Life is worth protecting

Securing critical infrastructure
for a more resilient society.



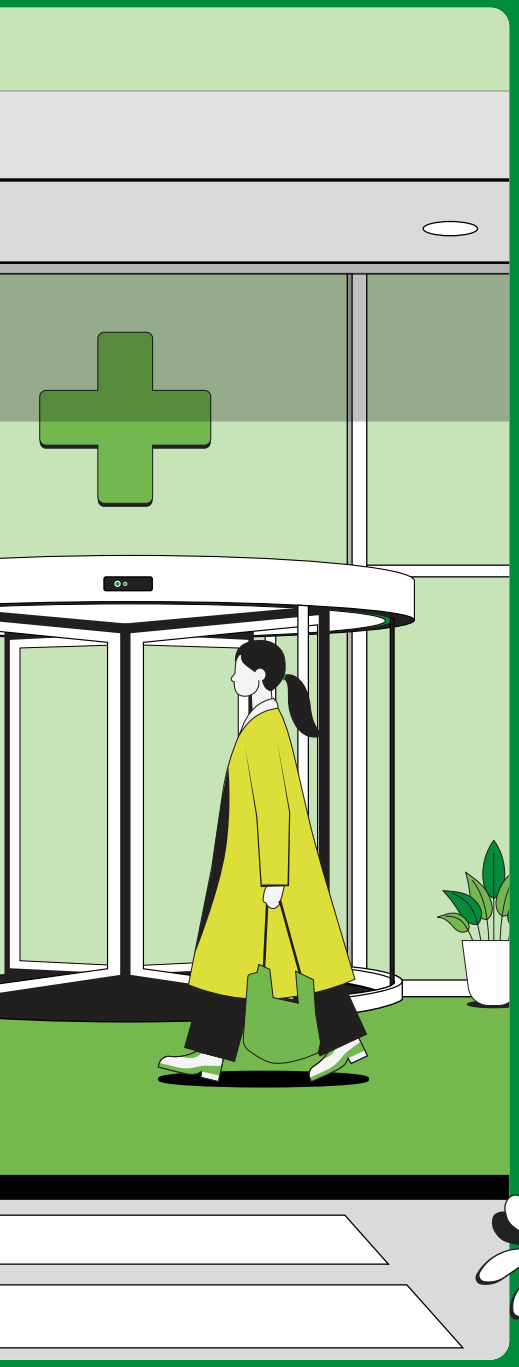
BOON EDAM

Life is worth protecting

Securing critical infrastructure for a more resilient society.

Why critical infrastructure matters	4 - 5
What is critical infrastructure?	6 - 7
Every critical environment is unique	8 - 9
Why movement matters	10 - 11
The changing threat landscape	12 - 13
How disruption spreads	14 - 15
Regulation, guidance & responsibility	16 - 17
Physical & cyber resilience	18 - 19
Ecosystem thinking	20 - 21
Physical access as strategic infrastructure	22 - 25
Modernising through retrofitting	26 - 27
The questions that matter	28 - 29
Preparing for tomorrow	30 - 31





Why **critical infrasturcture** matters

Some buildings protect more than business.

They support healthcare. Energy. Transport. Government. Communications. Data. Daily life.

They are part of the invisible infrastructure that quietly keeps society moving.

The lights turn on.
Trains arrive.
Hospitals operate.
Networks connect.
Emergency services respond.
Life moves forward.

Most people never think about the systems making it all possible. Until disruption occurs. Only then do we realise how dependent modern life is on the buildings, systems, and people operating quietly behind the scenes.

Today, critical infrastructure operators face growing pressure from:

- cyber threats
- geopolitical instability
- climate disruption
- operational dependency
- rising public expectations
- increasingly interconnected environments
- evolving regulatory requirements

Protection is no longer only about preventing disruption. It is about keeping essential services safe, reliable and available when conditions change.

That is why resilience has become a strategic priority: the ability to prepare, adapt, and continue delivering the services people depend on.

Security is no longer measured only by what organisations stop. It is measured by what they keep moving.

How people enter, access and move through critical environments is an important part of that resilience.



