

WHITEPAPER

Protecting data centres by layering physical security



GUNNEBO[®]
Entrance Control

“With threat levels around the world on the rise today, no matter what sort of sensitive data you’re trying to store, the critical part of it, is the environment it’s housed in.”

George Dionisopoulos, Head of Security at NEXTDC.



In the digital age, data centres are the silent guardians of our connected world. These mission-critical facilities house the technological infrastructure that powers our businesses, communications, and everyday lives. As the value and importance of the data they hold continue to grow, so too does the need for robust security measures.

Securing data centres goes beyond firewalls and encryption; it begins at the very threshold of these facilities. The ramifications of allowing a data breach can, and have been devastating to companies of any size. Besides the loss of confidence by business partners or customers that may entrust their data to you, there is often a significant financial fallout.

One proven way to steal data is to gain physical access to a network or servers. While strong firewalls and other cybersecurity measures can help prevent unauthorised logical access, hackers are more frequently breaking into data centres where they can easily plug into any IP connection — or steal a laptop or server and walk out with it.

With security often perceived as an afterthought, criminals have the potential to talk their way through even the most professional security guards, slip in behind an employee who politely holds the door open for them, tailgate through access control, or use stolen credentials to get into (and out of) a facility.

In the current climate, when cybersecurity teams are overstretched, intelligently supporting and managing data centre security challenges is critical. The same is true for data centre security admins, as threat actors learn new ways of launching and hiding their attacks, they will need support to be more proactive to defend their estate.

With an increased reliance on smarter technology and outsourced security services, the need for authorised and controlled access is vital. Here, compliance with legislation that covers security controls continues to grow in complexity and must also be addressed.

This white paper looks at how organisations can invest strategically in layered systems that help protect operational technology and guarantee physical security.

It poses the question: “How can a physical layered approach to data centre security ensure necessary protection as new categories of threats arise?”

By exploring various entrance control security solutions, such as access control systems, biometric identification, and integration, the white paper underscores how these technologies act as a powerful automated deterrent against intruders and provide a robust first line of defence for data centres.

Deploying physical security measures is offered as an essential way to mitigate this risk and comply with industry expectations for data centre security, with security entrance control as a core component of this strategy.

By producing this discussion paper, Gunnebo Entrance Control wishes to stimulate debate and encourage contributions from many voices. We look forward to engaging with you and your colleagues in this dialogue and would be pleased to share additional points of view and insights.

About the Author

Tina Hughan has a security focus spanning over two decades. She has worked for leading brands including ASSA ABLOY, with key responsibilities for Marketing and Sustainability across a large array of sectors, including data centres.

At Gunnebo Entrance Control, Tina strategically coordinates plans and develops data centre marketing strategies, which focus on how Gunnebo experts can support and guide risk assessments and layered security through a complete site to offer the ultimate protection to essential data.



Introduction

Staying connected has never been more important. As borders closed amid a global pandemic, people around the world turned to the internet for their daily work, entertainment and to stay in touch with family and friends.

It seems our habits have changed permanently. The internet, if it wasn't before, became the core foundation through which information is shared and consumed in today's modern society, with 40% using technology in new ways.¹

It's now estimated there are over 5.3 billion users in the world, meaning over 65% of the world's population has access.² This is expected to reach 6.54 billion by 2025.

So, it's no surprise the need for uptime operations in data centres is crucial as access to data becomes the basis of business continuity.

Operational sustainability³ and the centre's ability to meet long-term business goals including data centre security "to ensure the confidentiality, integrity and availability of housed data and services,⁴" is a significant influencing factor on the ranking 1-4 (the best-performing level) tier system data centres are allocated.

It's also unsurprising that data centres and the data they hold are attractive targets for criminals as one of the world's most valuable assets. Together with the data centres that hold and process it, they underpin almost all facets of modern life.

Threat actors are continuing to evolve their ways to try to hack access to the large and diverse amount of information that supports our global infrastructure and businesses. Cybercrime itself was up 600% due to the COVID-19 pandemic and is estimated worldwide to cost \$10.5 trillion by 2025⁵.

The opportunities for attack are diverse. Vulnerabilities in data centres include ownership, geography, physical perimeter, data halls, Meet Me Rooms (MMRs), supply chains, staff, visitors and cyber security in a concerted effort to breach data centres' defences tamper with sensitive information or disrupt critical services.



