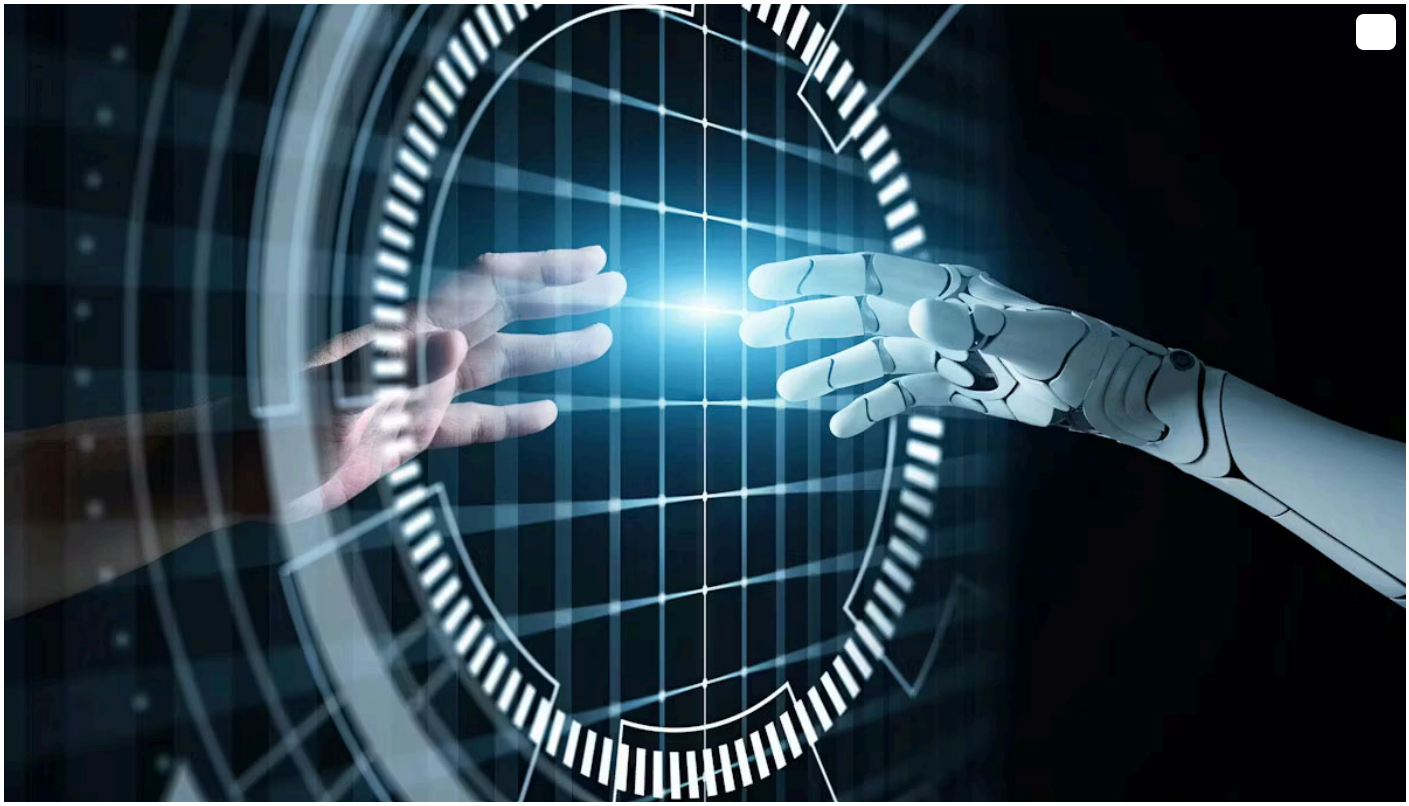

A recent Gartner report projects the Digital Twin market to grow from $35 billion in 2024 to $379 billion in 2034, representing a 900% increase over the coming decade.

ARTIFICIAL INTELLIGENCE

Zero Hour: The Promise and Peril of Digital Twins in Security Systems

Zero Trust unlocks the data integrity and confidence that delivers the promise of AI to electronic and physical security systems.

Steven Brown, Thomas Segars, Jason Beers

The Skinny

- **Digital Twins + AI = Game-Changing (but Risky):** High-fidelity Digital Twins, especially when AI-enabled, offer security professionals powerful tools to simulate and optimize physical

and cyber defenses—but their effectiveness hinges entirely on trustworthy, high-quality data inputs.

- **Data is the New Perimeter:** In today's converged cyber-physical environments, protecting data from edge to archive is critical. Flawed or poisoned data can cripple decision-making, making Zero Trust (ZT) architectures essential to mitigate risk and ensure AI-driven systems remain reliable.