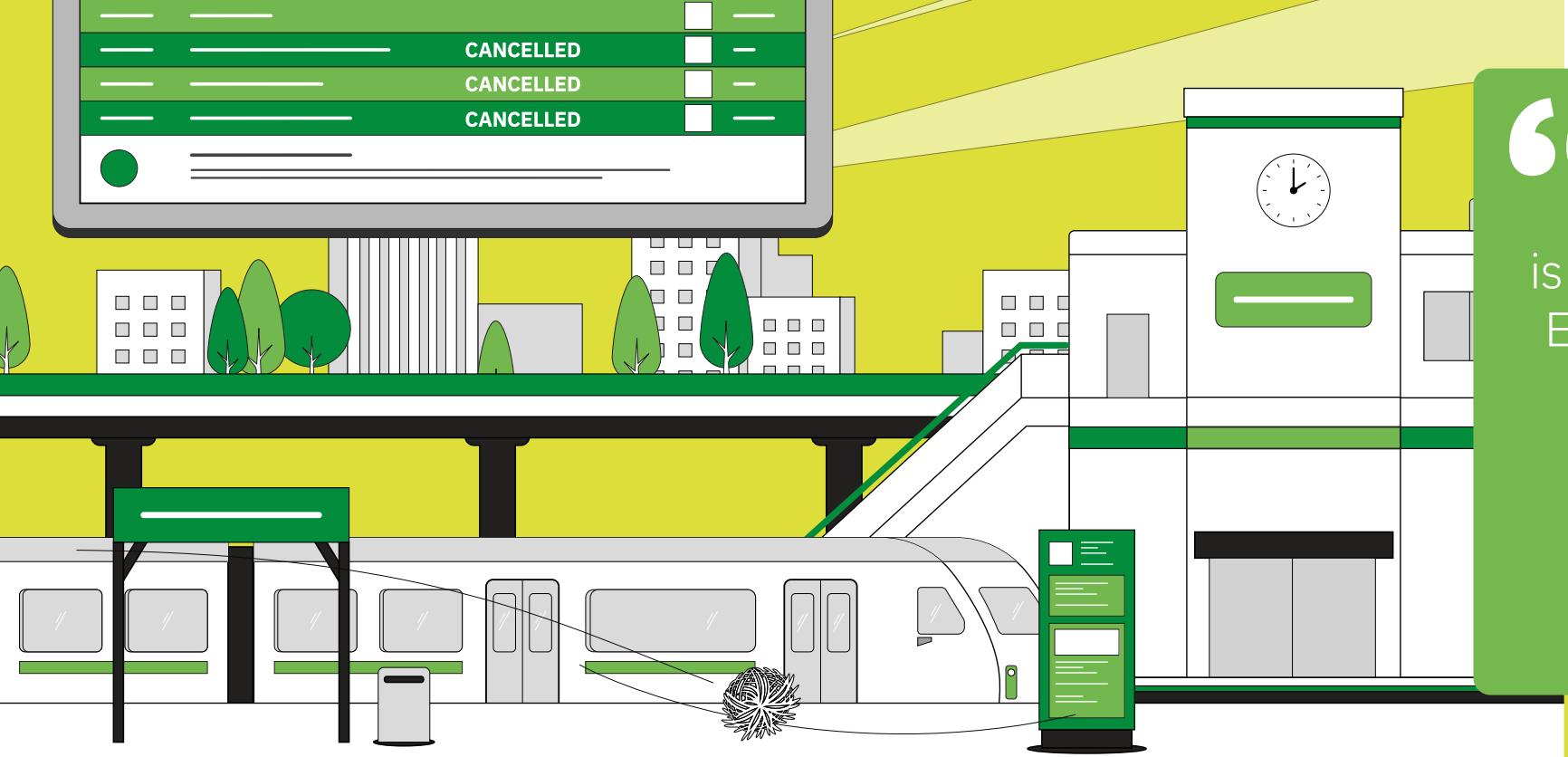
Preparedness begins long before disruption occurs. It begins with planning, collaboration and intelligent design. It begins with the decisions we make today.

Protecting critical infrastructure is a shared responsibility.
Every organisation.
Every facility.
Every decision-maker.

Together, they strengthen the resilience of the essential services society depends on.

