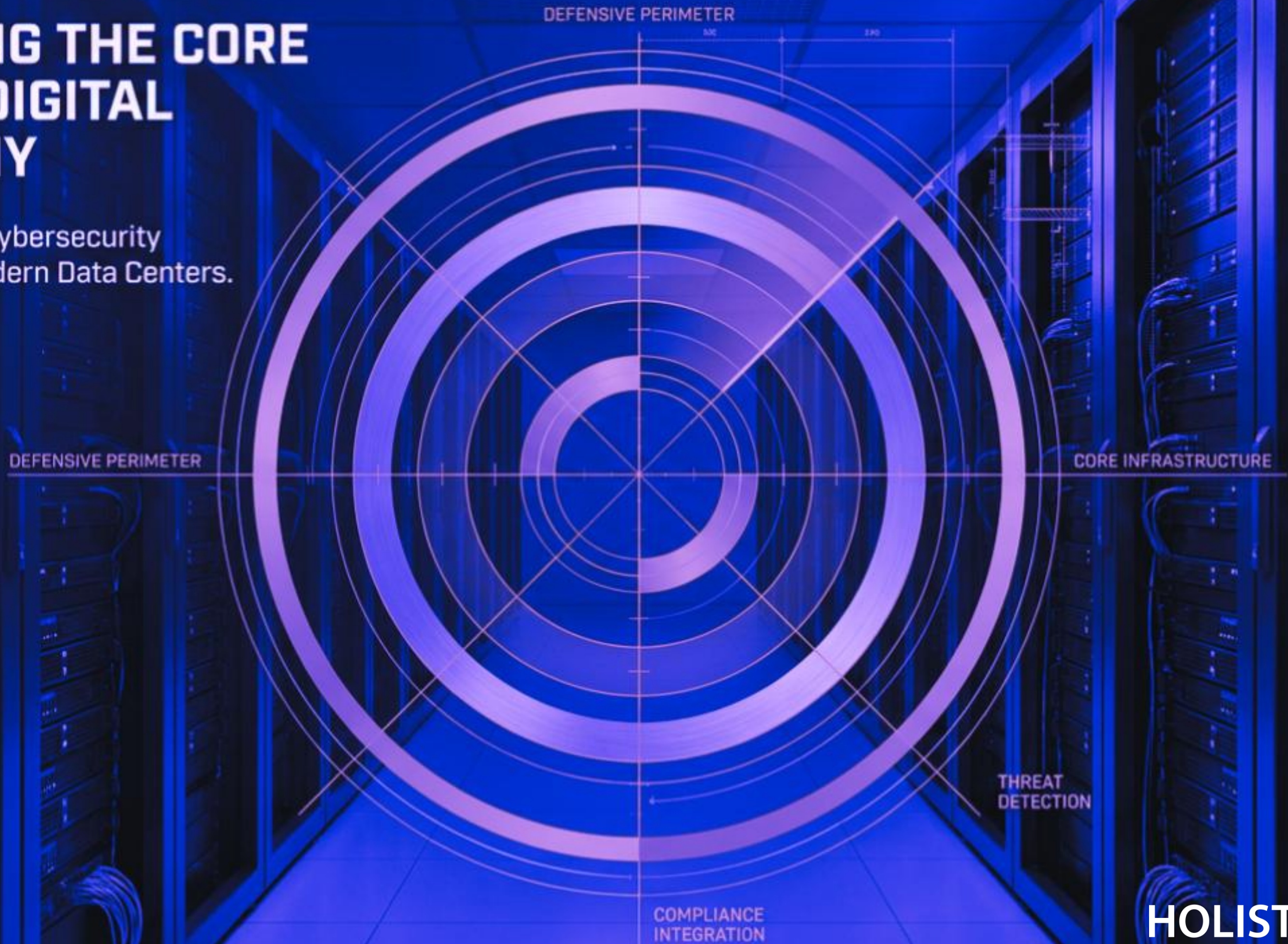


SECURING THE CORE OF THE DIGITAL ECONOMY

A 360° Holistic Cybersecurity Blueprint for Modern Data Centers.



