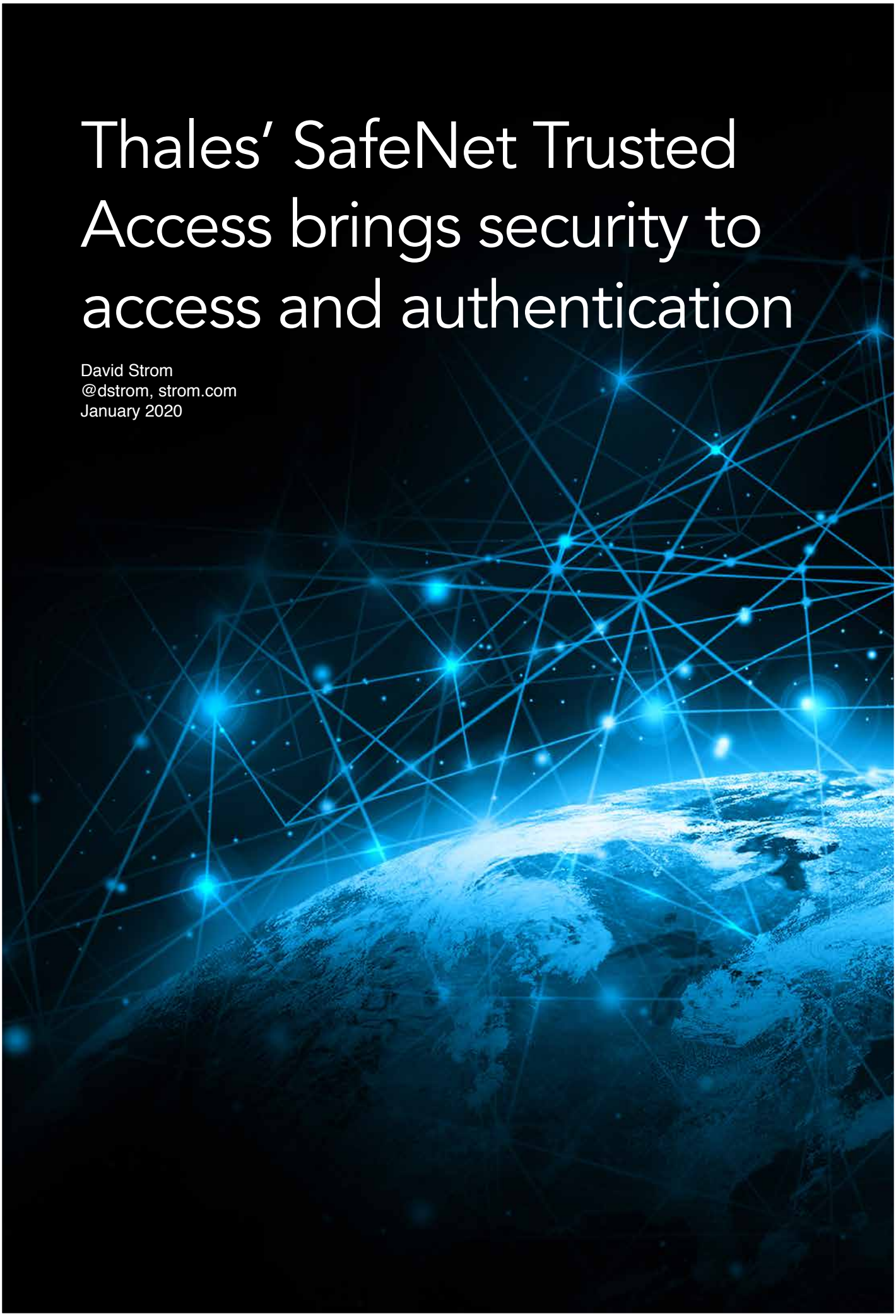
Thales' SafeNet Trusted Access brings security to access and authentication

David Strom
@dstrom, strom.com
January 2020



About the author

David Strom (@dstrom, strom.com) is one of the leading experts on network and Internet technologies and has written and spoken extensively on topics such as VOIP, convergence, email, cloud computing, network security, Internet applications, wireless and Web services for more than 30 years. He has had several editorial management positions for both print and online properties in the enthusiast, gaming, IT, network, channel, and electronics industries, including the editor-in-chief of Network Computing print, DigitalLanding.com, and Tom's Hardware.com. He has also written two books on computer networking. He began his career working in varying roles in end-user computing in the IT industry. He has a Masters of Science, Operations Research degree from Stanford University, and a BS from Union College.