> The strongest organisations aren't the ones with the most security. They're the ones that understand what they're protecting and what they are trying to prevent.

Neil Simons,
Sales Manager, Boon Edam UK



> “Critical infrastructure is not one market. Every sector has its own risks, operational priorities, and security requirements.”

Kurt Measom,
Group Business Development Manager,
Boon Edam

What is **critical infrastructure?**

The systems society depends on.

Critical infrastructure includes the essential systems, facilities and services that society relies on every day.

It supports:
- healthcare delivery
- transport networks
- energy and water supply
- communication and digital systems
- public services
- economic activity
- everyday life

It includes sectors such as:
- energy
- transport
- water
- food supply
- information technology
- telecommunications
- finance
- healthcare
- media
- government and public administration

Different sectors. Different risks.
One shared responsibility.

Every sector has its own operational challenges, but they share one defining characteristic:

When they are disrupted, the impact extends far beyond a single organisation.

A disruption can affect communities, supply chains, essential services and public confidence.

That is why critical infrastructure cannot be protected in isolation. Every decision about risk, access, technology, people and preparedness contributes to the resilience of a wider ecosystem.

Protecting critical infrastructure is therefore more than an organisational responsibility.

It is a responsibility to everyone who depends on it.

Every critical environment is **unique**

Different priorities.
One shared objective.

Every critical infrastructure organisation is working towards the same goal: maintaining essential services.
How that goal is achieved depends on the environment.

A hospital, data centre, airport and energy facility all require resilience, but each has different operational priorities, movement patterns and security requirements.



Healthcare
Maintaining patient care, emergency access and clinical continuity.

Data Centres
Protecting digital services, operational uptime and trusted connectivity.

Energy
Maintaining reliable services that communities depend on.

Transport
Keeping people, goods and networks moving safely.

Airports
Managing secure movement across complex, high-volume environments.

Government
Supporting public services, coordination, and public trust.



> “Every critical environment is different. The right security strategy starts with understanding how that environment operates.”

Kurt Measom,
Group Business Development Manager, Boon Edam

Why **movement** matters



Trusted movement through critical environments.

Critical infrastructure depends on the continuous movement of people, services and operations.

Movement is not simply about getting people from one place to another. It is an operational capability that supports continuity and coordination.

Security decisions should reflect how an environment actually works - from expected volumes and shift patterns to accessibility, movement routes and future operational needs. With security entrances often remaining in service for decades, today's decisions influence tomorrow's resilience.

Every movement decision is an operational decision.

But movement doesn't remain constant. People move differently under pressure. When familiar routines disappear, stress increases, movement patterns change and small points of friction can quickly become operational risks.

That is why preparedness means understanding how people move, respond and make decisions - both during everyday operations and when conditions change. Environments designed around people perform better under pressure.

Effective security doesn't create unnecessary barriers. It creates clarity, confidence and controlled movement.

The right people. The right spaces. The right time. The right level of protection.

> The right security strategy starts with understanding how people move through the environment.

Martin Oppitz, Sales Manager, Boon Edam Germany



The **changing** threat landscape

A world defined by uncertainty.

Critical infrastructure has always faced risk. What has changed is how quickly disruption can spread.

Critical environments are becoming more connected, more digital and more interdependent. At the same time, threats are no longer confined to a single domain.

A physical breach can create digital consequences.

Congestion at an entrance can delay operational response.

An access control failure can disrupt movement into critical operational areas.

The challenge is no longer understanding a single incident in isolation. It is understanding the wider consequences it can create. Disruption rarely stays where it starts. Its effects can spread across:

- people
- operations
- technology
- physical security

As a result, the role of security is changing.

