TechVision RESEARCH

Multi-factor Authentication

4/25/2019

Doug Simmons, Senior Managing Partner
and Consulting Analyst,
TechVision Research

TechVision RESEARCH

TechVision Research at a glance

Our model is built around industry experts with strong track records of execution.

We go beyond the trends. Our deliverables-based engagements give you the action plans you need to get the job done.

We offer tested templates, tools and reference architectures to assist your decision making.

Founded in 2015 by veterans of the research industry to bridge the gap between enterprise board-level strategy and technical solutions through cutting-edge research and pragmatic consulting.

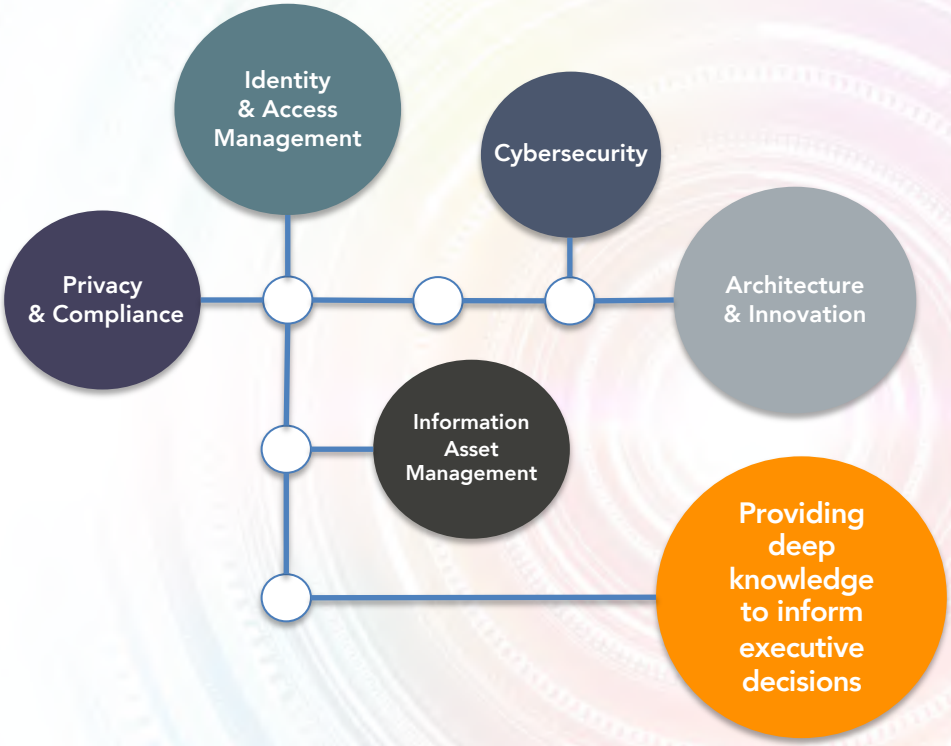
TechVision RESEARCH

What we do

Take a client theme

- Zero Trust Networking
- Microservices Level Set
- Identity of Things
- Evolving against Vulnerabilities, Breaches and the next Cyber Attack
- AI Executive Level Set—The Three Waves of AI
- Innovation Reference Architecture
- Customer Identity and Access Management (CIAM)
- Multi-Factor Authentication (MFA)
- Developing an Enterprise Blockchain Strategy
- Future of Identity Management (2019-2024)
- Developing an Enterprise DevOps Strategy
- The Future of Work
- Robotic Process Automation (RPA)
- Consent Management
- Best Practices in Securing Unified Communication
- An Emerging Decentralized Identity/Verifiable Claims Ecosystem
- Developing a Digital Transformation Reference Architecture

and Connect the Dots



Research

- ✓ Enterprise-focused research with unlimited access
- ✓ Answers the hardest technology questions
- ✓ Research agenda driven by disruptive and emerging technologies

Consulting

- ✓ Deliverables-based engagement model using proven techniques
- ✓ Performed by one or more of our Principal Consulting Analysts
- ✓ Tailored to your specific situation

TechVision RESEARCH


The TechVision Research
Conference 2019
11-14 November
Manchester Grand Hyatt, San Diego

Today's Presenters

Doug Simmons brings more than 35 years of experience in IT security and identity and access management (IAM). He has performed hundreds of engagements as the subject matter expert, and for the past several years has lead a team of senior consultants focused solely on IT security, risk management and IAM.

Doug consults with Global 1000 organizations to assess, strategize and design extensible IT security infrastructure, policies and processes. He also researches emerging IT security-related initiatives, such as blockchain, smart contracts, distributed ledgers and microservices in order to develop research reports that are then used within customer environments to develop the business case, technical strategy and migration plan to incorporate such initiatives.

Doug is a frequent public speaker at IT security and identity management events to share good practices, lessons learned and research findings

Gary Rowe is a seasoned technology analyst, consultant, advisor, executive and entrepreneur. Mr. Rowe helped architect, build and sell two companies and has been on the forefront the standardization and business application of core infrastructure technologies over the past 35 years. Core areas of focus include identity and access management, blockchain, Internet of Things, cloud computing, security/risk management, privacy, innovation, AI, new IT/business models and organizational strategies.

He was President of Burton Group from 1999 to 2010, the leading technology infrastructure research and consulting firm. Mr. Rowe grew Burton to over $30+ million in revenue on a self-funded basis, sold Burton to Gartner in 2010 and supported the acquisition as Burton President at Gartner.

TechVision RESEARCH

Agenda

- Thesis – Why MFA?
- Overview of MFA including Key Business Drivers
- Discuss the types of MFA approaches currently being deployed
- Overview of MFA standards
- Describe MFA in the IAM Reference Architecture
- Review of our short-list of vendors and solutions
- Summary Recommendations

Thesis

- Multi-Factor Authentication is gaining traction as a best practice for enterprise security programs.
- It is based on the premise that traditional, single factor authentication schemes (like IDs and passwords) are relatively easy to break and as threats escalate, simply not good enough.
- It is a good time to consider making MFA a cornerstone of your enterprise IAM infrastructure given improved MFA vendor offerings and the inherent weaknesses of phishing-vulnerable password-based authentication.

