BUYER'S GUIDE:

MFA BUYER'S GUIDE

Evaluating and Getting Started with Multi-factor Authentication Solutions

Ping Identity.

NEW CAPABILITIES

One-size-fits-all authentication is a relic of the past, and the days of hard tokens as the default strong authentication method are behind us. While stolen credentials remain the most important factor in rolling out a multi-factor authentication (MFA) solution, the methods of deployment, endpoint visibility, authentication methods, supported applications and administrative capabilities have changed dramatically.

The expanding use cases for MFA are driving innovation in this highly critical corner of security. Modern MFA expands beyond the traditional what you know, have or are protocol to include location and other contextual factors. This allows you to apply the right type and level of authentication for any given user at any given time.

NEW EXPECTATIONS

Your applications are migrating outside the firewall, and your security demands—including providing access to customers and partners—are growing more complex. To meet these demands and protect your enterprise, you need to expand beyond single-factor and two-factor authentication.

Modern MFA solutions allows you to contextually step up your security and mitigate the costly risk of stolen credentials, while providing a frictionless user experience. When deploying MFA for partners and customers, there are dozens of new requirements and considerations. Make the authentication process too inconvenient, difficult or insecure, and users might opt-out entirely. Making the best choice for your enterprise can feel overwhelming. Use this guide to help you make the right decisions for your organization and users.

NEW OBJECTIVES

ACCELERATE DIGITAL TRANSFORMATION.

According to a recently completed survey of 200 IT decision makers, mobile usage of employee apps is the most widely implemented of all digital transformation initiatives that are fully deployed and in progress. The right MFA solution can give your users a seamless, frictionless experience and the mobile access they expect to all of their cloud and on-premises applications. Giving users secure access to the information and insights they need, when and where they need it, allows your companies to operate smarter, create value and strengthen its competitive advantage.

REDUCE RISK OF BREACH.

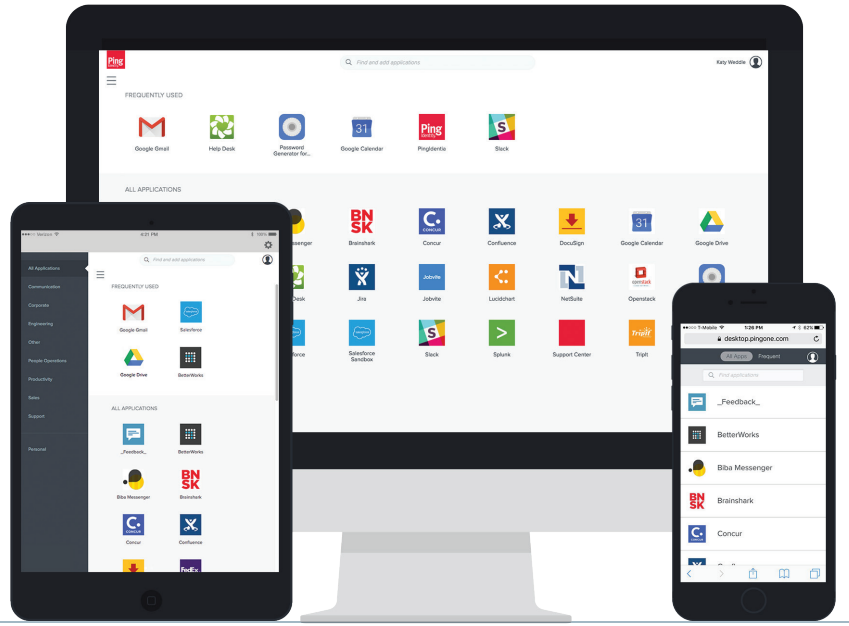
Stolen credentials and brute force attacks remain the most common MFA conversation starter. Given the magnitude of costs associated with a typical breach—not to mention the lost revenue and residual damage to your company's reputation—reducing your risk has tangible business benefits. With customers and partners trusting organizations with an increasing amount of personal data, employee credentials are no longer the singular focus for breaches.

LOWER COSTS.

If MFA is deemed necessary or required by policy, modern solutions have a much lower cost than legacy, hardware-based token solutions. Plus, some MFA solutions allow you to contextually step requirements up or down depending upon the associated risk of the activity. This can reduce the expense of one-time SMS passcodes, voice calls and other push methods by only employing those controls when the risk is warranted. Finally, investing in an MFA solution is usually offset through significant cost reduction in helpdesk overhead, as well as end user productivity improvement.

BALANCE CONVENIENCE AND SECURITY.

Modern MFA solutions can help balance convenience and security. This is particularly important for customers. Customers are not always willing to go out of their way to download a third party MFA application, but still need the security that MFA provides. To strike this balance it's important to implement MFA into a medium your customers are already familiar with, such providing MFA within your own mobile application. Additionally, customer devices may change as they upgrade and replace their phones. For that reason, it's also important to give customers a convenient way to add or remove trusted devices from their account.



SELECTING THE RIGHT VENDOR & SOLUTION

To identify vendors for consideration, you can consult industry organizations, trade publications and peers. You'll also gain third-party expert insights from leading analysts like Gartner, Forrester and KuppingerCole. Each regularly reports on MFA trends, technologies and solution providers.

Once you've identified a shortlist of vendors, invite each of them to respond to your requirements. You'll want to request presentations, demonstrations and other support materials, like white papers, eBooks, datasheets and so on. This can be as formal (or informal) as fits your organization, but clearly communicating your objectives and requirements is imperative.

