



The visitor management vulnerabilities

Mitigating physical risks
in data center security

Content

01

Executive summary

The data center security challenge04 →

The Zero Trust visitor mandate05 →

02

Security audit

Understanding the vulnerabilities 07 →

Most common physical access vulnerabilities08 →

Securing the audit trail: global standards09 →

Securing the audit trail: regional frameworks 10 →

03

People flow

Anatomy of of access points in a data center 12 →

Street-to-rack: The 6-layer physical security blueprint 14 →

HVAC contractor journey: Isolating the gray space 15 →

VIP visitor/IT technician journey: Enforcing limits in the white space 16 →

04

Perimeter access

Segregation and pre-vetted access 18 →

Segregated, secure, and seamless at Layer 1 19 →

05

Building entrance

Safe and seamless credential validation..... 21 →

Fast, fluid, and foolproof at Layer 2 22 →

06

Floor access

Prevent tailgating and unauthorized routing 24 →

Screened and segmented at Layer 3 25 →

07

Server hall

Deadlocked entry. Safe exit. 27 →

Sealed, steadfast, and safe at Layer 4 28 →

08

Cage access

Secure cage access30 →

Isolated and impenetrable at Layer 5 31 →

09

Rack access

Cabinet-level authentication 33 →

Precise, protected, and proven at Layer 6 34 →

10

Conclusion & outlook

Holistic visitor management 36 →

Unified, visible, and verifiable at every Layer 37 →

Our offering 38 →

Executive summary

The data center security challenge

Data centers form the physical backbone of the digital world, housing servers and networking equipment that support AI, cloud services, e-commerce, finance, and public services. While organizations tightly secure their virtual networks with firewalls and encryption, the physical security of the facilities often presents challenges.

Shared spaces create vulnerabilities that demand detailed, layered security protocols beyond just perimeter defenses. Protection must extend to every layer all the way down to the rack level. An effective defense against both cyber and physical threats depends on integrating IT and physical security systems.

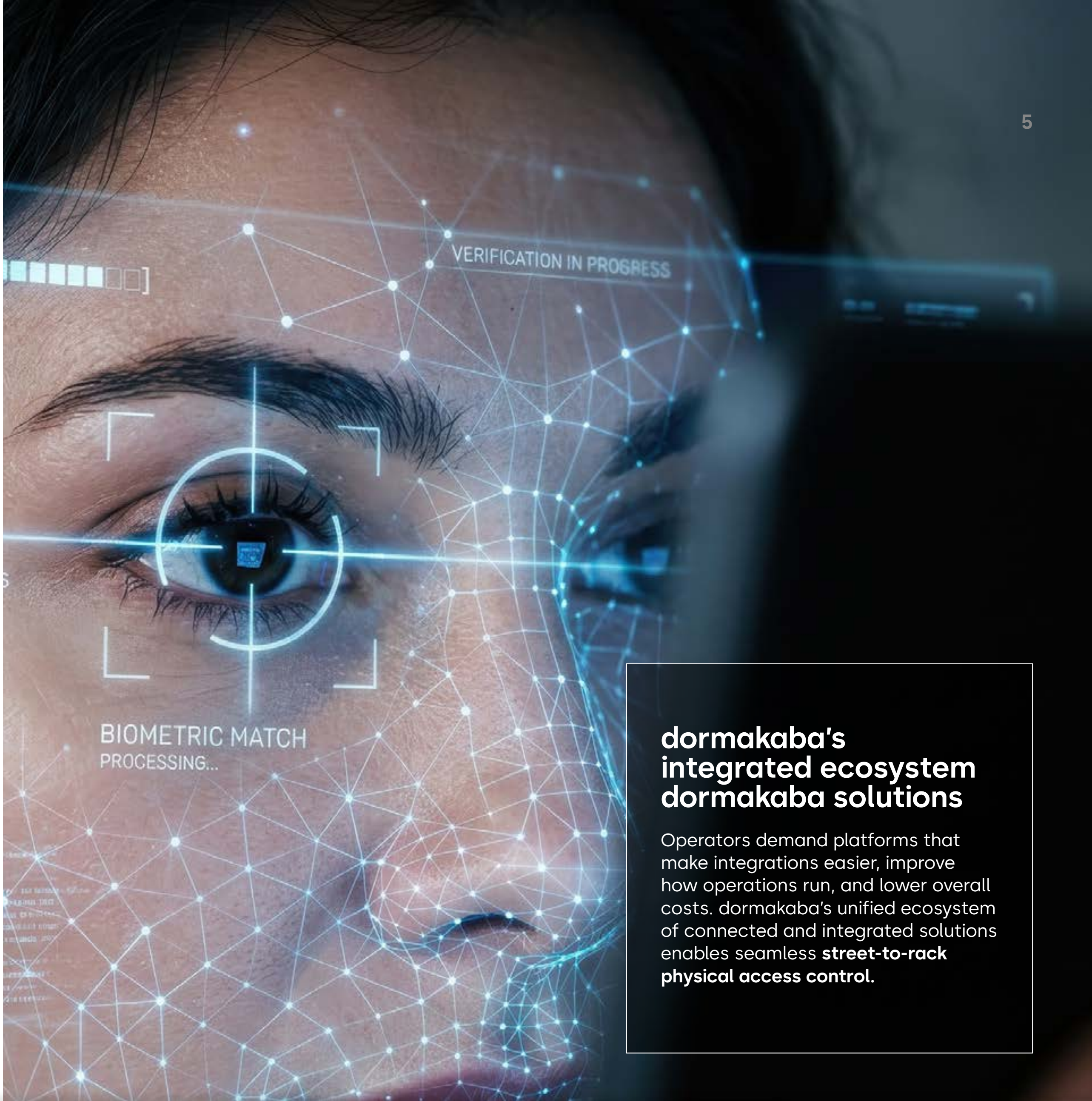


The Zero Trust visitor mandate

Currently, the main physical vulnerability is unmanaged third-party access.

In a modern colocation facility, visitors are more than just guests. Daily logs include a wide range of third-party profiles, from essential maintenance crews and outsourced IT staff to VIP investors and auditors. Visitor management for data centers must combine access control, visitor and contractor management, identity verification, and audit-ready logs.

Zero Trust, which originally was a cybersecurity framework stating that no digital user or device is trusted by default, now needs to be applied physically as well. A facility cannot inherently trust anyone. Security requires ongoing identity verification within a layered physical security strategy.



dormakaba's integrated ecosystem dormakaba solutions

Operators demand platforms that make integrations easier, improve how operations run, and lower overall costs. dormakaba's unified ecosystem of connected and integrated solutions enables seamless **street-to-rack physical access control**.

Want to keep reading?

Complete the contact form to access the full
whitepaper on data center visitor management.