KASTLE

Enterprise Office Security Comparison Guide - Before and After Kastle

Only Kastle delivers comprehensive physical security solution that enables your business to confidently scale office access control across multiple locations with consistent oversight. See how Kastle increases both security protection and operational efficiency for your business.

Before	With Kastle
Each office has different access technology, causing operational inconsistency, poor scalability, and workflow redundancy.	Offices share a unified database and administrative hub, delivering consistent control across locations with a centralized workflow.
Installation, maintenance, and operations are performed by different vendors at each site with no shared practices, creating inefficiency and security risk.	All systems are designed and installed by the same vendor that will monitor and maintain the operation. The entire network is managed by one accountable team.
Employees must use different credentials to enter each office location.	Employees can conveniently use the same credential across the portfolio of office locations.
There is no central source for data collection and reporting on access activity.	One central data dashboard aggregates activity reporting and auditing with detailed data for each office.
Monitoring and software updates are performed by a mix of internal staff and external vendors varied by location.	Software updates, data storage, and monitoring oversight are outsourced to experts remotely at a Kastle operation center.
Operating costs are scattered, duplicated, or hidden by untracked inefficiency of staff or hit as unbudgeted ad-hoc capital expenses for repairs.	Operating costs of all monitoring, maintenance, and repairs are covered for all offices in one consistent service fee and are Kastle's responsibility.