Requiring multiple authentication factors for high risk or high value transactions is the emerging security best practice

TechVision RESEARCH

Background

- Multi-factor authentication (MFA) is one of the most active and important areas within information security and IAM today
- For well over a decade, the use of passwords to authenticate identities has been suspect; in particular for high value transactions the use of simple, relatively insecure and often recycled, easily guessed or stolen passwords are not good enough
- One of the most sought-after pieces of personal identifiable information (PII) is the username and password
  - this is especially problematic in that individuals often reuse the same username/password combinations at multiple sites
- Requiring other factor(s) to access valuable content or to conduct high-value transactions is increasingly required

Background

- MFA is a subset of the authentication market and is often evoked based on adaptive authentication or step-up authentication based on security policy and/or contextual data regarding the person requesting access
- The challenge with MFA is to balance the need for security with ease of use
  - This balance is supported by the execution of policies that build on reliable contextual data to dynamically determine when MFA is needed and when single factor authentication is sufficient
- Measuring the degree of certainty that a user is who they say they are will increase as more data from more categories are collected

The more data that are collected in support of the user's request across the four ranges of what a person knows, who they are, what they have, and their history—the greater the degree of certainty

Business Drivers for MFA

- ***Business Facilitation***
  - the need to improve interoperability and efficiency through interconnected systems to support employees, affiliates, business partners and customers
- ***Enhancing User Experience***
  - simplifying the process of authentication and letting the end user *not* have to remember another password
- ***Cost Containment***
  - planning to reduce the cost of management of multiple disparate authentication systems and processes
- ***Security Effectiveness and IT Risk Management***
  - improving the level of assurance that maps to an identity for appropriate authentication
- ***Support Administrative and End-user Efficiency and Effectiveness***
  - consolidating the authentication infrastructure and better defining and reducing the number of access points

What is MFA?

- The use of more than one set of credentials from multiple categories that are used in concert to better determine (hopefully unequivocally) that you are who you say you are
  1. Typically, one category of 'factors' is something that you know, such as a user ID and password
  2. A second factor that is added to this is often something that you have, such as a smart phone, smart card, token fob or other such unique device that when paired with the first factor (something that you know), increases the veracity of authentication
  3. A third factor can be something that you are
     - Biometrics typically fill this bill with digital representations of your face (facial recognition), fingerprint, retina scan or voice print
  4. Fourth is something that you have done
     - This can include where you have logged into from before (IP network address), recent transactions, time of day, last password reset, and flags for multiple failed login attempts

Why MFA Now?

- MFA is a critical in the area of fraud prevention, and identity theft is one of the most prevalent and harmful forms of fraud in existence today
- Over the past few years, significant advancements in the ability to deploy MFA to wide ranging constituencies – from employees, contractors, business partners to customers have made it much more palatable for enterprises of all sizes and types to consider
- Now is a good time to consider making MFA a cornerstone of your enterprise IAM infrastructure and start saying goodbye to the inherent weaknesses of phishing-vulnerable password-based authentication

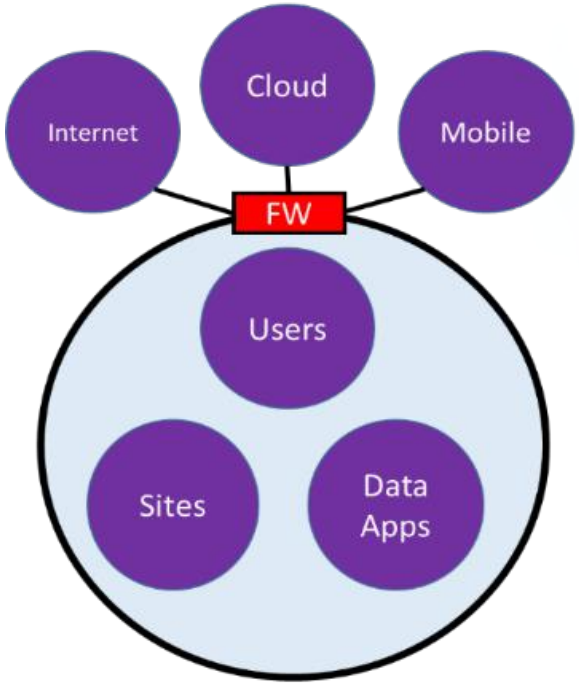
Without the appropriate deployment of MFA, the authentication function remains one of the – if not *the*, weakest link in the enterprise and it is incumbent upon the enterprise security leadership to close this gap

Why MFA Now?

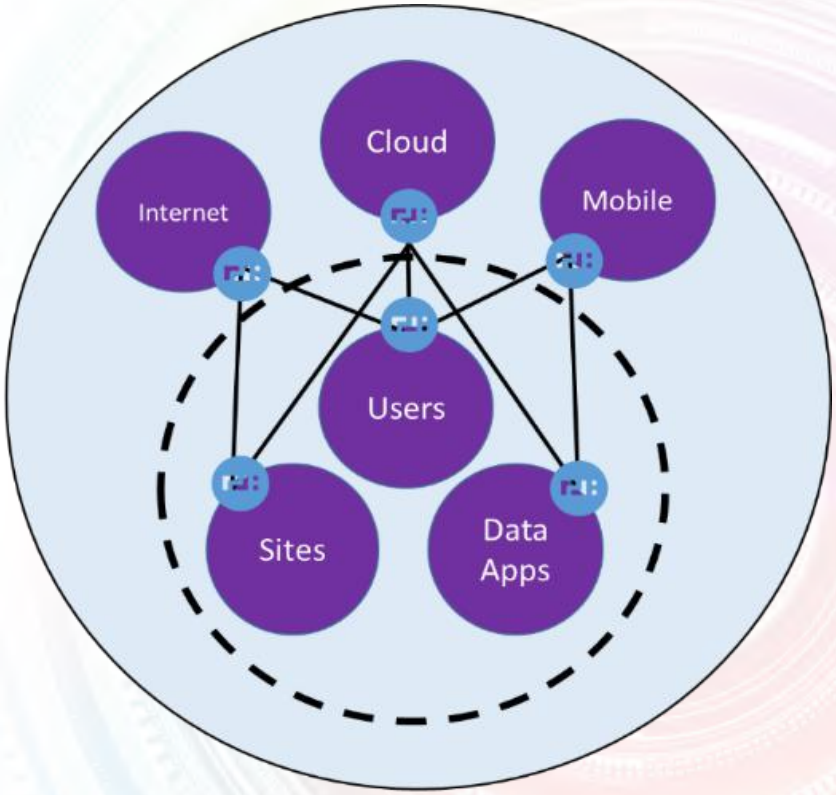
- With the advent of mobile device ubiquity and the willingness for end users to deploy apps on these devices, techniques such as ‘mobile push’ have gradually broken down the barriers of cost and complexity to deploy MFA
- As we begin re-architecting our enterprise environments to incorporate elements of Zero Trust, MFA becomes a critical piece of the ZT-puzzle
  - With the notion of ‘identity as the new perimeter’, it is actually “identity + device” that becomes the perimeter
  - In a ZT environment, the most critical facet of security is knowing who (or what) the end user is as well as the device being used to authenticate that user or thing

This is the new perimeter; this combination of coupling an identifier with something the user has with them (like a mobile phone)

ZT: Gone Is The Secure Network Perimeter



Secure Network Perimeter
With Clear Demarcation Point



Fluid Network Perimeter

The Digital Economy blends customers, suppliers, organizations.
Cloud, Mobile, BYOD, IoT create a fluid network perimeter

TechVision RESEARCH

Why MFA Now?

