization</div><div></div><div>Troubleshooter</div><div></div><div>Organization policies</div><div></div><div>Quotas</div><div></div><div>Service accounts</div><div></div><div>Labels</div><div></div><div>Settings</div><div></div><div>Privacy & Security</div><div></div><div>Cryptographic keys</div><div></div><div>Identity-Aware Proxy</div><div></div><div>Roles</div><div></div><div>Audit Logs</div></div>	<div><input type="checkbox"/></div>	<div></div>	Access Approval Approver	Access Approval	Enabled	⋮					
	<div><input type="checkbox"/></div>	<div></div>	Access Approval Config Editor	Access Approval	Enabled	⋮					
	<div><input type="checkbox"/></div>	<div></div>	Access Approval Viewer	Access Approval	Enabled	⋮					
	<div><input type="checkbox"/></div>	<div></div>	Access Context Manager Admin	Other	Enabled	⋮					
	<div><input type="checkbox"/></div>	<div></div>	Access Context Manager Editor	Other	Enabled	⋮					
	<div><input type="checkbox"/></div>	<div></div>	Access Context Manager Reader	Other	Enabled	⋮					
	<div><input type="checkbox"/></div>	<div></div>	Access Transparency Admin	Organization Policy	Enabled	⋮					
	<div><input type="checkbox"/></div>	<div></div>	Actions Admin	Actions	Enabled	⋮					
	<div><input type="checkbox"/></div>	<div></div>	Actions Viewer	Actions	Enabled	⋮					
	<div><input type="checkbox"/></div>	<div></div>	Admin	Cloud Talent Solution	Enabled	⋮					
	<div><input type="checkbox"/></div>	<div></div>	Admin of Tenancy Units	Service Consumer Management	Enabled	⋮					
	<div><input type="checkbox"/></div>	<div></div>	Android Management User	Android Management	Enabled	⋮					
	<div><input type="checkbox"/></div>	<div></div>	API Keys Admin	Service Usage	Enabled	⋮					
	<div><input type="checkbox"/></div>	<div></div>	API Keys Viewer	Service Usage	Enabled	⋮					
	<div><input type="checkbox"/></div>	<div></div>	App Engine Admin	App Engine	Enabled	⋮					
	<div><input type="checkbox"/></div>	<div></div>	App Engine Code Viewer	App Engine	Enabled	⋮					
	<div><input type="checkbox"/></div>	<div></div>	App Engine Deployer	App Engine	Enabled	⋮					
	<div><input type="checkbox"/></div>	<div></div>	App Engine Service Admin	App Engine	Enabled	⋮					
	<div><input type="checkbox"/></div>	<div></div>	App Engine Viewer	App Engine	Enabled	⋮					
	<div><input type="checkbox"/></div>	<div></div>	AutoML Admin	AutoML	Enabled	⋮					
<div><input type="checkbox"/></div>	<div></div>	AutoML Editor	AutoML	Enabled	⋮						
<div><input type="checkbox"/></div>	<div></div>	AutoML Predictor	AutoML	Enabled	⋮						
<div><input type="checkbox"/></div>	<div></div>	AutoML Viewer	AutoML	Enabled	⋮						
<div><input type="checkbox"/></div>	<div></div>	Beacon Attachment Editor	Proximity Beacon	Enabled	⋮						
<div><input type="checkbox"/></div>	<div></div>	Beacon Attachment Publisher	Proximity Beacon	Enabled	⋮						
<div><input type="checkbox"/></div>	<div></div>	Beacon Attachment Viewer	Proximity Beacon	Enabled	⋮						
<div><input type="checkbox"/></div>	<div></div>	Beacon Editor	Proximity Beacon	Enabled	⋮						
<div><input type="checkbox"/></div>	<div></div>	BigQuery Admin	BigQuery	Enabled	⋮						
<div><input type="checkbox"/></div>	<div></div>	BigQuery Connection Admin	BigQuery	Enabled	⋮						
<div><input type="checkbox"/></div>	<div></div>	BigQuery Connection User	BigQuery	Enabled	⋮						
<div><input type="checkbox"/></div>	<div></div>	BigQuery Data Editor	BigQuery	Enabled	⋮						
<div><input type="checkbox"/></div>	<div></div>	BigQuery Data Owner	BigQuery	Enabled	⋮						
<div><input type="checkbox"/></div>	<div></div>	BigQuery Data Viewer	BigQuery	Enabled	⋮						

