Cloud-born Management Complexities
By default, each new cloud app adopted by an organization, adds complexity to its access management workflows. Employees are burdened with an additional credential set which they need to create and maintain, fueling password fatigue. Helpdesk overheads increases due to lost and forgotten passwords, while security becomes a major concern as sensitive data residing in the cloud is accessed only with weak, static passwords. Managing identities from disparate consoles becomes inefficient, while compliance becomes harder to maintain, as IT lack visibility into who is accessing which app, when and how.

Without centrally managed access controls, the use of cloud apps within an organization cannot be scaled, and results in security holes, high administration costs, user frustration and organizational inefficiencies.

Identity is the New Perimeter
To address these identity management complexities, identity federation protocols have emerged, serving as the foundation of single sign-on solutions, which enable using the same enterprise identity across different websites. Instead of creating a new identity for each cloud-based service, enterprises can use identity federation protocols to enable their employees to access all their cloud applications with their familiar Active Directory username and password, or other enterprise credential. In this way, each time a user accesses a cloud or web service, the authentication process is relayed to a central trusted system that validates the user’s identity.

Thanks to identity federation and cloud single sign-on, instead of maintaining dozens of separate username and password sets, users can maintain just one. And the process of validating identities becomes more effective and secure, as a specialized service or system is used to ensure that users are who they claim to be each time they access a web or cloud resource.
Managing the new identity perimeter with cloud access management

SAML-based Single Sign-On
The predominant identity federation standard used for cloud single sign on is SAML, the Security Assertion Markup Language, which is an XML-based open standard for exchanging authentication and authorization data between organizations. A single SAML-supporting system called a trusted Identity Provider (IdP) governs the authentication of users, with cloud and web apps (called Service Providers, or SPs) relaying the authentication process to the trusted Identity Provider each time a user attempts to access them.

How It Works
1. The user opens a cloud application and enters their credentials.
2. The user’s credentials are validated in the background by the trusted identity provider.
3. The identity provider sends a SAML assertion to the cloud or web application with an accept or reject response.
4. Depending on the response, the user is granted or denied access, or is prompted to step-up authentication.

A Solid Foundation for Cloud IAM
By extending employer-issued identities to the cloud with SAML, employees and consultants can use just one identity to access all their cloud and web apps, and enjoy cloud single sign-on for increased access speed and convenience. Meanwhile, IT benefit from single-pane management of cloud identities and the ability to step-up authentication in risky situations based on fine-grained access policies that can be defined per app or group of apps. Using contextual attributes such as user role, location, source network and device, users can gain immediate access or be prompted for an additional authentication factor.

SafeNet Trusted Access – Intuitive Cloud Access Management
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 their cloud and web applications.

To learn more about access management from Gemalto, visit https://safenet.gemalto.com/access-management or join a live demo webinar.

Benefits of SAML-based cloud access management
> Simplified access with cloud SSO
> Reduced password resets owing to lost or forgotten passwords
> Scalable cloud adoption through single pane access management
> Scenario-based access policies that meet business and compliance needs
> Unified visibility into cloud access events for easy compliance
> Industry-vetted standard widely recognized by the experts

About Gemalto’s SafeNet Identity and Data Protection Solutions
Gemalto offers one of the leading portfolios of enterprise security solutions, enabling its customers to benefit from industry-leading protection of data, digital identities, payments and transactions - from the edge to the core. Gemalto’s SafeNet Identity and Access Management solutions enable enterprises across many verticals, including major financial institutions and governments, to utilize access management, PKI credential management, strong authentication and identity management solutions to secure access to sensitive resources and protect digital interactions. 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/contact-us
Follow Us: blog.gemalto.com/security

GEMALTO.COM