IDC MarketScape

IDC MarketScape: Worldwide Advanced Authentication for Identity Security 2021 Vendor Assessment

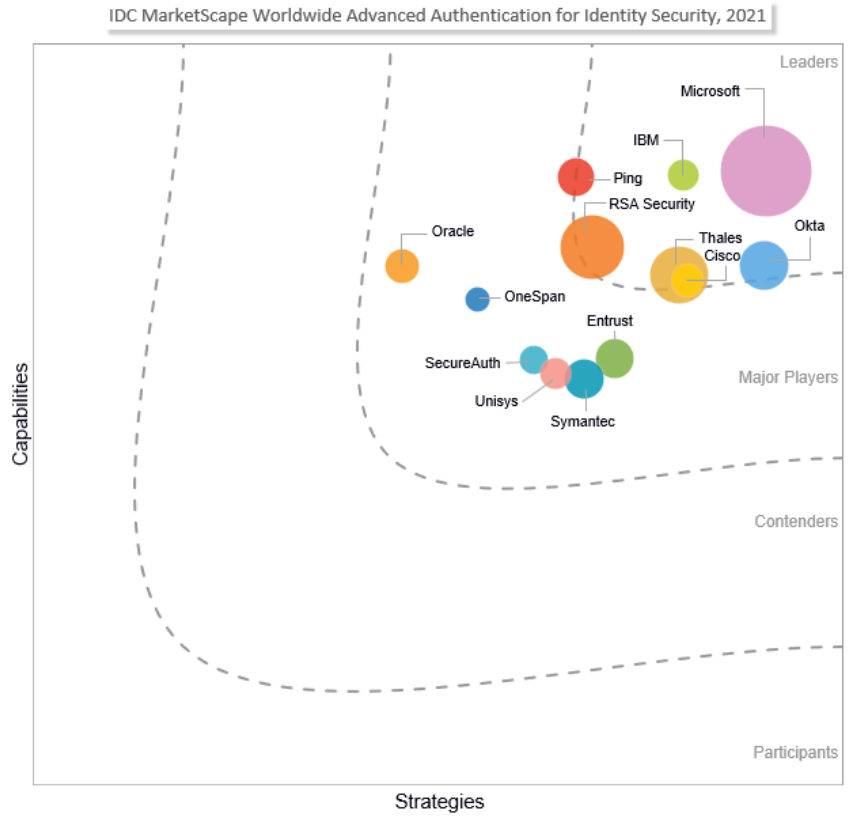
Jay Bretzmann

THIS IDC MARKETSCAPE EXCERPT FEATURES THALES

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Advanced Authentication for Identity Security Vendor Assessment



Source: IDC, 2021

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

July 2021, IDC #US46178720e

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Advanced Authentication for Identity Security 2021 Vendor Assessment (Doc # US46178720). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Essential Guidance, Vendor Summary Profile, Appendix and Learn More. Also included is Figure 1.

IDC OPINION

If complexity is the general enemy of security, IDC believes friction is the enemy of multifactor authentications (MFA). Any security team member who doesn't know that compromised identity credentials are the leading cause of network security breaches and/or data losses is living under a virtual rock. Yes, passwords are … well bad. People make up silly ones and reuse them repeatedly. They do this because it's easy, and they generally got away with the practice until the network perimeter crumbled and social media provided both identity intelligence insights and "you got to see this" temptations to click and share.

The easy fix was to add a second identity factor (2FA) via reCAPTCHA, security questions, or one-time passcodes delivered through email or SMS. Better than nothing, but accomplished cybercriminals found ways around these using either information available via the internet or taking advantage of a telephony protocol (SS7) never meant to be used as a secure communications channel. And while one can make security questions work better using nonsensical answers to typical questions, most people didn't think of that option or couldn't remember the make-believe answers like they couldn't remember passwords. In 2016, NIST deprecated the use of SMS as a second factor saying it was among the worst of the available options.

Today when IDC speaks with buyers seeking an MFA solution, they typically fall into two motivational camps: SMS upgraders and hard token technology migrators. Those hoping to follow NIST's advice about the exposures associated with SIM swaps and MitM attacks are looking for something incrementally better that won't carry all the time and expense of dealing with tokens. Those who have already been working with – especially hardware – tokens, know there are lower-cost options out there these days. Both are hoping to pick a technology they can afford and feasibly implement that will last their organizations for the next 5-10 years – hopefully with headlights toward a passwordless future.

Replacing telecommunications and physical "mail" carriers means securely distributing a software code. It's the private key side of the PKI public key asymmetric cryptology approach for encrypting data, email, document signatures, network sessions, device identities, and so forth. These codes are usually 256-bit hashes of two integers (prime numbers), and for most identity authentication use cases, this is a one-time activity after which the endpoint or device becomes registered. This code is then supplied as a more robust form of identity than a password, but creating this infrastructure is expensive and sometimes the device is hard to reach.

