IRIS ID

Advanced Identity Authentication™

IRIS RECOGNITION FOR DATA CENTERS

CASE STUDY

Iris ID Technology Plays a Vital Role in Increased Security & Efficiency with Our Customers

CERN cisco citi ebay

FirstEnergy Google IRON MOUNTAIN®

Microsoft NTT ORACLE

QTS أرامكو السعودية saudi aramco Scotiabank®

TD Bank America's Most Convenient Bank®

tierpoint

Iris ID installed at Google Data Center

THE PROBLEM

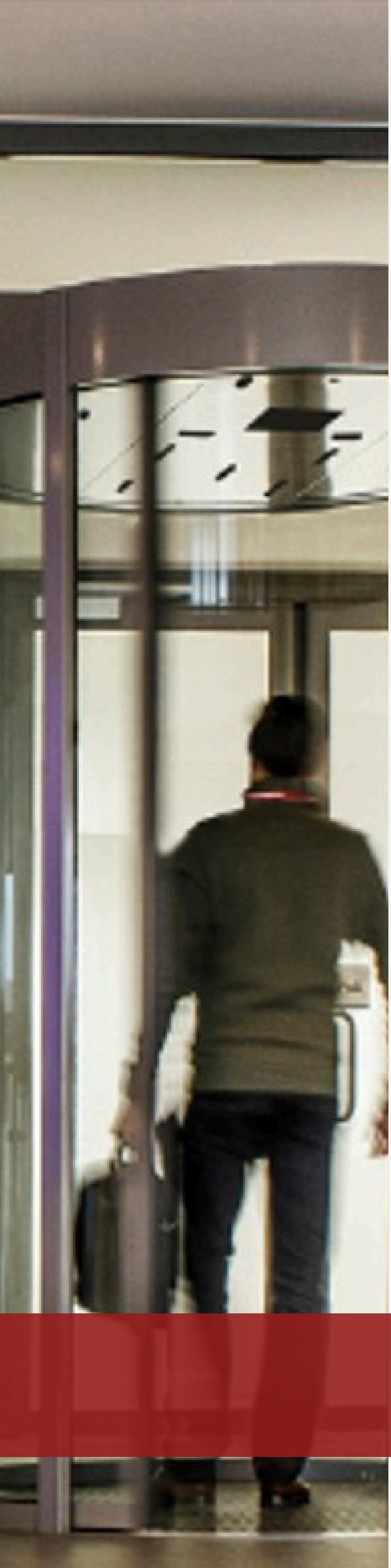
Defending against an increasing number of cybersecurity and physical security threats requires a layered solution.

THE SOLUTION

Iris ID technology and solutions have been selected by many organizations both nationally and internationally, including Fortune 100 companies and CERN, a European nuclear research facility to secure their physical data center locations. Data Centers are the hub of an organization's operations and processes and have evolved over the years to not only be a physical location but also in the cloud. Regardless of location, the sensitive information that is housed by these connected servers demands the highest level of protection and security.

The foremost reason for implementing a biometric solution for data center access management is to ensure that only the people with approved credentials get in and/or out of the location. Aside from DNA, iris recognition is the most accurate authentication solution on the market. It is also fast and noncontact.

The scalability of the solution and capability to work with existing access control solutions providing Wiegand and OSDP communication make it a chosen leader in the global market.

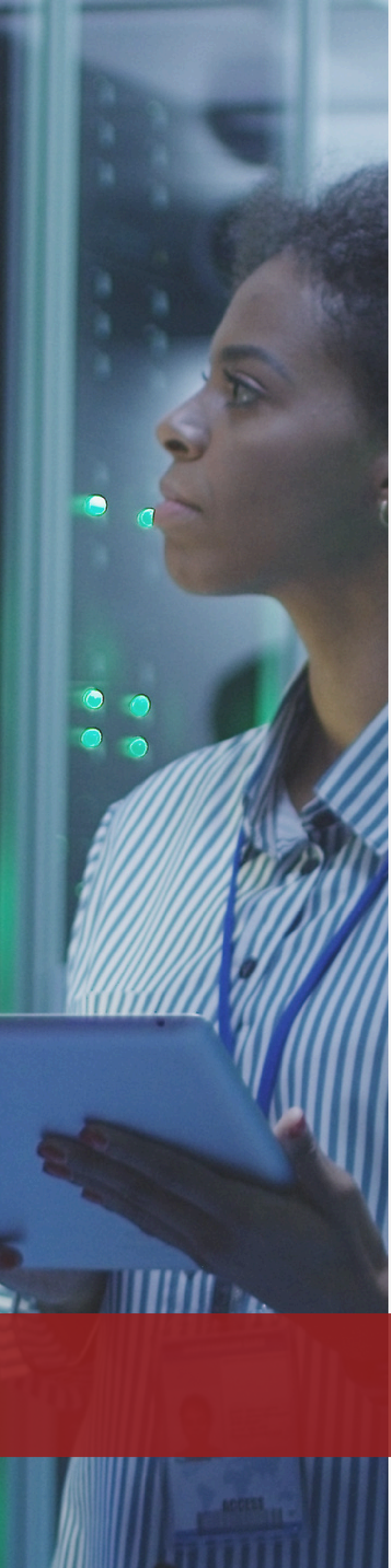


WHY IRIS TECHNOLOGY?

