AI 2020 Cyber Security Awards WINNER

End-to-End Authentication. Simplified.

Compliance deadlines, passwords, and complex login solutions getting in the way of productivity?

Password security issues are a known cause of countless company breaches. Yet, many organisations rely solely on passwords to keep their business secure. In an attempt to upgrade security, some have turned to 2-factor authentication which still relies a passwords. Get back on track to password freedom with Authlogics.

Passwords are weak by nature, leaving them vulnerable to being stolen and reused. While most multi-factor authentication (MFA) solutions attempt to reduce the risk of a breach, they too often are just a band-aid, increasing inconvenience for the user, and failing to address the real problem: the inefficiency of the password.

Back to Password Basics

In June 2017, the National Institute of Standards and Technology (NIST) published new prescriptive guidance on password security (SP 800-63B). This change highlighted the need to evolve with the times and protect passwords against modern threats; in addition to adopting MFA. This guidance has largely gone unnoticed by the majority of authentication vendors, but at Authlogics, it is core to our security strategy.

Everybody loves to hate passwords, so let's imagine a world without them... There would be less risk, less cost and less wasted time.

There is no magic switch to renounce the password overnight, but it is not an impossible goal.

The Authlogics Journey

Before passwords can be eliminated, it is critical to first secure the way in which they are currently used. Authlogics achieves this by maintaining a Password Breach Database of over 2 billion known breached credentials, containing over 520 million clear text passwords, and with it, we can protect your network in real-time with our Password Security Management (PSM) solution.

Once the network is protected, our MFA solution can be implemented and

applications migrated to use it with, or preferably without, passwords. Even if you have an existing MFA solution, Authlogics can work alongside it.

When all applications are configured to log in using password-less MFA, passwords can be removed entirely.

Authlogics MFA supports a range of password-less login technologies to achieve this.

Simplicity is Key

Authlogics' solutions are designed to be deployed quickly and integrate well with existing applications through a mixture of agents and support for industry standards such as SAML 2.0 for Single Sign-On, and RADIUS for VPN and network access.

IFTTT automation, orchestration (Web API) and user self-service (Web Portal) are the essential keys to a successful deployment and ongoing management.

Our industry-leading device-less authentication can significantly reduce deployment time. Step up security can be used as needed via the Authlogics Authenticator mobile soft token, YubiKey USB token or even SMS, all while maintaining a consistent user login experience.

Password Compliance
- Real-time checks
- Auto Remediation
- Reporting

Multi-Factor Authentication
- 4 technologies
- Device-less tokens
- Offline support

Password-less
- Alternative knowledge factors
- Secure Password Vault for AD

Authlogics

Not all Multi-Factor Authentication solutions are created equal. See how we stack up.

Authlogics: Competitor Breakdown

Functionality	Authlogics	RSA SecurID	OneSpan / Vasco	Gemalto	Duo	Microsoft (Azure)	Symantec VIP	SaasPass	Swivel Secure	SecurEnvoy
Deviceless Authentication (1.5 Factor)	✓	✗	✗	✓	✗	✗	✗	✗	✓	✗
2 Factor Authentication	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Transaction Signing (3 Factor)	✓	✓	✓	✓	✗	✗	✗	✗	✓	✗
Multiple authentication technologies	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓
Works 100% offline	✓	✗	✗	✓	✗	✓	✓	✓	✓	✓
Password-less/PIN-less logon options	✓	✗	✗	✓	✗	✗	Cloud	✓	✓	✓
Emergency Override access (lost token)	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗
User Self Service Portal with AD password reset	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗
Web Services API (full automation & workflow)	✓	✗	✗	✓	✓	✗	✓	✓	✓	✓
Secure Password-less logon to Windows	✓	✓	✓	✓	✗	✗	✗	✓	✓	✓
Federated access to cloud applications (SAML 2.0)	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓
Active Directory Password security (NIST 800-63B compliance)	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
Multi-platform Soft Token	✓	✓	✓	✓	✓	✓	✓	*No Windows App	✓	*No Windows App
Multiple tokens per user	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗
Hardware token option	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓
SMS/Text token option	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Email token option	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓
Non-Clonable soft token	✓	✓	✗	✓	✗	✓	✓	✗	✓	✗
Direct Active Directory integration	✓	✗ *Requires Schema update	✗	✗	✗	✗	✗	✗	✗	✓
FIPS compliant cryptography	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓

Authlogics