transmit security

DATASHEET

WorkID™

Trust-Based Workforce Identity and Access Management

Every year there are bigger and bolder data breaches where nearly 70% of them can be attributed to password-related hacking events according to Verizon's 2020 Data Breach Investigations Report. Many organizations see multi-factor authentication (MFA) as a first step to eliminating passwords, but unless they are eliminated totally from authentication factors and centralized repositories, the risks still remain.

Many vendors claim their solutions are passwordless, but instead mask stored credentials on the device or point to centralized stores such as LDAP and Active Directory services. The best solution is to completely eliminate them across the board from devices, applications, directories, and even SaaS services.

WorkID: Passwordless Authentication and Access

WorkID is Transmit Security's risk-based, passwordless workforce identity and access management solution powered by the Transmit Security Platform. Whether logging into a workstation, a company-managed website, or a SaaS application using single sign-on, WorkID provides a consistent and hassle-free process that eliminates passwords for convenient, fast and secure access.

Real-time threat detection is combined with authentication technologies to quickly identify suspicious behavior then automatically deploy security measures to validate or re-validate the user. WorkID can use any combination of third-party authenticators or built-in options including OTPs, soft tokens, and FIDO-certified biometrics to securely authenticate a user. Administrators get precision control of business policies and risk management tools using a streamlined centralized management console with drag and drop simplicity.

- **Passwordless workstation login**
- **Passwordless SSO/ federation**
- **FIDO-based MFA and soft tokens**
- **Supports assigned, shared, and BYO devices**
- **Continuous adaptive trust**

Feature	Benefit
Risk-based authentication	Real-time anomaly detection identifies suspicious activity then automatically challenges it before continuing
API-based integration	Vendor-agnostic integration supports seamless deployment into legacy environments
Identity orchestration	Configure and deploy new policies, authenticators, and risk mitigation controls centrally with drag and drop simplicity
Broad OS/device support	Supports FIDO and non-FIDO devices along with common OS platforms including Windows 8/10, Macs, and Citrix

A Foundation Built on Continuous Adaptive Trust

WorkID uses a unique approach that integrates and orchestrates identity and access management based on a foundation of real-time risk assessment and decisioning. Everything a user does is monitored by the adaptive risk engine. It continuously looks at all activity across all services and all devices over time to provide a continuously updated risk snapshot.

Based on risk levels, WorkID determines the type of authentication method that is required to validate the user before the activity is allowed. Should the user pass authentication, WorkID's risk-aware authorization provides numerous controls that can be called to minimize risk and deploy new dimensionality to business policies. These include requiring more secure authenticators, step-ups, or second channel validation such as requiring a web login and a device biometric. Additional tools including third-party approvals and device management can be used to further restrict access or ensure that sensitive activities are managed.

Passwordless Workstation Login

With WorkID's passwordless workstation login, users can quickly, conveniently, and securely sign into their workstation or laptop using a variety of supported methods including mobile device biometrics, USB security keys, and enterprise-grade soft tokens.

WorkID supports FIDO, non-FIDO devices, operating systems including Windows 8/10 and Macs, and access for both online and offline login where the devices cannot connect to a network for authentication. WorkID also supports Citrix VDI for secure virtual device access.

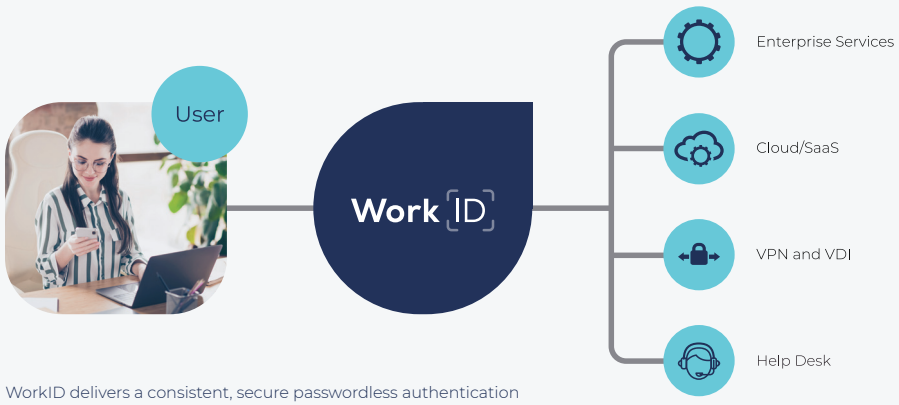
Organizations can easily enable passwordless login for employees and any third parties such as consultants and contractors with flexible BYOD tools that allow secure device onboarding and replacements. Even shared devices such as workstations, kiosks, phones and tablets are supported with comprehensive management options to make the job easier for administrators.

Passwordless SSO and Federation

WorkID gives users the convenience to seamlessly connect to on-premise, VPN, and cloud applications using a single passwordless login both within an application or tied to WorkID's workstation login solution. Passwordless single sign-on (SSO) removes passwords for all federated systems while increasing security by continuously monitoring risk to automatically deploy mitigation tools in real time.

Passwordless MFA and Soft Tokens

Use any combination of third-party or built-in authenticators including OTP, soft tokens, and biometrics to create secure passwordless multi-factor authentication methods with WorkID. Leverage existing tools you already have or replace them with the latest in FIDO-certified authentication technologies available with WorkID.



WorkID delivers a consistent, secure passwordless authentication experience across all enterprise services including the help desk

Securing the Help Desk

Despite an organization's best efforts, security is only as good as the weakest link. For many that's the help desk where a simple call can reset an employee password whether it's the employee or an attacker impersonating them. WorkID delivers full 360° visibility that spans every channel to identify and stop threats that target weaknesses across all systems and channels.

Easy to Deploy and Manage

Using an API-based approach, existing identity, risk and access control services can quickly be connected to WorkID. Use what you already have or replace components quickly and painlessly with drag and drop simplicity using WorkID's management console. There's even a ready-made mobile application that can be customized to make roll out as easy as downloading an app from the iOS or Google app stores.

DS-WKDS-EN-20201204-01