50 Years of Growth, Innovation and Leadership

Don’t Wait for a Data Breach, Modernize Authentication Now

Target Agility as You Make a Solution Selection

A Frost & Sullivan Executive Brief
Sponsored by RSA

Stratecast FROST & SULLIVAN

INTRODUCTION

Agility is required in authenticating users. The reason is simple. Access scenarios are too diverse and dynamic to depend on a single means of authentication. Your authentication approach must evolve with access scenarios.

If your business is like most, this is what you are experiencing in access scenarios:

- Your users are increasingly mobile and frequently remote
- Their work activities occur at any time
- They insist on using their personal devices for work
- Their use of cloud services is escalating and with that, the security assurance of line-of-sight between users and your business applications and sensitive data is erased
- They are not just your employees but a growing digital ecosystem of third-party personnel
- And in the accelerating pace of work, your users gravitate to convenience even if ill-advised (e.g., reused and guessable passwords)

As access scenarios have expanded, access decisions must be multi-dimensional. Intelligence on who, what, when, where, and how must be gathered and assessed in real-time so access decisions properly balance business needs against risk for each access scenario. Additionally, gathering intelligence and engaging users in authentication must take into consideration the impact on user productivity.

Further adding to this need for modernization is the prominent method of user authentication is under attack. According to Verizon in the 2017 version of its Data Breach Investigation Report (DBIR), “81% of hacking related breaches leveraged either stolen and/or weak passwords.” This outcome has not changed. In the 2018 version of DBIR, “Use of stolen credentials” was the most frequent hacking method (‘action variety’ in DBIR parlance). The obvious takeaway is this: as long as passwords are used as a principal means of authentication, hackers will exploit them.

The future state is clearly in view. Businesses must modernize authentication and access decision-making to counter the susceptibility passwords present while also flexing with the expansion in access scenarios and protecting far-flung applications and data. Additionally, this modernization must be straightforward for users and administrators. Otherwise the security gains of stronger authentication unravel. For example in an attempt to strengthen authentication by dictating lengthy passwords, multiple unique passwords, and frequent password changes, frustrated users resort to unsafe practices such as password reuse and recording passwords on paper or in an unencrypted file.

Fast forwarding to this future state requires that you make a sound decision on how. In this paper, we provide our list of recommendations in selecting a modern authentication solution. Potentially your business is already using a form of strong authentication, like hardware or software tokens, for a subset of access scenarios. While you need to strengthen authentication to more, if not all, of your access scenarios, replacing what is already operationalized and effective is seldom an optimal choice and can have financial repercussions. Instead, augmenting from a pool of authenticators that strengthen but also have a light touch on users and administrators is preferable. Our recommendations take ‘the present’ into account.

VALUE MAXIMIZING SOLUTION ATTRIBUTES

The value of strong authentication in making better access decisions depends on use, and use depends on adoption. If adoption of strong authentication is limited to only a subset of your access scenarios or users, or if administration is complex and cumbersome, you the buyer of an authentication solution will be disappointed in your return on investment (ROI). To avoid ROI disappointment and to guide you in your selection, Frost & Sullivan organized its recommended solution attributes into three constituent groups: Users, Administrators, and Business Owners. Your goal is to satisfy all three as that maximizes adoption and deepens the use of available features and functionality, which in turn, leads to a satisfying ROI.

User Constituent

To claim that this constituent is uniform is patently incorrect; your user community could be highly diverse. Even so, there is strong uniformity in desired solution attributes for this diverse constituent. Those attributes are authenticator choice, self-service, and Single Sign-On.

Authenticator Choice

Users naturally want to take advantage of authenticators built into their devices: those they own and those they have been assigned. If their smartphones have facial recognition or a fingerprint reader, those authenticators should be in the pool of available authenticators. If they like the simplicity of push notifications, that too should be in the pool. And for those that routinely use hardware tokens, let use of them continue.

The variety of authenticators has expanded rapidly over the last decade (far more than the few previously highlighted) and will continue to expand as the risk of password-based authentication continues to mount. The comparative merits of each vary (e.g., identity-proving strength, operational reliability, and lifecycle cost) and not just by authenticator type but also across supporting devices (e.g., make and model of smartphones). While choice is essential in accommodating users’ personal preferences and in driving broad adoption, administrators, as discussed later, need intelligence at their fingertips to define and enforce access policies that balance user preferences and risk management. Fortunately, more choice for users also gives administrators several strong options to attain this balance.