SETUP Profiles	
Profiles	
All Profiles Clone	
A B C D E F G H I	
Profile Name	User License
Analytics Cloud Integration User	Analytics Cloud Integration User
Analytics Cloud Security User	Analytics Cloud Integration User
Authenticated Website	Authenticated Website
Authenticated Website	Authenticated Website
Chatter External User	Chatter External
Chatter Free User	Chatter Free
Chatter Moderator User	Chatter Free
Contract Manager	Salesforce
Cross Org Data Proxy User	XOrg Proxy User
Custom: Marketing Profile	Salesforce
Custom: Sales Profile	Salesforce
Custom: Support Profile	Salesforce
Customer Community Login User	Customer Community Login
Customer Community Plus Login User	Customer Community Plus Login
Customer Community Plus User	Customer Community Plus
Customer Community User	Customer Community
Customer Portal Manager Custom	Customer Portal Manager Custom
Customer Portal Manager Standard	Customer Portal Manager Standard
External Identity User	External Identity
Force.com - App Subscription User	Force.com - App Subscription
Force.com - Free User	Force.com - Free
Gold Partner User	Gold Partner
High Volume Customer Portal	High Volume Customer Portal
High Volume Customer Portal User	High Volume Customer Portal
Identity User	Identity
Marketing User	Salesforce
Partner App Subscription User	Partner App Subscription
Partner Community Login User	Partner Community Login
Partner Community User	Partner Community
1-36 of 36	
Previous Next	

Managing Complexity is Not Easy

☁ Especially with spreadsheets

Example shown is from GCP

Number of Permissions: 2065	Number of Permissions: 1858	Number of Permissions: 850	Number of Permissions: 533
Owner	Editor	Viewer	Security Admin
accessapproval.requests.approve			
accessapproval.requests.dismiss			
accessapproval.requests.get	accessapproval.requests.get	accessapproval.requests.get	
accessapproval.requests.list	accessapproval.requests.list	accessapproval.requests.list	accessapproval.requests.list
accessapproval.settings.get	accessapproval.settings.get	accessapproval.settings.get	
accessapproval.settings.update			
accesscontextmanager.accessLevels.create	accesscontextmanager.accessLevels.create		
accesscontextmanager.accessLevels.delete	accesscontextmanager.accessLevels.delete		
accesscontextmanager.accessLevels.get	accesscontextmanager.accessLevels.get	accesscontextmanager.accessLevels.get	
accesscontextmanager.accessLevels.list	accesscontextmanager.accessLevels.list	accesscontextmanager.accessLevels.list	accesscontextmanager.accessLevels.list
accesscontextmanager.accessLevels.update	accesscontextmanager.accessLevels.update		
accesscontextmanager.accessPolicies.create	accesscontextmanager.accessPolicies.create		
accesscontextmanager.accessPolicies.delete	accesscontextmanager.accessPolicies.delete		
accesscontextmanager.accessPolicies.get	accesscontextmanager.accessPolicies.get	accesscontextmanager.accessPolicies.get	
accesscontextmanager.accessPolicies.getIamPolicy	accesscontextmanager.accessPolicies.getIamPolicy	accesscontextmanager.accessPolicies.getIamPolicy	accesscontextmanager.accessPolicies.getIamPolicy
accesscontextmanager.accessPolicies.list	accesscontextmanager.accessPolicies.list	accesscontextmanager.accessPolicies.list	accesscontextmanager.accessPolicies.list
accesscontextmanager.accessPolicies.setIamPolicy			accesscontextmanager.accessPolicies.setIamPolicy
accesscontextmanager.accessPolicies.update	accesscontextmanager.accessPolicies.update		
accesscontextmanager.accessZones.create	accesscontextmanager.accessZones.create		

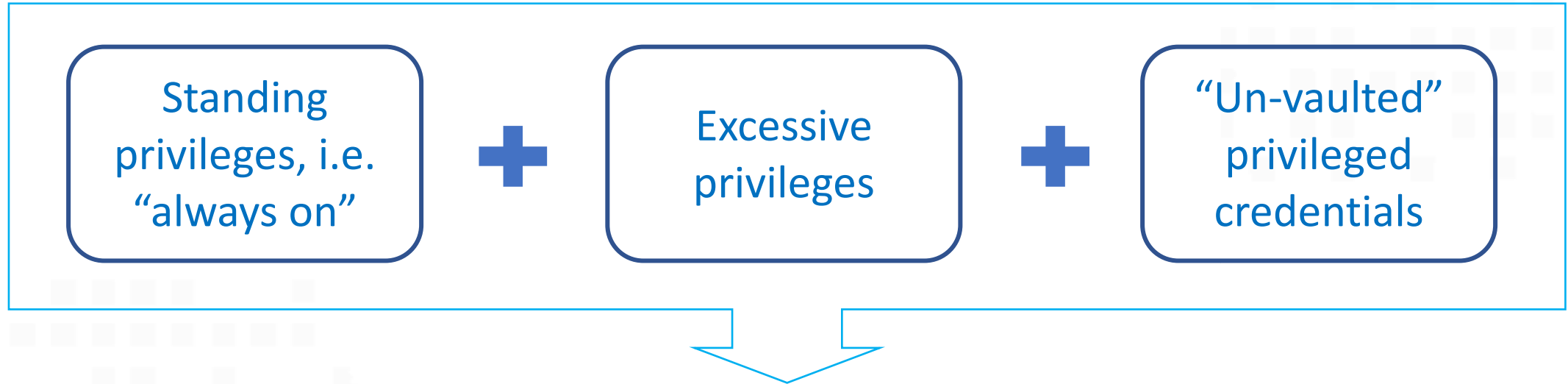
It's even worse when there is no process and consistency!

