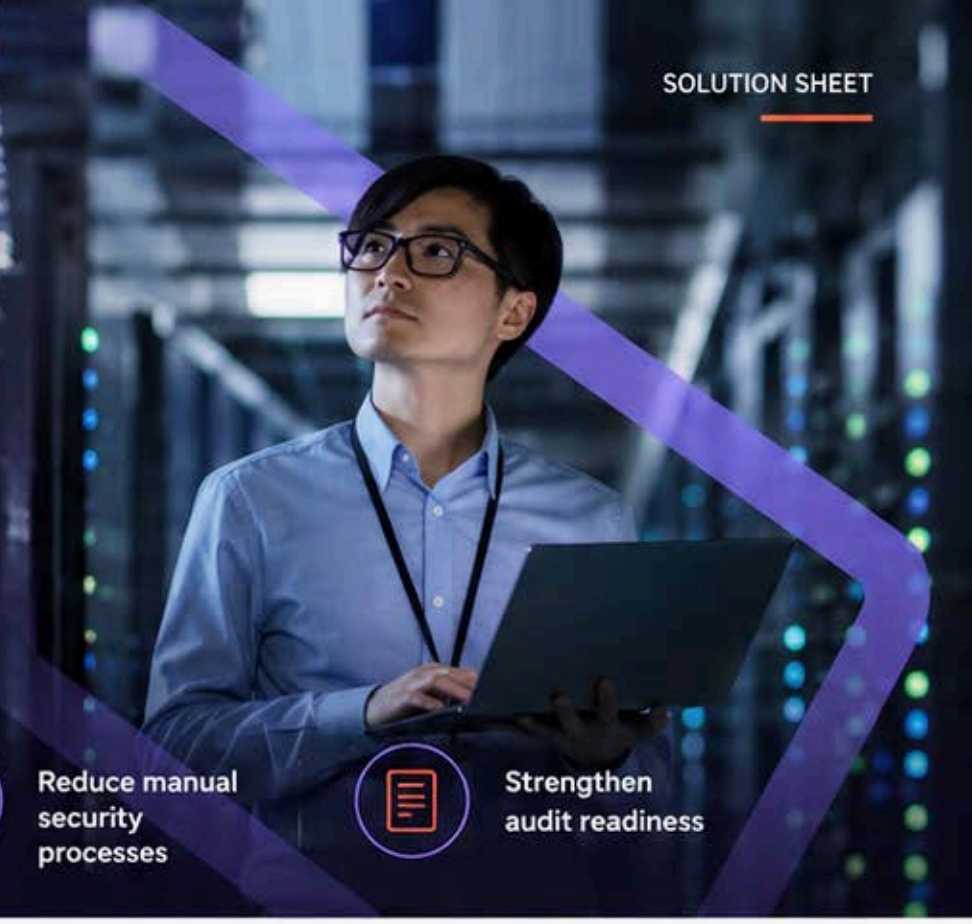
Alert Enterprise

SOLUTION SHEET

Physical security built for always-on data centers

Protect critical infrastructure by connecting identity, physical access and security operations across every site, facility and restricted environment.



- Control privileged physical access
- Automate contractor and vendor access
- Reduce manual security processes
- Strengthen audit readiness

The right person. The right access. The right amount of time.

Access to critical infrastructure should never depend on a badge alone.

Alert Enterprise connects identity, role, location, training, assignment and policy with physical access so permissions reflect what someone is actually authorized to do.

Automatically provision, adjust and revoke access as employees join, change roles or leave — and give contractors, vendors and technicians temporary access based on their assignment, approvals and business needs.

Less standing access. Fewer manual processes. Greater control.

Temporary work shouldn't create permanent access.

Data centers depend heavily on contractors, technicians, maintenance teams and equipment vendors. Alert Enterprise helps govern third-party access from beginning to end.

- Grant access based on facility, assignment or work requirement
- Validate approvals, training and certifications before access is provisioned
- Automatically expire access when the approved period ends
- Maintain a centralized record of requests, approvals, changes and revocation

When the work ends, the access should end with it.

Protect your most critical areas.

Not every door carries the same risk. Apply identity-driven policies and additional controls to sensitive environments including:

- Data halls
- Server rooms
- Network rooms
- Operations centers
- Restricted cages
- Mechanical infrastructure
- Security operations centers

Know who has access and why.

Centralized visibility into who has access, what they can access, why they have it and whether they should still have it.

One security model across every data center.

Connect HR, identity, contractor, IT and physical security systems without replacing your existing infrastructure.

Strengthen compliance and audit readiness.

A complete, traceable history of access requests, approvals, policy validation, provisioning, access reviews, exceptions and revocation.

One identity. One governed access lifecycle.

Connect the systems that know who someone is with the systems that determine where they can go.