The first line of defence

It seems as though not a day goes by without a headline highlighting how an organisation, Government unit or business data has been breached. The biggest recorded remains Yahoo between 2013 – 2016 which affected over 3 billion user accounts⁶.

The common causes of data breaches are often weak or stolen credentials but coming equally close is the application vulnerabilities. Why bother with the complicated world of hacking when there are vulnerabilities on the site itself?

27% of data centres see the current security of their site as inadequate⁷ and in urgent need of updating. Organisations with a poor security posture are more likely to lose customers, alongside being scored to a low tier level.

Businesses that don't keep a tight rein on who has access to what within their organisation are likely to have either given the wrong permissions to the wrong people or have left out-of-date permissions around for a smiling hacker to exploit.

The same is true for insider threats. The rogue employee or the disgruntled contractor may have already been permitted to access your data; but what's stopping them from copying, altering or stealing it? Any unusual behaviour must be instantly recognised and revoked.

Guidance suggests⁸ a data centre must operate in a secure location, have limited entry and exit points and “a well-rounded threat protection strategy that accounts for all possible physical and virtual risks to the facility.”

Close to the core, is the entrance control, which lies in its ability to be the first line of defence against physical security threats.

By implementing effective entrance control measures, data centres can mitigate the risk of unauthorised access, theft, or sabotage. They ensure that only authorised personnel gain entry, reducing the potential for data breaches and physical security incidents.

Entrance control solutions often integrate with access control systems, providing real-time monitoring and audit trails, enhancing compliance with regulatory requirements, and providing invaluable data for forensic analysis in the event of a security incident.

Regain Physical Security Control

To combat these diversified threats, operators need to approach data centre security holistically and early on.

By bringing together the physical, personnel and cyber security of data centres into a single strategy, security and facility managers can better withstand the diversified methods state threat actors, cybercriminals and others may use to attack them.

There is no one-size-fits-all approach to holistic data centre security. Every data centre operator will need to consider their risk assessments prior to the design and installation of critical security infrastructure.

Data centre operators and their customers should both have individual risk management strategies designed to protect their critical assets and systems.

It will need to be based on understanding the risks and protective security strategies available to mitigate the individual risks and consider worst-case scenarios to enable every consideration of how a threat actor could manipulate the system and gain access.

As a basis to consider, the National Protective Security Authority, identified seven areas of risk from which attacks can originate and these should be factored into an overarching risk management strategy.⁹ These include:

- Geography and ownership security
- Datacentres physical perimeter and buildings
- The data hall
- Meet-me room considerations
- People security considerations
- Supply chain considerations
- Cyber Security

Continued over the page >



From the perspective of the physical perimeter and buildings, it states “data centre owners should be able to demonstrate a robust layered approach to physical security at their sites, including perimeter and buildings.”

Any risk-based assessment should consider the entire site of the data centre, right from the perimeter protection, In the ever-evolving landscape of data centre security, entrance control remains an indispensable component, safeguarding the integrity and continuity of digital operations in an increasingly connected world.

Internally, every angle should be considered from a security perspective, incorporating physical layers of mechanical, electromechanical, electronic and digital solutions – all using powerful biometric, RFID and cloud capability.

Once security measures are in place, there is an essential priority to maintain and monitor security to ensure systems are optimised to protect from the latest cyber security attack methods, themselves constantly evolving.

¹ The Internet and the Pandemic: Paw Research Centre, Published September 1st 2021: <https://www.pewresearch.org/internet/2021/09/01/the-internet-and-the-pandemic/>

² Demand Safe Internet User Statistics in 2023 – (Global Demographics) <https://www.demandsage.com/internet-user-statistics/#:-:text=There%20are%205.3%20billion%20internet,has%20access%20to%20the%20internet.>

³ What factors are considered for data centre tier classification? <https://phoenixnap.com/blog/data-center-tiers-classification>

⁴ Guide to data centre security: <https://phoenixnap.com/blog/data-center-security>

⁵ Cyber Security Statistics The Ultimate List of Stats Data & Trends for 2023: <https://purplesec.us/resources/cyber-security-statistics/>

⁶ 10 of the biggest data breaches in history, updated July 14 2023: <https://dataprot.net/articles/biggest-data-breaches/>

⁷ Cyber Security Statistics. The Ultimate List of Stats, Data and Trends for 2023: <https://purplesec.us/resources/cyber-security-statistics/>