If you are looking for a comprehensive identity and access management (IAM) tool that can cover just about any authentication situation and provide iron-clad security for your enterprise applications, you should consider Thales' SafeNet Trusted Access (STA). It has a wide range of tools that can lock down your network, cover a variety of multifactor authentication (MFA) methods and token form factors, and provide single sign-on (SSO) application protection and risk-based authentication. That is a lot of acronyms and buzzwords, but STA brings together the authentication and access management worlds in a nice coherent and elegant way.

Thales is now the keeper of the security flame that began in Israel with Aladdin Knowledge Systems, which was subsequently acquired by SafeNet, which in turn was bought by Gemalto. The SafeNet products have remained as a business unit of the French multinational company that has 80,000 employees in 68 different countries and sells a wide range of communications electronics, defense and aerospace products. More than 30,000 of the world's largest organizations rely on Thales digital identity products to grant access to services and encrypt their data.

As a result of these acquisitions, Thales is now one of several security vendors (the others are Dell's RSA division, HID and One Span) that offer IAM, SSO and MFA product lines. The difference is that Thales has done a better job integrating all three into a single coherent service offering. It is completely cloud-based, requiring only local agents to manage Windows and other services. That is an important point and one of the reasons why I like the product. Its competitors have been slower to embrace cloud services.

I tested the product in November and December 2019. This review covers the following elements: how it delivers MFA protection, its policy creation and management features, its SSO support, reports and automation routines.

MFA delivery

MFA has become more important as a first line of breach defense, as more passwords are compromised, and as other network protective measures have been ineffective at preventing phishing attacks. The issue has always been that many applications – both on-premises and SaaS-based – don't come with much if any support for the additional authentication factors. STA has figured out an elegant way around this and made step-up or risk-based authentication easier to implement across an entire application portfolio for an enterprise. SafeNet has always done a great job with integrating its MFA toolset; STA plays to this strength in its support for a wide collection of MFA tokens, including both hardware and software, SMS and email, push notification and biometrics. That is by no means a comprehensive list of how it delivers MFA.

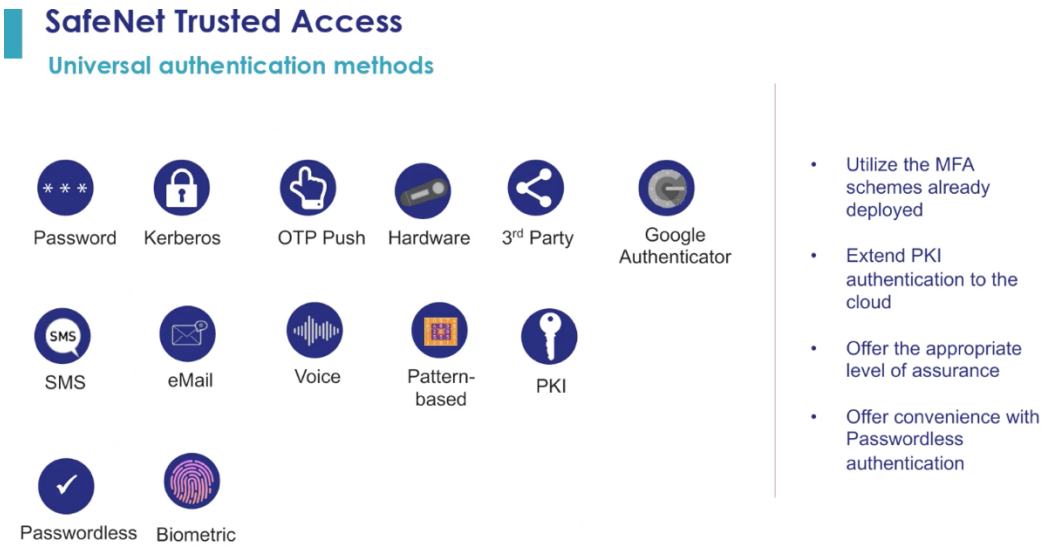
Token provisioning is handled with a comprehensive series of rules and integrations into Active Directory, along with support for two non-token methods: using the built-in Windows Kerberos and other certificates.

