

Assessing the True Cost of Strong Authentication

The Total Cost of Operation of On-premise vs.
Cloud-based Authentication



White Paper

Contents

03	The True Costs of Authentication – Hard Costs vs. Soft Costs
04	Soft Costs
06	Hard Costs
07	Putting Costs into a TCO Perspective
07	The Affordability of Cloud-based Authentication
08	Conclusion
08	Key Benefits
08	About Thales

Many organizations rarely look closely at the Total Cost of Operation of their authentication solution and instead make a decision heavily driven by the up-front purchase price. This approach to assessing authentication costs shows that infrastructure investments and management overheads dominate the total cost of the solution. Lowering these overheads, therefore, would reduce Total Cost of Operation. Cloud-based services are increasingly becoming an integral part of the enterprise, precisely because they lower costs and management overhead while increasing flexibility.

Authentication-as-a-service is no exception and can help organizations achieve:

- Up to 60% savings in Total Cost of Operation
- 99.999% service availability
- More effective budget utilization and flexibility with OPEX pricing
- Up to 90% reduction in administrative overhead costs

This paper can be used by security or compliance leaders to compare the Total Cost of Operation of an on-site authentication solution vs. a cloud-based authentication service, and further understand the business and technology benefits of cloud-based authentication when evaluating their authentication infrastructure.

The True Costs of Authentication – Hard Costs vs. Soft Costs

This white paper provides detailed cost analysis metrics and discussion points that will help a business of any size decide which is the most appropriate solution to meet their authentication needs. The paper delivers facts based upon technical research and comparison, as well as commercial input from organizations (CIOs, CISOs, IT managers) and suppliers (systems integrators, service providers and resellers).

Firstly, we need to consider the different costs associated with the implementation of a solution. We can break these down into two different types of cost:

Soft costs are typically related to the overall solution and can be seen as being related to the desired outcome that a business wants to achieve. They are business driven but technology influenced.

Hard costs are items that are essential or mandatory to the implementation and use of the solution. The solution would not deliver the level of service required without them. Hard costs are generally calculated on a per user basis and are technology driven but business influenced.

Soft Costs

The following areas have been highlighted by organizations and their suppliers as being the key areas that they need to consider when purchasing an authentication solution. The priority and relevance of each area varies greatly between organizations – dependent on factors such as size, number of locations and type of user.

The table below provides a detailed breakdown of the soft costs and explains how this data can be used to evaluate both options against the needs of the organization.

Desired Benefit	Factors to Consider	Server-based Authentication	Cloud-based Authentication
99.99 % Availability	<ul style="list-style-type: none"> Infrastructure availability Server resilience Network connectivity Out of hours support Incident resolution 	Implementing this level of service availability would typically require significant investment in IT infrastructure, tools and people resources.	Delivery of a service that leverages high availability infrastructures and behind the scenes resources to underpin effectiveness and use satisfaction by minimizing disruption or outages.
Minimal license and token management costs	<ul style="list-style-type: none"> Cost of re-provisioning tokens in year 4 Cost of replacement tokens in year 4 Disruption to users of replacing tokens 	Usually require perpetual license for authentication server software, in addition to limited-time token licenses that need to be renewed	Per-user, per month licensing .
Resilience	<ul style="list-style-type: none"> Fully redundant architecture Performance maximization Availability and replication of core data Network redundancy Monitoring resources and tools 	Design, implementation and support of a fully resilient network infrastructure could be a significant investment.	Fully redundant architecture that delivers maximum performance, availability and replication of core data.
Need for 24x7 support	<ul style="list-style-type: none"> Availability of resources on 24x7 basis Holiday cover for expert resources Cost of training resources Keeping resources up to date Availability of support/test model office 	Developing the knowledge and skill in house, as well as investing in resources to deliver a high level of 'on tap' responsiveness is likely to be prohibitive.	Cloud based services are managed by trained and experienced resources who maintain the high level of SLA, as well as offering fast response to technical questions.
Providing expert 1st and 2nd line support	<ul style="list-style-type: none"> Escalation process management Managing multiple suppliers (server, network, 2FA etc) Speed of response to key users 	Building sufficient in-house knowledge can be time-consuming and expensive.	A service provider will ensure that all problems are escalated rapidly to specialists to assure fast resolution, maximum up-times and high levels of user confidence.
No up-front purchases	<ul style="list-style-type: none"> Investment in server and associated O/S and licences Purchase of 2FA application Purchase of tokens Purchase and manage support contract 	A server model is likely to require the up-front purchasing of a server, associated licenses, the 2FA application, tokens and a support contract.	A cloud based service leverages a full software-as-a-service (SaaS) oriented model – where on-going payments and an all-in pricing will also means there are no up-front purchases – not even tokens.

