SECURITY ENTRANCE

TREND REPORT

2025.

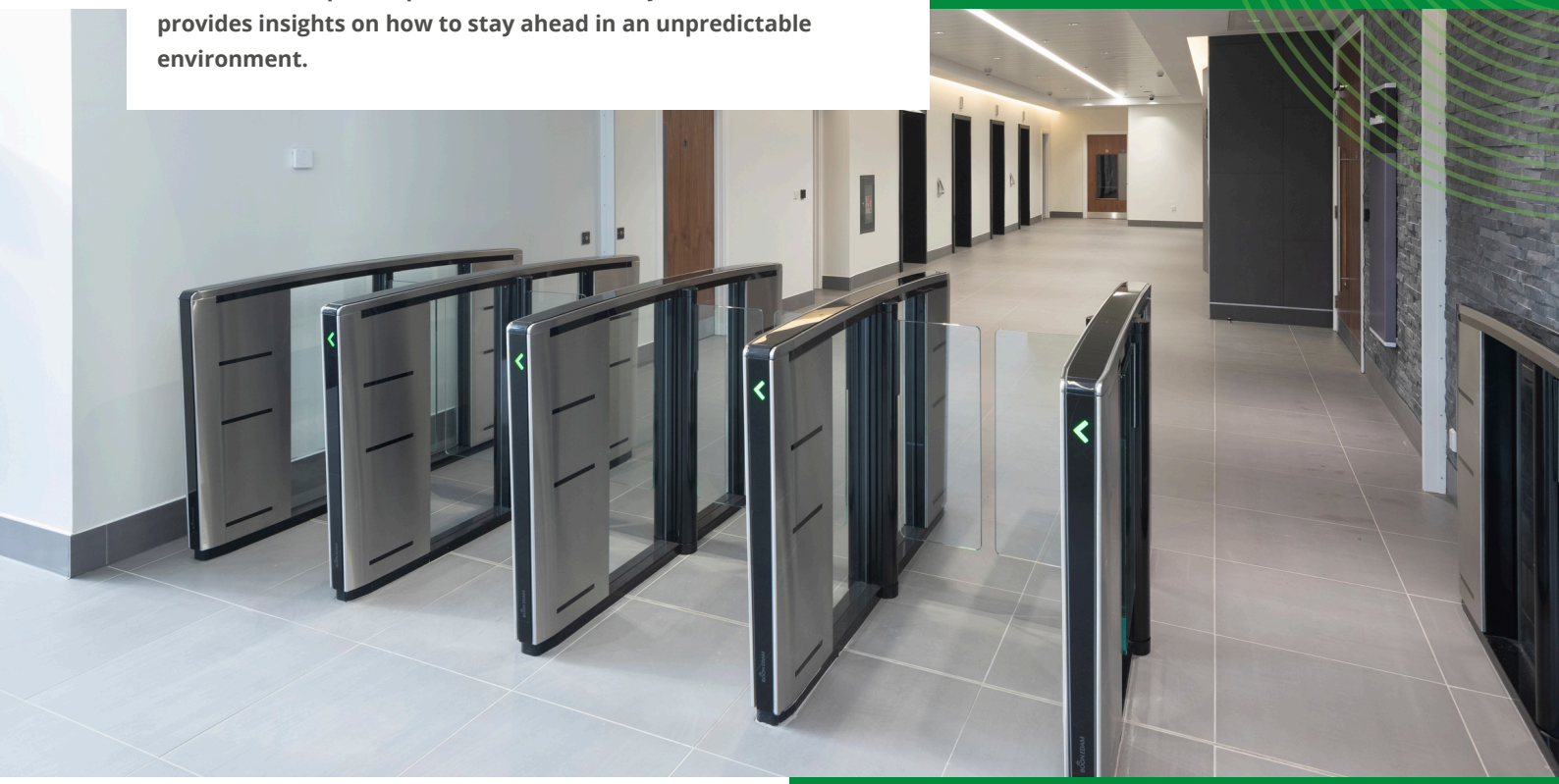
SHAPING TOMORROW'S **SECURE ENTRANCES.**

BOON EDAM

YOUR **ENTRY** EXPERTS.