Self-service

Adoption will stall if the process to register users, their devices, and authenticators is cumbersome. Similarly, change will occur across all of these dimensions. Placing users front and center in registration and updating puts them in control. Positively for a growing population of users, a self-service experience is ingrained into their digital lifestyles. The same should be present in authentication. Doubly beneficial, self-service means less one-on-one user support demanded of administrators. Administrators, instead, devote more of their time to other responsibilities and initiatives—a favorable redistribution of time and talent.

Single Sign-On

Requiring separate authentication credentials for each on-premises and in-the-cloud application contributes to user aggravation. No surprise users reuse passwords, gravitate to the least complex

All rights reserved © 2019 Frost & Sullivan

password convention, and grumble when password change edicts appear. This situation does not have to be the status quo. Single Sign-On (SSO) unwinds unsafe user behaviors, uplifts authentication strength across previous bespoke password-based authentications, and transforms unproductive time to productive time. SSO is an obvious built-in feature to demand in authentication solutions.

Administrator Constituent

Administrators with authentication and access responsibilities have a tough job in having two sets of internal clients to serve and support: users and business owners. At times, the objectives and motivations of the two diverge. Our recommended attributes listed in the User and Business Owner constituent sections assist administrators in accommodating the preferences of each, but not entirely. Other hands-on solution attributes need to be present for administrator use. They include: unified policy administration, risk-based authentication, support for enterprise application storefronts, and out-of-the-box integrations.

Unified Policy Administration

With expanding and fluid access scenarios, the sheer effort to administer authentication and access policies mushrooms if administration is fragmented. Rather than viewing a single dashboard with hands on a single wheel, administrators are confronted with multiple dashboards and wheels. Certainly not an optimal situation and also one that undermines administrators’ responsibility to set, enforce, and report on policies. Receiving a demonstration of single dashboard policy administration is in your best interest in evaluating authentication solutions.

Risk-based Authentication

Effective authentication depends on choosing the appropriate authenticator as access circumstances unfold. For example, if a user changes devices or locations or his or her patterns of access (what and when) change from the past, his or her standard authentication may no longer be sufficient to produce the level of identity assurance required for the access requested. Knowing when or if to require alternative or additional forms of identification fits into the realm of Risk-based Authentication (RBA). RBA collects contextual indicators on past and current access sessions. Fed into a Machine Learning engine, RBA conducts real-time detection of the abnormal and illogical so that appropriate actions can be taken. When risk indicators are low, users can be granted access without additional authentication measures. If risk indicators are high, RBA can request an additional form of authentication. Other RBA-triggered actions that accompany high risk indicators can include: blocking access, restricting access permissions, disallowing specific user actions (e.g., downloading files), and/or generating an alert on a potential rogue user. As a real-time operation, the power of RBA is in preventing security incidents, but only if RBA is included in your selected authentication solution.

Enterprise Application Policy

The quilt of applications users are accessing is expanding and is an ever-changing mix of on-premises and cloud-based. As sensitivity of applications varies (e.g., email versus CRM), so too does the appropriate authenticator, and the importance of RBA. Additionally, access policies based on user, role, and affiliations (e.g., company, business unit, and department) are contributing factors on what applications each user is allowed to access. Facilitating an alignment of user, authenticator, and application calls for an enterprise application storefront automatically populated for each user and directly linked to unified policy administration rules and contextual RBA indicators. Behind the scenes administrators stock this enterprise application storefront. For them, ready-to-use application connectors for common business applications and a simplified means to build custom connectors are invaluable in injecting scalability, efficiency, and access policy consistency into the enterprise application stocking function.

Out-of-the-box Integrations

A strong security posture demands that separate security technologies operate as a collective. But, integration should not be expected of the security technology buyer; vendors should own this task. Authentication solutions should come equipped with certified integrations with other security and networking technologies (e.g., firewalls, routers, and network access controllers) to strengthen overall security posture, and with common workflow systems to streamline hand-offs and create an audit trail.