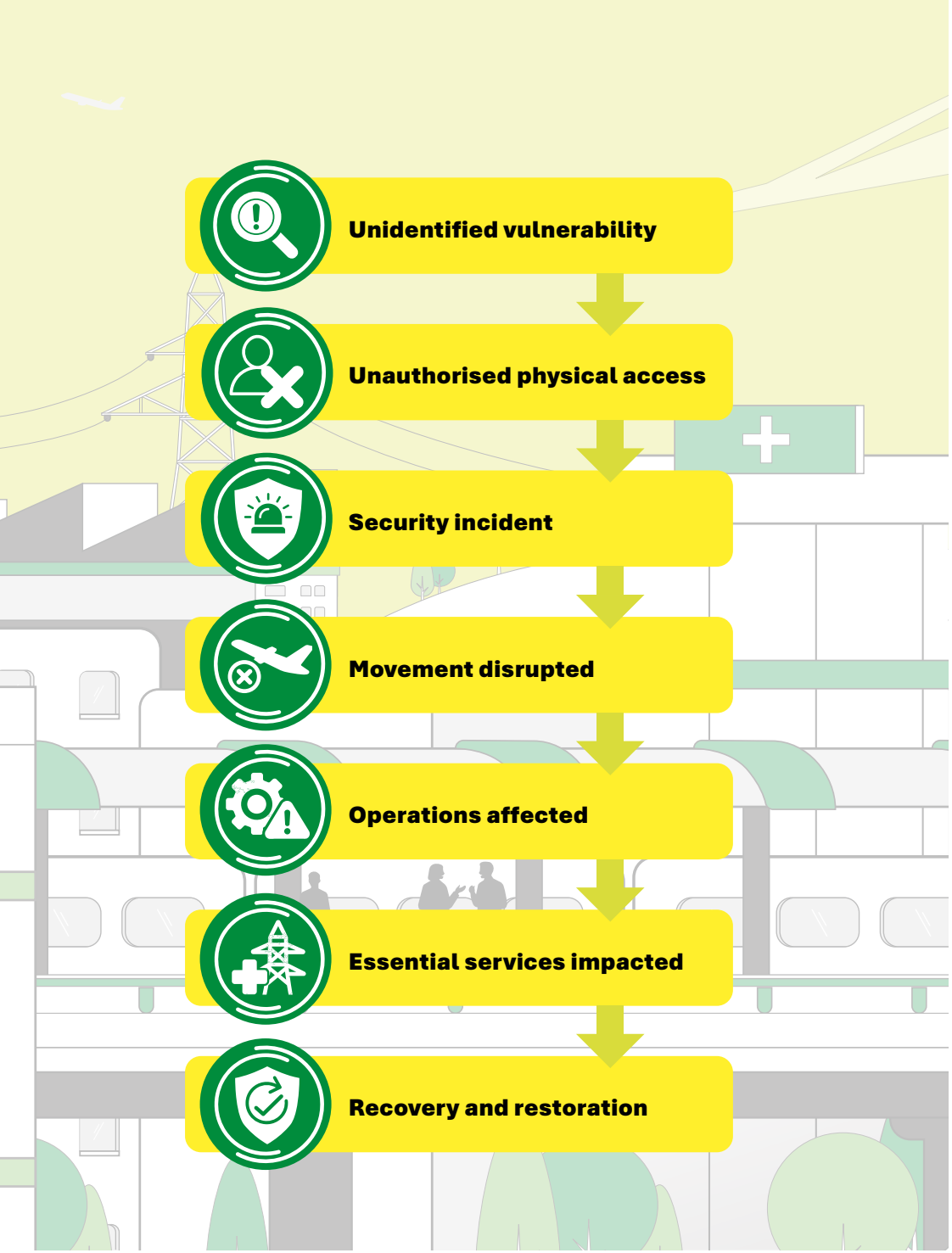
Security must now do more than prevent disruption. It must help organisations anticipate, adapt and continue operating.

The question is no longer whether disruption will happen. The question is whether your organisation is prepared when it does.



