



# Streamline physical security to enable data center growth in the era of AI

A world-class physical security program, can absolutely be a competitive advantage in the race for AI dominance



# Introduction

AI is the new space race for datacenters, and consistency at speed is the rocket fuel colos and big data companies need for reaching orbit. Everything you know about physical security is still relevant—but it won't matter unless you have the right plan and partnerships to scale up without sacrificing quality. If growth isn't utterly intentional, you risk being an also-ran instead of a competitor. Only a flexible, scalable security business plan and optimized end-to-end best practices will enable your AI-ready datacenter business to succeed.



# The future of datacenters is today

You know it: The next big thing in datacenters is already here, and it's a whopper. If cloud computing was the blockbuster movie we all saw ten years ago, AI is the mega film festival that's now on screens everywhere, every single day. 2021 saw more than 100 hyperscale datacenter construction starts, and the number is climbing steadily. Where the global datacenter market was around \$187 billion in 2020, it's on track to surpass \$517 billion by 2030 (AMR), driven mostly by AI demand. At ZBeta, we've seen this firsthand: one Fortune 15 client has more than 250% of net-new megawattage on its docket for 2024 than it had just two years ago.

Building your business to compete in this market means planning and executing on a new level. The good news is, if you're already adept at delivering cloud capacity, you're positioned for success—at least for now. But as you scale up, your tolerance for error quickly reduces to zero, because only the error-free players are going to edge out their competition. It's not as simple as turning up the production dial. You need a thoughtful, rigorous framework that takes everything you know about datacenters and elevates it to address the added physical security risks, change agents, and design impacts that come with AI. These changes can range from new hyperscale considerations to newly robust security requirements that address emerging threats facing tech giants, nation states, and other entities whose protection of AI compute power can have massive impact across the world.

You're no longer going from A to B; it's A to Z and beyond, at a rate so rapid you can't afford to let these and future change factors break your stride. You don't have time to evolve organically. Your business needs to not only speed up—it needs to mature. ZBeta helps its client partners do this every day, and we've done it more than ever these recent years, so we wanted to share some of our key learnings.



# Think beyond delivery

The first step in maturity is expanding how you think about your delivery model overall. Every business is an economy of projects, but at some point those projects must coalesce into larger, program-level functions. Building an AI datacenter design and production capability entails implementing an innovative, fast-moving program based on everything you know about individual projects, and then finding ways to deliver them at new levels of market expectation.

Global datacenter market growth rate  
will be **270%** by 2030,  
projected to reach **\$517 billion**  
in capitalization

Source: [Allied Market Research](#)

Intelligent re-use of project elements, including toolsets, IP libraries, and best practices, has never been more important. Each project in your program sets a precedent for the projects that follow it, so rapid growth will depend on repeating and compounding as much knowledge and information as possible and putting it to use with clarity and agility. Customizable work packages and accessible program knowledge bases, together with constant vigilance for new work that can be packaged and repeated, are essential for escalating smooth operations.

As part of this, the ways your physical security team uses BIM technology must be tested for going the distance. Applying 3D modeling and digital twin capabilities in tools like Revit to visualize new spatial conditions isn't just beneficial, it's table stakes. What matters is how adeptly you can streamline BIM processes by leveraging intellectual property from past projects or a shared volume of client use cases.

Reusable IP for AI datacenters includes:

- + Standardized, yet adaptable, Revit/BIM templates and families
- + Data-driven libraries for project details and system diagrams
- + Toolsets for automated load calculation and system programming

Build your program to last. Make all steps repeatable—even when they're bespoke or when you use them to effectively manage exceptions. Structured and sophisticated change and exception management tools are essential to success in the AI datacenter vertical. Treating your business as an integrated, well-oiled delivery machine will enable you to build a durable, world-class program that serves your business needs going forward, all while meeting existing and future standards of excellence in accuracy and design.

# Evolve your notion of requirements

AI-scale development affects all four points of the project control compass—requirements, budget, resources, and time. Of these, the requirements you proceed from will need the most special attention because they often pertain to emerging technologies or design approaches, and enter the project dynamically rather than as part of any boiler plate you start out with. A good security partner owns each client’s program and regulatory requirements, maintains tight fidelity to policy, and dispenses with curve balls in an organized, systematic way. Keeping forward momentum while preserving the integrity of your design means knowing new requirements holistically—not just the fact of each one, but its intent, as well as its impact on the larger requirements ecosystem.

Also important is differentiating between the types of requirements and taking action accordingly. On one hand are the obligatory policies, standards, and regulatory mandates that serve as a project baseline and that you know up front must be incorporated. But elsewhere you have the issues and exceptions that arise over time. New requirements are frequent, often driven by what started as exceptions, and with multiple projects in flight at once, agility means triaging to assess impact, update build books, and roll out the requirements to active design and construction efforts.