I tested two advanced token methods by setting them up for a sample web app and to authenticate various SAML apps. They worked flawlessly. One of the nice features of STA is that it makes setting up the admin user easy by leveraging its smartphone authentication app called MobilePass+. This gets administrators comfortable with the technology from the first moment of use. Once MobilePass+ is downloaded, the authentication code is pushed to the phone to complete the setup process. It just takes a few seconds and is very elegant compared to how some of Thales' competitors do this.

By the way, MobilePass+ is available on iPhones and Android smartphones and Windows desktops. Many of Thales' competitors don't offer any Windows authenticator app.

These smartphone apps are gaining traction for two big reasons: first, you don't need your users to carry around a separate piece of hardware, like a one-time password fob, because they already have their smartphones. Second, they are not compromising security such as when they use an SMS or email factor. The smartphone app is a big step up because SMS (and to some extent, email) can be vulnerable to man-in-the-middle and account takeover attacks. The One big plus for MobilePass+ apps is that they are very easy to use and have gotten high user ratings in both the Apple and Google app stores.

In addition to token types, STA also supports a wide variety of authentication methods, including OTP push, pattern recognition (to avoid passwords being captured by keyloggers), PKI credentials, Google Authenticator, biometrics and voice methods. (see the illustration below) The modern MFA app needs to be as pluralistic as possible and STA delivers across this collection and is continually widening its coverage.

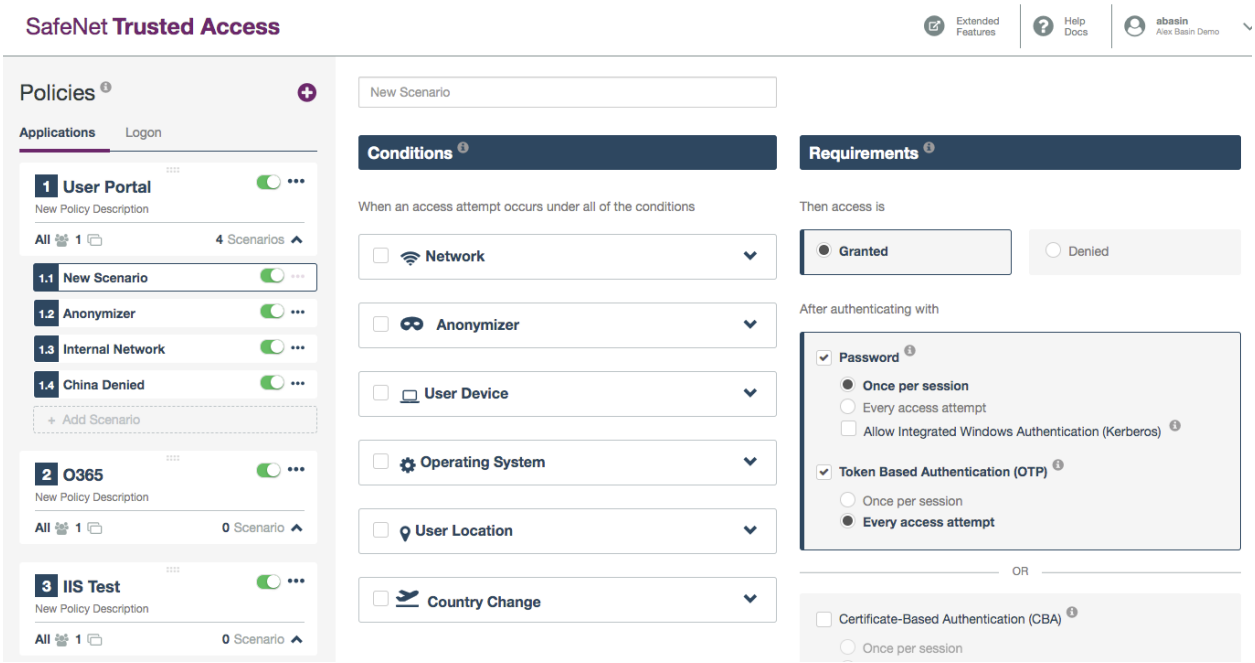


STA interoperates with the usual collection of authentication standards, including Radius, OpenID and SAML. A lot of effort has gone into crafting a very flexible identity infrastructure that can work with these standards. Its design is like how the Fast Identity (FIDO) Alliance has been constructed: separating the authentication methods from the actual authentication data stream.