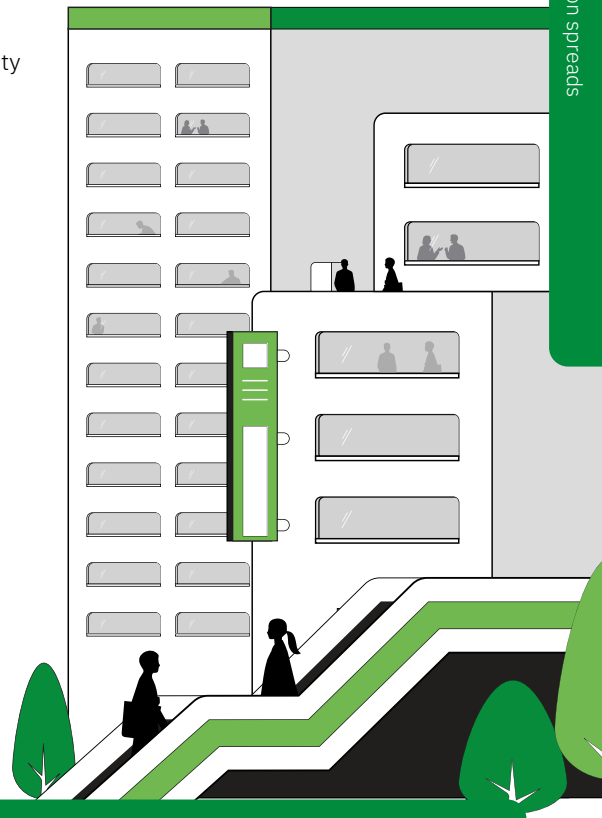
> “Today’s challenge isn’t responding to one threat. It’s understanding how physical security, cybersecurity and operational response all work together.”

Neil Simons, Sales Manager, Boon Edam UK



How **disruption** spreads

The impact of disruption can extend far beyond the initial event. One vulnerability can create consequences across an interconnected environment.



> Security isn't only about preventing unauthorised breaches. It's about what happens next if one occurs.

Neil Simons, Sales Manager, Boon Edam UK

Regulation, **guidance** & responsibility

Expectations are evolving.

Globally, expectations around critical infrastructure are changing. New and evolving requirements are placing greater emphasis on cybersecurity, physical resilience, risk management, operational continuity and incident preparedness. For organisations, understanding the landscape means more than knowing which regulations apply.

It means understanding **what they require, where responsibility sits and what action may be needed.**

How prepared is your organisation?

What do evolving requirements mean for your physical entrance and access strategy?

Complete the Critical Infrastructure Risk Assessment to assess your organisation's approach to security, resilience and operational preparedness.

Scan the QR code to get started.

Start the Risk Assessment

> Meeting requirements is one part of security. The real question is whether every measure supports the people, operations and critical spaces it is there to protect.
>
> **Martin Oppitz**, Sales Manager, Boon Edam Germany

European regulatory landscape

European Union

NIS2 Directive — EU legislation | Cyber resilience
Establishes EU-wide requirements for cybersecurity risk management, governance and incident reporting across essential and important entities.
What it means for organisations:
NIS2 goes beyond digital security alone. Its broader approach to cybersecurity risk means organisations must consider physical security and access alongside digital protection measures, strengthening cyber-physical resilience.

CER Directive — EU legislation | Physical & operational resilience
Establishes requirements to strengthen the resilience of critical entities providing essential services against a broad range of natural and human-caused threats.
What it means for organisations:
Critical entities identified under national implementation are expected to assess relevant risks and put appropriate technical, security and organisational resilience measures in place, supported by resilience planning.

Germany

NIS2 Implementation Act — National legislation | Cyber resilience
Implements NIS2 requirements within German law.
What it means for organisations:
Organisations within scope need to understand their cybersecurity obligations and ensure appropriate governance, risk management, physical security and incident response arrangements are in place.

KRITIS Framework — National framework | Physical & operational resilience
Germany's established approach to identifying and protecting critical infrastructure.
What it means for organisations:
It provides the wider national context to help organisations understand whether their infrastructure or services are considered critical and what responsibilities and protection requirements may apply.

KRITIS-Dachgesetz — National legislation | Physical & operational resilience
Germany's legislation strengthening the resilience of critical infrastructure and implementing key requirements arising from the CER Directive.
What it means for organisations:
Organisations within scope need to identify and understand risks to critical operations and strengthen the physical and organisational measures needed to prevent, withstand and recover from disruption.



> Cybersecurity may dominate the conversation, but every digital environment still depends on controlled physical access.

Martin Oppitz, Sales Manager, Boon Edam Germany

Physical & cyber **resilience**

Every digital environment still relies on physical access.

Physical security and cybersecurity have traditionally been managed as separate disciplines. Today, the boundary between them is increasingly blurred.

A physical breach can compromise information, systems and operations. A cyber incident can affect access control, surveillance, communications and other physical security systems.