⁸ Data Centre Security: Physical and Digital Layers of Protection. Published August 3 2023: <https://phoenixnap.com/blog/data-center-security>

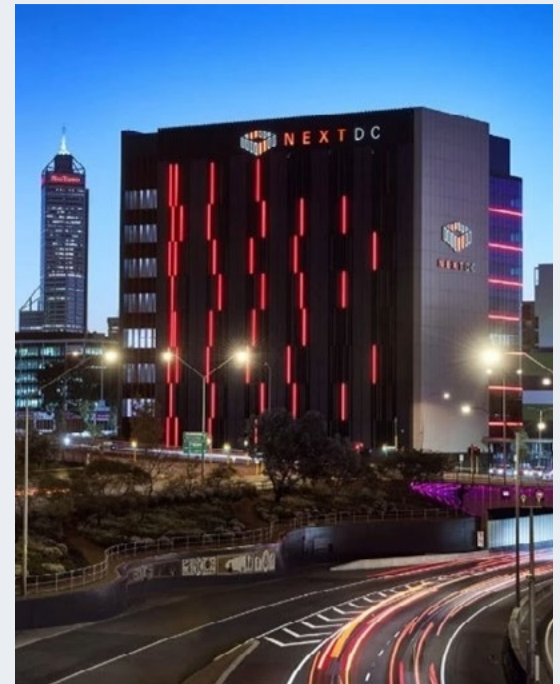
⁹ 7 Areas of Risk: Data Centre Security: Guidance for users: <https://www.npsa.gov.uk/data-centre-security-users>



CASE EXAMPLE:

NextDC

NextDC is Australia's leading data centre as a service company, designing, constructing and operate data centres across the country. Currently operating 10 data centres in all major capital cities as well as a number of regional centres, certified to Tier III and Tier IV standards for design documents, built environments and Gold Operational Sustainability.

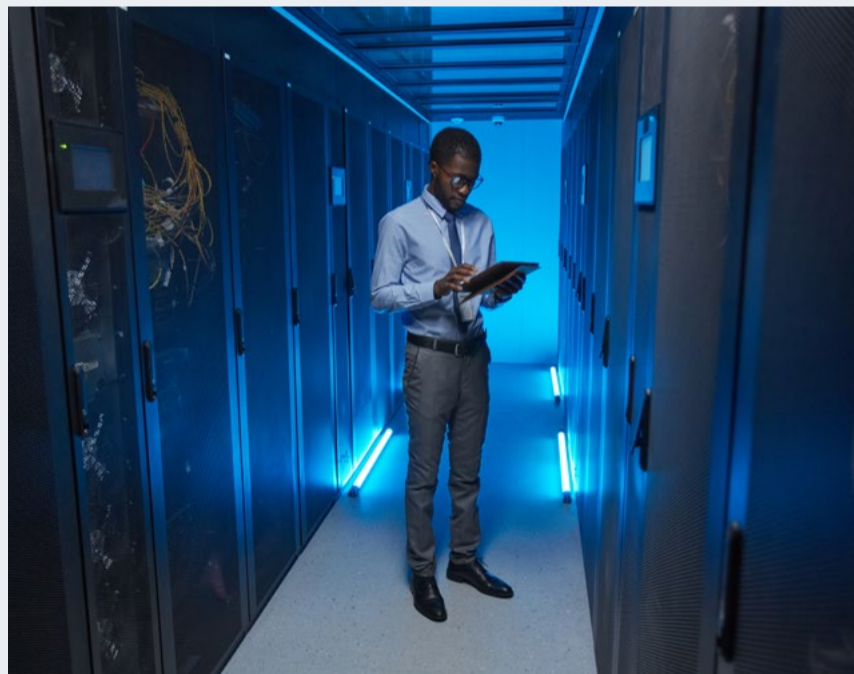


Recognised by the Government as a critical infrastructure from July 2021¹⁰, NEXTDC is also certified to the highest strategic level across all of its sites. To maintain this high standard, its data centres rely on a range of security products, protecting the complete sites and their assets.

As David Dzienciol, NEXTDC Chief Customer & Commercial Officer explains: 'This level puts NEXTDC in a class of our own with respect to delivering services that are sovereign and secure.'

NEXTDC works with Gunnebo from the security specification, to ensure design and installation can offer the ultimate protection. On entering the facilities, staff and visitors are met with the Gunnebo "hostile vehicle mitigation system," and then it forms into the next barrier: a secure guardhouse fitted by Gunnebo with bullet-proof glass.

