COMPETITIVE BATTLECARD: DATA - ACCESS MANAGEMENT AND PROTECTION

SOLUTION AREAS: ACCESS MANAGEMENT, DATA ENCRYPTION, KEY MANAGEMENT

KEY DIFFERENTIATORS

Access Management

- Combined solution for MFA and Access Management: manage multi-factor authentication, cloud SSO and customisable policies from one platform.
- Broad range of authentication methods: the current threat landscape requires different methods of authentication depending on the type of users, the type of application and the use-case.
- Smart SSO: our solution is different in that the SSO and authentication are applied per policy, not globally. With smart SSO, IT maintains security.
- Use-case based policy setting: STA lets you start global and go granular, making it easy to set up scenario-based access policies.
- Data-driven insights: data on passed/failed login attempts, access stats per day and access steps per app.
- Easy app integrations: template-based integrations make it quick and easy to add new cloud and SAML apps.

Key Management

- Customers own and control encryption key lifecycles, independent of third parties in any environment - physical, virtual, multi-cloud or a combination of any of these.
- Flexible deployment models - physical application, virtual appliance, cloud-native k170v appliance.
- FIPS 140-2 Level 4 HSM for high assurance and security.
- Granular access controls and auditing for compliance
- High-performing, scalable platform with no limit to the number of appliances that can be addressed to a cluster.
- Superior ecosystem of storage, data, application vendors.

COMPANY STATS

- 80,000 employees
- Presence in 86 countries
- 19bn revenue
- 1bn self-funded R&D

TARGET VERTICALS

- All!

TARGET CONTACTS

- CISO
- IT Security Manager
- IAM Manager (Access Management)

SALES PITCH

Thales (Gemalto) offer comprehensive ‘best of breed’ solutions to allow your customers to manage access to their cloud applications, encrypt data at rest and in transit (layer 2 network encryption) as well as securely manage their encryption keys.

The award-winning suite of SafeNet Access Management and Authentication solutions allow organizations to effectively manage risk, maintain regulatory compliance, gain visibility into all access events and simplify the login experience for their users. Utilizing policy-based SSO and universal authentication methods, enterprises can securely move to the cloud while maintaining access controls to all corporate resources, regardless of the device being used.

The encryption offering provides a comprehensive solution that can encrypt sensitive data wherever it resides, including structured and unstructured data at rest and data. Data in motion is also addressed in the form of high speed encryption of data, real time video and voice. This is complemented by an industry leading enterprise key management platform. Regardless of its location, be it stored in a database, file server, application, traditional or virtualized data center, or public cloud environment, your sensitive data is secure from compromise.

THALES

EXCLUSIVE NETWORKS

COMPETITIVE LANDSCAPE

Microsoft

- Microsoft is far above the market price average
- Licensing is extremely complex and customers are forced to buy licenses they may not fully use
- Gaps in functionality for support of non-standard applications means many customers are opting to purchase a separate AM

Azure AD

STA has:

- Stronger security for all your cloud, web and on-premise apps
- Broader MFA options
- Superior access policy management
- Felxible business model
- Lower TCO

Okta

- Thales are specialists in authentication and access management, while Okta are generalists
- Only STA offers the breadth and depth of MFA included in an integrated AM service, within one flat license
- Okta pricing is the highest on the market and customers complain of low quality post-sales support

RSA

STA has:

- A quicker and easier setup
- A lower total cost of ownership
- Stronger reporting
- A simpler-to-manage system

Duo

Why is STA better?

- Lower total cost of ownership
- Easier to deploy
- Supports more use-cases
- Broader MFA options
- A more flexible policy engine
- Superior reporting

AREAS OF FOCUS

	Customer Problems	Qualifying Questions
Access Management	• Password fatigue: 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 helpdesk costs are a result of lost or forgotten passwords.	**Customers who aren't currently using a web SSO/AM solution:** • How many cloud apps are deployed in our organisation? • How is your company approaching cloud adoption and how are you defining security best practice? • Do you have or are you moving to Office 365 in the future? • What problems do your users face when having to manage multiple passwords for various apps? • How do you plan to apply 2FA and SSO to other cloud apps? **Customers already using an AM/password vault/federation solution:** • What are you using today? • How does it allow you to set policies per application and user? • What type of 2FA methods can you use? • What additional features would you like to see that are not available with your current solution? • What other types of solutions are you looking into?
Key Management	• Data theft is becoming more and more of a risk for your customers - 95% of data thefts are of unencrypted data. • Compliance and GDPR are now key considerations - encryption is strongly encouraged to protect data. • The proliferation of fragmented encryption solutions from internal projects and compliance mandates - crossing multiple tiers and multiple vendor platforms. • Security teams struggle with the administrative efforts of managing encryption deployments and the associated key lifecycle operations.	• Where is your sensitive data? • Are you concerned about GDPR and compliance? • What kind of data do you need to protect? • Where do you need to protect - on the cloud, on-premise or hybrid? • What other vendor products do you have in your ecosystem? • Do you have any custom systems that need protection? • Do you have any compliance mandates to work with? • What are you doing to protect keys and achieve compliance? • Are your encryption use-cases growing? • Are you aware of pitfalls due to encryption silos? • What are your High Availability and Disaster Recovery needs?

WANT TO KNOW MORE? CAN WE HELP SUPPORT CONVERSATION WITH YOUR CUSTOMERS?

Please reach out to the team at Exclusive Networks: Hannah Woodbourne | 07810 208025 | Thales_UK@exclusive-networks.com