- **Infinite Game, Infinite Stakes:** As attackers and defenders alike harness generative AI, the battle for system integrity becomes faster and more complex. Digital Twins reflect both our most significant security capabilities and vulnerabilities, making ZT not just a best practice, but a necessity for the AI-enabled future.

Abstract

The convergence of Artificial Intelligence and Cyberphysical Systems, including Electronic and Physical Security Systems and Digital Twins, offers unparalleled opportunity and unprecedented risk. Adopting a Zero-Trust framework will mitigate risks and enhance the effectiveness of Digital Twins, enabling the maximum exploitation of cutting-edge technology while improving safety and security.

Introduction

"All models are wrong, some are helpful."

A friend's rephrasing of 20th-century statistician George Box's axiomatic admonishment, "Remember that all models are wrong; the practical question is how wrong do they have to be not to be useful." Digital Twins, high fidelity synthetic doppelgangers that model everything from automotive engines to the grid, are powerful tools that in the contexts of electronic, physical, and cyber security solutions enable security professionals to understand the effects of incidents ranging from environmental anomalies to physical and cyber intrusion attempts on operational networks, facilities, and systems. The insights gleaned from these disruptive technology tools, particularly Artificial Intelligence (AI)-enabled real-time variants, can equip planners to understand efficiencies, vulnerabilities, and optimization opportunities across the entire system life cycle, from design to obsolescence.

Despite risks inherent in Cyber Physical Systems (CPS) and high-profile attacks like Volt Typhoon, Sandworm, CyberAv3ngers, the market has embraced the promise of efficiency and revenue-saving potential. A recent Gartner report projects the Digital Twin market to grow from $35 billion in 2024 to $379 billion in 2034, representing a 900% increase over the coming decade. This technical article, the third in a four-part series exploring the convergence of cutting-edge technology and Zero Trust (ZT), examines the importance of getting data security right in the relentless pursuit of cost-effective, reliable, and frictionless security.

It's The Data, Stupid!

In the late 1950s and early 1960, mathematicians, computer scientists, and strategists started using the phase, "garbage in, garbage out", or GIGO, to convey that the quality and credibility of a system's outputs–actions, analysis, recommendations, and decisions–are dependent on the quality and credibility of that system's inputs–data. Today, with AI dominating headlines and investment portfolios, GIGO is truer than ever as we rush to innovate at the speed of relevance. AI unleashed on dubious, poisoned, or corrupted data sets can drive equally flawed actions, analyses, and recommendations. The implications are even more dire as we recognize the reality we have been living with for at least two decades and will continue to do so for decades to come: the ubiquity of AI-informed or AI-rendered decisions.

Bad data in = bad data out. A more extended version of that statement might read: Questionable data can prompt both indecisions, driven by skepticism as to its credibility, and overconfidence, driven by the mistaken belief that unprotected data is accurate, credible, and unpoisoned.

In 1992, James Carville admonished, "It's the economy, stupid!". Thirty-three years later, political pundits may still debate the Ragin' Cajun's pithy tirade. Still, politics aside, the debate is over in the context of converged cyber and physical security systems in 2025. It's the data, stupid! High fidelity Digital Twins mine petabytes of data generated by myriad edge devices deployed at scale across CPS

and industrial control systems (ICS) including supervisory control and data acquisition (SCADA), operational technology (OT), or Industrial Internet of Things (IIoT) sensors (i.e. thermostats, motion, smoke detectors, etc.) and actuators (robots, lighting controls, valves, hydraulics, etc.). For today's connected industrial controls, building automation, and security systems to deliver the promise of a better, safer connected future, it is paramount to protect the data these systems produce, ingest, and analyze from inception to archive and everywhere in between. Unless sufficiently protected, planners, decision-makers, and operators should be cautious of system-generated recommendations based on the data.

Understanding Digital Twins

Digital twins are generally characterized by the physical or virtual object, entity, or system to be modeled, a digital counterpart to that physical or virtual entity, and, often, a data connection that feeds data from the sensors and actuators in the live entity or system to the digital twin.

Paradoxically empowered and encumbered by an intrinsic reliance on data, Digital Twin solutions require massive compute power and access to raw data streams from the myriad sensors and actuators of their operational opposites to realize their full potential. Though access to raw data uniquely empowers Digital Twins to synthesize systems states to deliver real-time analysis, which identifies vulnerabilities, streamlines processes, and highlights inefficiencies that could unlock massive bottom-line savings, the threat of

manipulated, corrupted, or otherwise poisoned data is very real and must be mitigated.

