onelogin
by ONE IDENTITY

Elevating Organizational Security with Advanced Authentication

The shift towards a digital-first approach has exposed organizations to a wide range of cybersecurity risks. Employees, customers and partners access organizational resources from various locations and devices, making it challenging to establish trusted access points. Similarly, organizations struggle with password-related issues, including weak or reused passwords. These issues are compounded when employees use the same passwords across business and personal accounts, as a single breach can have far-reaching consequences.

As evidenced by the 2023 Verizon Data Breach Investigations Report (DBIR), the traditional username-password approach to access management has proven inadequate against the alarming rise in credential theft attacks. According to the report, credential theft remains the most prevalent form of hacking and accounts for 49% of all reported breaches. In the case of web application attacks, 86% are due to stolen credentials, underscoring the urgent need for enhanced security measures to protect critical resources and safeguard sensitive data.

Navigating Access Management Challenges

In today's modern IT world, organizations must strike a delicate balance between enabling convenient access and ensuring robust security measures are in place. In this process, they may face several challenges:

Access Management Challenges

- **Managing a diverse and distributed workforce**
- **Balancing security and user experience**
- **Combatting credential-based attacks**
- **Ensuring compliance and regulatory requirements**
- **Adapting to dynamic IT environments**
- **User Lifecycle Management**

- **Managing a diverse and distributed workforce:** The modern workforce is often scattered across different geographic locations, creating complexities in managing identities and access privileges. The need to provide appropriate access to the right resources for different user roles while ensuring strict security measures can become a challenging task that is prone to human error.
- **Balancing security and user experience:** Achieving the appropriate balance between security and user experience remains a constant challenge for access management implementations. Overly stringent security measures can lead to cumbersome authentication processes, causing user frustration and potentially leading to workarounds that

compromise security. Conversely, lax security measures may expose organizations to significant risks. An effective access management solution must prioritize both security and user convenience to foster widespread adoption.

- **Combatting credential-based attacks:** Credential-based attacks, such as phishing and brute force attacks, continue to be a persistent threat. Cybercriminals capitalize on the human element in cybersecurity, tricking users into revealing their credentials or exploiting weak passwords. Organizations must implement robust authentication methods to prevent unauthorized access and data breaches caused by these common attack vectors.
- **Ensuring compliance and regulatory requirements:** Organizations face stringent compliance requirements related to data protection, user privacy and identity verification. Meeting these compliance standards while managing access to sensitive data across multiple systems and applications can be difficult. A robust access management solution must also offer the necessary controls and audit capabilities to demonstrate compliance and pass regulatory audits.
- **Adapting to dynamic IT environments:** As organizations embrace digital transformation, their IT environments become increasingly dynamic. Frequent changes in user roles, permissions and access requirements necessitate a solution capable of rapid adaptability without compromising security. Integrating access management seamlessly with new technologies, cloud services and emerging applications requires careful planning and coordination.
- **User Lifecycle Management:** Managing user identities throughout their lifecycle, including onboarding, role changes and offboarding, demands a well-orchestrated access management solution. Ensuring current employees have access to resources and revoking access promptly upon termination requires streamlined processes and automation to avoid security gaps and potential data exposure.

To address these challenges, it is essential for organizations to adopt a comprehensive and secure access management solution.

Advanced Authentication offers a holistic solution that combines strong authentication and adaptive authentication techniques, effectively mitigating these challenges **while providing a seamless user experience**.

onelogin by ONE IDENTITY

The Key to Secure Access: Advanced Authentication

Advanced Authentication is a modern and more secure cybersecurity approach to access management that goes beyond the traditional username-password model. It combines the use of strong authentication factors as part of Multi-Factor Authentication (MFA) flows and the adoption of adaptive authentication methods to enhance security and access controls.