HOLISTI  **YBER**

DEFEND WHAT MATTERS

THE DATA CENTER IS NO LONGER JUST A FACILITY

EDITORIAL BLUEPRINT // ARCHITECTURAL COMPARISON MATRIX

HOSTING & CO-LOCATION

Shared infrastructure and multi-tenant physical environments.

PRIMARY VULNERABILITIES:

- Tenant isolation failures
- Cascading DDoS impacts
- Compromised shared management interfaces



NEO CLOUD PLATFORMS

High-density compute built for AI workloads and GPU clusters.

PRIMARY VULNERABILITIES:

- Misconfigured cloud APIs
- Multi-cloud interconnectivity exploits
- Control-plane hijacking



EDGE DATA CENTERS

Geographically dispersed compute close to real-time applications.

PRIMARY VULNERABILITIES:

- Latency-sensitive localized disruption
- Weak remote access
- Physical-cyber tampering at minimally staffed sites



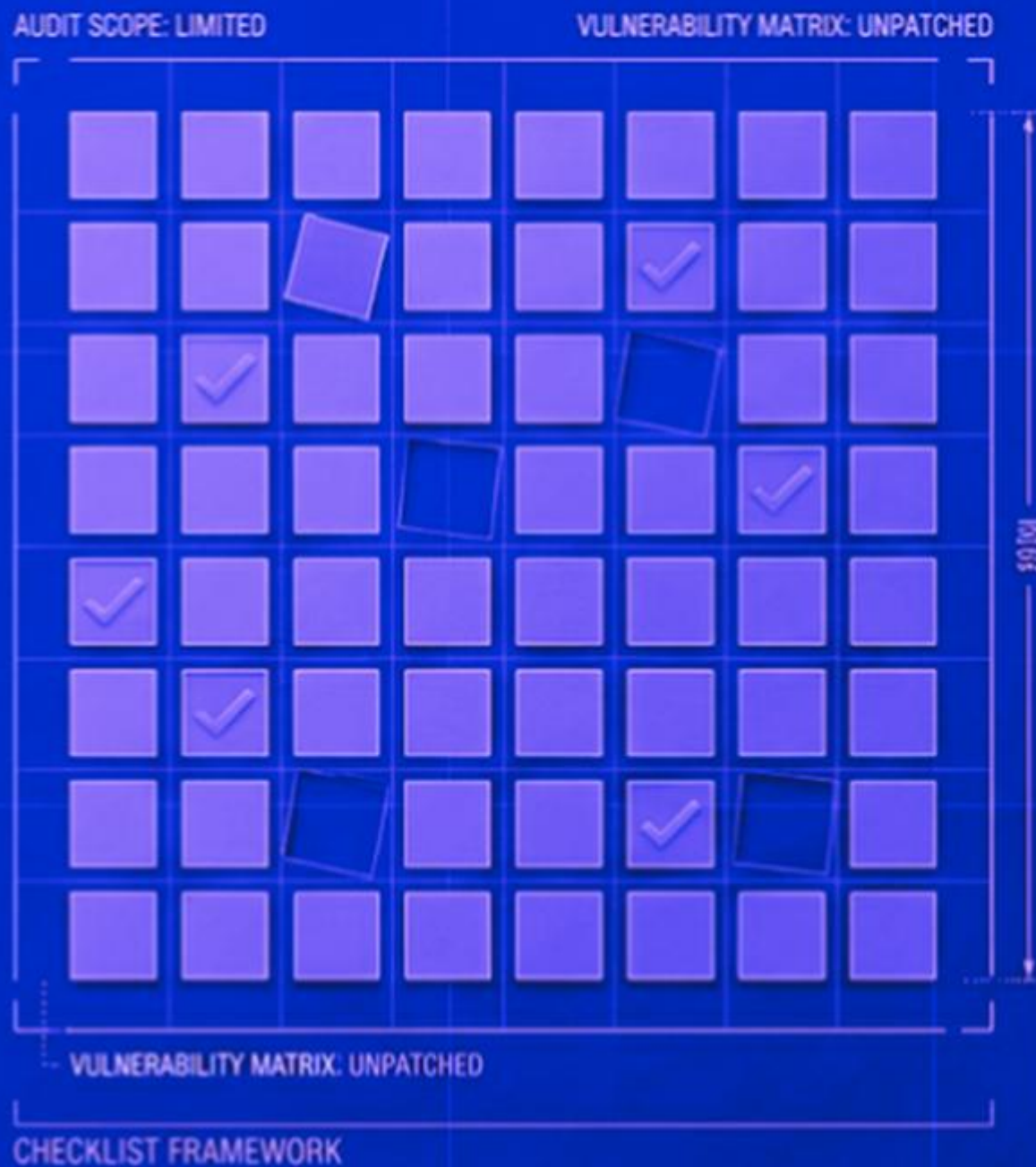
HOLISTI  **YBER**

DEFEND WHAT MATTERS

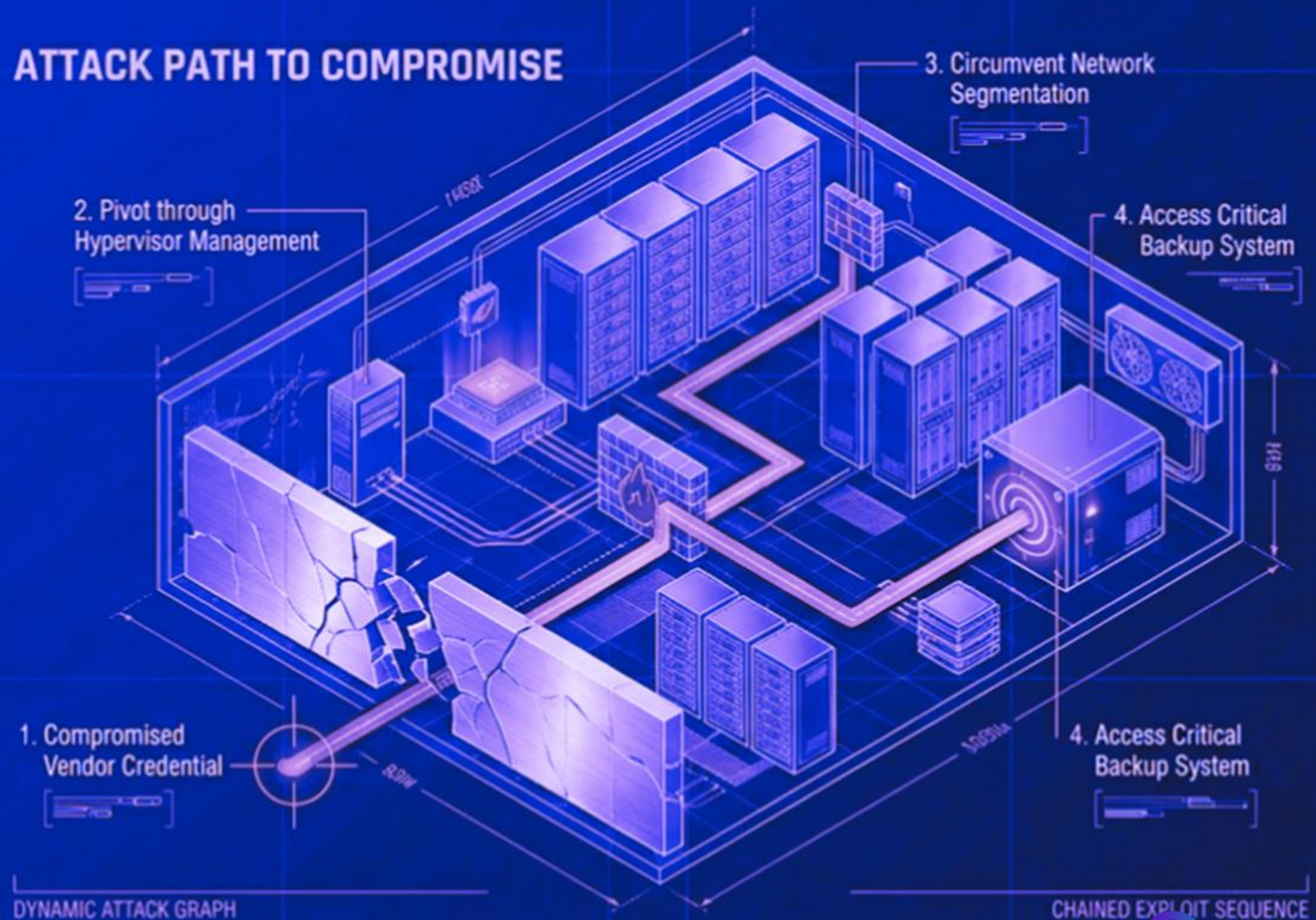
DEFENDERS THINK IN CHECKLISTS. ATTACKERS THINK IN PATHS.

