PASSWORDLESS ACCESS & ADAPTIVE AUTHENTICATION

Enabling a Zero Trust Model

Incorporate Access Management to support Zero Trust in your Enterprise.

SECUREAUTH
Home
USER MANAGEMENT
User Data Stores
APPLICATIONS
Application Manager
Admin
Hello!
Welcome to SecureAuth IdP 9.3
Now it's easier than ever to determine identities with confidence, and provide frictionless access for your users.

SECUREAUTH

CONTENTS

INTRODUCTION

Business and IT leaders are continuously focused on driving digital transformation to accelerate strategic initiatives in order to maintain competitive advantage, meet customer expectations, and ultimately deliver business outcomes. However; one area impacted by digital transformation is how enterprises approach Security.

Protecting valuable resources and data across the enterprise is a top priority. And many organizations are evolving their defenses and moving from securing wide network perimeters to focusing on securing groups and individual users.

A Zero Trust model is a strategy rapidly being reviewed and adopted by enterprises to secure and protect the business as the technology landscape continues to shift and user expectations evolve.

Read on to see how a robust Access Management solution including Multi-factor Authentication (MFA) with risk analysis via Adaptive Authentication integrates seamlessly with a Zero Trust model to secure the enterprise.

A NEW APPROACH TO SECURITY

The Evolution of Digital Business

Traditional security architectures were designed for an era that is rapidly evolving and no longer provides the dynamic secure access requirements for today's digital business. The introduction of cloud-based services and SaaS offerings has changed the complexion of an organization's corporate data center. And due to this evolution, a new approach to security is required as traditional data centers are no longer the center of access requirements for users and devices.

A Zero Trust model, as the name implies, is a security model rooted in denying access by default.

The growth in remote workers over the past decade is a good use case for a Zero Trust model. Over the past 10 years the number of remote workers has grown 91%. These associates are 65% more productive and 57% report higher job satisfaction[4]. As the growth trend continues, this segment of the workforce requires attention and addressing from a security perspective. Organizations must ensure a secure model is in place enabling the entire workforce, including remote workers, to securely access valuable resources to protect the business while providing a positive user experience.

Characteristics of a Digital Enterprise:

- More user work performed off of the enterprise network than on the enterprise network
- More workloads running in IaaS than running in the enterprise data center
- More applications consumed via SaaS than consumed from enterprise infrastructure
- More sensitive data located outside of the enterprise data center in cloud services than inside
- More user traffic destined for public cloud services than to the enterprise data center
- More traffic from branch offices heading to public clouds than to the enterprise data center

The Perimeterless Enterprise

A Zero Trust approach places users at the center of the security strategy and enables access to resources based on policies and rules to ensure the appropriate permissions are granted at the right time for each unique user to access applications, portals, and services.

A comprehensive Access Management solution is critical to the success of a Zero Trust model. The solution must be capable of supporting modern cloud-based workloads, legacy on-premises applications, and multiple user types (employees, contractors, partners, & customers). And the solution must deliver an exceptional user experience coupled with strong authentication capabilities to support an organization's security requirements.

A straight-forward example is a Single Sign-on (SSO) solution. With SSO, a user signs in and authenticates themselves one-time and the SSO solution logs the user into resources needed on their behalf eliminating the need to memorize multiple username/password combinations. SSO is quick and convenient for users but does present some security risk. Adding additional security measures such as Multi-Factor Authentication and Adaptive Authentication capabilities improves availability and security with minimal friction.

THE VALUE OF ZERO TRUST

Why organizations are making the move

Zero Trust is gaining substantial traction with organizations. The recent 2019 Zero Trust Adoption Report(5) notes 78% of IT security teams are looking to embrace zero trust, 19% are actively implementing zero trust, and 15% already have zero trust in place. At the same time, nearly half of enterprise IT security teams (47%) lack confidence in their ability to provide zero trust with their current security technology. And the report identifies the highest security priority for application access is privileged account management of users and multi-factor authentication capabilities (68%).

