SECUREAUTH
Welcome to Better Identity.

eBook

The Case for Passwordless Authentication in a Zero Trust World

Get Started

Table of Contents

Introduction

As a business leader, you're driving digital transformation to stay competitive, meet customer expectations, and deliver business outcomes. However, this shift also demands a new approach to security.

With the evolution of digital business, many companies are moving from securing broad network perimeters to focusing on individual users and small groups. That's where[2] a Zero Trust model comes into play. It ensures every access attempt is verified, and no one is trusted by default. Your organization can enhance its defenses by adopting a robust Access Management solution that includes Multifactor Authentication (MFA) and risk analysis through Adaptive Authentication.[1]

Outdated Security Models Are Failing: Why Zero Trust is a Compelling Option

The traditional security models you've used in the past no longer meet today's dynamic access requirements. The rise of cloud services, SaaS offerings, and remote work has created new challenges. As of 2023, 80% of security breaches involve stolen credentials (Verizon Data Breach Investigations Report). A Zero Trust model addresses this by denying access by default and requiring every connection to be authenticated.

With 91% growth in remote workers over the past decade, securing remote access to critical resources while maintaining a seamless user experience is essential. Moving toward a Zero Trust model ensures your workforce, including remote workers, can securely access applications, portals, and services.

The Perimeterless Enterprise

A Zero Trust approach places your users at the center of your security strategy. By setting policies and rules based on user identities, device recognition, and other factors, you can ensure appropriate access is granted only to trusted users. Implementing a Single Sign-On (SSO) solution with MFA and Adaptive Authentication enhances security without creating friction for users.

The Value of Zero Trust

Zero Trust has become a top priority for organizations like yours. 63% of data breaches in 2023 were due to weak or stolen passwords (Verizon DBIR). A Zero Trust model mitigates these risks by ensuring only verified users and devices gain access. Your security team can implement stronger measures, such as risk-based authentication, to stop attackers before they compromise your data.

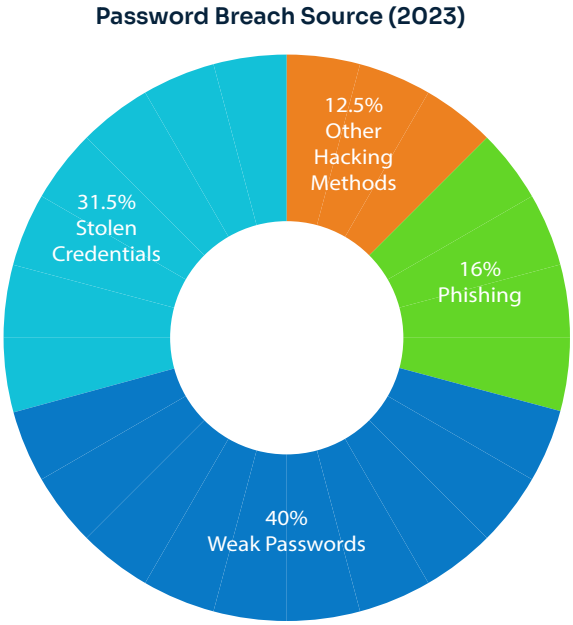

Figure 1: Based on Verizon Data Breach Investigations Report (2023) LastPass Psychology of Passwords Report (2023)

Stop Trusting Passwords: The Case for Going Passwordless Now

You know passwords are a weak point. **More than 60% of users** reuse the same password across multiple accounts (LastPass Psychology of Passwords Report, 2023). This puts your organization at risk of credential-stuffing attacks, where attackers use stolen credentials to access accounts. In 2023, **over 15 billion compromised credentials** were available on the dark web (Digital Shadows).

Passwords alone are not enough to protect your systems, applications, and data. Adopting passwordless authentication reduces this risk, while also improving user experience.

The Need for Strong Access Management

Cybercriminals aren't going away. They continue to evolve their tactics, and every organization—yours included—is a target. The cost of a data breach in 2023 reached an average of $4.45 million (IBM Security Cost of a Data Breach Report, 2023). Implementing strong access management, such as MFA and Adaptive Authentication, reduces your attack surface and helps you stay ahead of these threats.