Built-in Privileged Access Management

The authentication solution’s administrative portal is an attractive target for hackers due to its controlling position over authentication and application access policies. Only the few, truly privileged should have access. Therefore access to this portal must be heavily guarded and administrators’ actions closely monitored. Supervisory features such as two-stage authorization for policy changes are also useful.

Business Owner Constituent

Although important attributes on their own, Business Owner attributes listed in this section cannot offset incompleteness or inferiority in the attributes listed under the User and Administrator constituents. In reality, the other solution attributes are equally important to Business Owners as they are intently focused of the positive outcomes of easing user access, ensuring effective administration, and mitigating the risk of weak authentication practices and procedures. Nevertheless, the next two attributes are noteworthy as they add icing to the cake if present in the authentication solution you select.

Multiple deployment options

Just as users appreciate choice in authentication methods, deployment options for the all-important policy server are also beneficial. As the cloud era continues to move forward, interest in policy server deployments *in the cloud* (i.e., a single business instance) and *policy server as-a-service* (i.e., a multi-customer cloud-hosted Software-as-a-Service – SaaS – offering) is growing. Businesses gain the common benefits of moving to the cloud, such as: offloading infrastructure and application (in the case of SaaS) ownership and management to the cloud provider, rapid scalability, and usage-based pricing. Cloud benefits notwithstanding, on-premises deployments also have appeal, especially for businesses that are uncomfortable with hosting this highly sensitive operation anywhere other than on-premises or already operate the policy server on premises. For businesses with existing on-premises deployments, they also need to evaluate if there is a bona fide economic justification in a ‘lift and shift’ to the cloud and the severity of challenges in migrating to the cloud. Depending on circumstances, remaining on-premises could be the best choice or remaining on-premises for current authentications and augmenting with cloud for growth in authentications (e.g., to SaaS applications). Regardless, deployment options allow businesses to make a choice that is best for their circumstances.

All rights reserved © 2019 Frost & Sullivan

Flexible pricing

Mentioned previously, cloud-based policy server options add pricing flexibility by virtue of shifting from an ownership (capex) model to a subscription (opex) model. Flexibility, however, does not always equate to best. An existing perpetual license for the policy server software can be a powerful economic incentive to continue as is. The same is true with hardware tokens. The sunk costs of procurement, user registration and training, and perpetual licenses makes continuing with hardware tokens highly viable.

But, as mentioned repeatedly, access scenarios and circumstances are not static but changing. Consequently, the costs associated with enhanced scalability, improved operational resiliency, and additional features (e.g., RBA)—essentially all the solution attributes that contribute to a modern approach to authentication—are material considerations. Pricing flexibility gives the business owner options to acquire the modern authentication capabilities it needs on a more pay-as-you-go basis (i.e., modularity) and gain the benefits of tiered pricing.

RSA SECURID ACCESS PROVIDES A PATHWAY TO MODERNIZATION

Building off its storied history in authentication, RSA has built a comprehensive authentication solution. Shown in the table below, RSA SecurID Access hits on all cylinders by having all of our recommended solution attributes. For existing RSA SecurID clients and other businesses that are not currently users of RSA SecurID but are poised to modernize their approach to authentication, RSA SecurID Access fits our criteria as a prime solution candidate.

SOLUTION ATTRIBUTE	REMARKS
User Constituent	
✓ **Authenticator Choice**	Widely known and respected for RSA SecurID, RSA’s pool of authenticators also includes the following: mobile OTP, push-to-approve, fingerprint, facial ID, SMS OTP, voice OTP, FIDO-compatible authenticators, as well as hardware and software tokens. Also, there are no restrictions on the mix of authenticators that customers can use.
✓ **Self-service**	In addition to user self-enrollment and MyPage capabilities, bulk provisioning is also available—highly beneficial for large scale user enrollments that are common with merger and acquisitions.
✓ **Single Sign-on**	The comprehensive nature of SSO allowing log-in for all on-premises and cloud applications eliminates multiple password frustration for all users that has been known to cause poor password hygiene such as writing down passwords and taping them inside of desk drawers.