The true risk to a data center is rarely a single missing patch. It is the chained sequence of vulnerabilities that leads to critical infrastructure compromise.

STATIC COMPLIANCE POSTURE

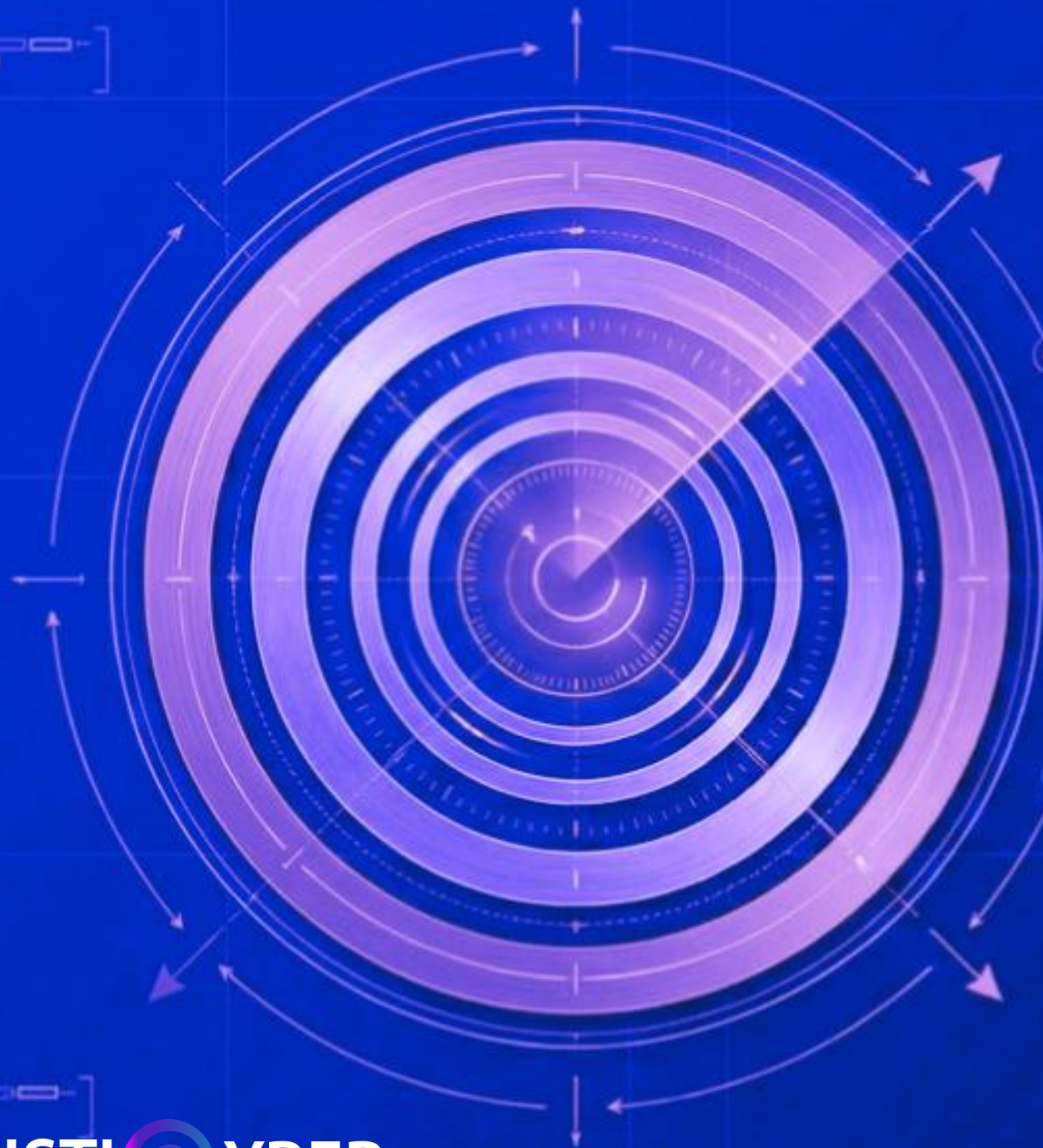


ATTACK PATH TO COMPROMISE



NATION-STATE GRADE DEFENSE BUILT ON ATTACKER INTELLIGENCE

EDITORIAL BLUEPRINT // PROACTIVE DEFENSE STRATEGY



01. SIMULATE REALISTIC ATTACKS

We evaluate the environment from the adversary's point of view, identifying how they gain initial access and move laterally.