The relationship works both ways.

European regulations increasingly recognise this interconnected approach. NIS2 acknowledges that cybersecurity risk extends beyond digital systems to the physical environments and access controls they depend on.

As critical infrastructure becomes more connected, resilience depends on understanding these dependencies rather than managing them in isolation. Physical security, cybersecurity, identity verification, intelligent access and operational visibility all contribute to a connected security ecosystem.

Together, they help organisations protect access, maintain visibility and keep critical operations moving.

Ecosystem thinking

Stronger security starts with the whole picture.

Critical infrastructure does not operate through independent systems. Buildings, people, technology and operations all interact.

Understanding these connections is central to creating a security concept that works for the whole environment.

That means looking beyond individual products and bringing together people who understand the environment – from operations and facilities to architecture, security, technology and physical access specialists.

A strong security concept considers:

- How the building is designed and used.
- How people need to move through it.
- What needs to remain operational.
- Where different levels of protection are required.
- How requirements may change over time.

Technology can then become part of a connected security ecosystem, rather than a collection of isolated measures.

The result is security shaped around the people, operations and environment it protects.



Physical access as **strategic** infrastructure

Trusted movement starts at the entrance.

Every secure environment begins with a decision.

Who should move forward?
Who shouldn't?

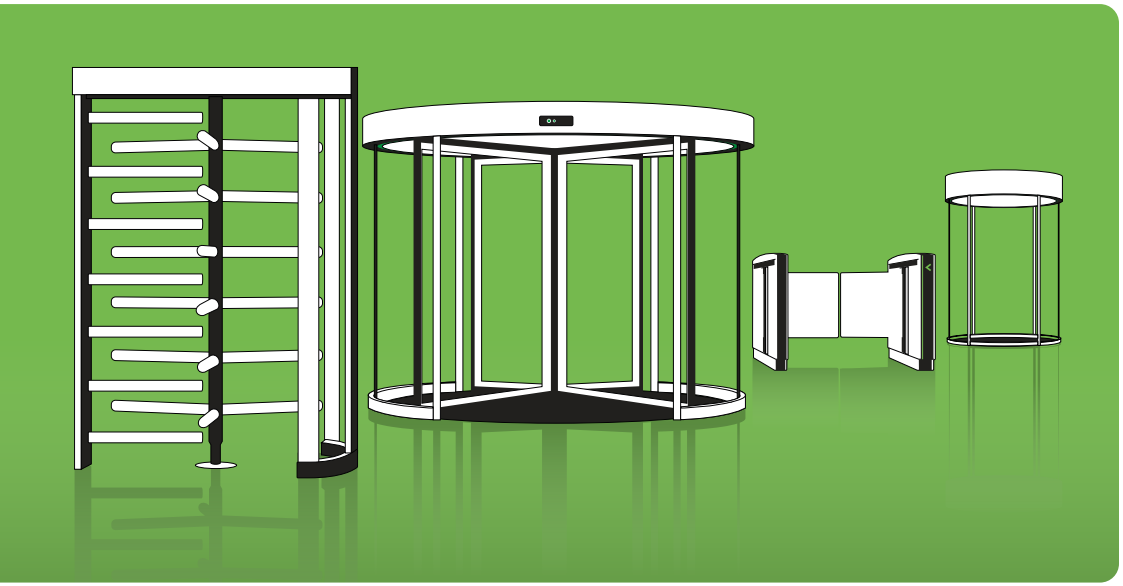
The entrance and access points are where those decisions become operational - where identity is verified, access is controlled and trusted movement begins.

In critical infrastructure, they form part of a wider network of access points and secure areas, helping protect critical spaces while supporting the movement of people and operations.

For more than 150 years, Boon Edam has been shaping how people move through buildings. Today, that experience helps us create entrance and access strategies that balance trusted movement, appropriate protection and operational needs.

Strong security should never slow the right people down.

When movement is managed effectively, people can move naturally and securely, while organisations maintain visibility, protection and operational continuity.



> A security strategy is only as strong as its weakest layer. Every access point, process and system must support the wider protection concept.
>
> **Martin Oppitz**, Sales Manager, Boon Edam Germany

Intelligent Access Control

Access control has evolved beyond managing entry and exit.

