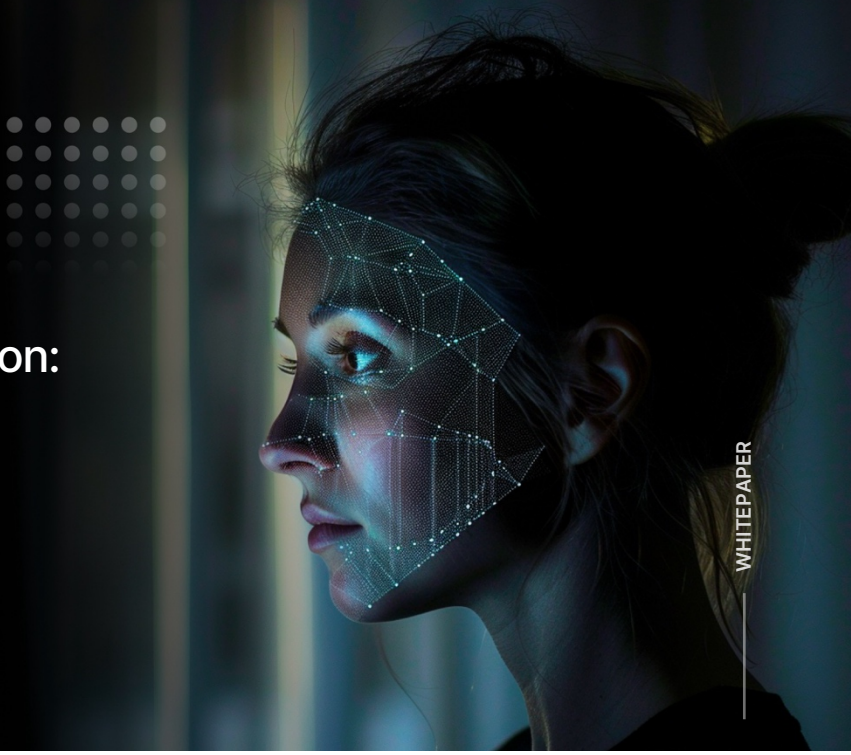
accops

The Future of Authentication: Simplifying Security with Contextual MFA & SSO



WHITEPAPER

INTRODUCTION

Authentication has an equal bearing on cyber security as well as user experience. In the modern digital organization, one cannot take precedence over the other. Here's how to navigate the fine line.

Rapid digitization of business systems and hybrid work models have made security a prime component of the organization's digital strategy. Modern business technology systems are complex, distributed, and connected – making them easy to infiltrate.

> The Identity and Access Management (IAM) market is expected to grow from **USD 15.7 billion in 2023** to **USD 32.6 billion by 2028**, achieving a Compound Annual Growth Rate (CAGR) of 15.6% during this period.[4]
>
> The Asia-Pacific region, including **India and ASEAN**, is anticipated to be the fastest-growing for IAM solutions due to rapid economic development, digitalization, and a heightened focus on cybersecurity.[5]

Authentication is also closely tied to the user experience. Strong authentication usually compromises the user experience (UX). This, in turn, undermines productivity as well as the efficacy of the authentication techniques.

However, this doesn't have to be. Organizations can now adopt user-centric authentication design strategies to effectively secure digital systems. In this white paper, take a look at some of the key risk factors and UX implications of authentication design, and how user-centric authentication techniques can mitigate security risks as well as UX tradeoffs.

Rising risk factors call for stronger security measures

The modern digital organization is characterized by a growing number of digital tools. On average, organizations use up to 90 different tools to get work done.[1] This distributes sensitive data across multiple systems and expands the attack surface of the organization.
Therefore, password-based authentication requires employees to remember many passwords. But most either set weak passwords and/or the same password across multiple tools – thus compromising the security of the entire organization.

In addition, here are some other risk factors that warrant stronger authentication measures today:

- **Human element**: When teams start growing large in mid-sized and scaling organizations, social engineering attacks become easier to orchestrate. Some users still have the habit of trusting requests as in smaller teams, which makes the success of phishing attacks or scams more likely.
- **Web browser access**: Many SaaS and PaaS apps are accessed through web browsers, which makes them prime targets for attacks based on malicious scripts and SQL injection.
- **Credential policies**: In many organizations, the lack of enforcement of credential policies leads to the use of weak passwords, or reuse across multiple systems. Moreover, some users revert to old passwords during resets, which increases the risk of unauthorized access.

Finally, attackers also make use of software supply chain attacks and sticky keys to infiltrate systems and escalate their access privileges. All of these risk factors have made stronger authentication measures like 2-Factor Authentication (2FA) and Multi-Factor Authentication (MFA) an essential aspect of access security and control.

Authentication and User Experience: an inevitable tradeoff?

In response to rising diversity and frequency of threats,[3] businesses have deployed numerous security solutions to mitigate the ensuing risks. However, these deployments have also resulted in a negative impact on the user experience. Take a quick look at the underlying reasons.