Smartphone devices and the FIDO Alliance standards have significantly changed the game though. Industry support is now in place to justify these MFA migrations wherever suitable authenticators can be used. Unlike SS7, WebAuthn includes identifying characteristics within its request/response exchanges and easily detects when either party has changed during the process, eliminating man-in-the-middle attack tactics. Smartphones (and workstations) can store and use distributed

token/certificates, but they can also use other locally generated forms of identification characteristics – think biometrics.

IDC believes IT buyers should already have MFA solutions included within their present year security software budgets; if not, include such next year. This is a must-do security thing, but we believe current market acceptance rates to be a disappointing 30% or less. That means 7 out of 10 users are all still making up passwords.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Using the IDC MarketScape model, IDC studied organizations that offer advanced authentication security software across the globe and surveyed plenty of customers using these technologies in 2020. Evaluated vendors provide global capabilities, and while there are approximately 25 total vendors in the broader market, the following specific offering criteria must've been met to have qualified for this assessment:

- **Revenue.** Each vendor was required to have at least $30 million in 2019 worldwide security software product revenue – as determined by IDC – associated with authentication technologies.
- **Technology.** Solutions must support at least one authentication technology not based on knowledge characteristics.
- **Endpoints.** Solutions must support more than one device per user ideally including smart mobile technology.

For these reasons, platform authenticator solutions (Windows Hello, Google Authenticator, etc.) were not included in the study.

In some instances, study vendors did not provide specific input nor any customer references, and in those cases, IDC used all available public information to apply a proper strategy or capability rating solicitating vendor feedback before publication.

ADVICE FOR TECHNOLOGY BUYERS

For many organizations, the adoption of advanced authentication rarely includes a one-size-fits-all Shangri-la option, so expect that some of your users may be stuck with passwords and SMS OTP approaches until certificate or token distribution issues can be resolved. Environments that ban the use of smartphone devices can be a problem; users' reluctance to deploy on their personal devices can be a problem; unsecure registration capabilities for unmanaged BYOD can be a problem; the costs and logistical challenges of managing hardware keys and tokens can be a problem; and ubiquitous support for all combinations of Windows/Android and Mac/iOS platforms can be a problem.

Resolving these sorts of issues involves a combination of segmenting user populations, performing risk analyses activities, tightening access controls with contextual policies, and sometimes relaxing tolerances (2FA) based upon user roles and exceptional circumstances. Maybe not cheap in the long run due to productivity hits and support costs, passwords were, however, way easier to simply create and deploy. Unfortunately, password creation responsibilities placed organizational security burdens on end users rather than security teams.

But these are still early days in the development of more friction-free approaches. Savvy vendors and IAM start-ups are developing very innovative solutions using combinations of biometrics, behaviors, locations or proximities, signal sensing capabilities, and more — usually in combinations — leveraging integrated machine learning (ML) and artificial intelligence (AI) engines. The majority of these new solutions will be delivered via a SaaS model, saving organizations from having to acquire and deploy hardware and software for what IDC believes should naturally be an outsourced service. The day is coming where true passwordless solutions will understand who we are based on what we do, but that day won't be in 2021 (or even 2022). As a technology buyer, should you wait? IDC thinks not; the current benefits exceed the downside. Authentication approvals are a binary event, so look to those open solutions and portability as a hedge to a bad adoption decision (LOBs are hard to keep happy).

Advanced authentication is one element of a full identity stack that begins with a directory source, includes an identity management capability, can involve a privileged user monitoring component, and may even include a sophisticated identity governance solution within specific industries or just to review who's doing what and who isn't that could. There are advantages to acquiring advanced authentication technologies that are part of a broader single or separate vendor stacks, but those advantages can disappear when too many use cases can't be widely supported.

In the end, as the IT/security buyer, you're going to vote with your dollars. The challenge for many is balancing elegance and "smart choice" perspectives with the whole concept of practicality. Buy what you can afford and credibly deploy for rather immediate results. Return with a broader agenda based upon a track record.

VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations underlying an assessment of the vendor's relative position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's position relative to its market strengths and challenges. Based on the evaluation criteria, understand that for you a Major Player can easily become a Leader in your segment when someone knocks out a requirement or two.

Along with our market quantification efforts, this is essentially our job/role within the security analysts' space. We're trying to interpret acronyms and transform them into user benefit-level analyses confirmed by product/solution sales. If nobody buys it, there might be a problem.

