thalescpl.com

THALES

Matching Risk Policies to User Needs with Cloud Access Management

Whereas traditional Single Sign-On solutions apply a blanket policy to all target resources, access management solutions have emerged to offer the convenience of SSO combined with the fine-grained security offered by customizable access policies.

By applying SSO to target web and cloud applications, while fine-tuning access controls and authentication requirements per specific use-case scenarios, organizations can offer their users frictionless access while remaining protected, compliant and in control.

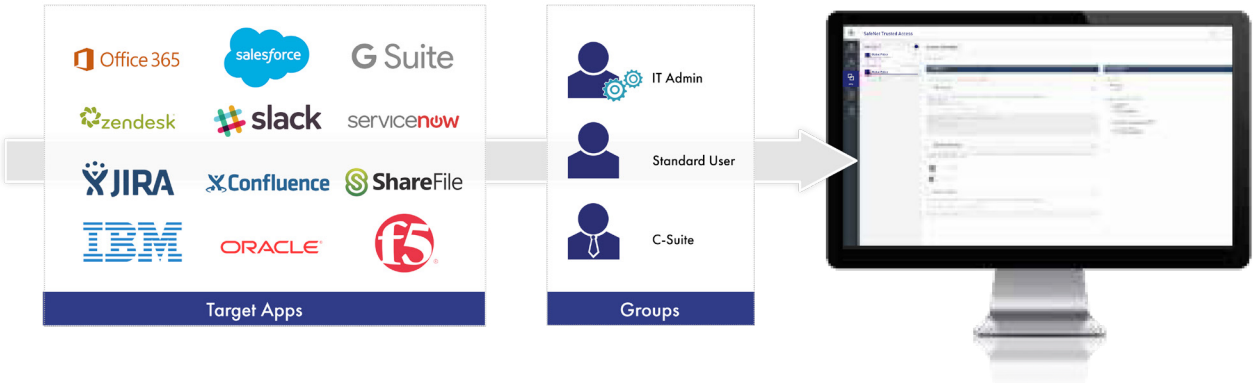
Fine-Grained SSO Access Security

When configuring policies for business critical applications, organizations normally opt for more stringent access controls to elevate the assurance that a user is who they claim to be. The same is true for securing access by privileged users, remote workers, external consultants or contractors and securing access from countries where your organization does not normally do business. These use case scenarios can be easily accommodated using dedicated, fine-grained access policies configured for cloud and webbased services.

Applying elevated Access Controls on Remote Workers

Remote workers logging in outside of the corporate network may require additional authentication factors, as compared to local

workers logging in from the office. To this end,a global policy can be set up, requiring only a domain password for users launching an SSO session from within the office, inside the corporate network. An exception policy can be added to require an additional authentication factor, such as a one-time passcode (OTP), for any user external to the known network, logging in from outside the office. In this way, users logging in from inside the office, log in to the SSO session only with a domain password, and can then easily move from one application to another (unless configured otherwise). Conversely, users logging in from outside the office would be prompted to enter a second factor in the form of an OTP.



Applying elevated Access Controls on Business Critical Applications

Some organizations may wish to offer SSO to most of theirapplications, while requiring elevated access controls to business critical applications that harbor sensitive data or underlie core infrastructure. Addressing this scenario, IT administrators can set up a policy requiring password-only authentication for users accessing their first app at the start of their day. An exception policy could be added to require additional authentication for users accessing businesscritical applications. For example, users could be prompted to enter an OTP, or approve a login request pushed to their mobile device.

Applying elevated Access Controls on certain Geographic Locations

Organizations concerned about access to their applications originating from geographic locations where they don't typically do business, can either deny access attempts coming in from identified countries, or they can define more stringent access controls for these access attempts. Configuring specific controls around access attempts originating from these countries, allows organizations to monitor activity originating from certain locales. For example, an exception policy could be set up to require multi-factor authentication each time a single sign on session is started from any of the identified geographies.

Apply elevated Access Controls on External Consultants

Businesses who wish to provide their core internal users an SSO experience, while elevating access controls for external contractors and consultants, can do so by configuring a policy based on this user group, which requires a second authentication factor each time a single sign on session is initiated. In this way, contactors can still enjoy frictionless access to all their applications, while IT can elevate the assurance level around SSO sessions launched by this group of users.

Strategic Value for your Business

SafeNet Trusted Access is a cloud access management service that offers single sign-on secured by granular access policy enforcement.

By enabling IT Administrators to create use-case based policies, SafeNet Trusted Access provides them with flexibility in protecting their organization and sensitive applications without adversely impacting the end users' SSO experience.

Granular exception policies empower IT to increase security on specific applications, geographies or groups of users, while providing a frictionless access journey to core users and use-cases.

By tailoring access policies to the scenario at hand, IT can ensure that policies are as stringent or as lax as required, prompting for no credentials, a single credential or multiple credentials each time a user logs in to an SSO session or an individual app.

To learn more about access management from Thales, visit https://safenet.gemalto.com/access-management/ or join a livedemo webinar at https://www.brighttalk.com/webcast/2037/334449

About SafeNet Access Management and Authentication Solutions

Thales's industry-leading Access Management and Authentication solutions let enterprises centrally manage and secure access to

enterprise IT, web and cloud-based applications. Utilizing policy based SSO and universal authentication methods, enterprises can effectively prevent breaches, migrate to the cloud securely and simplify regulatory compliance.

Benefits of Scenario-based Access Controls

- Offer the convenience of SSO without sacrificing security
- Require stronger access controls per SSO session or per individual app
- Tailor access policies per application, geography or user group
- Easily meet regulatory mandates by setting up dedicated access policies, e.g. PCI DSS, GDPR, PSN, EPCS etc.
- Configure access policies to be as stringent or lax as required

> thalescpl.com <

Americas – Thales eSecurity Inc. 2860 Junction Ave, San Jose, CA 95134 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com