- Zero Trust Architecture is an end-to-end approach to network/data security encompassing **identity, credentials, access management,** operations, **endpoints**, hosting environments, and the interconnecting infrastructure.
- It is a set of network **security** paradigms that move network defenses from wide network perimeters to focusing on **individuals** or small groups of resources with no implicit trust granted.
- **Access** to data resources is granted when a resource is required, and authentication of both the user and the device is performed **before** the connection is established.
- The approach is a response to enterprise network trends including **remote users** and **cloud-based** assets that are not located within an enterprise-owned network boundary.
- Zero Trust focuses on **protecting resources**, not network segments, based on policies as the network location is no longer the prime component to the security posture of the resource.
- Zero Trust is an architectural approach that is focused on **data protection.**

PASSWORDS CREATE RISK

Identity Theft Resource Center (ITRC) for the past 15 years has been releasing their annual breach report at the beginning of each year. And the data in the most recent report from the past year is telling and the statistics eye-opening.

It is clear from the report...

Passwords are not enough!

Compromised email addresses and stolen passwords are used by bad actors to execute credential stuffing attacks in which criminals use automated systems in attempt to access user accounts. And because a vast majority of people – up to 83% - use the same password for more than one account, the risk is high for organizations to experience and be exposed to such an attack.

For organizations to truly protect systems, applications, and data – all access requests to corporate resources must be required to provide more than simply a user-name and password.

80% of hacking related breaches in 2019 leveraged either stolen and/or weak passwords [(1)].

It takes one breach for an organization to realize relying on traditional username + password is not protecting the business.

29% of 2019 breaches, regardless of attack type, involved the use of stolen credentials [(1)].

A popular attack involves stolen credentials to access email accounts and web servers with the aim to compromise systems or steal data.

52% of breaches in 2019 featured a form of hacking [(1)].

No business is safe from the seemingly random acts of bad actors because any compromised data inevitably makes its way to the dark web.

32% of breaches in 2019 involved the use of phishing attacks [(1)].

Once a bad actor has possession of an email address, the ability to orchestrate phishing and other social attacks creates risk for any organization.

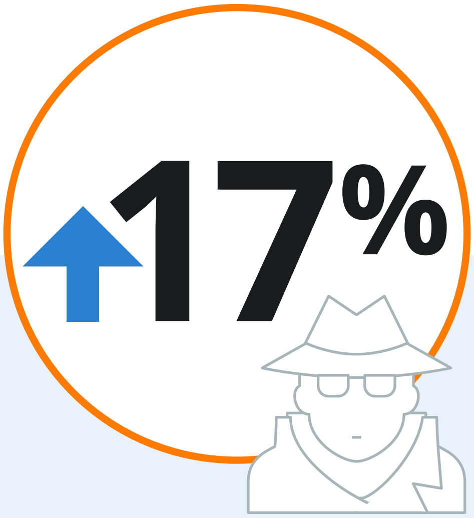
A NEED FOR STRONG ACCESS MANAGEMENT

A key tenet of a zero trust model

Data breaches continue to make the headlines year after year and every organization faces risk regardless of size or industry. Cyber criminals are not going away and continue to target companies of all sizes looking to steal valuable data.

The total number of breaches reported in 2019 was up approximately 17% to 1,473[4]. And C-level executives were 12x more likely to be the target of social incidents and 9x more likely to be the target of social breaches than in years past[1]. A key recommendation based on the Verizon 2019 breach report is - Two Factor Authenticate (2FA) everything[1].

The password no longer provides the level of protection businesses require. Security must incorporate the tools of identity to reduce the threat surface and enable the business. By moving to a modern Identity and Access Management solution businesses can improve security and enable features such as Passwordless authentication to improve the user experience.