INTRODUCTION.

Building security demands have risen dramatically in a world characterised by increasing polarisation, technological advancements, extremism and growing distrust. Industries that once required only moderate protection now face heightened risks, with threats extending beyond government buildings and data centres. This report explores current security entrance trends and provides insights on how to stay ahead in an unpredictable environment.



"As society envisions barrier-free, welcoming environments, the harsh reality demands robust security measures that balance accessibility with protection."

Douwe Jolles
PRODUCT MANAGER - DOOR SYSTEMS

INDEX

1 CYBER SECURITY MEETS PHYSICAL SECURITY.

The need for a unified approach to security has never been more critical. This integration drives a new era of protection strategies for organisations across industries, including data centres, government buildings, critical infrastructure and corporate headquarters. In our connected world, security isn't just about blocking unauthorised access or protecting digital systems - it's about seamlessly combining both into a comprehensive, unified defence.

Zero Trust Architecture

This security model is based on the principle of least privilege. It ensures that users and devices can only access the specific resources required for their roles - nothing more. Zero Trust makes it significantly more difficult for malicious actors to breach systems or steal sensitive information by limiting access points. This approach is especially critical in high-stakes environments like data centres, where any security failure can have severe consequences. In such settings, somebody must verify every interaction with physical and digital assets against authorised access permissions.

Raising the Bar for Cyber Security

New EU regulations are reshaping cyber security standards, directly impacting security entrances and access control systems. The NIS2 Directive and the Cyber Resilience Act (CRA) both aim to strengthen cyber protections, but focus on different aspects.

NIS2 is designed to secure essential services and critical infrastructure, requiring industries like energy, healthcare, and transport to implement stronger cyber security measures. These include improved risk management, supply chain security and stricter reporting of cyber incidents. Organisations that failed to comply by late 2024 could face heavy penalties and reputational damage.

The **Cyber Resilience Act** ensures that products with digital components - such as access control systems, IoT-enabled security doors, speed gates and revolving doors with digital integrations must adhere to higher cyber security standards. Manufacturers must integrate security into their product designs, maintenance and provide ongoing updates, with some high-risk products requiring third-party certification before entering the EU market. Products that meet these standards will carry the CE marking, making it easier for businesses to identify compliant solutions.

Together, these regulations set a new benchmark for cyber security, ensuring that both the infrastructure and the physical products used to secure it are resilient against cyber threats.

Building Security Ecosystems

In today's complex security landscape, a building's security ecosystem must integrate high, medium and low-security measures to create a dynamic, interconnected defence. Every layer of security serves a unique purpose in keeping the building safe, protecting assets and ensuring access where necessary.

While cyber security often dominates discussions about safeguarding sensitive environments, physical security is equally critical - especially for facilities like data centres. If someone with malicious intent gets direct physical access to a server, they can bypass even the most sophisticated firewalls, potentially leading to catastrophic data breaches. This underscores the importance of aligning physical and digital security systems to work in harmony.

High-security zones, such as server rooms, require robust physical security solutions, including biometric authentication, encrypted communication protocols and automated, unattended entry solutions. These safeguards prevent unauthorised entry and align with cyber security strategies by enabling swift authorisation changes to mitigate threats in real-time.

Medium-security areas, like administrative floors, rely on technologies like speed gates with advanced sensors, ensuring seamless access for authorised personnel while deterring unauthorised attempts. Low-security spaces, such as public lobbies, prioritise aesthetics and accessibility while maintaining essential security through monitored access points.

This ecosystem approach mirrors cyber security principles like multi-factor authentication. Just as digital systems require layered defences to protect sensitive information, physical spaces benefit from multiple complementary security measures. Each layer ensures that if one line of defence fails, others remain active to protect critical assets.

For physical security to remain effective, cyber security best practices must be incorporated. This includes implementing encrypted communication protocols, performing regular software updates, and using resilient access control systems against cyber attacks.

By designing a security ecosystem where digital and physical security measures function seamlessly together, organisations can create secure, operational and prepared spaces for modern challenges. This approach provides not only robust protection but also a balance between accessibility and security, creating welcoming and resilient environments.