Gunnebo's revolving security doors present a three-step verification process including biometrics, RFID and a pin-code. These sophisticated doors also offer single-person detection, anti-hostage threshold, bullet-resistant safety glass and high-accuracy verification through an inbuilt reader.



Gunnebo has provided further security doors and partitions at other points within these data centres, together with electronic surveillance systems.

On the way out of the facilities, there are security measures in place, like the spike tech grip which manages the flow and also negates any capability for persons to tailgate in through the precision exit gates.

With further lockdown options, teams and visitors can be assured of access only to where is required temporarily to provide the ultimate peace of mind for them and the security of the data centres and their assets.

“Security is often not prioritised during the design phase and is usually an afterthought, but it is a fundamental piece in delivering critical infrastructures and the security of the environment.”

George Dionisopoulos, Head of Security at NEXTDC.

99

¹⁰ Protecting the cloud is top priority for data centres: <https://www.gunnebo.com/gunnebo-stories/nextdc/>

Summary

Jeff Weiner famously wrote, “data really powers everything that we do.” In a world where data centres increasingly serve as the core component of our interconnected world, proactively safeguarding these critical facilities has never been more paramount.

Whilst the industry may still see security as an afterthought, not responding to the heightened risks and vulnerabilities of sites across the globe has been seen to have devastating effects.

Big eco-system brands, including Yahoo, VISA, Equifax, Facebook and Marriott have suffered breaches. With the extent of potential financial and reputational damage, data centre owners and operators need to ensure they leave no stone unturned in their pursuit to minimise downtime. Implementing robust security measures, both physical and digital, must be an integral part of the facility’s design, construction and operations.

Security should permeate every aspect of data centre planning, starting with entrance control and including access control, network security, surveillance, and disaster recovery. By making security a foundational principle, data centres can better protect their assets, maintain regulatory compliance, and provide their clients with the confidence that their data is in safe hands.

Data centres should also recognise that security is an ongoing commitment, not just a one-time installation.

To safeguard against ever-evolving threats, they must continually monitor security measures. Regular maintenance ensures security systems remain in optimal working condition. It embraces future-proof smart options including cloud and IoT technologies that can offer continuous detection from anywhere and address and resolve vulnerabilities in real-time.

Security should evolve alongside emerging threats and technologies, adapting to stay ahead of potential risks. By making security an ongoing, dynamic process, data centres can ensure the longevity and effectiveness of their protective measures, providing the highest level of confidence in the safety and integrity of their operations and data.

There is an understanding of the budget, time and resource-

stretched Facility and Security Managers looking to instigate security alongside several competing priorities. Here, scalable technology investment does not have to undermine the humanity of the physical security experience, but rather, be used to elevate as a data centre grows.

Security administration processes feel seamless to the visitor and add to the peace of mind experience that data centre complexes are safe and secure throughout a visit or working period from the moment a person enters a complex to the second they leave.

Data centres that take the time to understand the new dynamics, and see the need for a layered approach to physical security where entrance control security is far more than just a physical barrier, will survive and thrive in comprehensive data protection.

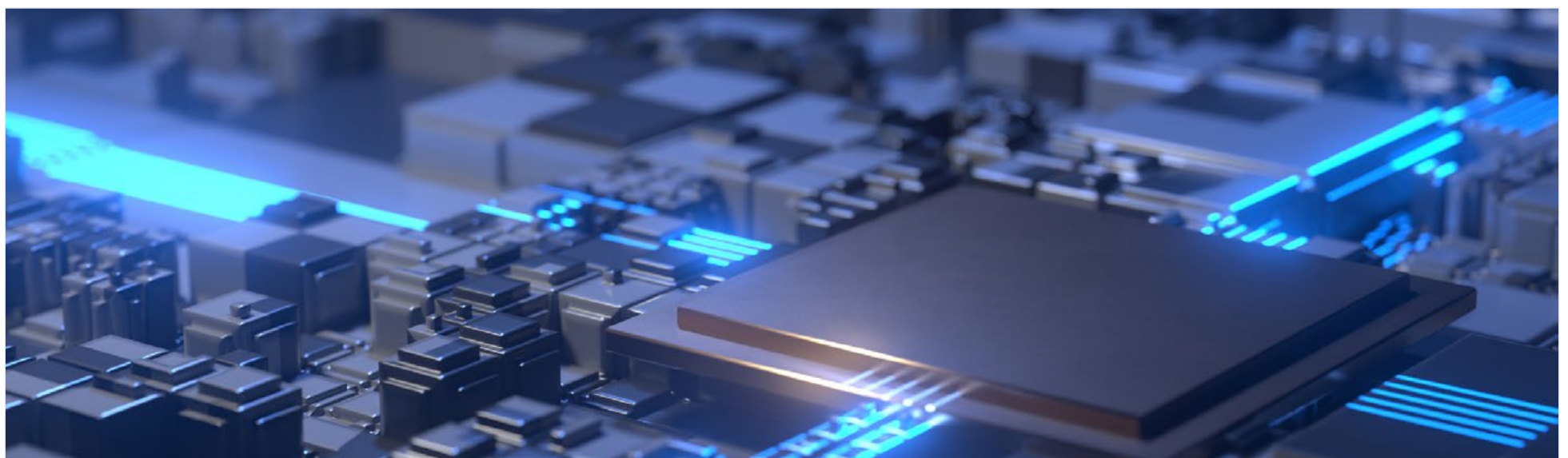
Says Adam Scully, NEXDC Vice President of Customer and Commercial Operations: “The defence in-depth that we provide in all of our security layers gives customers peace of mind and knowing that their data is safe.”