OPEX vs. CAPEX	<ul style="list-style-type: none"> • Ability to allocate costs to OPEX • Ability to pay quarterly • Availability of cash/budget 	It is unlikely that a server based model can be totally supported by an OPEX model due to the up-front investments in hardware and licenses.	With cloud-based services you typically have the choice of 100% OPEX payments or ability to blend this with a CAPEX model. This flexibility can improve business cash flow and budgeting.
Proactive monitoring	<ul style="list-style-type: none"> • Provision of management tools • Availability of resources • Speed of response • Speed of resolution • Diagnosis and resolution of trends and incidents 	Investment in the tools and resources to deliver fast and consistent diagnosis and resolution of trends and incidents can be prohibitive to even the largest of organizations.	The infrastructure of a cloud-based authentication service will be built to deliver immediate notification, action and resolution of issues to assure effectiveness, up-time and service delivery.
Simple integration	<ul style="list-style-type: none"> • Authentication specific software install • Server configuration and set-up requirements • Network re-configuration • AD schema change requirements 	Most server based installations require complex set-up and configuration – with some vendors even expecting you to pay for the agents required to get you going.	Cloud-based services require minimal change to an infrastructure to be up and running – typically the change can be made remotely.
High level of security	<ul style="list-style-type: none"> • Level of token and software OTP complexity available • Datacenter security – access to server • Regular server and infrastructure penetration testing 	Achieving audit and compliance can sometimes require heavy investment in tools and equipment. It also requires specialist knowledge and investment in consulting services.	Achieving audit and compliance can sometimes require heavy investment in tools and equipment. It also requires specialist knowledge and investment in consulting services.

Hard Costs

This section provides a detailed view of the key elements of cost and overhead that a company should consider when purchasing an authentication platform. The elements are based upon research and reflect best practice elements that a managed service provider or outsourcing company would calculate in terms of delivering a managed server environment.

Cost area	Description of Consideration
Incident resolution	Resolving faults within the infrastructure – either from the service desk or from automated tools (e.g. performance, disk space, user support)
Change installation	Implementing changes within the infrastructure, adding disk, service packs, memory, etc
System documentation	Documenting the infrastructure, maintaining the documentation and the configuration
Virus/security management	Ensuring solutions and updates are deployed to protect the server and the infrastructure
Reporting	Monitoring server and infrastructure performance and availability etc
Housekeeping	Clearing/archiving log files, general file management, storage reclaim, etc
Performance capacity management	Ensuring ongoing server availability and capacity
System software upgrades	Ensuring latest patches are implemented, preventative analysis and execution
Security audit	Checking security logs, maintaining service integrity etc, implementing and maintaining security policy
Print admin	File and print server management
User admin	Managing user accounts, MAC, permissions
Storage management	Storage connectivity, resilience, failovers etc.
Token administration	Managing provisioning, deployment, revocation and other life-cycle events
System monitoring	Ongoing monitoring using system tools and reports, correlation and investigation.
Back-up operations	Back-up and storage of the application, as well as user data. Includes: monitoring of tapes; storage; off-sitting
Team leadership	Managing the team who supports the server, application, infrastructure, help desk, escalation processes, etc.