Keeping intruders where they belong - outside - is the first line of defence. If an intruder breaches a building's entry points, all other security measures become reactive. Closing the security gap starts at the entrance."

Security Operations Centre

A Security Operations Centre (SOC) is a centralised unit responsible for real-time monitoring, detection, analysis and response to cyber security threats. Its primary goal is to maintain an organisation's security posture by safeguarding networks, systems, applications and sensitive data from cyber threats.

The SOC operates 24/7 to ensure continuous surveillance and minimise the risk of data breaches, cyber attacks or unauthorised access. Organisations structure their SOCs according to their specific needs and resources. The most common types include in-house SOCs, which provide complete control over security operations but require significant personnel and technology investments. Managed SOCs (or outsourced SOCs) are operated by third-party service providers with specialised expertise.

2 EXPLOSION AND IMPACT RESISTANCE.

The evolving security landscape is driving a growing demand for enhanced building protection across a broader range of industries. While traditional high-security sectors such as government, banking and data centres have long prioritised security, new threats are prompting other sectors, including media companies and commercial organisations, to upgrade their protective measures.

Rising risks such as vandalism, terrorism, extremist groups and societal polarisation are reshaping the approach to building security, with explosion-resistant and impact-resistant materials emerging as critical components of modern solutions.

Material Innovation

As businesses place greater emphasis on threat prevention, explosion and impact-resistant entrances are becoming a higher priority. The increasing use of advanced materials in building facades underscores the need for stronger barriers to address evolving security risks.

Materials such as polycarbonate layers - valued for their lightweight and impact-resistant properties - reinforced steel and shatterproof glass are becoming more widely used in modern security systems. Engineered to absorb and disperse energy from blasts or projectiles, these materials create durable barriers that minimise damage and protect occupants. By collaborating with material science experts, manufacturers are integrating cutting-edge technologies into entrance solutions, enhancing resilience against both intentional attacks and accidental impacts.

Security entrances are also being designed to withstand forceful breaches, whether from tools or vehicles. Features such as anti-ramming elements, reinforced frames and advanced anchoring systems provide robust protection, offering a first line of defence.

Additionally, bullet-resistant glass is gaining traction across industries that were previously considered low-risk. Designed to absorb and dissipate energy from high-velocity impacts, it offers essential protection against vandalism, arson and violent attacks.

Economic Implications of Downtime

The financial impact of disruptions caused by explosions or forced entry can be devastating, often extending beyond immediate physical damage. Operational interruptions, asset loss and reputational harm can impact businesses, particularly in sectors where downtime directly affects customer trust and revenue. Organisations are increasingly prioritising robust entrances as a key element of their security strategy, recognising the critical role these solutions play in safeguarding business continuity.

Balancing Accessibility with Security

As society increasingly prioritises openness and accessibility, a delicate balance must be struck between fostering welcoming building ecosystems and addressing pressing real-world security threats. Striking this balance requires innovative solutions that integrate advanced security features without compromising a space's openness and aesthetic appeal. Organisations must design buildings that are not only safe and resilient but also aligned with broader societal values, ensuring they coexist with the need to protect people and property in an increasingly unpredictable world.

3

AI.

Artificial intelligence (AI) continues to be a significant focus in the security entrance industry. While it may sometimes feel overhyped, its transformative potential is only increasing, fundamentally reshaping how security is approached and implemented.

Practical applications of AI, such as predictive analytics, threat detection and the automation of time-intensive processes, are invaluable. Its capacity to handle and interpret large volumes of data makes it an ideal tool for managing complex environments such as airports, hospitals and corporate organisations. In these settings, where traditional security methods often fall short, AI delivers the advanced insights and efficiency needed to ensure safety and security at scale.

Predictive Analytics and Threat Detection

One of the most impactful applications of AI in security lies in predictive analytics and threat detection. Traditional security systems often rely on reactive measures - responding to incidents only after they occur. AI changes this dynamic by enabling a proactive approach. By analysing access control data and other security inputs in real time, AI-driven systems can detect trends and irregularities that could signal a possible threat.