New capabilities, expectations and objectives are raising the bar for MFA vendors. The requirements below do not represent an exhaustive list of key capabilities, but are a good starting point to decide which vendors get a seat at the table.

USER REQUIREMENTS

EVALUATION CRITERIA	IMPORTANCE
Does the vendor offer a desktop application and other fault escalation processes?	Offering multiple fault escalation processes facilitates authentication when a user cannot authenticate under their normal process.
Does the vendor support registration of multiple devices per user?	Supporting more than one authentication device allows users to authenticate even when they don't have their primary device.
Does the vendor offer self-service enrollment and registration mechanisms?	Self-service enrollment and registration mechanisms lighten the IT team's administrative load and accelerate user adoption.
Does the vendor support multiple language and locale settings?	Global enterprises wanting to protect applications and data for users on a global scale must support a localized user experience to enable MFA adoption.
Does the vendor support authentication methods such as OOB push, fingerprint and OTP soft tokens?	Supporting multiple authentication methods allows the enterprise to choose authentication methods to achieve the appropriate level of security, and supports the disuse of methods recently deprecated by NIST such as out of band PSTN (SMS or voice) authentication.
Does the vendor support Android, iOS and Windows Phone?	Supporting multiple mobile platforms aligns with BYOD initiatives gaining traction in the enterprise.

IT REQUIREMENTS

EVALUATION CRITERIA	IMPORTANCE
Does the vendor support use cases such as Windows RDP, Linux/Unix SSH integration?	Providing MFA for remote and privileged users promotes protecting the enterprise's most critical assets whoever and wherever the user is.
Does the vendor allow for web-based administrative access and role-based entitlements?	Varied levels of trust support varied levels of access and permissions. Support for role-based entitlements and web-based access for subsets of users is important to scale access based on administrative permissions.
Does the vendor support administrative bypass codes?	In the rare case where a user can't authenticate through a variety of fault escalation processes, administrative intervention is key.
Does the vendor support contextual factors such as geolocation and IP address?	Utilizing passive user information—like geolocation, IP address, time of day and device identifiers—provides better security and a better user experience.
Does the vendor support cryptographically strong session maintenance?	Secure communication between the mobile application, MFA service and third party applications is vital to protecting your applications and sensitive data.
Does the vendor support endpoint visibility and basic remediation capabilities?	Endpoint visibility and remediation are generally served by enterprise mobility management and anti-virus vendors. However, basic capabilities within an MFA solution provide an extra layer of protection against vulnerable managed and unmanaged devices.

ENTERPRISE REQUIREMENTS

EVALUATION CRITERIA	IMPORTANCE
Does the vendor support co-branding of the application?	Co-branding provides a consistent and familiar user experience, as well as another level of assurance for the user that they're authenticating within the corporate environment.
Does the vendor's technology platform and pricing support a simple upgrade path to support additional use cases?	Enterprises protecting access to applications and sensitive data are more frequently doing so on behalf of their partners and customers.
Does the vendor have other capabilities across the identity and access management (IAM) spectrum?	Full-service IAM solution providers with a singular focus on the IAM space tend to provide more up-to-date features, better knowledge and stronger support.
Is the vendor considered a thought leader whose solution is built on open standards like OAuth2.0 and OpenID Connect?	Thought leaders generally provide today's leading-edge solutions and drive technology advancements to meet tomorrow's challenges.
Does the vendor and its solution receive high rankings with analysts such as Gartner, IDC, Forrester and KuppingerCole?	Analysts can provide reliable third-party insight into how solutions stack up.

CUSTOMER MFA REQUIREMENTS

EVALUATION CRITERIA	IMPORTANCE
Does the vendor have a mobile SDK to embed out-of-band MFA into your own mobile app?	Customer MFA should be fully customizable. Adding an SDK to your own mobile application can help achieve this. Additionally, customers are not usually willing to download a third party MFA app for added security and using SMS as a second factor isn't as secure as previously thought. .
Does the vendor allow customers to have self-managed networks of trusted devices?	Customers may have several devices they trust that include a primary device, secondary additional trusted devices or devices with reduced permissions. Customers should have the ability to self-manage these devices from web or mobile applications.
Does the vendor support MFA for transaction approvals?	Requiring MFA specifically for high-value transactions can help balance security and convenience for customers. Information about the transaction that is being approved should also be able to be passed along in the MFA notification to customers.
Does the vendor support strong mobile app authentication?	Mobile app authentication should be strengthened by confirming that the user has marked the device as a trusted. This will prevent hackers from using stolen credentials in a mobile app installed on a device that isn't trusted by the customer.

**use this section if you are deploying MFA for your customers*

VENDOR EVALUATION & SELECTION

After you've defined all of your requirements, you'll want to organize them in a way that makes it easy to evaluate how each vendor stacks up. A Sheets or Excel spreadsheet works well. Create rows for each of your final criteria, organized by core stakeholder requirements as we've done above.

Next, add columns for each vendor you want to evaluate. Rate each vendor on how well they meet your criteria using a point-based rating system like this:

0 = Does not meet requirement
1 = Very limited support for requirement
2 = Partially meets requirement
3 = Meets or exceeds requirement

Using this system, you rate each vendor from 0-3 on each of the criteria. Then tally each vendor's totals. The vendor with the highest total score is also the vendor that best meets your requirements.

Want additional guidance on making the right MFA decision for your enterprise?
Read our MFA best practices white paper.

#3140 | 6.2017 | v011