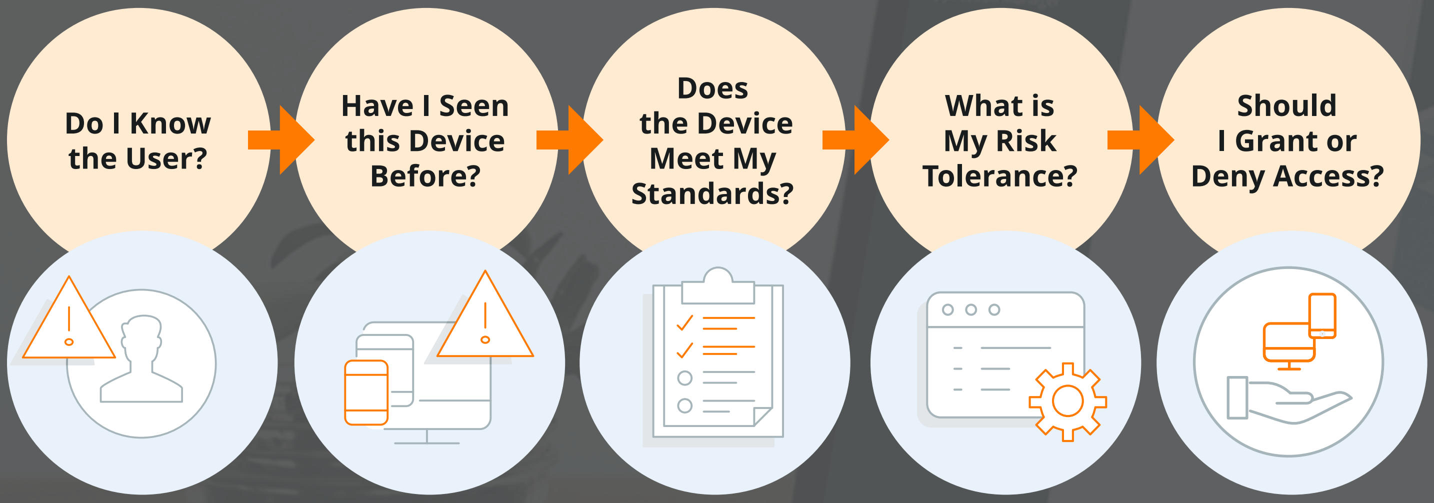


There was a 17% increase in the number of reported breaches in 2019 versus 2018 [4].

The number of non-sensitive records exposed in the Banking/Credit/Financial sector increased 5-fold to 100,621,770 from 20,000 and the Business sector exposed 99.99% of the non-sensitive records (+705.1 million) in 2019.

SECURE ACCESS IN A ZERO TRUST MODEL

The Logical Steps to Secure Authentication



Do I Know the User?

Have I Seen this Device Before?

Does the Device Meet My Standards?

What is My Risk Tolerance?

Should I Grant or Deny Access?

Do I Know the User?

Understanding the identity of the user attempting to access your systems, data, and applications is critical.

Usernames and passwords are no longer enough to adequately secure valuable corporate resources. 33+ million records were exposed in the top 5 unsecured database breaches of 2019 with 4 of the 5 breaches exposing username/email and password data [4].

Moving beyond Single Sign-On (SSO) and implementing dynamic adaptive authentication and multi-factor authentication (MFA) capabilities will put you on a path to a Zero Trust security model.

Is your organization only using the simple combination of username and password the only security in place to protect access to your valuable resources?

Have I seen this Device Before?

Recognizing a device being utilized by your users to request access to resources is imperative to assessing risk.

A strong Access Management solution enables an organization to inventory devices and associate the device(s) with a user's profile. Maintaining records of the devices each user possesses to request access helps keep bad actors from compromising security by using stolen credentials.

Providing users a self-service capability to easily enroll the devices they wish to use to request access enhances the user experience and reduces the burden on the help-desk team while maintaining access control and security.

Are you securely protecting both workforce and customer identities regardless of where and how they attempt to connect to the business and your resources?

Does the Device Meet My Standards?

Confirming the device is pre-approved and meets your security requirements (operating system, anti-virus, etc.) is paramount to the risk assessment.

Ensuring each endpoint device utilized to request access is recognized as belonging to the specific user and the device is up-to-date with respect to security standards is done via pre-checks and executed in the background to assess the risk associated with the request.