Cybersecurity

How Zero Trust hardware helps build sovereign resilience into technology supply chains

Phil Straw

Information Security

How the DOD is enabling its Zero Trust mission

Felipe Fernandez

Cybersecurity

Strategies Emerging to Fill in the Physical Security Gaps with Zero Trust

Patrick Miller

Where Digital Twins and the operational systems they mirror are often ostensibly “air-gapped”, the concept is, realistically, a myth. Examples of zero-day exploits of “air-gapped” systems are numerous and unsettling in terms of the profound impact and relative ease of compromise.

So, despite their promise, given their limitations, vulnerabilities, and dependencies, can security professionals trust their data, assets, and personnel to digital twins?

Role of Digital Twins in Security

Security environments are dynamic and require real-time monitoring, rapid response, and adaptive threat mitigation strategies. Digital Twins can bridge cyber and physical security

without impacting operational systems, offering organizations the ability to enhance surveillance, improve threat detection, optimize system performance, and refine response strategies. In terms of both understanding the current state of a security system and maximizing system effectiveness, Digital Twins are game changers in security. Physical exercises, scenario-based events that pit ***Red (the Aggressor)*** against ***Blue (the Defender),*** are among the most expensive, resource-intensive, and operationally disruptive events in which security teams and organizations participate. Think of fire drills or active shooter drills on steroids.

> *"Where Digital Twins and the operational systems they mirror are often ostensibly "air-gapped", the concept is, realistically, a myth. Examples of zero-day exploits of "air-gapped" systems are numerous and unsettling in terms of the profound impact and relative ease of compromise.*

Although these exercises have their place and no security policy or plan is complete without them, inherent artificialities, such as working hour limitations, off-limits areas, and safety restrictions, offer an abysmally low representation of overall system effectiveness. Furthermore, due to complexity, artificiality, and operational disruptions, even security-conscious organizations are often hard-pressed to execute more than a handful of small-scale events each year. Digital Twins offer high fidelity, physics-based models against which security professionals can perform thousands of simulations where they can tweak variables ranging from Red and Blue capabilities, construction materials, weather conditions, lighting conditions, etc.) to get a more granular understanding of baseline performance, breaking points, and the effects of potential upgrades. The same principle applies to cyber environments where Digital Twins can facilitate penetration or pen testing as both a vector and a model. In short, Digital Twins offer security professionals a more realistic and empirically defensible assessment of their systems' status, and as such, are invaluable tools.

While the outlook is promising, practical challenges remain on the path to wide-scale adoption. Organizations often struggle with integrating Digital Twins into environments that include both legacy infrastructure and modern platforms, as well as aligning CPS that were not originally designed to work together. Fortunately, new technologies which leverage ZT to authenticate and encrypt data exchanges between the IT, OT, and IIoT devices, like Prometheus Security Group’s Digitally Encrypted Security Interface (DESI) and

Universal Field Panel (UFP), are emerging to bridge these gaps—enabling modernization through attrition to enhance legacy systems rather than driving costly and disruptive rip and replace projects.

The Confluence of Zero Trust, Electronic Security, and Digital Twins

The ZT framework represents a fundamental shift away from traditional castle-and-moat cybersecurity models, predicated on building cyber walls high enough and thick enough to repel threats, to a model that assumes compromise. As the moniker implies, ZT is based on the principle of "never trust, always verify" and features concepts such as least privilege access, identity verification, data security, continuous monitoring, and microsegmentation to prevent and mitigate the consequences of compromise. Adopting a ZT framework enables the prevention, detection, and mitigation of threats. While the ZT narrative often focuses on IT systems, there is growing recognition of the criticality of protecting ICS, OT, and IIoT, including Digital Twins.

Worldwide threat reporting indicates growing levels of awareness among bad actors of the vulnerabilities in these systems and sufficient sophistication to exploit those vulnerabilities.

Electronic Security Systems, which monitor intrusion sensors, control facility access, open and close gates, raise and lower vehicle and personnel barriers, turn security lighting on and off, and monitor security system video, share many characteristics and

vulnerabilities of ICS and SCADA systems. For example, while the cost and efficiency drivers behind the great cloud migration and transition to "as a Service (aaS) solution models are apparent, so are the accompanying vulnerabilities. Compromises in one node can trigger cascading compromises and failures in other nodes, resulting in severe consequences ranging from minor inconveniences to global headlines. Connected Digital Twins share many of these same vulnerabilities. Adopting a ZT framework enables the maximal exploitation of cutting-edge technology while mitigating associated vulnerabilities and managing risk.

Everything is Different; Nothing has Changed

Security professionals manage a complex conundrum, balancing unprecedented capabilities with unprecedented exposure. They advise savvy decision makers and boards of directors who weigh the likelihood and consequences of successful breaches against the cost and efficiency losses of adoption, a tenuous balance between airtight security, frictionless convenience, ROI calculations, potential reputational damage, and revenue projections.