02. DEFEND WHAT MATTERS MOST

We move beyond generic vulnerability lists to prioritize the risks that actually threaten SLAs, customer workloads, and physical infrastructure.

03. CULTIVATE PRE-EMPTIVE RESILIENCE

We build active Defcons within your operations to ensure you can contain and eradicate threats without halting operations.

360° COVERAGE: FROM BOARDROOM STRATEGY TO INFRASTRUCTURE RESPONSE

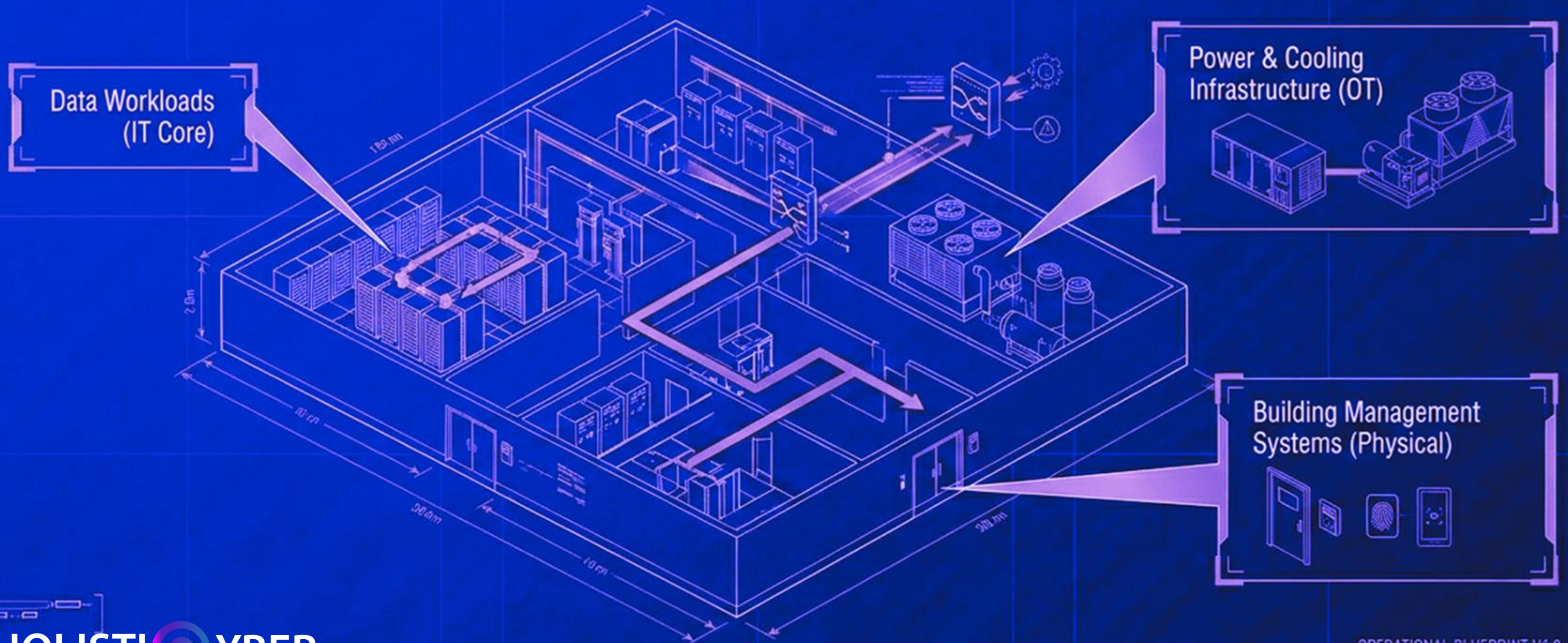
EDITORIAL BLUEPRINT // OPERATIONAL LIFECYCLE



