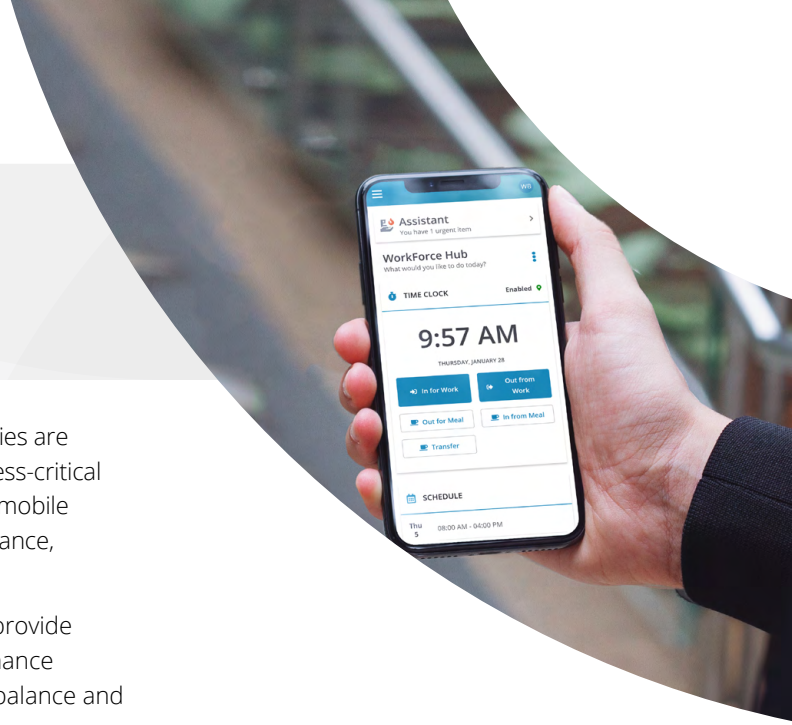
workforce SOFTWARE

The WorkForce Suite

Cloud Delivery



For many organizations, cloud migration is more than a priority—it's a necessity, especially now that business strategies are laser-focused on maintaining operational agility. When day-to-day operations depend on immediate access to business-critical systems, on-premise software simply can't keep up. On top of firewalls preventing outside access and limited (if any) mobile capability, IT teams are stretched thin managing physical hardware maintenance, upgrades, data and security compliance, technical support, and more.

As the "at-work" experience continues to evolve, employers are prioritizing the employee experience in ways that provide greater flexibility without disrupting operations. Not only does a cloud-based workforce management solution enhance security, improve compliance, and increase accessibility, it also offers employees greater control of their work-life balance and provides real-time communication from anywhere, on any device.

Hosted in world-class data centers around the globe and managed by SaaS experts, WorkForce Software's cloud delivery offers:

Unmatched Value
A predictable annual per-employee subscription fee covers all software, hardware, maintenance, and support.

Immediate Returns
Streamlined deployment maximizes return on investment.

Global Presence
Supporting organizations in 80+ countries with data centers in Australia, Canada, Europe, and the United States.

Continuous Innovation
Immediate access to new features that incorporate the latest workforce management best practices.

Automatic Updates
Ongoing maintenance—including three major annual releases—minimizes disruption to ensure businesses remain up to date.

Anywhere, Anytime Access
Mobile-first and responsive design for a personalized user experience and convenient employee self-service tools.

Rigorous Control
ISO 27001 and EU-US Privacy Shield certified while annual audits ensure strict security procedures and privacy control (SOC 1 Type II, ISAE 3402 Type II, SOC 2 Type II, General Data Protection Regulation [GDPR] Type I, and ISO).

99

"It's a matter of ease of use. WorkForce really has no upkeep maintenance that we have to do. It pretty much just runs."

Isaac Gordon,
Systems Technician
Chandler Unified School District

Keeping the System—and Data—Secure

WorkForce Software is heavily invested in cloud infrastructure and auditing procedures to make sure that the highest standards for security, reliability, and performance are met and exceeded. Selected highlights of security measures include:

Physical Security

Video surveillance monitors each facility 24/7. A key card, PIN, and/or biometrics are required to enter the premises. Just as in a police station or hospital, each facility is fully prepared with at least N+1 redundant power, air conditioning systems, and generators, with at least 24 hours of fuel and Priority 1 refueling. All equipment runs within dedicated space. WorkForce Software owns, maintains, and supports all equipment and applications.

Perimeter Security

Protection services defend against distributed denial-of-service (DDoS) attacks. Web application firewalls protect applications. Firewalls secure traffic from the internet and between key subnets. Intrusion detection systems continuously monitor the SaaS environment.

Data Encryption

The WorkForce Suite SaaS platform supports the strongest HTTPS (TLS) encryption available for use by browsers and web services. Data from clock terminals is encrypted over the internet, and secure protocols are used for bulk file transfers. Data at rest, including backups, are encrypted with AES-256 encryption.

Security Testing

Internal and external vulnerability scans are performed weekly while security logs are proactively analyzed to identify security threats. Third-party security firms perform independent vulnerability scans, annual data center penetration tests, and annual web application security tests.

Database Security

Database access is strictly controlled and monitored. Database entitlements are audited monthly.

User Authentication

Clients can customize password rules within the WorkForce Suite's native authentication systems and/or can use Single Sign-On (SSO) over SAML to authenticate against the directory services.

Internal System Security

Non-routable IP addressing, port-redirection, network address translation, and other mechanisms protect systems within the firewalls. Servers comply with Center for Internet Security Benchmarks, and systems are routinely patched for security.

Redundancy and Disaster Recovery

All network components, load balancers, proxy servers, application servers, and database servers have redundant hardware. WorkForce Software has multiple redundant internet providers. WorkForce Software maintains complete disaster recovery facilities with duplicate hardware, software, and internet connectivity. Data is replicated to standby servers at both the Primary Site and the Disaster Recovery Site.

Backups and Restores

Full weekly database backups and incremental daily backups are encrypted and stored at both the Primary and Failover SaaS sites. Routine restores are used to verify backup data is accessible.

Operating Procedures

WorkForce Software adheres to documented Change Management Procedures. All changes require approval from the Change Approval Board. Access to the SaaS environment is strictly limited, and access must be approved in advance by the Change Approval Board.

Bringing It All Together

Learn how the WorkForce Suite can help organizations migrate data to the cloud to enhance security, improve compliance, and increase accessibility. For more information contact: 877.4.WFORCE | workforcesoftware.com

workforce SOFTWARE