gemalto
security to be free

GUIDE BOOK

4 Steps to Cloud Access Management

A Practical Step-by-Step Guide to Managing Cloud Access in your Organization

Cloud Access Challenges in the Enterprise

Cloud apps in the enterprise have become mainstream, with 93% of organizations using cloud-based IT services[1]. But leveraging cloud-based applications comes with its share of challenges. As organizations embrace cloud apps for their quick time to value and best of breed technology, they are confounded with increasing management and usage complexities.

Password fatigue

Users need to maintain countless usernames and passwords. They are required to authenticate numerous times every day with each application they open, and often resort to security workarounds. This leads to password fatigue—the exhaustion that results from the endless need to create, update and reset passwords for different applications on a daily basis.

Poor security

By default, cloud apps are only protected using weak, static passwords—a reality that jeopardizes the confidentiality of sensitive information and increases the risk of a breach. The majority of worldwide data breaches can be thwarted using strong two-factor authentication[2].

Complex management

Each new cloud app brought into the enterprise requires management and user-troubleshooting from a different console or admin portal. When a dozen or more apps are used across the business, administration becomes unscalable.

Compliance risk

Proving regulatory compliance requires visibility into access events. IT departments need to know who is accessing what app and when. Furthermore, with sensitive data residing in cloud apps, administrators need to know how users' identities are being verified.

High helpdesk costs

The proliferation of cloud identities and access credentials results in frequent password resets, which account for 20% of an organization's helpdesk costs[3].

1 Source: Spiceworks, Survey: 93 Percent of Organizations Use Cloud-Based IT Services
2 Source: Verizon 2016 Data Breach Investigations Report
3 Source: Statisnet, Forgotten user passwords – Eliminate the Problem Dramatically Reduce the Cost

Four Easy Steps to **Full Cloud Access Control**

Step 1 –
Apply Cloud Single Sign On

To rid users of password fatigue and free IT from the hassle of password resets, apply cloud single sign on to all the cloud applications used in your organization.

What is Single Sign On?
Single sign-on (SSO) provides the capability to authenticate once, and be subsequently and automatically authenticated when accessing various resources. It eliminates the need to separately log in and authenticate to individual applications and systems, essentially serving as an intermediary between the user and target applications .

With Single Sign On (SSO), users log in just once in order to concurrently gain access to all their cloud applications. And they log in with their current enterprise identity—the same identity they use to login in to the network in the morning, or the VPN at night.

Tailor SSO per Role
Different users and user groups require access to different cloud applications, and single sign on can be enforced on any number of cloud apps as required by different teams, roles, departments and individual users. For example, in addition to company-wide applications, R&D may require access to apps such as Jira, Confluence and AWS, while Marketing may require access to Salesforce, Office 365 and WordPress. Business partners, such as contractors and distributors may require access to a more limited set of cloud apps, such as partner portals and productivity suites.

Create role-based user groups in your enterprise user store, be it Active Directory, MySQL or other repository, to simplify the subsequent configuration of group-based access policies.

Role-based groups also make it easy to provision, update and revoke access permissions, as users join or leave the company, or move from one role to another.

SSO Benefits: Convenience, Easy Management and Compliance
Not only does SSO provide convenient and frictionless access for users, but it also makes the administrator's life easier by allowing IT to maintain just one identity—just one username and password—per user, for all cloud resources. This eliminates the hassle of password resets and the overhead required to troubleshoot users from multiple administration consoles. not all applications require the same level of security, and not all users have just one username and password—per user, for all cloud resources. This eliminates the hassle of password resets and the overhead required to troubleshoot users from multiple administration consoles.

And with a single pane of glass for viewing all access events, IT gain visibility into who is accessing what and when, and using what authentication method, making regulatory compliance and security audits a breeze. With a unified view of cloud access, underutilized app licenses can also be identified.

The concept of single sign-on has long been implemented for on-premises applications, portals and networks (for example, using the Kerberos protocol). With the evolution in identity federation protocols (such as SAML 2.0) which extend enterprise identities to the cloud, organizations can now enjoy that same level of convenience across cloud-based resources.

> With Single Sign On (SSO), users log in just once in order to concurrently gain access to all their cloud applications.

Step 2 –
Protect Identities with Granular Access Policies

While SSO provides optimal convenience for users and ease of management for IT, it only solves part of the cloud access management puzzle. SSO allows maintaining a single identity for each user for all cloud apps, but what happens if that single identity is compromised? This is where scenario-based access policies come in, to let you determine the right level of authentication for the right user at the right time.