SECURING THE PHYSICAL-CYBER CONVERGENCE

EDITORIAL BLUEPRINT // INTEGRATED FACILITY SECURITY

Protecting hypervisors and customer workloads is only step one. Protecting the integrated facility systems is the true holistic requirement. Attackers actively seek paths from IT networks into Operational Technology to disrupt the physical environment.



DEFENDING THE EXTENDED PERIMETER: SUPPLY CHAIN & TENANTS



TENANT ISOLATION VALIDATION
Ensuring strict zero-trust segmentation so that a breach in one customer's environment cannot cascade across shared multi-tenant infrastructure.

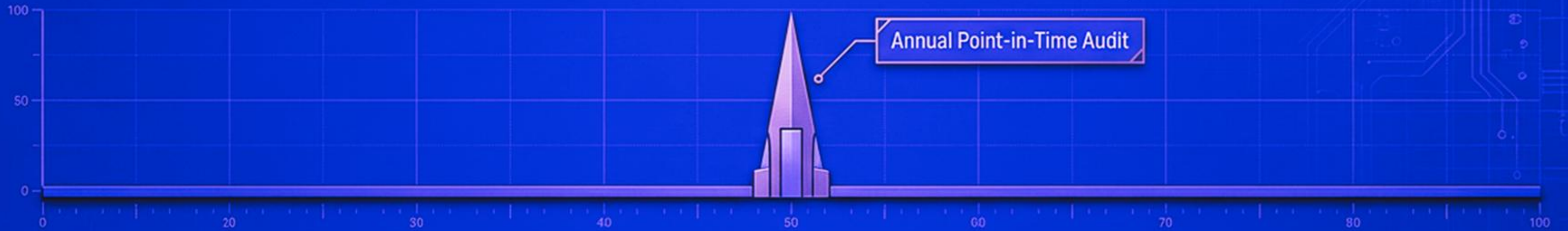
THIRD-PARTY RISK MANAGEMENT (TPRM)
Governing the ICT supply chain by strictly managing vendor access, securing remote management tools, and verifying firmware integrity.



FROM REACTIVE CHECKS TO CONTINUOUS RESILIENCE

EDITORIAL BLUEPRINT // COMPARATIVE RESILIENCE MODELS

TRADITIONAL COMPLIANCE APPROACH



HOLISTICyBER CONTINUOUS RESILIENCE



HOLISTI  **YBER**

DEFEND WHAT MATTERS

SECURITY AS YOUR COMPETITIVE DIFFERENTIATOR

EDITORIAL BLUEPRINT // SECURING SHARED INFRASTRUCTURE

PROTECT REVENUE & UPTIME



Eliminate single points of failure that threaten SLAs and service continuity.

ACCELERATE ENTERPRISE SALES



Utilize documented, nation-state grade compliance readiness to shorten sales cycles with heavily regulated enterprise clients.

STRENGTHEN CUSTOMER TRUST



Prove to tenants that their critical data and operations are strictly isolated and impenetrable, reducing operational uncertainty.

HOLISTI  **YBER**

DEFEND WHAT MATTERS

SECURE THE PLATFORM. PROTECT THE BUSINESS.

HolistiCyber doesn't just help data centers become more secure. We make them more trusted, resilient, and competitive in the AI era.

Engage with our experts for a Cybersecurity Holistic Risk Assessment.

[HolistiCyber.com](https://www.holisticyber.com)

New York, USA | Tel Aviv, Israel | London, UK

+1 646 568 5357



HOLISTI  **YBER**
DEFEND WHAT MATTERS