Multi-Factor Authentication (MFA) factors can include something the user knows (a password or PIN), something the user has (a smartphone, token or smart card) and something the user is (biometric data such as a fingerprint or facial recognition). By combining two or more of these authentication factors, MFA adds an extra layer of security to prevent unauthorized access even in the case of a compromised factor. This approach significantly reduces the risk of data breaches and unauthorized access attempts.

It is important to keep in mind that the security level an MFA solution provides will depend on the strength of the factors used, as well as how these are implemented and managed. Strong authentication factors are those that are hard to replicate such as physical security keys stored on a physical device, biometrics, passkeys and one-time passcodes generated by authenticator applications.

In addition to MFA, Advanced Authentication incorporates adaptive authentication, which continuously assesses various risk factors associated with access attempts. These risk factors may include the user's location, device, IP address, behavior patterns and other contextual information. Based on the risk level detected, adaptive authentication dynamically adjusts the level of authentication required.

For instance, if a user attempts to log in from a recognized device and location, with no suspicious behavior detected, the system may allow access with minimal friction. On the other hand, if the access attempt is from an unfamiliar device or location or shows signs of unusual behavior, the system may prompt the user for additional verification steps to ensure the legitimacy of the access request.

The Advanced Authentication implementation can vary among organizations. Some organizations may choose to combine MFA with behavioral analytics to achieve Advanced Authentication. Alternatively, other organizations may use adaptive authentication methods to determine the necessary security measures and combine them with passwordless authentication, which can significantly enhance security and make it more difficult for hackers to gain unauthorized access. An increasing number of organizations are adopting a combination of these approaches to ensure the highest level of security.

An organization's particular implementation strategy will depend on a range of factors, including their regulatory requirements, the need for strong security practices, and the tools and technologies available.

The Power of Advanced Authentication

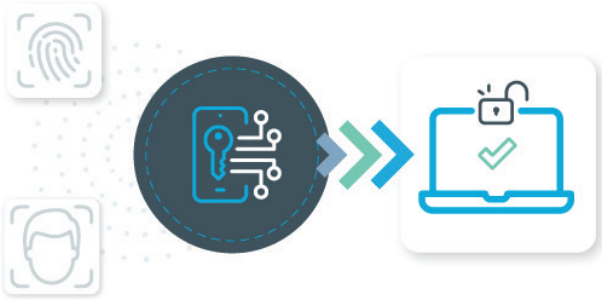
Embracing Advanced Authentication results in several benefits for organizations seeking to fortify their cybersecurity defenses. From heightened protection against unauthorized access to frictionless user experiences, here are the top five advantages of implementing Advanced Authentication:

Advanced Authentication Benefits

- **Enhanced security**
- **Protection against credential thefts**
- **Adaptive security**
- **Improved user experience**
- **Regulatory compliance**

1. **Enhanced security:** The foremost benefit of Advanced Authentication is its ability to significantly enhance security by adding multiple layers of protection. Users must provide two or more authentication factors before gaining access. This multi-layered approach mitigates the risk of unauthorized access and reduces the chances of successful credential-based attacks, such as phishing or brute force attacks.
2. **Protection against credential thefts:** An MFA implementation using strong authentication factors acts as a tough defense against credential theft. Even if one authentication factor is compromised, attackers would still need to overcome additional barriers to gain unauthorized access. This added layer of protection helps safeguard sensitive data and critical resources, minimizing the potential impact of stolen credentials.
3. **Adaptive security:** The inclusion of adaptive authentication in Advanced Authentication allows for a dynamic and context-aware security approach. By continuously analyzing risk factors like user behavior, device information and location, adaptive authentication can adjust the authentication requirements based on the risk level of each access attempt. This intelligent approach ensures that users face appropriate security measures, reducing unnecessary friction in low-risk scenarios while applying stronger authentication in high-risk situations.
4. **Improved user experience:** Contrary to the perception that enhanced security might hinder user experience, Advanced Authentication is designed to provide a seamless and user-friendly process. With adaptive authentication tailoring security measures based on context, users experience fewer authentication challenges in familiar and low-risk scenarios, leading to increased user satisfaction and productivity.
5. **Regulatory compliance:** For organizations dealing with stringent compliance requirements and data protection regulations, Advanced Authentication can be a game-changer. By bolstering security and providing detailed audit logs, the solution helps businesses meet compliance requirements more effectively. Advanced Authentication's capabilities align with various industry regulations, such as GDPR, HIPAA and PCI DSS, reducing the risk of non-compliance fines and penalties.