Legacy authentication techniques meet new security strategies

Modern security frameworks are based on continuous verification, zero trust, and identity-based access. However, when legacy authentication techniques are applied within such frameworks, the end result can significantly degrade the user experience.

For instance, when users are prompted to repeatedly enter passwords and one-time codes in the middle of their work, it causes frustration and affects their productivity. Moreover, zero-trust doesn't mean treating employees like adversaries.

Downsides of poor authentication design

Authentication systems can therefore be secure, but still result in poor user experience. This leads to:

- **Lower productivity**: Setting authentication expiry too short causes users to key in their credentials repeatedly, which taxes their productivity and output at work.
- **Slower processes**: Slow response times can keep users stuck at the login screen for too long. At an organizational scale, this wasted time compounds and accrues as a loss of productive time.
- **Bypassing behaviors**: Frustrating authentication experiences can drive users to try some bypassing behaviors – like working on alternative solutions, or setting short, vulnerable passwords.
- **Platform fatigue**: In the absence of a unified authentication experience, users will experience increased platform fatigue as they adapt to varying login interfaces.
- **Forgotten passwords**: Another consequence of password-based authentication is that users frequently forget individual passwords for the tools they use through their workday.

- **Reset requests**: Lastly, frequent forgotten passwords increase the volume of reset requests that must be verified by the security teams, thus creating a ticket backlog.

With the rising importance of digital security, enterprises are beginning to neglect these impacts of authentication design. Chief Security Officers (CSOs) eventually come to accept them as an inevitable consequence of better security – a trade-off that must be made to mitigate risks. So, what are the root causes of this perspective?

> Credential theft has witnessed a meteoric rise in the past couple of years with the surge in remote work. Reports suggest **over 4/5th of data breaches** resulting from hacking involve the use, or misuse, of lost or stolen credentials.

Gaps in traditional authentication design

Today's enterprise technology landscape is significantly more complex than that of the work-from-office era, where systems were located within a well-defined network perimeter, and were used to access 2-3 applications hosted on the company server.

Today, cloud-based and on-prem systems work alongside each other, with some application components spanning both. Moreover, various services are consumed in different models, including SaaS, PaaS, and IaaS. To further complicate things, users access these systems from multiple locations and devices.

This renders traditional authentication design ineffective, manifesting in the following ways:

- **Use of multiple authentication solutions across tools**
  Different solutions are used to safeguard legacy apps, cloud apps, SaaS solutions, and Linux and Windows applications.
- **Weak enforcement of password policies**
  Password policies are communicated and circulated amongst employees, but IT administrators and security teams are unable to enforce them effectively.
- **Using legacy protocols precludes MFA**
  Legacy authentication protocols like IMAP, POP, and SMTP are unable to enforce MFA, which undermines system security.
- **Complex login processes**
  This issue primarily manifests when onboarding new users. Poorly mapped dependencies and provisioning processes make login processes complicated, resulting in poor user experience.
- **Taking trust for granted**
  This is the opposite of zero-trust. Some systems trust users based on unreliable markers such as IP addresses, which can be exploited by attackers to gain unauthorized access.
- **Poor device and platform support**
  Lastly, a lack of support for multiple devices and platforms can lead to the use of multiple authentication tools. Moreover, login interfaces may bleed from the screen, creating accessibility issues for users.

So, how can these challenges be mitigated?

Simplifying enterprise security with modern authentication experiences

The first step is to recognize that authentication design concerns security as much as it does user experience. This compels CSOs to devise and adopt user-centric authentication technologies. The second step is to unify authentication technologies, access control, and ID management under a single umbrella, ideally with a single solution to handle these functions.

That said, here are six levers for enhancing the authentication experience while maintaining water-tight security across your digital enterprise.

Levers for enhancing the authentication experience

#1. Contextual authentication
This is also known as adaptive authentication. It is an intelligent approach for verifying users based on the context of a transaction, as well as deviations from normal behavior. Such frameworks use parameters like time of access request, device identity, location of the user, and access environment – to trigger string authentication. The parameters are used to calculate the risk score associated with an access request, and strong authentication (like 2FA or MFA) is triggered when the score crosses the configured threshold.

This mitigates the need for verifying users when their behavior falls in line with an established historical pattern. As a result, contextual authentication maintains security without affecting user productivity.

#2. Single Sign-On
Single Sign-On (SSO) is a technique that eliminates the need for maintaining multiple passwords for different tools. SSO solutions typically integrate with a range of applications and environments – including Windows and Linux desktops, cloud apps, SaaS tools, and mailboxes.

As a result, SSO unifies the authentication experience from the user's perspective. The user is required to maintain a single set of credentials to log in to all the tools used by them. SSO is not exclusive to other authentication design frameworks like MFA or contextual authentication. Instead, it can work in tandem with these techniques to further simplify the authentication experience.

#3. Passwordless Authentication
Bio authentication techniques are typically applied in conjunction with password-based authentication solutions. They are usually a superior alternative to credential-based techniques as the user is verified using their biological attributes rather than something they remember – for instance, their face, their retina, or their fingerprints.