Connected access can provide greater visibility into who is authorised, where people are and how they move through an environment.

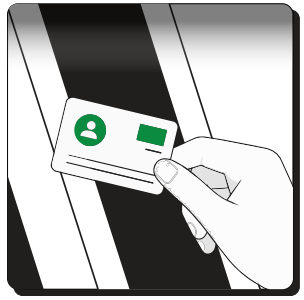
Modern access strategies can combine:

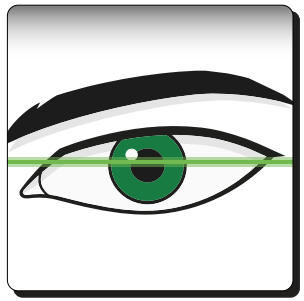
- biometric authentication
- digital and mobile credentials
- identity and access management (IAM)
- occupancy awareness
- role-based permissions
- access intelligence

When connected with systems such as video surveillance, visitor management, workforce management, building management and emergency response, access data can contribute to a clearer picture of what is happening across the environment.

Connected access creates connected awareness.

That visibility can support informed decision-making, greater accountability and more coordinated incident response.





Layered security strategies

Effective security applies the appropriate level of control as people move deeper into an environment. Each layer responds to a different level of risk, while working as part of the wider security strategy.

Public areas (low security)

Entrances, reception areas, and visitor spaces prioritise accessibility and intuitive movement while maintaining controlled, visible access.

Here, solutions such as revolving doors and accessible entrance systems can help balance welcome, movement and control.

Operational areas (medium security)

Site perimeters, staff entrances, administrative spaces and operational floors require greater accountability while supporting efficient day-to-day movement.

Security speed gates, perimeter gates and controlled entrance solutions can add stronger access control and identity verification without creating unnecessary friction for authorised users.

Critical areas (high security)

Control rooms, data halls, server rooms and other restricted environments require stronger identity verification and tightly controlled access to protect critical operations and assets.

High-security portals and security revolving doors can provide stronger physical protection, helping prevent unauthorised access and control movement into the most sensitive areas.

Together, these layers create progressively stronger protection while enabling authorised people to continue moving with confidence.

Turn insight into action

How prepared is your organisation? Assess your approach to access security, critical areas, operational visibility and preparedness with our **Critical Infrastructure Risk Assessment.**

Scan to complete the assessment.

Start the Risk Assessment

> Every layer should have a purpose. Most verify identity and act as a deterrent. Some provide stronger preventative protection. Together, they can create the time needed to respond if a breach occurs.

Neil Simons, Sales Manager, Boon Edam UK



Modernising through **retrofitting**

Preparing existing infrastructure for tomorrow.

Many of the critical infrastructure environments we rely on today were designed for a different era.

Security expectations have evolved, but replacing entire buildings or entrance systems is rarely practical.

Hospitals cannot pause patient care. Transport hubs need to keep people moving. Data centres, utilities and government facilities must continue operating while adapting to new requirements.

The challenge is to strengthen security without disrupting what already works.

Retrofitting enables organisations to modernise existing entrances and access strategies while maintaining continuity, extending infrastructure life and protecting previous investment. Existing environments can be strengthened through enhanced access control, biometric verification, intelligent monitoring, connected systems and targeted physical upgrades.





Why retrofit?

- strengthen security
- support operational continuity
- respond to evolving requirements
- improve visibility
- minimise disruption
- extend infrastructure life
- increase long-term adaptability

Preparing for the future does not always mean starting again.

Targeted improvements can help existing environments adapt to changing security and operational needs while making better use of the infrastructure already in place.

The future is not always built from scratch. Sometimes it is built on what already exists.

> Most critical infrastructure projects still involve existing buildings. The challenge is to strengthen security without compromising the way those environments operate.
>
> **Martin Oppitz**, Sales Manager, Boon Edam Germany

The questions that **matter**

Are you prepared for what comes next?

Preparedness starts with asking the right questions.

Not simply whether an environment is secure today, but whether it can adapt, respond and continue operating when conditions change.