And then there’s orchestration. With AI, unprecedented scale will invariably tax the capacity and performance of current solutions. Along the way, other changes continue: clients require higher levels of identity and access assurance; threat vectors expand to include threats that originate in the air (drones) as well as vulnerabilities from data bearing devices and the ability to detect them. The complexities inherent in these many moving parts need creative problem solving, novel integration approaches, and true proof-of-concept capabilities.

In this way, innovation breeds innovation. If a new cooling technology runs on a chemical the client hasn’t used before, you’ll need to understand its physical properties and plan storage and security accordingly. If a client uses new sustainability practices to make datacenter construction more ecologically sound—such as updated specifications for power-efficient equipment and architectures, or solutions that make granular use of building system data for occupancy insights—you’ll be counted on to design new security capabilities for these as well. And as these changes arise on the requirements side, you’re challenged to adapt and keep going. There’s no slowing down for design dilemmas or avoidable RFIs. Every project must be done right, on time, the first time—now more than ever before.

Meanwhile, how you use the tools and processes you rely on must evolve as well. The trick with repeatable IP has always been taking work you’ve done before and putting it in motion confidently and strategically, so you can focus your assessment powers on project parts that are new or unknown. But if this ratio was 80/20 before, AI scale has pushed it closer to 95/5. Because security technology design responds to architecture and operations, supporting and enabling this “shrink the denominator” goal means readily recognizing the 5% while executing the 95% in ways that are seamlessly accurate and efficient.

To put it simply, success with the 95% will speak to how well you’ve organized and refined your processes and subject matter knowledge, of both the client’s environment and of enduring physical security techniques. And in that remaining five percent must live the capability to flex and respond to innovation, coming from either your clients, your own design team’s ingenuity, or the ever-changing laboratory of the data technology market.



**Shrinking the denominator:** Maximize the scenarios where rules can be universally applied, and minimize the scenarios where work-arounds are needed. Mature agility means identifying bespoke, high-risk deliverables—and then somehow making their delivery repeatable and rote.

# Supercharge your success factors

As with any growing business, the benefits of your process are measured by how you roll with change. Every new requirement is an opportunity to advance datacenter quality, not just for your business but for the entire industry. You make your success sustainable and repeatable as long as you can keep pace with innovation and the changes it imposes on physical security requirements and design.

When you deliver spaces for AI, the margin for error and compromise is narrower than it's ever been. Next-level performance is necessary. If you don't have a plan for hitting all of the hallmark success factors, you can't design physical security for datacenters at AI scale. And in the pursuit of speed and growth, if you dilute your original formula for success, you're not going to get results.



Invest in physical security partnerships that offer dual expertise—deep subject matter knowledge, and the adaptability to master your unique style and requirements.

Two capabilities will separate laggards from world-class AI players in the datacenter market: automation of design, modeling, and QA functions; and scrupulous, intuitive attention to the details that impact success. Having the confidence to orchestrate smooth, intelligent physical security operations generates the frictionless productivity you need for pulling ahead of your datacenter competition.

Know your success factors, and double down. It's all in service of letting consistency and continuous optimization drive the momentum of your work.