If a device is not recognized or does not meet the standards in place, a unique workflow can be triggered requiring an action by the user to verify the device and user before the authentication process continues.

If the user and device are affirmed and approved, a workflow can be triggered enacting a second factor authentication that is not a password (i.e. symbol recognition, biometric, TOTP) to securely verify the user and present a positive user experience.

Are you securely protecting both workforce and customer identities regardless of where and how they attempt to connect to the business and your resources?

What is My Risk Tolerance?

Applying policies based on the user identity, device, and contextual data (adaptive authentication) ensures a healthy balance between security and the user experience.

Moving beyond Multi-factor Authentication, adaptive authentication adds additional layers of security by implementing risk checks which are contextual in nature including items such as inspection of IP address, geo-location, phone type, dynamic perimeter, phone porting status check, device recognition, geo-velocity, malicious IP check, and more.

The adaptive risk checks happen unbeknown to the user and automated actions are triggered based on results. Actions such as; 1) access without MFA (passwordless), 2) Require MFA (passwordless), 3) Force password reset, 4) Redirect to honeypot, or 5) Deny access

The ability to design adaptive authentication workflows and apply each for different user types based on your level of acceptable risk helps ensure each user is securely accessing resources while experiencing a frictionless authentication process keeping efficiency, productivity, and satisfaction high.

Is your organization cataloging and capturing pertinent data for the phones and computers used by your users to request access to resources in an ongoing active manner?

Should I Grant or Deny Access?

Executing a consistent process for every access request and ensuring compliance with policies and contextual authentication parameters validates establishing a secure connection for users to resources.

No session is ever created for any access request until each step in the authentication process is successfully completed. Once a session is created, the identify profile for each user dictates the systems, applications, and data which will be available to the user.

The ability to maintain a healthy balance between security and user experience is achieved with the implementation of a well orchestrated access management solution. Beyond **Single Sign-on,** the inclusion of **Multi-factor Authentication** and **Adaptive Authentication** policies empowers the business to enable passwordless access confidently ensuring not only a great user experience but also a secure perimeter-less environment.

Are your access management workflows flexible enough to support any use case to enable your preferred authentication methods every time to provide the exact right security and user experience?

CONCLUSION

In a Zero Trust model, security is a priority. And the balance between strong security and a good user experience is crucial to the success of your **access management** program. Disrupting users to achieve secure access is not an option and the cost of a poor experience may result in lost productivity, poor engagement, or lost revenue. Ensuring no unnecessary compromise exists between security and the user experience requires a breadth of options including **passwordless** authentication, to protect resources and deliver the perfect user experience every time.

Since its inception, SecureAuth has delivered the access management capabilities enterprises require to securely authenticate users and protect valuable corporate resources while simultaneously creating a great user experience. With over 34 patented and patent pending innovations, SecureAuth offers the access management solution suited to the needs of your organization with the flexibility to deploy a SaaS, Hybrid, or On-premises solution based on your business requirements.