Behind the scenes, Gunnebo Entrance Control is ready to support data centres to ensure the right security risk assessment and measures are in place.

As David Dzienciol of NEXTDC explains, “Selecting the right partner at the start of any construction phase or any build is integral to your overall success. This is why we’ve partnered with Gunnebo as they aligned with our overall vision and strategic goals.”

Experience counts and as we look to the future, with emerging technologies and evolving threats on the horizon, it is clear that entrance control security will continue to be at the forefront of data centre protection.

The commitment to maintaining, monitoring, and evolving security measures is paramount. Only by making entrance control security an ongoing, dynamic process can data centres guarantee the safety and resilience of their operations and data in an ever-connected world.



How can Gunnebo Help?

As we navigate an increasingly digital world where data centres play a pivotal role in our daily lives, the need for robust entrance control measures has never been more critical.

The challenges data centres face are multifaceted, from the ever-evolving threat landscape to the complex web of regulatory compliance. Entrance control solutions, such as access control systems, turnstiles, security revolving doors and security portals, serve as the first line of defence against these challenges.

They ensure that only authorised personnel gain access, mitigating the risk of data breaches, physical security threats, and unauthorised entry.

Gunnebo's innovative approach to entrance control security, as explored in this white paper, empowers data centres to rise to these challenges effectively. With sophisticated technologies, scalable solutions, and seamless integration capabilities, Gunnebo Entrance Control offers data centres the tools needed to bolster their security posture while optimising operational efficiency.

The benefits of implementing Gunnebo's entrance control solutions are evident: enhanced security, streamlined operations, and regulatory compliance. Real-world case studies highlight the success stories of data centres that have enhanced their security with Gunnebo's solutions, underscoring their effectiveness in diverse environments.

Gunnebo Entrance Control operates in long-term partnership with its customers, taking the time to understand individual sites for their vulnerabilities and bespoke requirements. This enables Gunnebo to offer continuous support and advice on the latest entrance control solutions that can protect against emerging threats, all with no compromise to aesthetics, quality or compliance.

For more on how Gunnebo can help protect your data centre and ensure total protection, safety and excellence for your critical infrastructure, please visit: www.gunneboentrancecontrol.com/en/data-centers



About Gunnebo

Gunnebo Entrance Control, the global provider of entrance control solutions, has proven its capability to work with data centres to improve critical infrastructure protection and the physical security of high-risk sites.

With a commitment to innovation and precision engineering, using the latest Gunnebo entrance control technology can increase security, future-proof buildings, and deliver automated, touchless efficiency.

Turnstiles, speed gates, and barriers can provide data centres with a robust defence against unauthorised access while allowing seamless entry for registered personnel.

With Gunnebo, data centre operators can achieve optimal security and operational efficiency, safeguarding valuable assets as they continue to play a pivotal role in an increasingly digital world.

Our solutions are always tailored to customer needs and requirements, providing the most value and impact on their business. Gunnebo is a global organisation with local network support working to define processes so that we can always be with our customers and operate as a partnership.



For more information on Gunnebo's range of entrance control solutions, please visit www.gunneboentrancecontrol.com