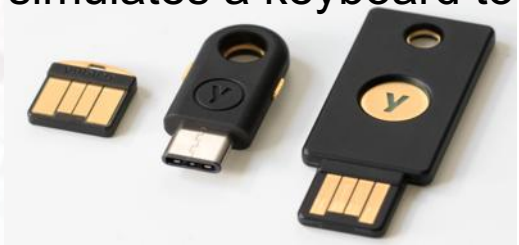
- While other, more ‘legacy’ types of MFA such as One Time Password (OTP) tokens and smart cards still have a place in the IAM ecosystems for certain high-risk environments such as defense, finance, health-care, and IT administration, they can be considered deprecated in most enterprise situations
- In many instances, the new age of mobile device-based MFA is more convenient and sufficient in many use cases to improve identity verification upon system login
  - Caveats to be considered include the actual ubiquity of mobile devices and network coverage/reliability in your environment – but in most cases, these caveats are in the minority.

Early MFA: Token FOB for Remote Access

- Early MFA was called two-factor authentication (2FA) and generally used a token FOB for remote access to systems via corporate Virtual Private Networks (VPNs)
- The pioneer in this space, starting in the mid-1990's was RSA with their SecurID 'token', a fob that generates a one-time password (OTP) periodically (e.g., every 30 seconds) and is synchronized with a remote access server (RAS) supporting the VPN
- This rotating, synchronized password method makes OTP solutions impervious to replay attacks, which is one of the key vulnerabilities of the 'static' passwords so widely used
- These solutions work with the end user using the one-time password provided by token fob to authenticate to the corporate VPN – along with their user ID and associated password.

Early MFA: Token FOB for Remote Access

- Some factors that limited the impact of these early 2FA approaches
  - Access to the VPN via 2FA didn't mean single sign-on to the corporate intranet – it simply let a person access the network.
  - The token fobs were relatively expensive– typically in the $45 per user range, so it was a significant expense item and required additional scrutiny and corporate expense if they were lost (or stolen).
  - The seed algorithm used to generate the synchronized one-time passwords on fobs and servers was not as secure as had originally been thought. In 2011, RSA's SecurID platform had been breached at Lockheed-Martin – a major U.S. Defense contractor.
- Variations on the SecurID token fob theme have since emerged
  - For instance, Yubico offers a small USB token with an embedded chip that creates an OTP when a key is pressed and simulates a keyboard to facilitate easily entering a long password.



Soft Token OTP

- In the early 2000's it was recognized that the cost, deployment and management of hardware tokens in support of OTP were in many cases overly burdensome
  - In response, vendors such as RSA, Entrust, Gemalto and others developed software tokens that could be stored on general-purpose electronic devices such as desktop computers, laptops, or mobile phones
  - Because software tokens are something one does not physically possess, they are exposed to certain threats based on duplication of the underlying cryptographic material - for example, computer viruses and software attacks
- Software tokens do have benefits over hardware tokens: there are no physical tokens to carry, they do not contain batteries that will run out, and they are generally less expensive than hardware tokens.

Many enterprises have deployed 'soft tokens' as a way to improve authentication, but enterprises recognize and consider efforts to mitigate the potential threats we just described

PKI and Smart Cards

- In the 1990's, X.509 PKI certificates were issued to individuals holding credit card-sized smart cards that contained a cryptographic chip
- Similar to OTP token fobs, the smart card constitutes something you have, and when authenticating to a system with a smart card reader, the card holder enters a PIN (something you know) to enable the authentication process
- In a nutshell, the challenges with deploying trusted certificates to large numbers of end users, coupled with supplying card readers on virtually every desktop or laptop the end users would access was costly and complex
  - Cards were lost, certificates needed to be revoked and reissued, Certificate Authority (CA) servers were needed, certificate revocation lists (CRLs) maintained and so forth – leading to a slow adoption rate that has since petered out even more

Enter the Smartphone

- The advent of the iPhone and Google's Android mobile device operating systems coupled with cellular network providers who were rapidly improving SMS reliability and range brought the smart phone into the fold as a bona fide 'second factor'
  - 'something you have' that could obviate the need for a specialized token fob OTP generator or smart card for many organizations
- This sequence of events was the real harbinger for widespread adoption of MFA within organizations of all sizes as well as the consumer and e-commerce site interactions
- Financial institutions began to deploy MFA in the form of text messages with OTP 'codes' embedded in them to their customers' phones in order to enable a key second factor to the authentication process with online banking
  - Your UID, password and the code just sent to your cell phone on record in your account profile

Don’t PUSH Me!

- Major phone vendors have helped support the MFA movement
  - For example, Apple released the Apple Push Notification service (APN) back in 2009 and less than a year later Google released its own Google Cloud to Device Messaging service (C2DM) for Android devices
- A ‘push notification’ is a message that pops up on a mobile device
  - Push notifications look like SMS text messages and mobile alerts, but they only reach users who have installed an app on the device to receive the messages
- Because the person with the phone (something they have) must be the same person logging into the online system with their UID/password (something they know), the end result is 2FA

Don’t PUSH Me!

- Typically, the end user receiving the MFA push notification on his or her device must ‘push’ a soft button on the display that means they acknowledge the fact that they are logging into an online system
- Simply adding the requirement to provide their fingerprint (something they are) to this process-whether within the push app itself or by virtue of the smart device’s biometric capability, we can effectively deploy MFA

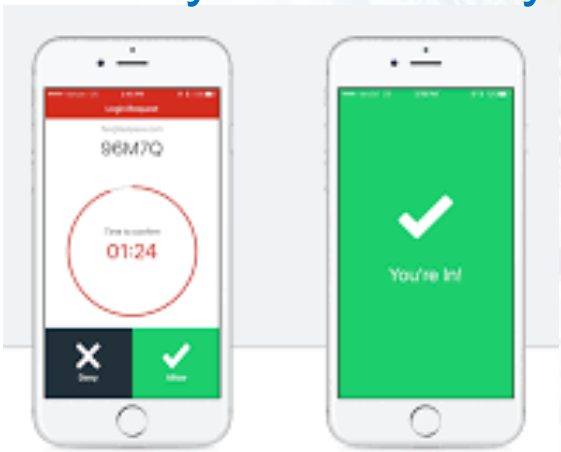
Here We Are!