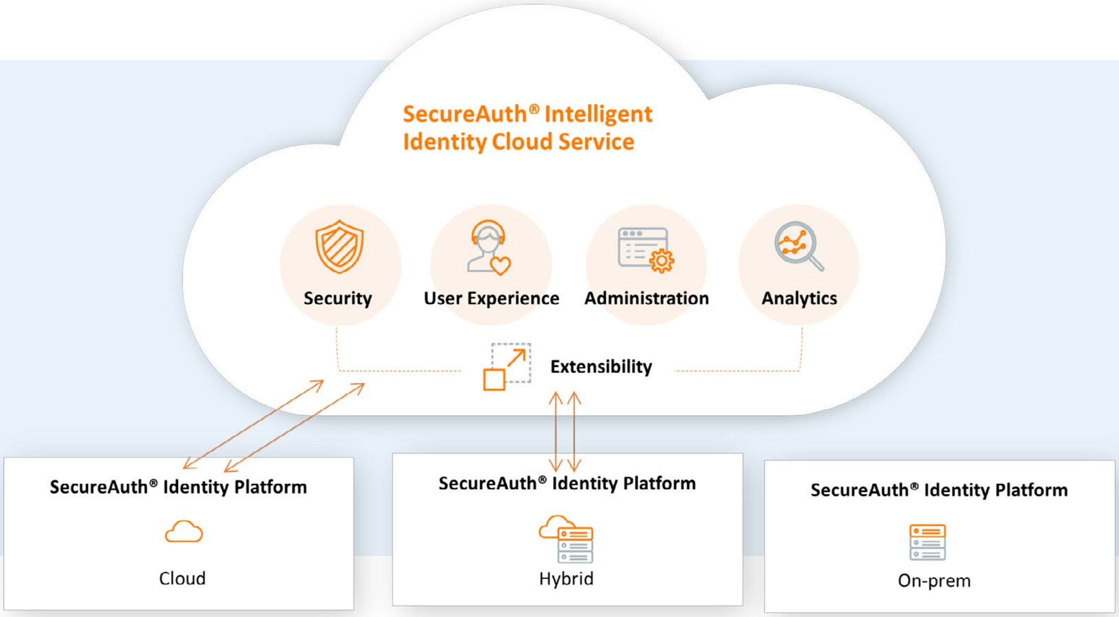
Through the end of 2020, enterprises that invest in new authentication methods and compensating controls will experience 50% fewer identity-related security breaches than peers that do not. [5]

Learn more about Adaptive Authentication & MFA and watch our webinar at www.SecureAuth.com

THE SERCUREAUTH IDENTITY PLATFORM

Identity is becoming the foundation for most businesses today. Digital transformation is forcing the need for nimble – yet secure – identity management. With attackers turning their attention to the identity as their attack vector, the stakes are high. Security and IT professionals are faced with the challenge of securing access for an increasingly diverse set of user identities connecting to their business. Sprawl — of identities, data stores, deployment models, geographies, applications and devices — is the new reality.

The right identity management program can be an enabler for your business and your workforce. With a flexible and adaptable approach to access management, you can accelerate the adoption of new technologies, increase security and meet your organizations digital transformation goals. The ideal solution will do all this while also reducing operating costs by decreasing helpdesk burden and improving user experience and productivity. Only the SecureAuth® Identity Platform can deliver this business agility.

