WorkforceHub
powered by swipeclock

The Strength & Security of Swipeclock

We work diligently to provide HR tech solutions that employers can count on to be accessible and secure.

We take application and data security seriously and follow the Zero Trust security model. This is a model that permeates our company and provides guidelines for security at all levels of the application, not only at the perimeter.

Some of our practices to protect the system and your data include:

- SOC II Type II security audit
- Employee and production endpoint protection
- Managed Detection & Response (MDR) service with 24/7 SOC monitoring and response matrix
- Regular penetration tests and vulnerability scans
- Secure cloud hosting environment
- System segmentation with minimum privilege and role isolation
- Near real-time backups of all data
- Recovery plan for all systems and data — documented and practiced
- Employee and developer required training on security concerns and best practices

Swipeclock solutions are delivered through partners and direct to employers across the U.S.

OVER 1 MILLION

MORE THAN 1,300

3 MILLION+ TIME PUNCHES

20+ YEARS FOCUSED ON THE SMB

TIME, SCHEDULING AND HIRING

What is Zero Trust?

Zero Trust is the term for an evolving set of cybersecurity paradigms that moves defenses from static, network-based perimeters to focus on users, assets and resources. A Zero Trust architecture uses Zero Trust principles to plan infrastructure and workflows. Zero Trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location.