Instead of waiting for human operators to notice these red flags, AI systems automatically flag them, prioritise the level of risk and provide actionable insights. This ensures faster response times and allows security teams to intervene before a situation escalates.

DID YOU KNOW?

The global AI in cybersecurity market is projected to grow from USD 25.35 billion in 2024 to USD 60.24 billion by 2029, at a compound annual growth rate (CAGR) of 19.02%*

*Mordor Intelligence. (2024). Artificial intelligence in security market report. Retrieved from https://www.mordorintelligence.com/industry-reports/artificial-intelligence-in-security-market

AI-Powered Innovations in Entrance Systems

Incorporating AI into entry solutions such as revolving doors and speed gates has ushered in a new era of intelligent security. AI can predict peak usage times, dynamically adapt functionalities and ensure efficient throughput without sacrificing safety. These capabilities enhance both security and convenience, offering a superior user experience while addressing operational demands.

Biometric authentication has also reached new heights. Beyond traditional fingerprint or facial recognition, advanced methods like vein pattern analysis and heartbeat recognition are integrated into high-security entrances. These innovations bolster access control for sensitive areas while maintaining a frictionless flow for authorised personnel.

Sustainable Innovation

Machine learning systems require significant computational resources, so their energy consumption and carbon footprint must be carefully managed. Developing energy-efficient models, optimising infrastructure and leveraging renewable energy sources are essential steps in reducing the environmental footprint of AI technologies. By prioritising these measures, organisations can ensure that the advancement of AI supports both technological progress and environmental stewardship.

Ethical Application

Machine learning models must be designed and implemented without bias. Bias in AI can lead to discriminatory outcomes, perpetuating inequalities and undermining trust in the technology. To mitigate this, organisations must prioritise diverse and representative datasets, transparent algorithms and continuous evaluation. At the same time, it is crucial to balance security with privacy considerations, ensuring that the pursuit of safety does not compromise individual rights or personal privacy.

The Human Element: Augmenting Decisions with AI

While AI provides immense power, humans remain central to effective security solutions. Smarter decisions are achieved when machine learning insights are paired with human judgment. The partnership between AI and human expertise creates a robust system capable of addressing complex security challenges. However, there is still an apparent hesitation to rely entirely on AI for decision-making without human oversight to validate those decisions.

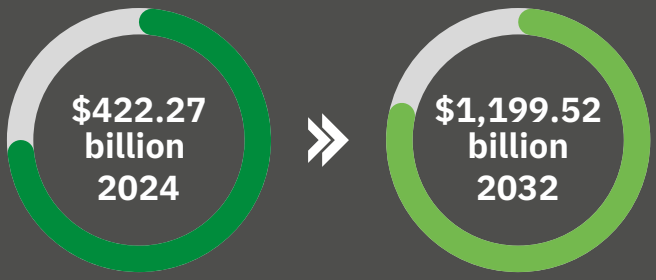
Ultimately, AI is not about replacing humans but empowering them to achieve more. By automating routine tasks, enhancing threat detection and improving response capabilities, AI enables security teams to focus on their core mission: protecting people, assets and environments. Despite its many advantages, AI is not a substitute for human expertise. Security professionals bring critical thinking, intuition and contextual understanding that AI cannot replicate. The most effective security strategies rely on this human-AI collaboration, where AI manages the heavy lifting of data analysis and automation while humans interpret insights and make informed decisions.

4 SUSTAINABILITY.

The demand for sustainable and eco-friendly solutions is becoming an increasingly important consideration in the security industry as organisations look to incorporate environmental responsibility. While security remains the primary focus, there is a growing recognition that sustainability plays a role in long-term business strategies. More companies are seeking solutions that balance security performance with energy efficiency and environmental impact, reflecting a shift towards a more responsible approach to operations.

True sustainability isn't just about recycling or reusing; it begins with designing products so reliable that those steps become secondary."

Amine Bouchareb
PRODUCT MANAGER - SECURITY ACCESS



In 2024, the global green building materials market was valued at approximately $422.27 billion.

It is projected to reach $1,199.52 billion by 2032, exhibiting a compound annual growth rate (CAGR) of 12.3%.