Speaking of FIDO, STA also has solid FIDO support in a variety of methods, including MobilePass+ support for FIDO-based Windows Hello authentications and FIDO-based USB tokens and smart cards. Thales plans on coming out with software-based FIDO tokens next year.

STA's policy management

At the heart of STA is its security policies. These are extremely flexible, allowing you to create very granular and specific rules and do so quickly with its visual policy editing tool that is part of its web dashboard. (see screen shot below)



Policies can be set up for specific applications (more on that in a moment), apply to network ranges, operating systems, and user collections and geolocations. These policies are enumerated on the left-hand menu pane and work like a firewall rule set, with the more permissive ones listed first. You can also check to see if a user is accessing the network through an anonymizing proxy. And you can make its authentication rules as dynamic and as context specific as needed: for example, they can be set to check at every access attempt or for particular circumstances, such as requiring step-up authentication under riskier conditions.

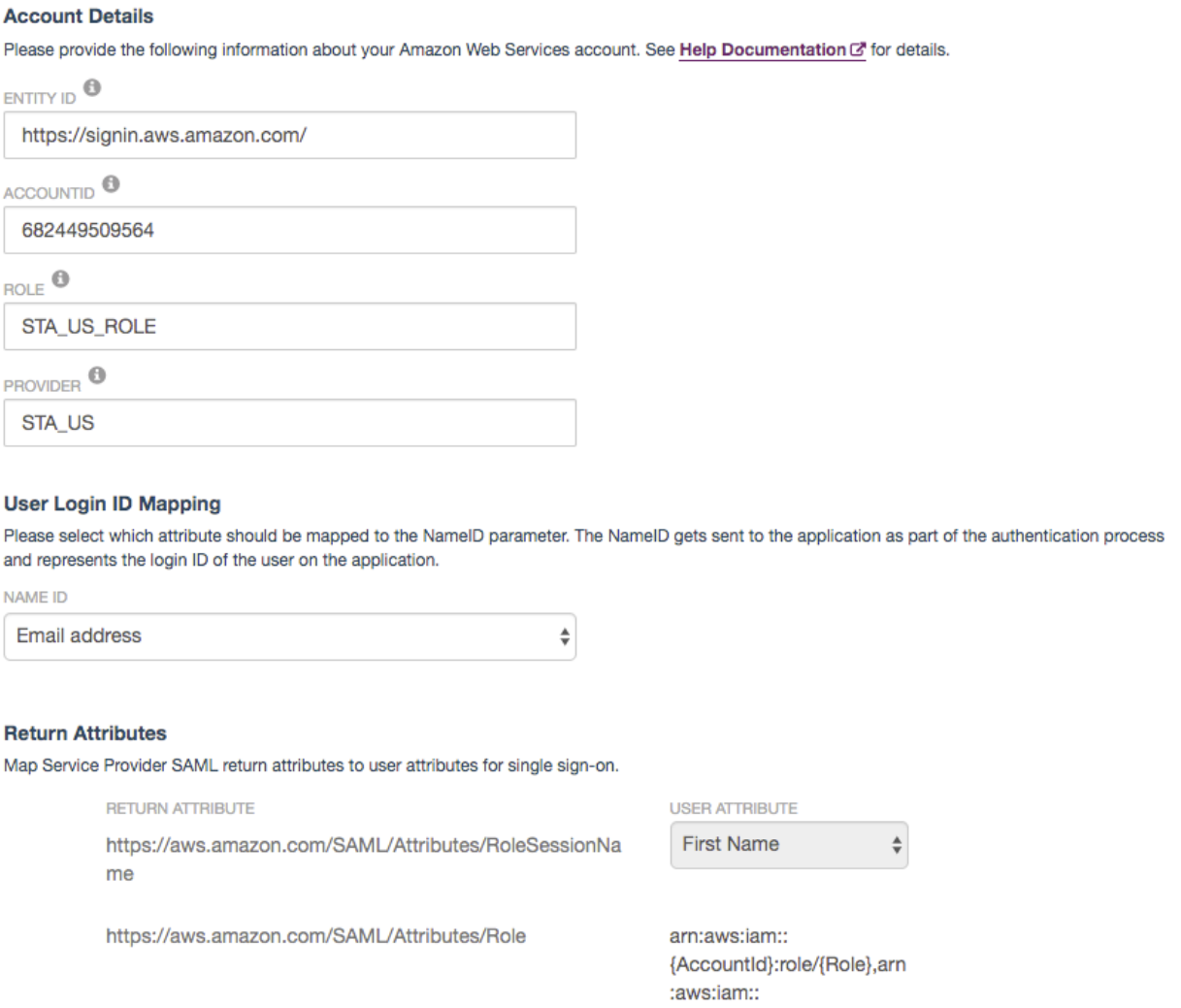
Unlike some of its competitors, Thales has integrated this deeply into STA, and its flexibility here is a big bonus when it comes to other security products.