- This advancement in cellular messaging provided a big push (no pun intended) to make MFA much more user-friendly MFA
- Along with Google and Apple, a new breed of MFA has vendor emerged; vendors that created MFA applications for iOS and Android devices as well as laptops running Windows and OSX
- Companies like DUO Security and Authy quickly gained favor with enterprises in the MFA space because of the popularity of the tool with end users (including consumers) and relative ease of deployment and integration

Here We Are!

- Legacy 2FA vendors like RSA adopted push technology in addition to their existing solution sets.
- Additionally, many IAM vendors that enable and support the authentication processes of their customers, such as Microsoft, ForgeRock, Okta, Janrain, Gigya/SAP and many others added push authentication capabilities to their products
- *The smart phone enabled push notification has emerged as the leading class of MFA solutions*

While this approach isn't perfect for all situations and certain high-risk use cases, it is very user friendly and readily integrate



MFA Standards

Authentication standards are emerging and should be considered as a starting point for an enterprise MFA program

- The Initiative for Open Authentication (OATH) addresses authentication integration challenges with standard, open technology that is freely available to application developers
- OATH is a collaborative effort of IT industry leaders aimed at providing a reference architecture for universal strong authentication across users, devices networks
  - The OATH standard has been ratified in a series of IETF RFCs
  - OATH standard is currently being contributed to by a large number of vendors, including Gemalto, HID, Symantec, VASCO, Yubico and many others
- Intended that OATH will offer more hardware choices, lower cost of ownership, and allow customers to replace existing disparate and proprietary authentication systems whose complexity often leads to higher costs

MFA Standards

- OATH designed to be interoperable in solution development and deployment by enabling straightforward integration with existing identity and access management platforms and infrastructure (e.g. LDAP directories, web access management and single sign-on servers)
- OATH standard describes implementation of a core set of authentication credentials:
  - One Time Password (OTP) - based authentication
  - Public key infrastructure (PKI) - based authentication (using X509.v3 certificate)
  - Subscriber identity module (SIM) - based authentication (using GSM/GPRS SIM)
- OATH assumes that LDAP (including Active Directory and Azure Active Directory) is used to enable the validation server and the directory to exchange information

MFA Standards

- FIDO (Fast Identity Online) Alliance, an industry consortium launched in February 2013 to address the lack of interoperability among strong authentication devices
  - PayPal and Lenovo were among the founders
- Supports biometrics, Trusted Platform Modules (TPM), USB security tokens, smart cards, and near field communication (NFC)
- FIDO standards define a common interface at the client for the local authentication method that the user deploys
  - Client can be pre–installed on the operating system or web browser

FIDO members totaled more than 260, including a Board made up of Aetna, Amazon, American Express, Bank of America, Gemalto, Google, Intel, Lenovo, MasterCard, Microsoft, NTT DoCoMo, PayPal, Qualcomm, RSA, Samsung Electronics, USAA, Visa, VMware, Yubico and many others

Biometrics and MFA

- Biometrics is an important element of the “who you are” category
- Investment, adoption and advancement of biometric technology by vendors such as Apple, Google, Samsung, LG and many other smart phone manufacturers has led to a dramatic improvement in biometrics capability and reliability
- Many MFA vendors can leverage the Trusted Platform Module (TPM) interface in these mobile devices to determine that the user had authenticated to their device via facial recognition or fingerprint biometrics and can incorporate this awareness into the overall strength of the end-to-end MFA session
  - leading to the elimination on the reliance of a user inputting a PIN (something she knows) and instead relying on biometric authentication to the mobile device as the second factor (something/who she is) in addition to possession of the device (something she has)

Biometrics and MFA

Some biometric considerations:

- Voice biometrics works well if a user calls on a regular basis and there is a long sample history
  - Voice biometrics needs a quality connection so that the voice quality has a mean opinion score above 4.0 Voice biometrics systems will return a probability score on how well the voice heuristics match that of previous samples
- Facial recognition works well for users signing into a device such as a phone, tablet, or kiosk
  - Recently, airlines such as Delta have added facial recognition to their self-service check-in kiosks to improve security and user convenience
- Fingerprints are used for secure access to systems such as Clear for airport security entrance identification
  - Iris scanning is another example, but is less prevalent because of the inconvenience to users, especially those wearing contacts.

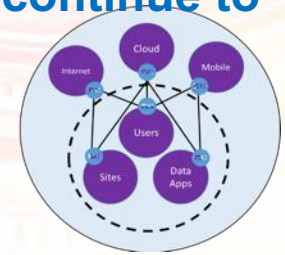
Biometric systems can be spoofed, so they should be used in conjunction with other types of authentication

MFA in the Future

We have anticipated the demise of password-centric authentication for decades - the time has arrived to deploy MFA within your enterprise

- Device and network ubiquity, reliability, Bring Your Own Device (BYOD) initiatives coupled with the accelerating levels of fraud associated with password-based authentication
- Many large, influential vendors such as Microsoft, Cisco and others have laid down the gauntlet - the password is truly dead
- The shift to the cloud provides the opportunity to reinvent authentication
  - If your organization is migrating to Azure, there will come a time within the next 18-24 months when passwords are deprecated

Furthermore, as the concepts associated with Zero Trust continue to evolve and take hold, MFA will be an imperative



TechVision RESEARCH

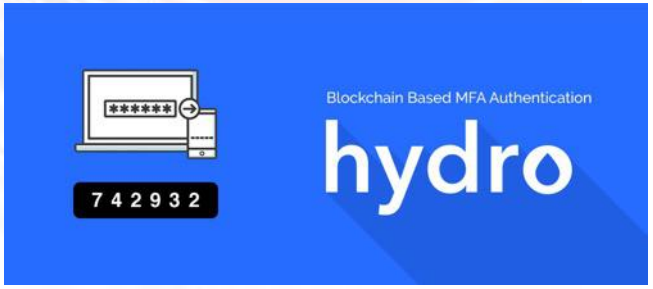
The Future or Now? MFA and Blockchain

Furthering the development of identity solutions using blockchain and distributed ledger technology, emerging vendors are bringing MFA solutions that foster true BYOID

- ShoCard recently introduced ShoBadge, which allows identity management to be controlled by each user and shared within the workplace
  - With identification information stored on the mobile device, employees can securely share their personally identifiable information (PII) with their employer, while their information is independently verified with one way digital signatures of hashes of their data on the blockchain. The blockchain holds no PII - only verification signatures
- Drupal's now offers Hydro Raindrop MFA - its Blockchain based MFA plugin that uses a blockchain-based authentication layer

ShoCard

Watch This Space!