In addition to being the most accurate, reliable and fastest, non-contact biometric on the market, iris recognition technology satisfies GDPR regulations. GDPR compliance is crucial for global companies, as fines for non-compliance are steep, reaching up to 4% of an organization's global revenue. GDPR requires that individuals have a right to know how their opt-in data is being used and stored, and - if requested - the company managing the data must delete it.

In order for iris recognition to be used in an integrated access control management system, the user must agree to have their irises scanned and stored on a template. This acknowledgement satisfies the opt-in requirement put in place by GDPR. The stored images are then converted into a 512-byte digital template, ensuring maximum protection for the user, as no sensitive or personal identifiable information can be extracted.

Iris technology is also more inclusive than other non-contact technologies; it can be used in extreme weather conditions as well as with users wearing goggles, hard hats, lab suits, and religious garb. Iris technology is not affected by weight gain and will produce accurate results regardless of race or gender.



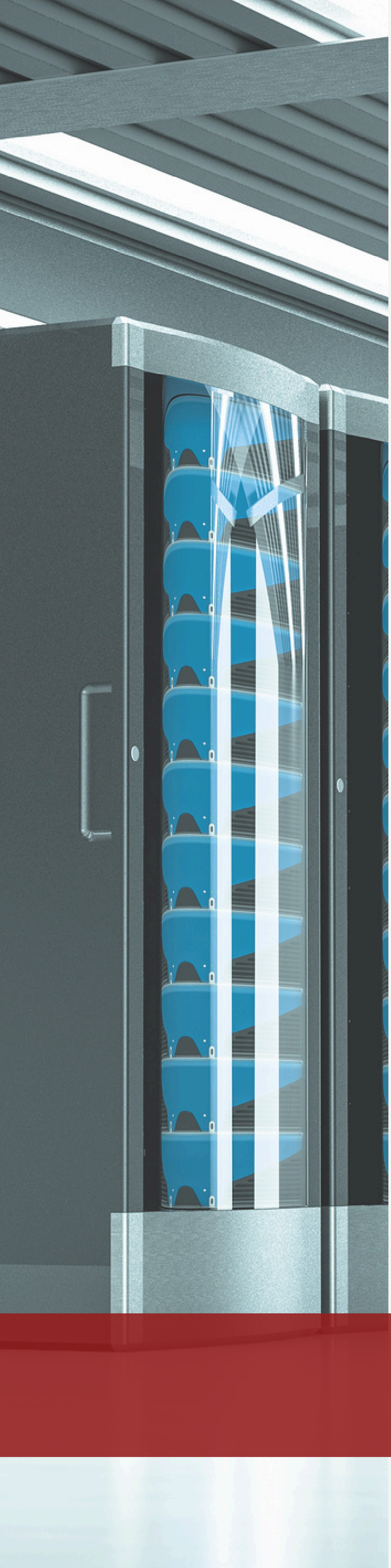
HOW OUR CLIENTS USE IRIS ID SOLUTIONS

When developing a concrete plan for data center security, several factors must be taken into consideration including physical security and technology. Our solutions mesh well with the preferred layered security approach. This means our technology can work with a mix of technologies delivering the highest security to the actual data center floor and then varying levels of security for other departments. Additionally, not everyone has the same level of access privilege; our solutions can set and validate those credentials for different security levels.

Iris ID solutions are used because they deliver the highest standard of secure protection and allow data centers and colocations to stay ahead of potential threats in a rapidly changing technological environment.

Iris Technology Delivers:

- An easy, non-intrusive and non-contact user experience
- Capacity for optional third-party surveillance camera
- Leverage existing infrastructure
- Remote management
- Easy installation and maintenance
- 24 x 7 security



IRIS TECHNOLOGY: ROI

The benefits and ROI of using biometric monitoring in data centers are manifold. From time savings to increased security and efficiency, many organizations - not just data centers - are implementing biometrics into their security mix because it offers the best means to fight against costly physical and cyber security threats.

- **Reliable:** Biometric access control will only allow those with the proper credentials in and out of controlled areas. The system cannot be hacked or compromised and requires users to be present on-site for access to be granted - remote access is prohibited.

- **MFA Capability:** Iris technology and Iris ID products offer the ability to work with MFA solutions such as pins, cards and other biometrics such as face. This offers an added layer of protection and customization to accommodate varying levels of security.

- **Low Operational Costs:** Once the biometric access control system is installed, software and system updates can be carried out automatically, reducing overhead and IT workload so teams can focus on more critical support work.

IRIS ID TECHNOLOGY VALUE PROPOSITION

- Securely restricts access to sensitive areas and information
- Eliminates keycard and password sharing
- Integrates with existing access control systems and works with MFA solutions
- Is easy to manage and administer on an individual user basis
- Delivers an access control solution that is compliant with federal and global requirements
- One-time, lifetime enrollment - no recurring costs
- 25 years of Access Control expertise

ACCESS CONTROL PARTNER MANUFACTURERS

LENEL:S2 Honeywell

Software House AMAG TECHNOLOGY

APOLLO intelligent security solutions GALLAGHER

brivo RBH ACCESS

Learn more about our solutions at www.irisid.com.

NEW PRODUCT NEW PRODUCT NEW PRODUCT

VERIFIED OSDP™ VERIFIED

IrisAccess™
iCAM 7S Series
Iris Recognition Reader
The only iris biometric
OSDP verified device

IrisAccess™
iA1000 Iris & Face Recognition
Available Q4 2024

www.irisid.com | sales@irisid.com