Cloud Proliferation and Password Fatigue
As enterprises adopt cloud applications, users are plagued with password fatigue—the never-ending burden of creating and maintaining separate identities and passwords for the multiple cloud and web apps they need to access on a daily basis. Adding to the frustration and downtime, when accessing certain resources, users are also required to validate their identities with strong multi-factor authentication, slowing down the access journey even further.

Simplifying Cloud and Web Access
To offer the most frictionless experience possible without sacrificing security, organizations can leverage cloud single sign-on (cloud SSO) combined with contextual information and step-up authentication. This lets users access all their cloud and web applications with a single identity and password, and lets IT require stronger access security only in high risk situations.

In fact, cloud access management solutions have emerged, providing organizations with the ability to set flexible access policies that include:

- Single Sign On
- Granular access policies
- Context-based Authentication
- Session management

Access policy is applied:
• What level of authentication is needed?

Evaluate context:
• Is there a current SSO session?
• Are you in the office?

Context is evaluated:
• Are you in the office?
• What device are you using?

Access policy is applied:
• What level of authentication is needed?

Long in to App 1

Long in to App 2
Cloud and Web Single Sign-On
Cloud single sign-on enables users to access all their cloud and web applications using a single identity – a single username and password set. So instead of maintaining 10 or 20 passwords, users can maintain just one!
Cloud SSO removes the need to re-authenticate separately to each cloud application, allowing users to easily move from one cloud app to another.

Contextual Authentication
Contextual authentication is central to creating compliance-based access policies and preventing security fatigue. Taking into account variables, such as your network, location and operating system, contextual data provides additional information on a login attempt, and fires the appropriate access policy.

By assessing a user’s contextual login attributes, single sign on and access management solutions can continuously match the level of authentication required from the user with the access policy defined for each application.

In this manner, authentication is applied granularly—in the most frictionless manner possible—per an application’s access policy, rather than as a blanket, uniform rule for all enterprise resources.

Continuous Authentication through Contextual Data
When context-based authentication is utilized as part of a broader access management solution, authentication is no longer a binary yes / no decision.

Rather, using contextual attributes, authentication becomes a process that verifies identities in the background each time a user accesses a new application, without the user even knowing it.

Essentially, contextual authentication enables continuous, unobtrusive identity verification.

How It Works
Each time you log in to an app, the cloud access management solution checks for the appropriate policy for that app and your user role, and enforces the appropriate controls while leveraging contextual data.

In the morning you could access Office 365. If you’re in the office, and you’re logging from a recognized laptop, you could be provided immediate access.

Then in the afternoon, you may be at a meeting, using your tablet to access Salesforce. Since you’re logging in from a new device, while still connected to the company network, you may be required to enter your single sign-on password.

If you go to an off-premises meeting, the solution will see that you’re logging in from outside the network, and require a one-time passcode to initiate a new single sign on session.

You are then free to move from one app to another with no further authentication.

Benefits of Contextual Authentication within an Access Management framework
- Simplified cloud access with SSO secured by contextual access security
- Customizable access policies protect access for workers logging in from within or outside the office
- Enables privileged access policies for C-Suites, IT admins and other privileged users
- Facilitates compliance with PCI DSS, GDPR and other regulatory mandates as policies are tailored per target app

SafeNet Trusted Access - Context-sensitive SSO
SafeNet Trusted Access is an access management service that combines the convenience of single sign-on with context-sensitive access security. By validating identities, enforcing access policies and applying Smart Single Sign-On, organizations can ensure secure, convenient access to all their cloud applications.

Smart Single Sign-On lets users log in to all their cloud applications with a single identity, eliminating password fatigue, frustration, password resets and downtime. SafeNet Trusted Access processes a user’s login requests and ensures that SSO is applied intelligently, based on previous authentications in the same SSO session and the specific contextual policy requirements applicable to each access attempt. In this way, users may authenticate just once in order to access all their cloud applications, or provide additional authentication, as required by the policy.

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

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 2018. All rights reserved. Gemalto, the Gemalto logo, are trademarks and service marks of Gemalto and are registered in certain countries. SB(IN)-Feb.03.2018 - Design: ELC