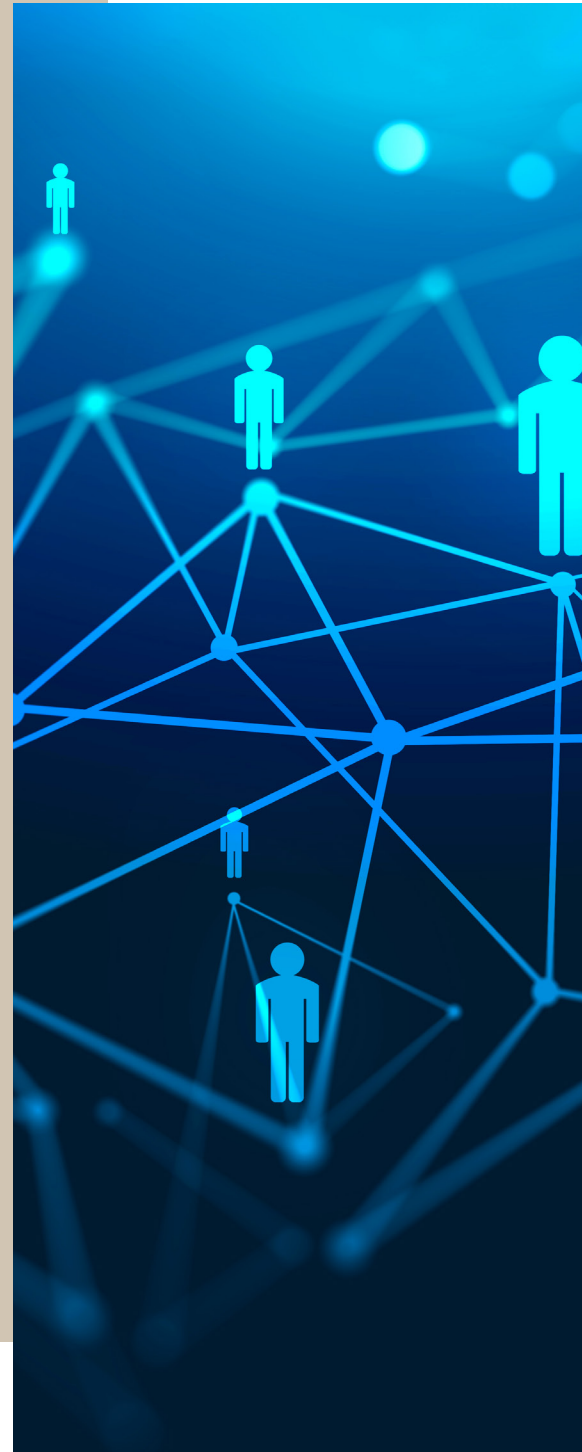
# Engage partners, not suppliers

They say the best-matched spouses know all about each other there is to know. When choosing your physical design partner in a bold enterprise like building datacenters for AI capacity, look for a savvy, proven team that demonstrates a vested interest in your business and its long-term plans. You need a partner to consult with, not a supplier who just shows up. Without any skin in the game, a supplier becomes a transactional party, and nothing becomes repeatable—every project just starts over again.

At ZBeta, we've chosen a business model that's based on this consultative, not transactional, approach. As such, we focus our work on clients who select us as team players in their long-range vision. We believe the best physical security partners for AI datacenters will:

- + **Join you at the strategic level.** Bring in physical security early so they can learn your business and be part of your long-term roadmap. Forming a partnership early on yields the best working synergy on present and future projects.
- + **Run like clockwork.** Choose partners with a rich combination of know-how, methodology, and information sharing techniques that empowers them to integrate with your people when needed and function the rest of the time as an autonomous unit.
- + **Force-multiply your subject matter experts.** The best consultants work seamlessly with each client's in-house resources to ensure high-quality work sharing, whether remotely or on-site. At ZBeta, the LabZ program is an example of how hands-on collaboration can produce future-proof results, leveraging deep expertise in datacenter security and many other areas to support innovative problem solving, solution testing, and optimization proofs of concept.
- + **Own the program.** Winning physical security partners are capable of taking ownership of all needs for a client, almost as if they were a functional arm of the client's existing business, representing your program in the same ways you would do yourself.
- + **Play well with others.** For projects that extend to multiple design consultants and VARs, all partners must collaborate to avoid lapses in communication and productivity. Choose teams that understand the art of cooperation—working together while also competing to shine—and who are well positioned to act as a lighthouse partner, ensuring delivery where others can not.

Overall, the value you get from a physical security consultant will track to their capacity to operate as a smart, sophisticated business unto themselves. Invest in partners that offer triple-threat expertise—superior thought leadership, visionary strategic planning, and a can't-fail method for mastering and delivering on your unique style and requirements. The right partnership will create the brand new efficiencies you need to keep your datacenter business humming along as you scale it up.





## Build the future with us

In the burgeoning datacenter race for AI-driven capacity, join forces with a physical security consulting and design partner who helps you grow in ways that are effective, efficient, programmatic, and future-proof.

ZBeta is a world-class physical security design and managed services firm providing services to some of the most dynamic, highest-profile organizations and individuals in the world. Using a data-driven, technology-led, human-centered approach, we help our clients design and engineer superior physical security solutions, implement them seamlessly, and operate them at peak efficiency. For datacenter projects or any other, we operate at scale, move at the speed of today's projects, represent your program as you would, and assure delivery where others cannot.

At ZBeta, there is no finish line in how we think about our clients' business. We continually seek innovative ways to enable competitive marketplace advantage for the companies and organizations we serve. The bold opportunity presented by AI for datacenters is big enough for us to take part together, and in doing so, we can help you outpace the competition and make your business vision ever more real, from today into the next unknown era of technological advancements.

---

### Our Office:

700 Larkspur Landing Circle, Suite 150  
Larkspur, CA 94939

### E-mail and Web:

[info@zbeta.com](mailto:info@zbeta.com)  
[www.zbeta.com](http://www.zbeta.com)

### Phone:

(855) 559 2382