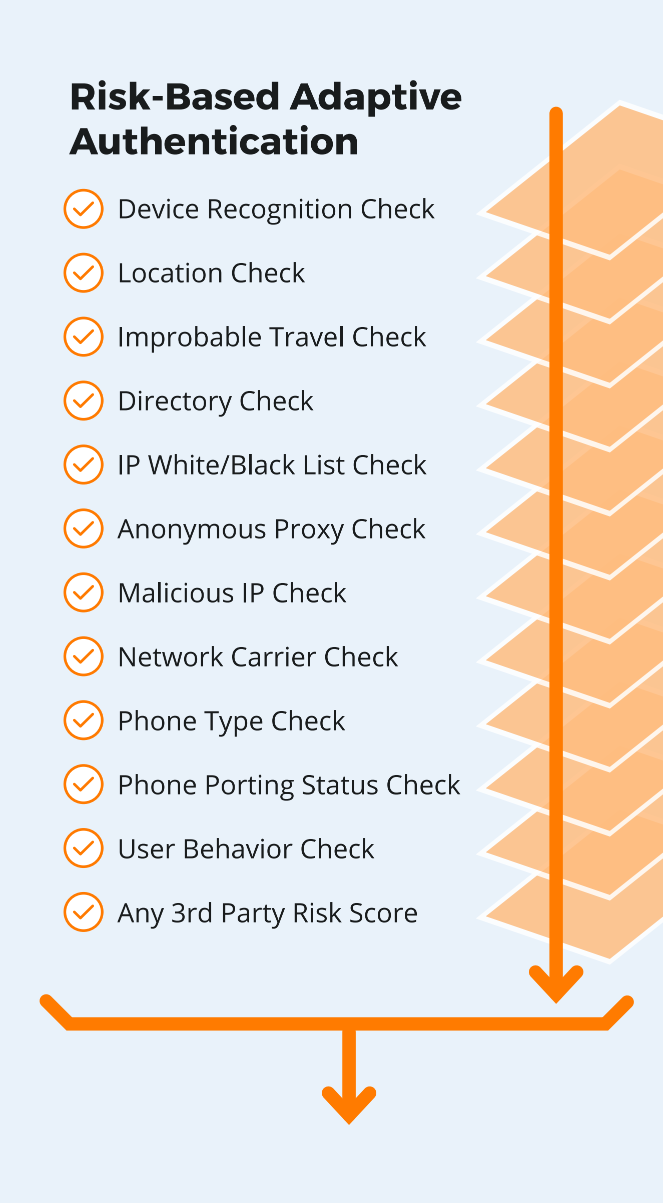

SecureAuth® Intelligent Identity Cloud Service
Security
User Experience
Administration
Analytics
Extensibility
SecureAuth® Identity Platform
Cloud
SecureAuth® Identity Platform
Hybrid
SecureAuth® Identity Platform
On-prem

SecureAuth brings together multi-factor authentication, risk-based adaptive authentication, single sign-on and user self-service in a highly flexible, standards-based platform. With SecureAuth, you can provide a unified and low-friction user experience that also delivers strong access control for all your workforce identities. With the ability to customize each authentication experience to the exact right combination of security and usability, you can easily meet the requirements of each use case. Flexible deployment options for hybrid, on-prem, or SaaS mean you can build secure access for your business, your way. Improve business delivery and gain a competitive advantage with the SecureAuth® Identity Platform .

THE SERCUREAUTH IDENTITY PLATFORM

The SecureAuth Identity Platform Delivers

- **The most multi-factor authentication methods** – provide options and choices for users while security professionals meet more use cases and conquer security concerns
- **The most adaptive authentication risk checks** – protect your organization while preserving experience with behind the scenes risk analysis that will not burden users
- **The most federation protocols** – deliver a unified and seamless user experience for all your workforce identities
- **Flexible authentication workflows** – our highly flexible workflows enable the creation of authentication experiences that meet the security and usability needs of every workforce identity
- **User self-service options** – self-service features for password resets, account unlocks, device enrollment and profile updates mean users stay productive and you reduce helpdesk calls delivering an immediate return on investment
- **Deployment freedom** – deploy any way you want — hybrid, on-prem, or SaaS — our platform delivers the flexibility enterprises need
- **Simple administration** – globally managed configurations and policies combine with an extensive application template library to enable rapid creation and easy management of authentication experiences
- **Intelligent Identity Cloud** – cloud-based analytics and administration that employs a big-data approach to delivering identity intelligence that informs adaptive authentication to ensure strong security and maximum usability for all your identities.



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 Behavior Check
- ✓ Any 3rd Party Risk Score

To learn more about the value of SecureAuth, please visit www.SecureAuth.com

Sources cited in this document

(1) Verizon Communications Inc., ‘*2019 Data Breach Investigations Report*’, 2019 Verizon Data Breach Investigations Report (DBIR), 2020, https://enterprise.verizon.com/resources/reports/dbir/

(2) Scott Rose et al. ‘*Zero Trust Architecture*’, The National Institute of Standards and Technology (NIST) U.S. Department of Commerce, September 2019, https://doi.org/10.6028/NIST.SP.800-207-draft

(3) ‘*Zero Trust Adoption Report*’, Cybersecurity Insiders, 2020, https://www.zscaler.com/resources/industry-reports/zero-trust-adoption-report-cybersecurity-insiders.pdf

(4) ‘*2019 End of Year Data Breach Report*’, Identity Theft Resource Center, 2020, https://www.idtheftcenter.org/2019-data-breaches/

(5) Ant Allen, ‘*Don’t Waste Time and Energy Tinkering With Password Policies; Invest in More Robust Authentication Methods or Other Compensating Controls*’, Gartner, April 4 2019, https://www.gartner.com/en/documents/3773163

SECUREAUTH