In this sense, bio authentication can add a layer of security to the authentication framework, and deliver passwordless login experiences to users. However, it may need specialized equipment to implement, especially if the user's device doesn't have built-in support for bio-authentication.

Other passwordless authentication techniques can prove useful where a user is not registered in a central directory, and needs to access a system only temporarily. For instance, QR code-based logins require a user to scan a QR code which changes every few seconds. Such capabilities can be especially useful when working with contractors and vendors.

#4. Continuous authentication
Continuous authentication is an extension of adaptive authentication. It augments zero-trust strategies by continuously vetting the user and their actions, ideally in a user-centric fashion. This means that various attributes associated with the user – like their behavioral footprints, device reputation, mouse movements, device location, and input patterns are monitored in real-time.

Based on this activity and how it compares to normal activity associated with the user, the authentication solution prompts a repeat authentication. This helps assess and manage both insider risks and external threats in real-time, without degrading the user experience.

#5. User-friendly 2FA solutions
Two-factor authentication is considered a foundational security technique these days, given the vulnerability of password-only verification systems. However, some 2FA implementations may reiterate the shortcomings of password-based techniques. This is especially the case with 2FA deployments that use security questions as the second factor.
However, more user-centric and secure 2FA techniques can now be deployed. These include one-time passcodes delivered via email, SMS or push notifications, or mobile apps, and hardware tokens (physical keys) that are plugged into the user's system.

#6. Robust ID management
This is one of the most important elements for implementing a user-friendly and secure authentication experience. A centralized ID management system stores all the data associated with an organization's users within a centralized repository – including their past activity across business systems.

This ID management system is integrated with various authentication techniques to verify if the user is actually who they claim to be. ID management also drives access control, which makes it the foundation of access security. Authentication solutions should either offer robust ID management capabilities or integrate seamlessly with the organization's ID management solution (typically Azure Active Directory).

How to pick an authentication solution for your enterprise?

A modern authentication solution is the cornerstone of a secure and user-friendly authentication design. While it should bring the above capabilities for activating user-friendly authentication, it should also have the following attributes:

- **Integrates with a wide variety of applications**
  Ideally, your authentication solution should integrate with SAML applications, provide REST API support for cloud apps, and support Microsoft Desktop and Server and Linux Login.

- **Offers a range of multi-factor authentication options**
  2FA and MFA should not be limited to SMS or email OTPs. Your authentication solution should support a range of options that meet your compliance requirements and offer a flexible experience to your users.

- **Offers high-availability for fast authentication**
  Because authentication solutions safeguard access to enterprise systems, they must be based on high-availability infrastructure, and have solid failover pathways. Otherwise, they can lock users out for extended periods and expose the enterprise to significant risks.

- **Protects network logins and traces actions of privileged users**
  Lastly, an authentication solution should integrate with managed network devices as network virtualization becomes a commonplace feature of enterprise networks. Look for 2FA support via TACACS and RADIUS protocols.

- **Provides a range of robust, passwordless login capabilities**
  While bio-authentication is an important passwordless authentication technique in modern authentication solutions, other capabilities can be useful in some scenarios. For instance 3rd party users who need to access a system only temporarily can be authenticated with QR codes that change every few seconds.

Next steps

Authentication is one of the most important aspects of enterprise security today. However, authentication design can significantly impact the user experience, thus tying it to other organizational attributes like productivity and process velocity.

This makes it crucial to adopt user-centric authentication techniques that apply smart approaches to secure systems, without getting in the way of day-to-day work. This is the key to building a secure and intuitive digital workspace that is loved by users and cannot be compromised by attackers.

Simplify authentication without compromising security with Accops HyID

Accops HyID is a comprehensive authentication solution that offers modern authentication capabilities like MFA, bio authentication, QR code-based passwordless login, and contextual authentication. It enables organizations to enforce security policies in a centralized manner and integrates exhaustively with all enterprise applications and environments. This makes Accops HyID the only authentication solution that enterprises need in their security stack. With the ability to track and audit the actions of privileged users, Accops HyID activates a closed-loop authentication framework to safeguard enterprise systems.

[1] https://www.ibm.com/reports/data-breach
[2] https://www.inc.com/dana-severson/24-must-have-tools-for-running-a-growing-company-today.html#:~:text=The%20reality%20is%2C%20it%20takes,different%20tools%20according%20to%20Siftery).
[3] https://hbr.org/2023/04/cyber-risk-is-growing-heres-how-companies-can-keep-up
[4] https://www.marketsandmarkets.com/Market-Reports/identity-access-management-iam-market-1168.html
[5] https://www.expertmarketresearch.com/reports/identity-and-access-management-market

Accops enables secure and instant remote access to business applications from any device and network, ensuring compliant enterprise mobility for business users while keeping governance with the organization.

For further details, feel free to reach out to our dedicated team at contact@accops.com.