Retrofitting Security Entrances

Retrofits offer a cost-effective, sustainable way to upgrade security entrances, enhancing protection and efficiency without requiring a full replacement. By modernising access control and improving security, businesses can extend the lifespan of existing entrances while reducing waste and minimising disruption.

There are two main types of retrofits, each meeting different security and operational needs:

- **Modification** enhances an existing product's functionality, performance, or features without changing its core identity. For example, modifying an entrance door may include replacing sensors, finetuning security, or changing access control—allowing organisations to adapt to new requirements while maintaining their current installations.

- **Upgrade** involves significant changes to a product's performance, materials, or features, resulting in a new product classification. Unlike a modification, an upgrade alters the product enough to require a new product code. For example, upgrading a security entrance may involve replacing key components, integrating advanced technology, or improving structural elements to meet higher security standards.

Energy Efficiency and Eco-Friendly Materials

Modern security entrances are now equipped with energy-efficient motors, low-power IoT components and smart sensors that adjust operations based on real-time usage. These advancements reduce energy consumption and enhance the overall efficiency of security systems. Revolving doors also help regulate indoor climate by limiting air exchange, making them ideal for green building projects and energy-efficient ratings like NABERS and Green Star. Additionally, non-toxic materials are becoming a standard in security entrance designs.

These elements contribute to sustainability and align with corporate social responsibility goals, allowing companies to align their security investments with sustainability objectives.

Building to Last

Durable solutions reduce waste by minimising the need for frequent replacements. Companies are shifting away from quick fixes and adopting strategies that prioritise durability, reliability and minimal environmental impact. This isn't just about today's challenges - it's about building for the next 100 years and beyond. Investing in expertly crafted, high-quality products ensures long-term performance, security and a seamless user experience that stands the test of time.

5 THE NEIGHBOUR EFFECT.

Managing Security in Multi-Tenant Buildings

In multi-tenant buildings, the security needs of one tenant can be significantly influenced by their neighbours. Whether you are a building manager or a tenant, it is essential to consider how the surrounding businesses and occupants may impact your operations. Security challenges are no longer limited to individual organisations. For example, if a neighbouring business experiences threats - such as criminal activities, protests or other disturbances - it can directly affect your security. This issue is referred to as "The Neighbour Effect," which highlights the collaborative nature of modern multi-tenant environments.

Balancing Diverse Needs

Multi-tenant buildings function like small communities or "mini-cities", where each tenant has unique requirements and concerns. Some businesses may require high-security measures, while others choose multi-tenant options due to the connected business community. This diversity can lead to political tensions or heated discussions among tenants as building managers strive to maintain a harmonious balance. Clever placement of physical security solutions that manage the balance of hospitality and security can address these challenges.