Complexity Results in Excessive Privilege

- ☁ Privileges are granted too broadly
- ☁ Privilege “creep” is common
- ☁ Privilege right-sizing is not a regular process

Excessive Privileges = High Risk of Access Breach

Standing Privileges Multiply the Risk

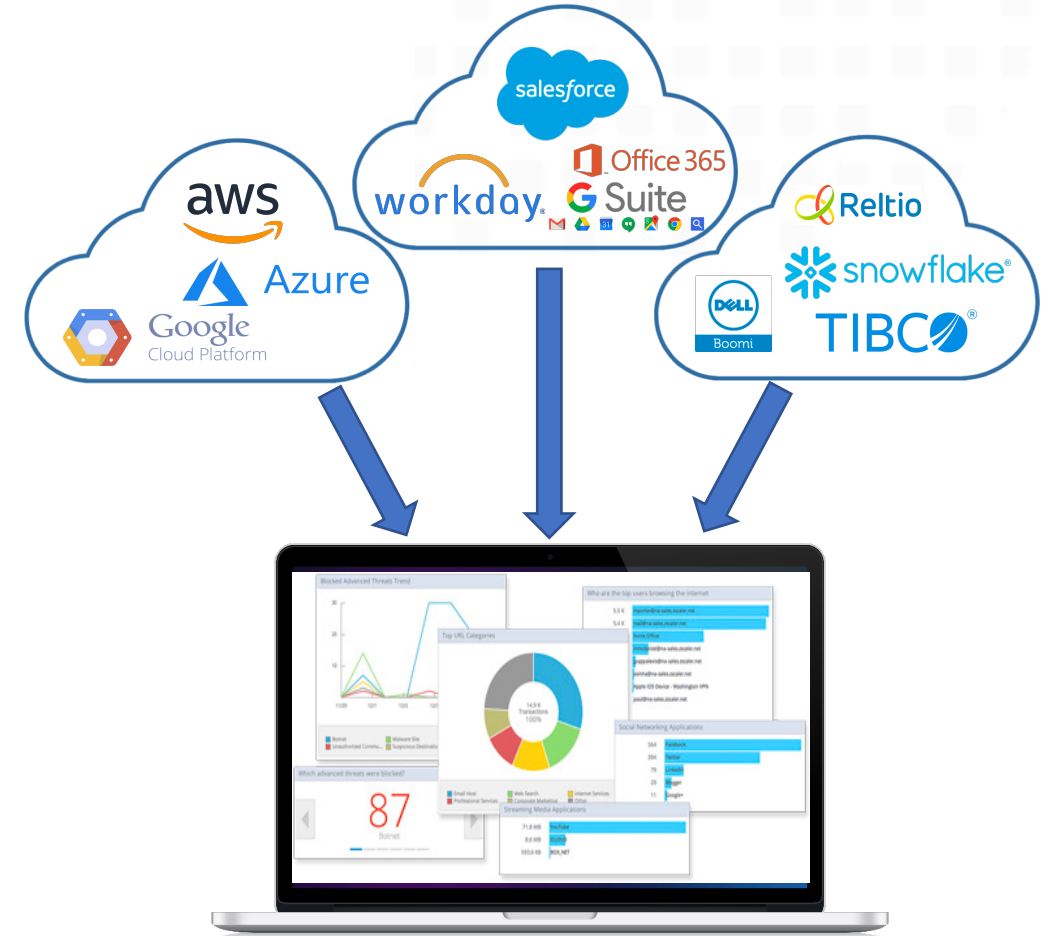


The result is exponentially higher risk of access breach that is mostly unmanaged!

Transforming Cloud Privileged Access from Weakness to Strength!

You Can't Control What you Can't See

- ☁ Discover and inventory
 - ☁ Accounts & creds
 - ☁ Privileges & permissions



Define Privilege Use Cases

Who	What	Where	When	Why
DevOps	Console, CLI, API, Containers, Servers	AWS, Azure	Continuous	Normal work
Security	Security Functions, Containers, Servers	AWS, Salesforce	Continuous	Normal work
Business	Admin Functions	Workday, Salesforce	Periodic	Delegated admin
Service Desk	Configuration/ Admin Functions	ServiceNow, Salesforce	Continuous	Normal work
Project Staff	Configuration/ Admin Functions	Workday	Occasional	Project needs

Building the Privilege Governance Framework

- ☁ Basic PAM first - credential vaulting
 - ☁ break-glass accounts, cloud “root”, keys, etc.