Scenario-based Access Policies
We are all familiar with two-factor authentication (2FA) but 2FA may be excessive for low risk apps accessed from the corporate network and similar access scenarios. Therefore, to protect that single identity at the right level of trust—using the right level of authentication—granular access policies can be applied to match the level of authentication with the specific scenario at hand. For example, the level of trust required for a low-risk time management app may be different from the level of trust required when logging in to a sensitive resource such as the corporate VPN. Likewise, logging in to an IT administrator or CEO account may require stronger security.

Since not all applications require the same level of security, and not all users have the same account privileges, scenario-based access policies can be defined to take into consideration the sensitivity and risk exposure of a cloud app, as well as the privileges held by any user group (for example, C-suite executives and IT administrators).

Where the level of trust is low, such as when logging in from an unrecognized network, security can be stepped up with an additional authentication factor, such as out-of-band push authentication or other 2FA method. When the level of trust is high, such as when logging from the office network and a known device, the user can gain immediate access.

Leverage Context for Continuous Authentication
By leveraging contextual information such as whether the user is logging in from a trusted network or recognized device, access management solutions ensure the most convenient user experience possible --demanding users to step up authentication only in high risk situations. As users move from their laptops in the morning, to their tablets at lunch and back to their laptops at night, the appropriate access policy is enforced according to the app they are logging into, the team of which they are part and

> The level of trust required for a low-risk time management app may be different from the level of trust required when logging in to a sensitive resource such as the corporate VPN

the contextual information gleaned from their behavior --ensuring continuous authentication at the right level of trust throughout the day.

So after applying single sign on to all the cloud apps utilized by each user group, for example C-Suites, R&D, Sales and Operations, enforce scenario-based access policies that tailor the authentication method to the scenario at hand. This will let you trust every login, while keeping access frictionless.

Start Global and Go Granular
To simplify the setup of access policies, consider starting with a single global policy, and then adding exceptions to that policy as necessary.

Your global policy serves as the default access policy for all cloud apps and users, requiring employees, for example, to login once to each SSO session using an OTP, and proceeding without any additional authentication afterwards to all their cloud and web apps.

Once the global policy is in place, exceptions can be made to require stronger authentication in high risk scenarios, such as when accessing a certain sensitive app from outside the network. Non-sensitive apps would still require only the default access controls defined in the global policy.

Step 3 –
Optimize Access Policies with Data-driven Insights

How do you know if your access policies are too lenient, too cumbersome or just right? The answer is data-driven insights. By seeing what applications are accessed throughout the day, by which users they are accessed and using what access policy, IT can fine-tune scenario-based access policies over time.

For example, if users often access a sensitive app from an unknown network or high-risk location, as shown by the frequency in which a policy is invoked, the policy can be modified to increase the level of trusted mandated to access a certain app. If the policy heretofore only required a password or PIN, it can be fine-tuned to require entering a one-time passcode.

Conversely, if an access policy requiring a password and OTP is invoked frequently for all users, there may be room to consider simplifying the login journey by requiring minimal credentials, such as username and OTP only, with contextual information leveraged for additional authentication information (such as determining whether a login is made from a known or unknown device).

By incorporating statistical data into their access policies, organizations can implement effective risk management, and balance between security and usability expectations.

Step 4 – Ensure Scalability of your Cloud Estate

How many cloud apps does your organization plan to add next year? Are there any mergers and acquisitions on the horizon? When evaluating cloud access management solutions, ensure that you can scale and evolve your solution over time by easily adding user groups and new cloud-based applications as the need arises.

Industry-wide standards such as SAML 2.0 are supported by most cloud services, enabling you to scale cloud access management as you adopt additional applications. Built-in integration templates also simplify the deployment of new integrations.

SafeNet Trusted Access – **The Smart Way to Manage Cloud Access**

SafeNet Trusted Access is an access management service that combines the convenience of single sign-on with granular access security. By validating identities, enforcing access policies and applying Smart Single Sign-On, organizations can ensure secure, convenient access to numerous cloud applications, and reduce management overhead by centrally defining and enforcing access controls from one easy-to-navigate console.

Offering fast and easy set-up, SafeNet Trusted Access simplifies cloud adoption and enables increased visibility and compliance, while providing scalability through simplified workflows delivered from the cloud.

With flexible, customizable authentication and access controls, SafeNet Trusted Access removes complexity and frustration for end-users, allowing them to use a single enterprise identity to access all their cloud apps.

gemalto
security to be free

ABOUT GEMALTO'S SAFENET IDENTITY AND DATA PROTECTION SOLUTIONS

Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of digital identities, transactions, payments and data – from the edge to the core. Gemalto's portfolio of SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing strong authentication and identity management solutions, innovative encryption methods and best-in-class key management to secure what matters most: Data and Identities. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com
Follow Us: blog.gemalto.com/security

GEMALTO.COM

gemalto
security to be free