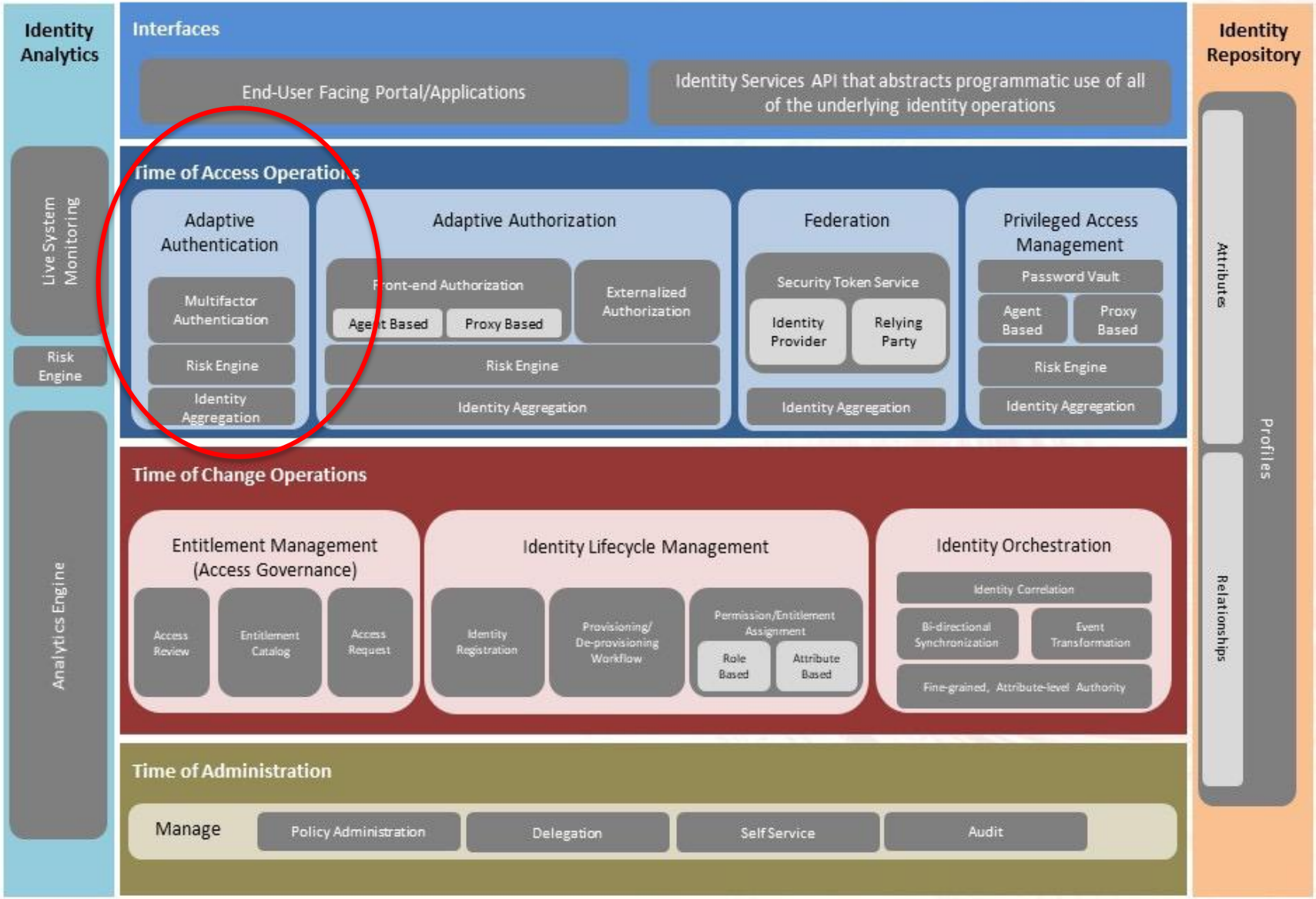


TechVision RESEARCH

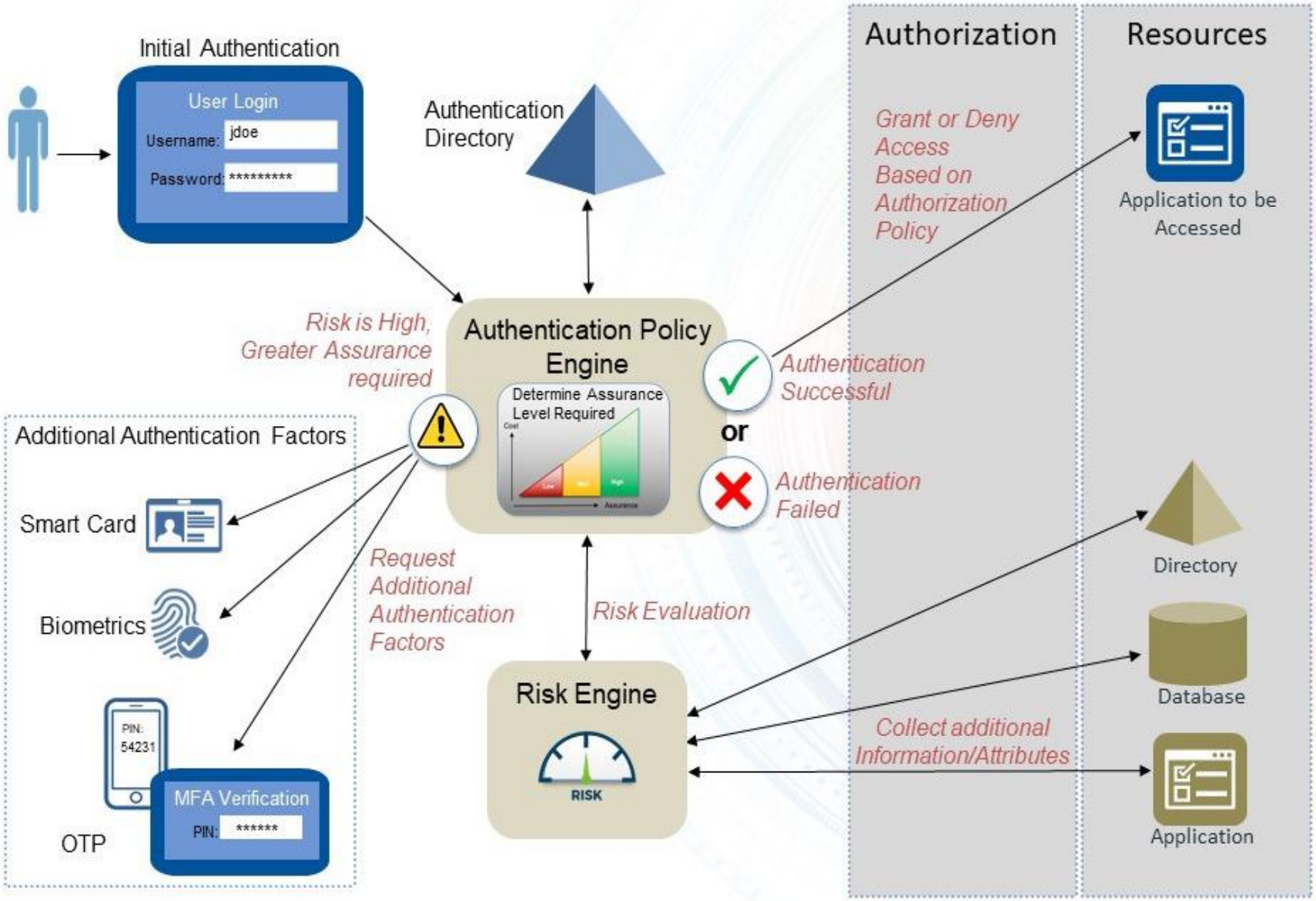
MFA Architecture Principles

- Encompass risk-balanced user authentication to systems, networks, applications and services for the target users.
- Support a strong user experience
- Address the full range of assurance levels identified by the organization along with associated requirements
- Support MFA from a suitably wide range of devices
- Provide authentication for the organization's people, applications, devices and services regardless of platform and architecture
- Enable the organization's business processes and workflows
- Ensure compliance and mitigate IT risks
- Are easy to use, sustainable and cost-effective.
- Authenticate users for services and applications hosted both within organization's networks and external to them