Because STA has decoupled the identity from the credentials and devices that are used to prove the authentication, you can mix and match your methods and processes and still maintain the tightest possibly security.

Thales always has had the lead in documenting its integration methods and APIs. The current version has expanded on these documents.

SSO support

The focus of an SSO product is how it controls application access, and STA has done a solid job in this particular area as well. The application rules are like numerous other SSO products, where you can add the specific URL codes to provide the automated logins of many SaaS services. STA supports both SAML and OIDC access methods and includes templates that you can use to use with custom applications. In addition to an apps launching page, STA creates a self-service web portal for users, to avoid tying up IT resources for common requests such as password resets, token requests or to add another authenticator method. Administrators can restrict portal access for specific groups in the policy management screens. (See screenshot below for an example of how SSO access to Amazon Web Services is configured.)



As I mentioned earlier, one of the big advantages of STA is its ability to add MFA to apps that don't ordinarily support it. As corporate app portfolios continue to enlarge, this is an important security feature. Policies can also be created to work with more than a dozen different software agents, including ones for Radius, the Cisco AnyConnect clients, and for various Windows and Microsoft tools.

Reports and automation methods

STA comes with 49 templates to help you create various reports, and they can be easily customized with its web dashboard, along with being scheduled to run at specified intervals and produced in various output formats, including HTML and comma-separated. In additional to these reports, numerous audit logs are available which can be useful in troubleshooting authentication problems and debugging other issues.

One final aspect of STA that I haven't discussed is its automation methods. Configuring any authentication product relies on many manual methods, as I have described. But what if you want to automate the application setup process, the ability to bulk register various tokens and

other tasks that can eliminate a large portion of management drudgery? That is another reason to use STA because it has these, and others, covered.

Summary and recommended actions

STA offers a compelling blend of security solutions that bridge the MFA, SSO and access management worlds in a single, well-integrated package. STA does this by offering policy-based access controls and SSO with very strong authentication features. These policies are flexible and powerful enough that you can address a broad range of access scenarios.

Because STA covers multiple security workflows, there are several places that it can fit into your overall data protection needs. Part of your own motivation for using this product will depend on the particular direction that you are coming from. What you need STA to do will depend on what you have already purchased and where your existing security tools are weakest.

If you presently use another SSO tool, or if you aren't happy with your existing identity management product, you might examine whether they can support or integrate with STA and use it as your principal identity provider. This will give you greater automation scope and move towards better MFA coverage for your consolidated logins.

If delivering MFA is your primary focus for purchasing a new identity product, STA should be on your short list of vendors. If you are rolling out MFA protection as part of a larger effort to secure your users and logins, then things get more interesting and the case for using STA becomes more compelling. For example, it can handle a variety of application authentication situations and be granular enough to deploy these methods for particular user collections and circumstances. Many older IAM products bolted-on their MFA methods with cumbersome or quirky integration methods or required you to purchase separate add-on products for these features. STA has had this flexibility built-in from the get-go and has a well-integrated MFA set of solutions.

If you presently use another vendor's authentication app or have a collection of hardware tokens that you are trying to migration away from, you might want to examine whether STA's MobilePass+ offers improvements to the user workflows that could increase MFA coverage across your application portfolio.

Thales SafeNetTrusted Access is available at this link. Pricing starts at $3.50 /user/month, which includes access management, SSO, authentication tokens and services support. A premium subscription which adds PKI MFA support is also available.