By providing these benefits, Advanced Authentication emerges as an essential cybersecurity approach in safeguarding sensitive data and identities in today's increasingly digital and interconnected world.



OneLogin's Advanced Authentication Solutions

With a focus on security, user convenience and adaptability, OneLogin provides a robust Advanced Authentication solution to protect organizations against modern cyber threats while delivering a seamless user experience.

OneLogin Single Sign-On (SSO)

OneLogin SSO seamlessly integrates with thousands of applications and cloud services, making it easy for organizations to centralize access controls. It enables users to log in once and gain secure access to multiple applications and systems, reducing the burden of password management. Additionally, OneLogin SSO provides MFA as an additional layer of security. Administrators can enforce MFA policies based on user roles or specific applications, requiring users to present a second authentication factor during login attempts. This combination of SSO and MFA strengthens an organization's security, safeguarding critical resources.

OneLogin MFA

OneLogin MFA supports a wide range of authentication methods, including passwordless, passkeys, one-time passcodes, push notifications, biometric data, security keys and many more. Organizations can choose the most suitable authentication factors for their users based on their needs.

OneLogin MFA provides administrators with the flexibility to enforce MFA on a per-application basis or for specific user groups, tailoring security requirements to align with the organization's risk tolerance. With real-time reporting and monitoring capabilities, administrators gain insights into authentication events, helping them detect and respond to potential security incidents proactively. OneLogin's MFA solution empowers organizations to enhance security without compromising user productivity, making it a vital component of the Advanced Authentication suite.

OneLogin SmartFactor Authentication

OneLogin SmartFactor Authentication offers a context-aware approach to access control. By continuously analyzing risk factors such as user behavior, device information, and geolocation, SmartFactor Authentication dynamically adapts the level of authentication required for each access attempt. In low-risk scenarios, users experience a frictionless authentication process, streamlining access to resources and boosting productivity. In contrast, higher-risk situations prompt users to provide additional verification steps, ensuring that security is appropriately strengthened.

OneLogin Desktop

OneLogin Desktop is a secure and user-friendly solution that simplifies device-level authentication for organizations. By integrating with existing operating systems, OneLogin Desktop allows users to access their devices using a single set of credentials, reducing the burden of managing multiple passwords. As an extension of OneLogin's MFA capabilities, OneLogin Desktop adds an extra layer of security to device logins, protecting against unauthorized access attempts while also reducing the need for users to continually enter passwords within their browser-based applications.

The solution seamlessly integrates with macOS and Windows operating systems, enabling a secure and efficient device-level authentication process for organizations of all sizes.

OneLogin's Advanced Authentication solutions address today's modern access management challenges, serving the needs of organizations seeking to protect sensitive data, mitigate cyber risks, streamline access management and deliver a seamless user experience.

To learn more about OneLogin Advanced Authentication and how it can benefit your organization, visit www.oneidentity.com/solutions/advanced-authentication.

About One Identity

One Identity delivers unified identity security solutions that help customers strengthen their overall cybersecurity posture and protect the people, applications and data essential to business. Our Unified Identity Security Platform brings together best-in-class Identity Governance and Administration (IGA), Access Management (AM), Privileged Access Management (PAM) and Active Directory Management (AD Mgmt) capabilities to enable organizations to shift from a fragmented to a holistic approach to identity security. One Identity is trusted and proven on a global scale – managing more than 500 million identities for more than 11,000 organizations worldwide. For more information, visit www.oneidentity.com.

onelogin by ONE IDENTITY