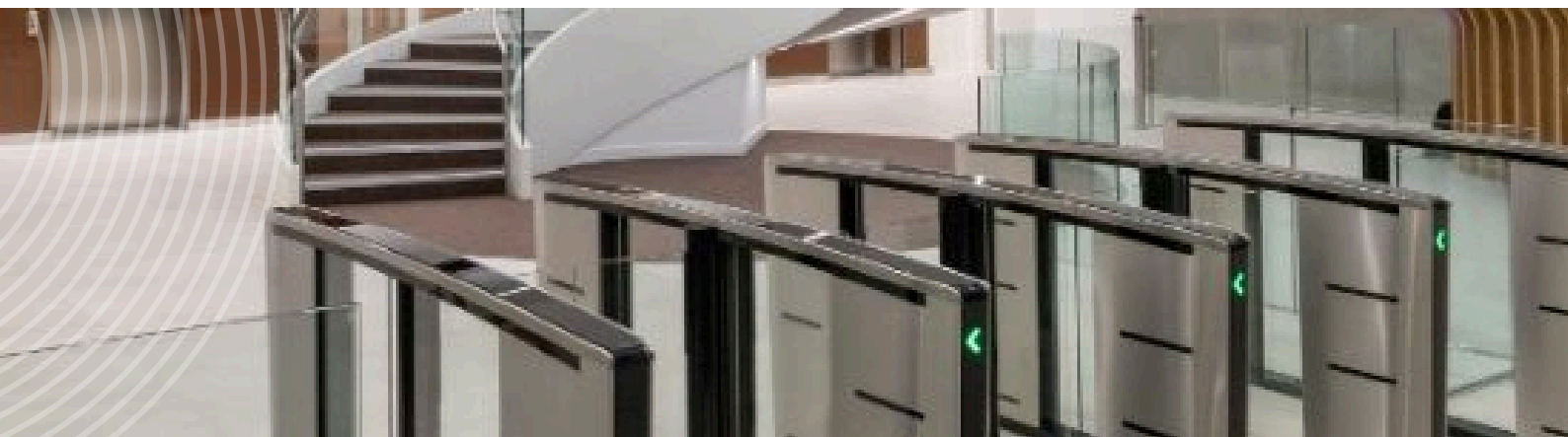
The Rise of Renting

Trends in commercial real estate show a shift from ownership to renting. Major organisations are increasingly choosing to lease spaces rather than own them outright. This shift can make buildings more vulnerable to security risks from neighbouring tenants, particularly as turnover rises and ownership structures evolve. It is crucial for building managers and tenants to adopt flexible security solutions that can adapt to changing occupancy patterns.

Threats from Within the Organisation

While external threats often dominate discussions, internal threats are equally significant. Disgruntled employees or former staff with lingering access rights can exploit vulnerabilities. To counter these risks, businesses need flexible and scalable solutions that facilitate the swift modification or revocation of access permissions, similar to how credentials are managed in digital environments like Microsoft systems.

Implementing physical barriers, such as Speedlanes on specific floors, adds an extra layer of security to buildings. These measures create a comprehensive defence system when combined with multi-factor authentication for digital access. The ability to quickly adapt to emerging threats - both physical and digital - sets genuinely secure organisations apart from those that are vulnerable.



6 IOT AND REAL TIME MONITORING.

The integration of Internet of Things (IoT) enabled systems is transforming how organisations address physical and digital threats. By leveraging innovative technologies, businesses can achieve continuous oversight, enabling real-time risk detection and response.

What is IoT?

IoT refers to a network of interconnected physical devices embedded with sensors, software and other technologies. By collecting and transmitting data via the internet, these devices support more intelligent automation and informed decisions. In security, IoT applications include real-time monitoring, access control and predictive maintenance for entry solutions.

Open Supervised Device Protocol (OSDP)

The digitalisation of hardware is transforming how products integrate with access control systems, resulting in greater efficiency and simplicity. Traditionally, connecting devices to these systems required multiple wires for power, communication and control, which led to complex wiring setups, installation and maintenance challenges.

However, advancements like OSDP are streamlining this process by enabling single-wire solutions for digital communication between devices. Instead of requiring multiple data cables, a single connection can handle multiple functions, significantly reducing physical infrastructure.

This enhanced interconnectivity allows products from different systems, such as access control, building management and fire safety systems, to work together seamlessly on a unified platform.

By reducing complexity and minimising the risk of errors during installation and maintenance, operations are simplified, setup time is shortened, and overall system management is improved, supporting smoother decision-making and control.

Enhanced Oversight and Monitoring

IoT-enabled systems empower organisations with comprehensive 24/7 monitoring capabilities. Sensors, cameras and connected devices work together to provide a seamless flow of data, delivering a complete view of security events as they unfold. This level of visibility allows security teams to quickly identify and assess potential threats, ensuring they stay one step ahead of possible breaches.