- Can our environment adapt when conditions change?
- Can movement continue safely during disruption?
- Can emergency teams move without delay?
- Do we know who is in the environment and where?
- Can systems coordinate effectively under pressure?
- Are physical and cyber security aligned?
- Can we modernise without operational shutdown?
- Are we prepared for changing risks and operational demands?

> “The conversation shouldn’t start with ‘Which product do we need?’ It should start with understanding what we’re trying to protect and prevent, and how we balance that with environmental compliance and user needs.”

Neil Simons, Sales Manager, Boon Edam UK

Every organisation will answer these questions differently.

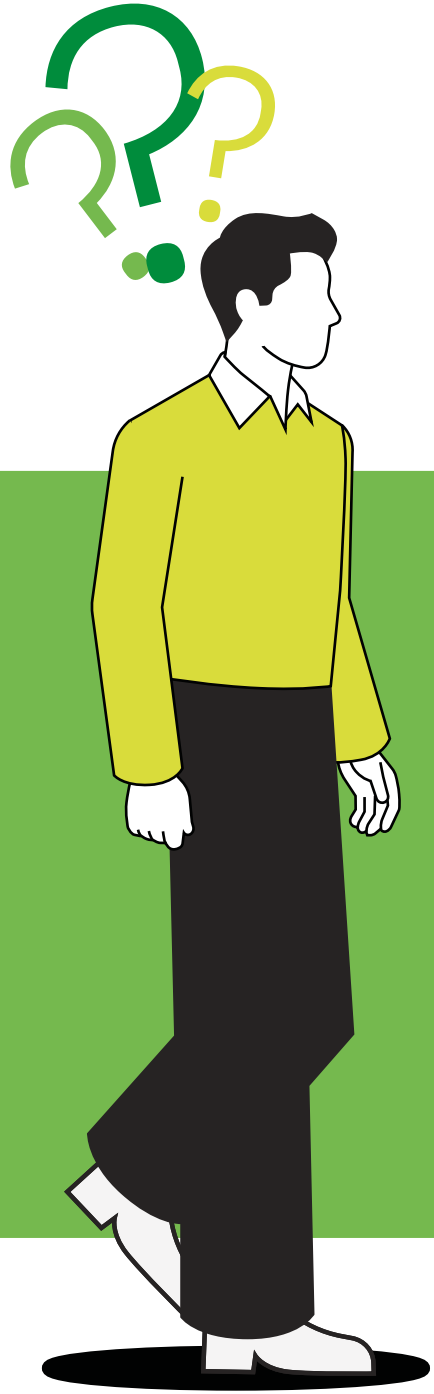
What matters is understanding where you are today - and where there may be opportunities to strengthen preparedness.

Turn insight into action

The **Critical Infrastructure Risk Assessment** provides a practical framework to assess your current approach to security, preparedness and operational continuity, and identify areas for further consideration.

Scan the QR code to assess your organisation’s readiness.

Start the Risk Assessment



Preparing for tomorrow

The future depends on the actions taken today.

Critical infrastructure keeps society moving.

It supports the services, systems and connections people rely on every day. Protecting them requires more than technology alone.

It requires preparation.
It requires collaboration.
It requires decisions made today with tomorrow in mind.

Every organisation has a role to play. The choices we make today influence how effectively critical infrastructure can adapt, respond and continue delivering the essential services people depend on.

The organisations best prepared for the future are those investing today in the people, processes and technologies that strengthen resilience over time.
So when conditions change, essential services can continue.

Communities remain connected.
People remain protected.
Life moves forward with confidence.

Because **life** is worth protecting

> The organisations best prepared for the future are those that have already planned how they'll continue operating when conditions change.

Kurt Measom, Group Business Development Manager, Boon Edam

Every environment is different. How prepared is yours?

You've explored the principles of resilient physical security. Now apply them to your own environment.

Assess.
Identify.
Improve.

Scan the QR code to complete the assessment.

Start the Risk Assessment

Want to discuss your results?

Our Critical Infrastructure specialists can help you explore your results, consider practical next steps and discuss the priorities unique to your environment.

Preparedness starts with understanding where you are today.

150+ YEARS
of experience

60+ COUNTRIES
across our global network

24/7
supporting the movement of people worldwide



BOON EDAM

boonedam.com/CI