Putting Costs into a TCO Perspective

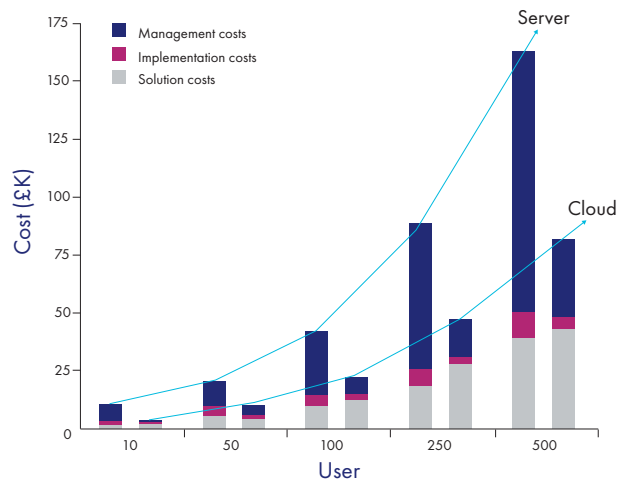
Let us now take a look at how the soft and hard costs analyzed above contribute to the Total Cost of Operation of an authentication solution. The graph below shows costs for each solution type across a defined numbers of users.

The management cost has been calculated by applying industry standard costs to the time taken to undertake each of the tasks outlined previously in the hard costs section. Soft costs have been included within the implementation cost figures and are based upon feedback from both customers and systems integrators. Solutions costs are based on the typical purchase prices of traditional server based authentication and SafeNet Authentication Service solutions across a range of business sizes.

As the graph illustrates, the solution cost for each type of authentication solution is a misleading indicator for the Total Cost of Operation. If a true like-for-like comparison is to be carried out, with consideration given to the full TCO of each authentication solution to the organization, it is clear that the cloud-based solution is more cost effective, with savings in the region of 44-60%, depending on the number of users.

Rather than having to implement on-site servers and spend time integrating applications within the network, authentication-as-a-service is an increasingly viable way to deploy authentication.

Authentication TCO Comparison



The Affordability of Cloud-based Authentication

The pervasiveness of remote access to the internet, web-based applications and cloud-based applications has enabled our business and personal lives to be transformed to the point where we can live in a 24x7 online world. The transition to software-as-a-service in particular (SaaS) is transforming the way that IT departments work and the investments that need to be made.

This technology is now also used to make authentication more affordable, easier to manage and easier to implement. Rather than having to implement on-site servers and spend time integrating applications within the network, authentication-as-a-service is an increasingly viable way to deploy authentication.

Deploying strong authentication using a cloud-based service is applicable to organizations of all sizes: large enterprises are using it to replace older, more traditional server-based approaches; mid-tier organizations are using it as an alternative to having a service provider manage their authentication server; SMBs are using it because it delivers an affordability and ease-of-implementation that was never previously available.

Conclusion

There are many drivers for organizations to consider using cloud-based services, regardless of their size. Cost reduction is a primary consideration, followed closely by ease-of-implementation, reduced administration and management, high availability and flexible pricing options. These benefits of cloud-based applications and software-as-a-service are broadly recognized – and are fully applicable to authentication-as-a-service.

Key Benefits

- **Protects everything:** Networks, applications and cloud services
- **Protects everyone and provides choice:** Tokens, policies and customization
- **Automates everywhere:** To reduce overheads and maximise effectiveness
- **Lowest TCO:** On infrastructure and resource investments
- **Easy migration:** Move from an existing solution whilst protecting the current investment

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.



Americas

2860 Junction Avenue, San Jose, CA 95134 USA
Tel: +1 888 744 4976 or +1 954 888 6200
Fax: +1 954 888 6211 | E-mail: sales@thalessec.com

Asia Pacific

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

> thalescpl.com <