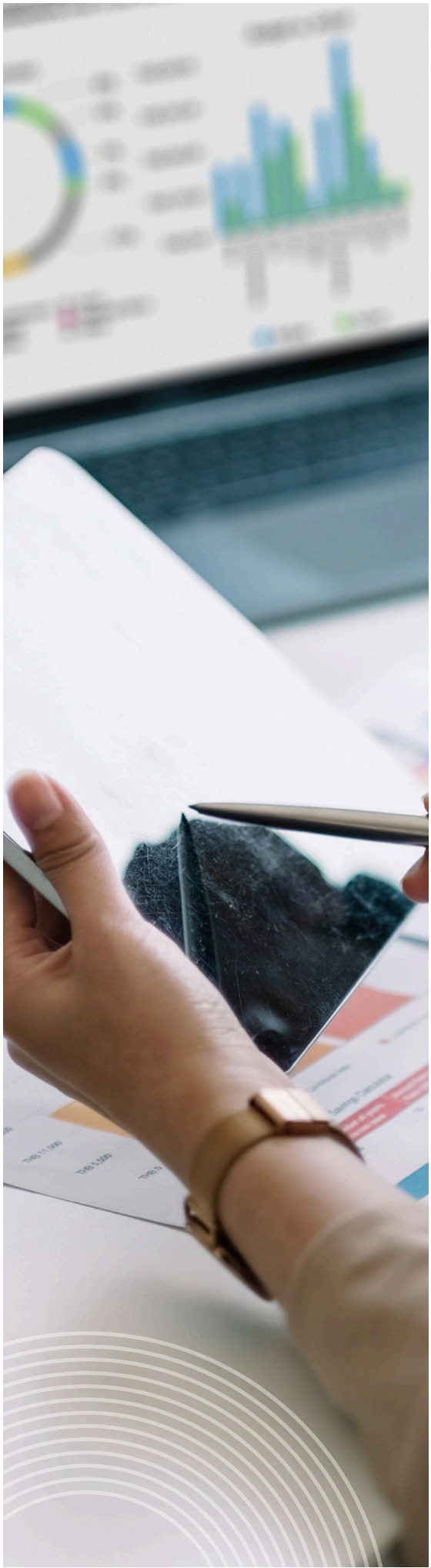
Remote Monitoring and Predictive Maintenance

In the evolving IoT landscape, remote monitoring and predictive maintenance have revolutionised the management of entry systems. Remote monitoring enables facility managers to track the status and performance of entry systems in real time by using advanced sensors and secure software integration. This connectivity provides immediate visibility into the health of revolving doors, security portal and speed gates.

Predictive maintenance, powered by IoT and machine learning, enhances this process by analysing data trends to forecast potential issues before they arise. Instead of waiting for equipment failures, predictive maintenance identifies signs of wear, irregular performance, or usage anomalies, enabling proactive servicing.

This solution maximises entry system performance by cutting downtime, fine-tuning maintenance schedules and increasing the longevity of key components. By addressing problems before they escalate, organisations can eliminate emergency repairs and unnecessary service calls, making maintenance more cost-effective.

Beyond operational benefits, remote monitoring and predictive maintenance offer valuable data-driven insights. By collecting and analysing usage patterns, facility managers can make informed decisions about optimising building operations and improving user experiences. This continuous flow of actionable data ensures that entry systems remain reliable, secure, and tailored to meet the facility's demands.



FUTURE-FORWARD.

AMINE BOUCHAREB

PRODUCT MANAGER - SECURITY ACCESS

Boon Edam's entry solutions are designed for the future - blending advanced security technology with flexible, space-conscious designs that create a welcoming and secure experience and address the evolving challenges of modern security.

By combining decades of expertise with a forward-thinking approach, we provide entry solutions that protect assets, enhance user experiences and inspire confidence.

The future of security entrances lies in seamless integration - merging physical and digital defences while embracing innovation and sustainability.

Organisations that prioritise these trends will be well-positioned to navigate an increasingly complex threat landscape.

> **"The future of security entrances lies in seamless integration."**

OUR REACH **IS GLOBAL.**

We have been in business for 150 years manufacturing premium aesthetic and security entrance solutions in the Netherlands, United States of America and China. We can confidently say that we cover every corner of the globe with subsidiary companies in major cities across the globe. Furthermore our global export division not only partner with our distributors, but also offer direct sales and service to every territory. This wide net allows us to have a strong global footprint as well as a personal grasp of local markets and their unique entry requirements.

To find your closest Boon Edam expert, please go to:
www.boonedam.com

Boon Edam Australia
T 1300 689 905
E info@boonedam.com.au
W www.boonedam.com.au

BOON EDAM
YOUR **ENTRY** EXPERTS.