MFA In the IAM Reference Architecture



MFA In Adaptive Authentication Pattern



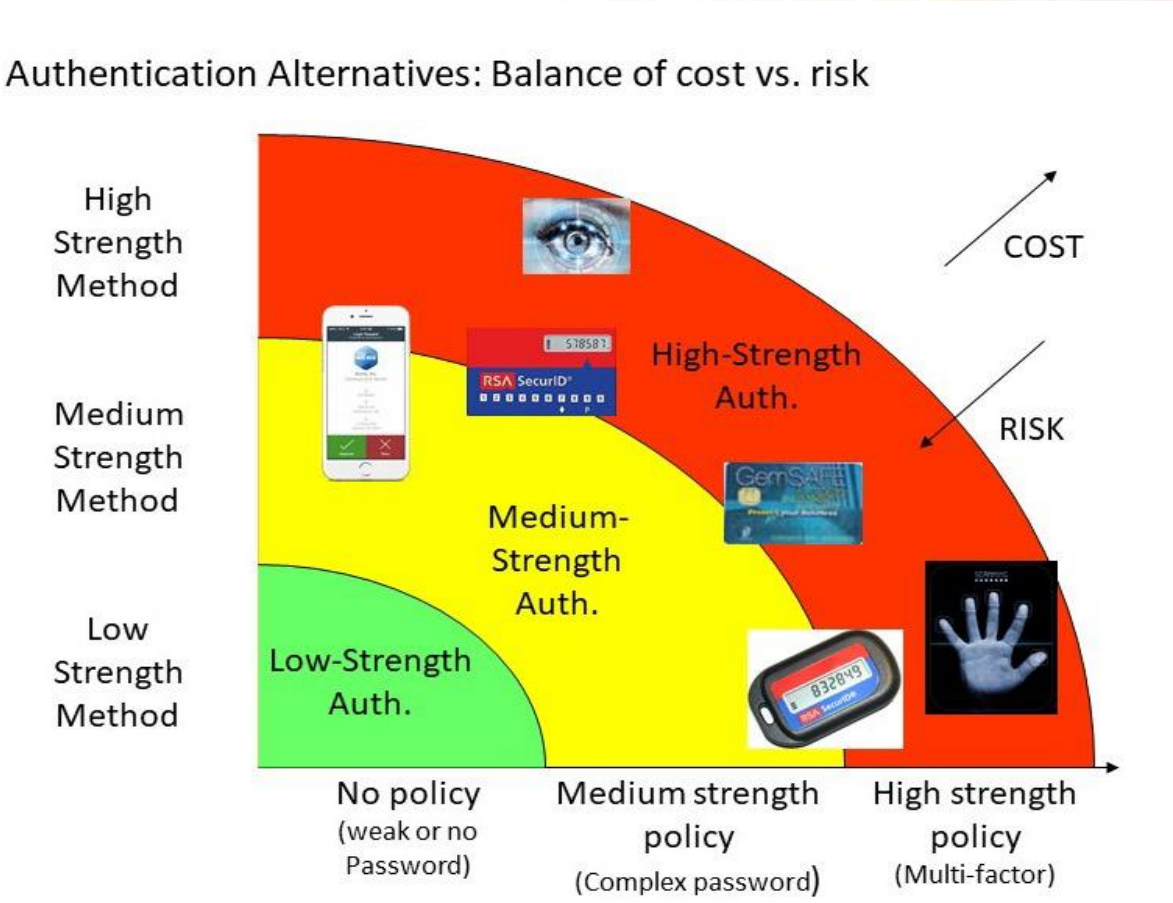
Identity Vetting and MFA

Don’t forget:

- Identities must be vetted before issuing credentials and is generally the first step towards establishing the requisite level of confidence that the authenticating user is in fact who they say they are
  - Evoking MFA on a suspect identity is like closing the barn door after the horses have escaped
- The level of identity verification must be commensurate with the level of risk associated with the IT asset to be accessed
  - The strongest MFA technology could be deployed by an enterprise, but if the initial identity vetting process is weak, the entire authentication topology is weakened, as well
- The appropriate level of identity vetting upon credential issuance is a key function of Enterprise Risk Management