Cloud Privilege Management Best Practices



Just in Time
(JIT) Privilege
Grant



Policy-Based
Privilege
Authorization



Zero Standing
Privileges (ZSP)

Cloud Privilege Management Best Practices



Cloud
SSO/MFA
Integration







Identity
Governance &
Life Cycle
Integration

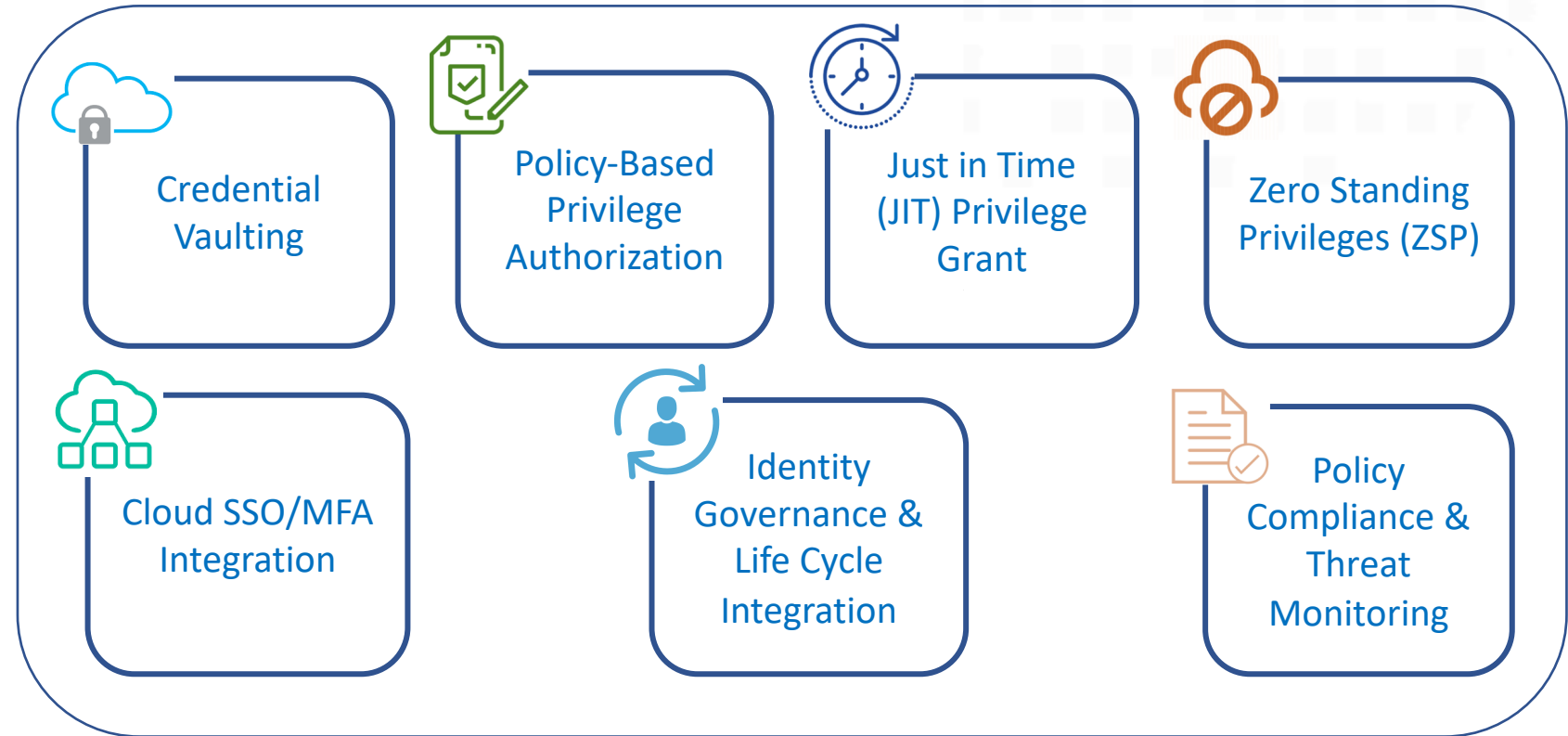


Policy
Compliance &
Threat
Monitoring

Cloud Privilege Access Governance Framework

Prioritize implementation

-  Use cases
-  Risk exposure
-  Cloud capabilities
-  Resource skills



Thank You!

Art Poghosyan

CEO, Britive Inc.

art@britive.com

