cpl.thalesgroup.com

THALES

SafeNet Trusted Access

Cheat Sheet

Customer Problem

Leveraging cloud apps in the enterprise comes with its share of challenges:

- **Password fatigue** -The ongoing need to create, remember, update and reset an excessive number of passwords
- **Poor security** - Cloud apps are by default only protected using weak, static passwords.
- **Inefficient management** -Managing users from disparate consoles is not scalable.
- **Compliance risk** -Visibility into access events across apps becomes a burden and increases compliance risk
- **High Helpdesk costs** -20% of help desk tickets are a result of lost or forgotten passwords.

Solution Description

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.

Value for Thales Partners

- Short sales cycle enabled by a cloud-based solution that requires only a short setup
- Simple per-user, per-month pricing structure
- Prepackaged fixed-scope, fixed-price Professional Services Packages facilitate sales and offer additional revenue
- Easy-to-sell package with choice of free hardware of software token (OTP app) included in the subscription price
- Easy to Demo and set up demo account
- Free Proof-Of-Concept for 30 days
- Customers can retain current token investments while migrating to Thales's solution, as its supports 3rd party RADIUS and OATH tokens

Value for your customers

- Reduce investment –no infrastructure or upfront costs
- Flexible Delivery –on-premises or cloud-based
- Simple and fast deployment
- Automated provisioning and administration
- Protect Everything: VPN, cloud apps, VDI, web portals, local networks
- Effective risk management with context-based authentication
- Self-service portals lower helpdesk costs
- Smooth incremental migration maintains current investments
- Subscription-based pricing
- Increased user convenience with frictionless authentication methods

Competitive Differentiation

How can we differentiate from competing solutions?

Differentiator	Why is it unique?
Combined solution for MFA and Access Management	• Manage multi-factor authentication, cloud SSO and customizable policies from one platform • Easier management: No need to manage two separate solutions • Lower admin costs
Broadrange of authentication methods	**No "One-Size-Fits-All" approach to AuthN** • The current threat landscape requires different methods of authentication depending on the type of users (admins, sales, finance), the type of application (sensitive or not), the use case (out of office, in the office). • Only a solution that offers a broad range of authentication methods can achievethe differentiated risk management that you need in order to address complex security needs. • Support methods include: hardware tokens, software tokens (OTP apps), out-of-band (OOB) push authentication, OOB via SMS and email, pattern-based authentication, contextual authentication.
Smart SSO	• No open-buffet approach to SSO. • Regular SSO can be risky since you are allowing accessto all apps with the same authentication credentials. If those credentials are compromised, all apps will vulnerable. • Our solution is different in that the SSO and authentication are applied per policy-not globally. With smart SSO, IT maintains security since the SSO is per policy, and not as a blanketrule to all apps and use cases (not"buffet style"). Thismeans that organizations can offer an SSO experience to users, but still maintain security.
Use case-based policy setting	• STA lets you start global and go granular, making it easy to set up scenario-based access policies. • Start with a global SSO policy for all your cloud apps. An exception policy can then be defined to require tighter security for higher sensitivity apps or user groups, while leveraging contextual conditions. • Ideal for compliance with PCI DSS, NERC, PSN, etc. Policies can be customized per app, user role, contextual conditions (e.g. IP address, location) and require password, MFA, or password+MFA authentication.
Data-driven insights	• Data on pass/failed login attempts, access stats per policy, access stats per app. • With data-driven insights on access events, organizations can fine-tune their access policies. • Ensures that your access policies are neither too lax nor too stringent. • Enables identifying underutilized cloud app licenses.
Easy app integration	• Template-based integrations make it quick and easy to add new cloud and SAML apps.

Market Segments

Enterprises (workforce authentication).
For internal users (employees) and external users (business partners, consultants)

Target Customer Profile

Our goal is to target customers who:

- Are using cloud apps, and planning on expanding their use
- Have not implemented an IDaaS / Web SSO solution
- Are looking to complement their enterprise SSO solution with a Cloud SSO solution

"By 2022, **SaaS-delivered AM will be the chosen delivery model** for more than 80% of new access management purchases globally, up from 50% today."

Gartner, Inc. | G00378701 – January 2019

"By 2023, 60% of large enterprises, and 80% of MSEs, will deploy **MFA consolidated with AM**, up from 10%-25%, today."

Gartner, ID729931, June 2020

Qualifying Questions

The first thing to verify is whether the customer already is using an IDaaS solution. Those that are not, will more likely be potential customers for STA.

- **Customers who are NOT using a web SSO or IdaaS solution:**
  - How many cloud apps are deployed in your organization?
  - How is your company approaching cloud adoption and how are you defining security best practices?
  - What kind of are your users facing when having to manage multiple asswords for the various apps? How do you handle that currently?
  - What other applications does SAS protect besides the VPN?
  - How do you plan to apply 2FA and SSO to other cloud apps?
- **Customers who ARE already using an IDaaS / password vault / federation solution:**
  - What are you using today?
  - How does it allow you to set policies per application and per user?
  - What type of 2FA methods can you use?
  - What additional features would you like to see in your current solution that are not available?
  - What types of other solutions are you looking into at this time?

Corporate position of strength

Today's enterprises depend on the cloud, data and software in order to make decisive decisions. That's why the most respected brands and largest organizations in the world rely on Thales to help them protect and secure access to their most sensitive information and software wherever it is created, shared or stored –from the cloud and data centers to devices and across networks.

Thales solutions enable organizations to move to the cloud securely, achieve compliance with confidence, and create more value from their software in devices and services used by millions of consumers every day. Decisive technology for decisive moments.

Thales is a global organization with operations on all continents serving five major markets, all of them of vital importance for our societies: aerospace, space, ground transportation, defense and security, and digital security. From the bottom of the ocean to the depth of space and cyberspace, Thales provides a unique range of technologies and services that make tomorrow possible, today. Thales is comprised of 80,000+ employees in 68 countries. And achieves a yearly revenue around €19 billion with €1 billion+ in self-funded R&D.