All rights reserved © 2019 Frost & Sullivan

SOLUTION ATTRIBUTE	REMARKS
Administrator Constituent	
✓ **Unified policy administration**	Eliminating the fragmentation of authentication and access policies, unified policy administration substantially reduces policy management time while simultaneously enhancing security via a single dashboard view for all users across the organization. Complementing unified policy administration, a package of basic risk analytics is included in all editions of RSA SecurID Access. Higher editions include advanced forms of analytics including using machine learning and conducting behavioral analytics.
✓ **Risk-based authentication**	RBA is commonly used by customers to determine when to step-up authentications, for example, request the presentation of an additional authenticator or answer a challenge question (i.e., second authentication factor) or when to reduce user access friction when risk indicators are low.
✓ **Enterprise application policy**	Role based user access to applications aligns the user, organizational role, business unit, and departmental affiliation with overarching access policies.
✓ **Out-of-the-box integrations**	Over 500 certified **RSA Ready integrations** that include HTTP Federated Proxy (HFED) and out of the box connectors to all leading SaaS applications such as Salesforce.com, Workday, Office365, as well as with leading VPN clients, and Next Generation Firewalls simplifies the task of modernizing authentication and access controls for IT administrators.
Business Owner Constituent	
✓ **Multiple deployment options**	The RSA SecurID Access can be deployed in the following ways: • Cloud hosted (AWS, Azure), • On-premises, • SaaS, or • Hybrid.
✓ **Flexible pricing**	Customers have the option to purchase the solution in a perpetual licensing model and pay for the solution upfront, or on subscription pricing model invoiced per user/per month. As customer user counts increase, discounted tiered pricing is applied—a benefit for customers that consolidate their authentication with RSA.

All rights reserved © 2019 Frost & Sullivan

STRATECAST: THE LAST WORD

At the start of this white paper we stated that agility in authentication is required as access scenarios have become increasingly varied. The implication is that any and all guardrails that are instrumental in aligning access permissions with needs of the business and risk management, which authentication clearly is, must be designed for variability. Anything less leaves an exploitable gap for malicious actors. Additionally, the varied access scenarios have also directed extra light on the inadequacy of passwords as a form of authentication. The metaphorical image of a screen door preventing burglaries comes to mind. As a consequence, how authentication is practiced must be modernized.

The other key point is that in order to succeed in modernizing authentication, the characteristics and preferences of each influential constituent group—Users, Administrators, and Business Owners—must be captured in your selected authentication solution. A solution that lacks this holistic perspective is apt to miss the mark in relevant measurements of adoption and use, risk mitigation, and ROI. Also relevant is that few organizations are new to authentication. Consequently, their decision on how to modernize and their solution selection must account for past investments in authentication and existing operations. A modernization decision made from a naïve perspective of an entirely ‘clean sheet of paper’ is also apt to miss the mark.

In conclusion, taking stock on how authentication is conducted in your organization is a worthy and perhaps an overdue exercise. Then, in making a modernization decision, do your homework with our three-constituent viewpoint as a framework.

Jarad Carleton
Global Program Leader, Cybersecurity
Stratecast | Frost & Sullivan
jcarleton@frost.com

ABOUT STRATECAST

Stratecast collaborates with our clients to reach smart business decisions in the rapidly evolving and hyper-competitive Information and Communications Technology markets. Leveraging a mix of action-oriented subscription research and customized consulting engagements, Stratecast delivers knowledge and perspective that is only attainable through years of real-world experience in an industry where customers are collaborators; today’s partners are tomorrow’s competitors; and agility and innovation are essential elements for success. Contact your Stratecast Account Executive to engage our experience to assist you in attaining your growth objectives.

Stratecast | FROST & SULLIVAN

SILICON VALLEY | 3211 Scott Blvd, Santa Clara, CA 95054
Tel +1 650.475.4500 | Fax +1 650.475.1571

SAN ANTONIO | 7550 West Interstate 10, Suite 400, San Antonio, Texas 78229-5616
Tel +1 210.348.1000 | Fax +1 210.348.1003

LONDON | Floor 3 - Building 5, Chiswick Business Park, 566 Chiswick High Road, London W4 5YF
TEL +44 (0)20 8996 8500 | FAX +44 (0)20 8994 1389

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

For information regarding permission, write:
Frost & Sullivan: 3211 Scott Blvd, Santa Clara, CA 95054