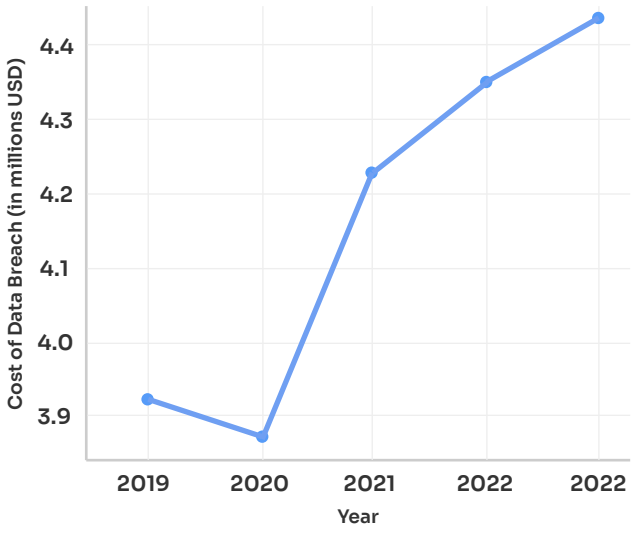

Figure 2: Average Cost of a Breach based on IBM Security Cost of a Data Breach Report (2019-2023)

Zero Trust Playbook: How to Secure Access with Adaptive Authentication

01 Do I Know the User?

Verifying the identity of every user who accesses your systems is critical. With 51% of passwords used in attacks being over a decade old (SpyCloud, 2023), relying on usernames and passwords alone is no longer sufficient. Dynamic Adaptive Authentication and MFA help you implement Zero Trust security while providing a frictionless experience for your users.

02 Have I Seen This Device Before?

Recognizing the devices your users utilize adds another layer of security. By maintaining a device inventory, you prevent attackers from using stolen credentials to gain access. Self-service device enrollment reduces the burden on your IT team and enhances the user experience.

03 Does the Device Meet My Standards?

Pre-approved, secure devices ensure your users meet your security requirements. By performing background checks on operating systems and security standards, you ensure only authorized devices connect to your network.

04 What is My Risk Tolerance?

Adaptive authentication allows you to adjust security policies based on user identity, device recognition, and contextual data, such as geo-location or IP address. With over 60% of attacks now involving credential compromise (Verizon DBIR, 2023), risk-based authentication ensures you respond dynamically to potential threats without inconveniencing users.

05 Should I Grant or Deny Access?

Every access request should be evaluated consistently. Your access management workflows must balance security with user experience. Implementing strong MFA and Adaptive Authentication policies ensures passwordless access with minimal friction, so your organization can remain secure while providing a seamless user experience.

The SecureAuth Approach

As you implement Zero Trust, the balance between strong security and a good user experience will determine the success of your access management strategy. You can't afford to disrupt your users. Adopting passwordless authentication helps you protect your resources without compromising productivity or customer satisfaction.

Since its inception, SecureAuth has delivered the access management capabilities you need to securely authenticate users while providing a frictionless experience. With over 34 patented innovations, SecureAuth offers the flexibility to deploy a SaaS, hybrid, or on-premises solution tailored to your business requirements.

Risk-Based Adaptive Authentication

- Device Recognition Check
- Location Check
- Improbable Travel Check
- Directory Check
- IP White/Black List Check
- Anonymous Proxy Check
- Malicious IP Check
- Network Carrier Check
- Phone Type Check
- Phone Porting Status Check
- User Behaviour Check
- Any 3rd Party Risk Score

About SecureAuth

With leading Identity and Access Management solutions from SecureAuth, organizations worldwide find it easier than ever to create digital experiences that are as welcoming as they are secure. Our AI-driven Risk Engine helps deliver dynamic – and often invisible – authentication and authorization for users, combined with a data privacy framework that protects their information and ensures their consent.

It all adds up to a virtual handshake at the digital door to your company. Making you more effective than ever at eliminating bad actors or incorrect authorizations. Keeping your employees engaged and productive. And delighting your customers so you can fuel your digital growth. Welcome to Better Identity.

Learn more at SecureAuth.com

Sources

Verizon Data Breach Investigations Report (2023)
https://www.verizon.com/business/resources/reports/dbir/

LastPass Psychology of Passwords Report (2023)
https://www.lastpass.com/resources/research/psychology-of-passwords

IBM Security Cost of a Data Breach Report (2023)
https://www.ibm.com/security/data-breach

Digital Shadows Report (2023)
https://www.digitalshadows.com/resources/reports/

SpyCloud Credential Exposure Report (2023)
https://spycloud.com/resources/reports/

NordPass Top 200 Worst Passwords Report (2023)
https://nordpass.com/most-common-passwords-list/

F5 Labs Credential Stuffing Attack Report (2023)
https://www.f5.com/labs/articles