Balancing Risk Reduction vs. Cost

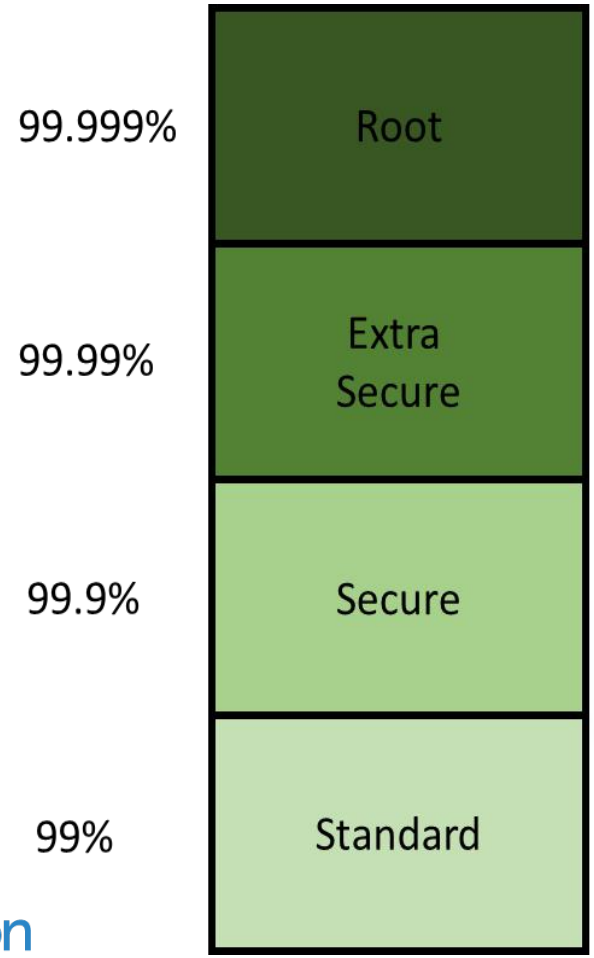
- MFA must be deployed without a well-thought-out strategy that weighs the risks, costs and usability
  - An enterprise MFA strategy must consider the association between authentication cost and risk reduction



TechVision RESEARCH

Balancing Risk Reduction vs. Cost

- One critical step is to identify the level of identity assurance required for data, application, and system access
- Many organizations adopt a 4-tier model:



TechVision RESEARCH

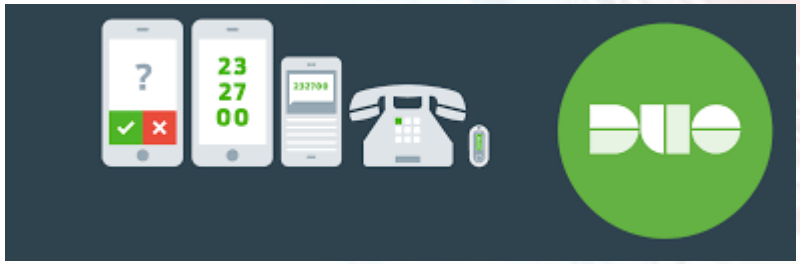
MFA Vendor Shortlist

TechVision feels that the following vendors (listed in alphabetical order) are strong candidates for consideration in that they address key enterprise MFA requirements and have a solid future state plan:

- Authy (Twillio)
- DUO (Cisco)
- ForgeRock
- Gigya/SAP
- Google
- Janrain
- Microsoft
- Okta
- RSA
- Symantec
- Yubico

MFA Vendor Shortlist

- Authy (Twillio)
  - supports MFA by generating a time-dependent six-digit code, which the user enters after submitting a username and password
  - ability for users to access their data across different devices
  - can work offline
- DUO (Cisco)
  - Duo Security was acquired by Cisco, September 2018
  - strategic addition to Cisco's portfolio and is in alignment with their *intent-based* networking strategy by extending it into multi-cloud environments and simplifying policy for cloud security and expanding endpoint visibility coverage
  - Duo Push, sent by the Duo Mobile authentication app, allows users to approve push notifications to verify their identity



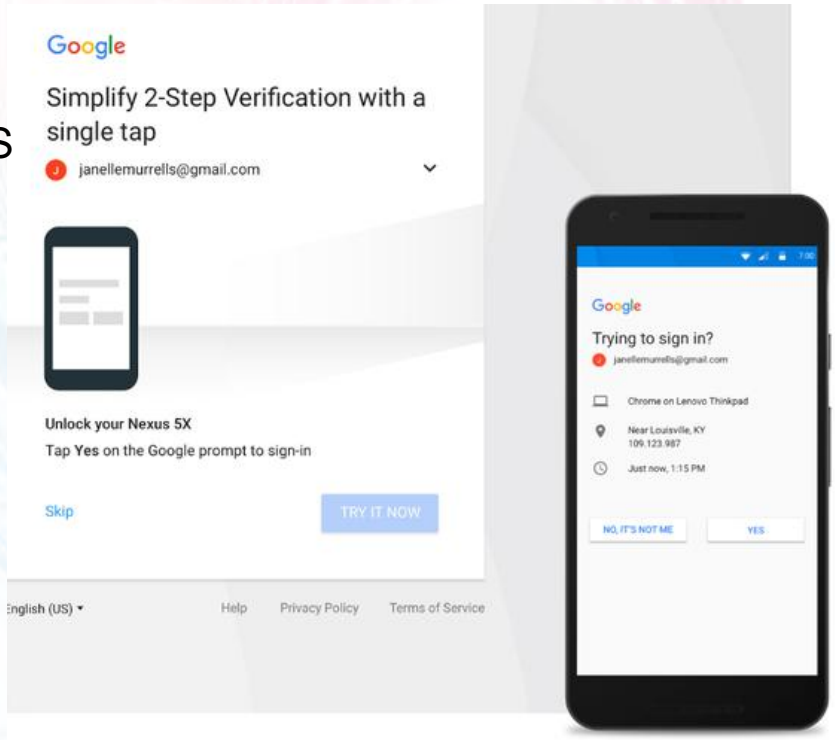
MFA Vendor Shortlist

- ForgeRock
  - developed a currently 50-company Trusted Partner Network that includes leading MFA solution vendors such as Duo/Cisco, Symantec, Yubico and many others and fits well into their overall IAM platform
  - investment has been leaning toward expansion of its access and identity management capabilities – notably its development of Authentication Trees to support more granular capabilities when establishing authentication with an end user
  - Authentication trees provide fine-grained authentication by allowing multiple paths and decision points throughout the authentication flow
- Gigya/SAP
  - C(ustomer)IAM solution running on their Customer Data Center (CDC) cloud
  - SMS-based one-time password (OTP) capability out-of-the-box
  - Also partners with a 3rd party called SAASPASS in order to enable its MFA and SSO solution
  - SAASPASS can be integrated with existing Active Directory environments in order to leverage enterprise user accounts and groups for enabling B2E MFA

MFA Vendor Shortlist

- Google
  - Google Authenticator is a software token that implements a two-step verification service using a Time-Based One Time Password algorithm (TOTP) and a HMAC-based One-Time Password algorithm (HOTP), for authenticating users of mobile applications by Google
  - provides a six- to eight-digit one-time password that users must provide in addition to their standard username and password to log into Google services or other sites

- Added device push as another MFA option that can be sent directly to users' Android devices as well as the Google client on iOS devices
- Last year began manufacturing their own USB security keys that are similar to Yubico's Yubikey hardware fob
- As part of Google's growing presence in the IDaaS and cloud platform arenas, their Google Security Keys are being positioned as their most secure MFA offering.