Thales

Thales is positioned in the Leaders category in the 2021 IDC MarketScape for advanced authentication for identity security vendor assessment.

Thales' Digital Identity and Security Division offers a range of products spanning the digital and physical worlds using three business units (Cloud Protection and Licensing, Banking Payment Services, and Identity and Biometric Services) to address workforce, B2C, and B2G opportunities.

In terms of offering a full IAM stack, Thales maintains a narrower focus than other larger vendors but is continuing to evaluate feature/function adjacencies the company can add to the core advanced authentication solution using a cloud delivery rather than a separate packaging approach. Identity proofing, self-service user capabilities, improved directory integrations, single sign-on, and so forth are relevant examples of use case–oriented investments. The company is also actively contributing to the

CAEP/SSE OpenID standards effort to enhance its risk management capabilities and improve its zero trust competitiveness.

SafeNet Trusted Access is the ready-made cloud-based service coming from the Gemalto acquisition, offering similar features and complemented by scenario-based access policies. It now contributes more than half of all identity revenue.

Strengths

Thales supports every form of authentication technology available in the market and can leverage technology across multiple business units to deliver unique capabilities to large enterprises.

The company is a respected security technology vendor with access to a €1 billion research and development fund for the broader organization. Thales has offered passwordless identity options for at least a decade.

The company holds a dominant market share position in the European Union market and is an independent supplier of security software – apart from a cloud service provider – which can be a GDPR (Schrems II) issue.

Challenges

Thales is still in the process of building out some of its cloud-based services, bringing together identity technologies available within the company as its on-premises customers increasingly convert to a services-led model. Consequently, in the enterprise space, the cloud platform actually offers broader authentication capabilities than the on-premises solution.

North American sales channel investments must attract skilled new partners to increase the company's share of the largest advanced authentication market.

Consider Thales When

You already have other elements of an identity stack in place and you are a large organization that needs to support a broad range of authentication devices including advanced biometrics and increasingly sophisticated AI-driven and contextual user insights. Thales may have a narrower IAM security development focus but goes to the ultimate depths to support 2FA/MFA options. These conditions more typically surface in multinational accounts where physical, electrical, and cellular challenges present themselves.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the 2019 estimated market shares of each individual vendor within the advanced authentication for identity security market.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. Many of the technology components have been previously identified and assessed for their importance to the industry as part of an earlier IDC TechScape analysis and document.

IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

The market for advanced authentication for identity security solutions is very diverse. Participating vendors include specialty point solution providers, identity management platform providers, large software technology companies offering authentication inside an enterprise application business solutions suite, and even a full software stack platform provider that created an identity service inside a traditional on-premises or PaaS offering.

IDC has defined and advocated a new approach to authentication, dubbing the term *modern authentication.* Modern authentication has the following primary attributes:

- Solution centric
- Simplified user experience
- Invisible authentication whenever possible
- Authentication appropriate to the mitigated risk

Passwordless authentication is clearly a modern authentication technology, and using a factor such as a biometric certainly provides a strong foundation; however, a strong passwordless solution does not eliminate other authentication technologies and the need for situational reassessments. Risk-based analytics plays a major role, providing continual authentication based on user activities, and suitable engines are augmenting user/device/network health checks within leadership offerings.

LEARN MORE

Related Research

- *Akamai MFA: What's Different Here?* (IDC #IcUS47586321, April 2021)
- *Okta Leverages its Financial Evaluation to Acquire Auth0* (IDC #IcUS47513721, March 2021)
- *Modern Authentication 2020: Passwordless Enables a Future of Trust* (IDC #US45922320, January 2020)
- *IDC TechScape: Worldwide Advanced Authentication, 2019: Using Technology to Reduce Friction in Accordance with Assessed Risk* (IDC #US44775319, October 2019)

Synopsis

This IDC study presents a vendor assessment of the 2021 advanced authentication for identity security vendor market using the IDC MarketScape model. Most of the vendors in this space will typically explain how they're following a "land and expand" strategy for MFA. It's the same one used years ago in the single sign-on space where near-term needs were obvious and SAML was young. MFA can be effectively delivered as a SaaS offering and really ought to be for your business or organization. Technology exists that will allow you to trust this outsourcing equation; just understand some PKI basics.

"Helping restore order from chaos, multifactor identity solutions are available in the form of the simple to the extremely complex," said Jay Bretzmann, program director, Cybersecurity research, IDC. "The challenge users face is buying enough capability now without eliminating a route to a truly passwordless future complementing a zero trust networking environment."

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com

Copyright and Trademark Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights. IDC and IDC MarketScape are trademarks of International Data Group, Inc.

Copyright 2021 IDC. Reproduction is forbidden unless authorized. All rights reserved.