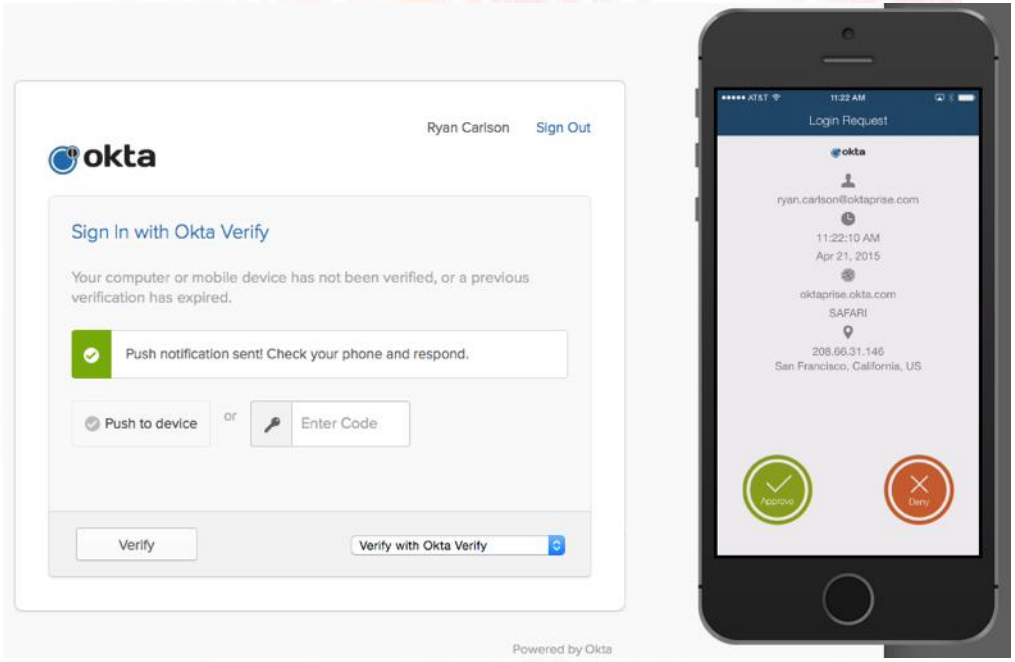
TechVision RESEARCH

MFA Vendor Shortlist

- Janrain
  - a leading cloud-based Customer IAM (CIAM) solution
  - focuses on streamlining account registration, reducing fraud and improving customer protection by adding MFA during the registration and login process, which further enables phone verification to improve account security, simplify account registration process
  - SMS text passcode and ‘push’ (app) notification
- Microsoft
  - Microsoft MFA server was introduced in 2014 as an on-premise server integrated with AD
  - recently announced it was going to discontinue Microsoft MFA Server as an on-premise solution and only offer Azure Multi-Factor Authentication (MFA) – a fully cloud-based solution
  - Fully committed to password-less authentication moving forward
  - Integrates with most leading 3rd party MFA solutions via OATH and FIDO

MFA Vendor Shortlist

- Okta
  - Leading B2E IDaaS (cloud) solution vendor
  - Okta Verify is an MFA factor type designed for end user identity verification with the Okta service
  - available for iPhone, Android, and Windows devices
  - includes the option to deploy Okta's MFA app to enable push notifications to these mobile devices
  - also supports Touch ID technology to guard against unauthorized use of Okta Verify, requires additional factor (fingerprint) when accessing high risk applications



MFA Vendor Shortlist

- RSA
  - well known for its SecurID product that provides two-factor authentication utilizing hardware tokens, software tokens, and one-time codes
  - RSA Authentication Manager from RSA Security is an MFA tool that adds additional security measures (via smartphones and biometrics) to standard username and password logins for a number of services and servers
  - RSA Authentication Manager is especially suitable for those organizations that want to make use of a variety of external SaaS products, such as Google Drive, Salesforce and O365
  - a number of authentication methods available, such as risk-based authentication, two-factor authentication, on-demand text messaging and token (SecurID)

MFA Vendor Shortlist

- Symantec
  - Symantec Validation and ID Protection (VIP) Service is a multifactor authentication (MFA) product that uses biometrics and smartphones to supplement standard username/password logins on a variety of servers and services - initially developed by Verisign
  - VIP is a cloud-centric solution that provides SSO and OATH-compliant MFA to B2E customers primarily
  - being positioned as a ‘better alternative’ to Microsoft MFA for Azure tenants
  - also offering endpoint protection and other integrated services beyond what Microsoft provide

MFA Vendor Shortlist

- Yubico
  - manufactures a hardware authentication device – called Yubikey that supports one-time passwords, public-key encryption and authentication, and the Universal 2nd Factor (U2F) protocol developed by the FIDO Alliance
  - allows users to securely log into their accounts by emitting one-time passwords or using a FIDO-based public/private key pair generated by the device
  - Yubico has been working with Microsoft to further enhance Microsoft's MFA on Azure by further developing the FIDO 2 specification in order to move toward true password-less authentication – one of Microsoft's (and Yubico's, among others) major objectives

Summary and Recommendations

- MFA is rapidly becoming the default standard for authentication
  - the combination of increased scale, the lack of well-defined perimeters, increasingly sophisticated threats and improvements in MFA offerings are influencing this phenomenon
- MFA services are getting better, smarter and easier to use and that is accelerating a more wide-spread movement to MFA
- The lesson with MFA programs is that the better you prepare, document your use cases and 'user stories', involve your key stakeholders, select the right vendor/tool for the mission and roll-out in a controlled, well-governed manner – the better your chance for success
- Good luck and let TechVision know if you'd like a dialogue or follow-up in the MFA area

Questions?