While the technological landscape has undergone a dramatic transformation—from physical locks to quantum encryption and fortress walls to Zero Trust architecture—the fundamental security dynamic remains essentially unchanged. The core security challenge has remained constant throughout history: protecting assets from those exploiting vulnerabilities to gain unauthorized access. Whether considering medieval defenses or modern cybersecurity

frameworks, the essential pattern persists—a continuous cycle of protection, vulnerability discovery, exploitation, and adaptation.

Although in principle, very little has changed in security since the advent of supercomputers in the 1960s and microcomputers in the early 1970s, the ongoing emergence of quantum computing has led to significant changes in complexity, scale, and speed.

- The attack surface has expanded exponentially. Organizations must now secure physical perimeters and vast digital ecosystems spanning cloud environments, remote endpoints, IoT devices, and supply chains.
- The speed of the security cycle has accelerated. Vulnerabilities that might have taken years to discover and exploit in the past can now be compromised within minutes, and in the not-so-distant future, seconds.
- The technical sophistication of defense and offense has increased by orders of magnitude, moving from simple locks and hasps to AI-powered threat detection, from basic intrusion to polymorphic malware and advanced persistent threats.

Beneath these transformations, the psychological and strategic elements remain remarkably consistent:

- Attacker advantage persists; defenders must secure everything, while attackers need only find one vulnerability.
- Asymmetry of effort continues; it's generally easier to destroy than to build.

- Humans are unpredictable; The human element remains the most unpredictable variable—the Achilles' Heels and Knights in Shining Armor of security systems.

This paradox creates a strange continuity between ancient and modern security professionals. A Roman sentry watching for weaknesses in a fortress wall would salute the vigilance of a modern SOC analyst monitoring network traffic, despite the vast technological gulf between them.

The perpetual contest between security personnel and adversaries represents not just a technical challenge but a profoundly human one—a contest of wits, resources, and determination that has characterized human conflict throughout history, now playing out across digital landscapes.

Artificial Intelligence

In simple terms, traditional AI is like a highly sophisticated analysis tool that helps cultivate understanding and support decision making about existing information, while generative AI is more like a creative partner that can produce entirely new content based on what it has learned. Generative AI then perpetuates, but fundamentally shifts, the endless chess match between blue and red teams, working to maximize their respective strengths while identifying and exploiting the vulnerabilities of their opponents. Specifically, the ability of Generative AI to autonomously design and test both attack and defense schema, which consider real-time

variables (environment, outages, traffic, personnel, threat posture, etc.), is as potentially revolutionary as it is terrifying.

In his latest contemplation of humanity, philosophy, and technology, Nexus: A Brief History of Information Networks from the Stone Age to AI, Yuval Noah Harari asserts that today's AI tools are the worst they will ever be. Furthermore, he examines the uncomfortable reality that AI will create as many issues as it solves and potentially rival human intelligence. Throughout history, innovators have fashioned tools, weapons, and shields fated for inevitable conflict on common anvils. AI is no exception; with its real promise, it presents an accompanying pacing problem. Attackers will employ the exact cutting-edge technology solutions that security professionals use to innovate protective schemes in equally innovative pursuits, but to compromise those assets by exploiting novel vectors and methodologies. Suppose we accept that the AI tools that crawl the web and power large language models (LLMs) and search engines in 2025 are less capable and more expensive than their successors in 2030 and beyond. In that case, it is plausible that AI-designed and optimized systems will soon outperform human-designed systems.

The convergence of Generative AI and Digital Twins presents unique capabilities and vulnerabilities that defenders must identify and mitigate to stay ahead of attackers seeking to infiltrate and exploit. The infinite game of defend and attack and the broader security landscape has evolved to AI-enhanced attacks engaging AI-powered defenses. As such, security systems have never been more capable

or more susceptible. Given this reality, protecting security data from its inception at the edge (sensors, readers, cameras, etc.) through transmission, archiving, and AI exploitation is critical.

Conclusion

The intersection of AI, Digital Twins, and ZT presents an unprecedented opportunity and unparalleled risk. Adopting a ZT framework for CPS, such as Digital Twins, and incorporating ZT architecture that continuously authenticates, monitors, and protects data, users, and devices is key to protecting the data, the lifeblood of an AI-enabled future, and enabling security professionals to embrace vigilant innovation. Bad data drives worse decisions and poses a greater risk to operations, assets, the bottom line, and people.

The final article in this series will outline a concept of operations that leverages Zero Trust Architecture to stay ahead in the ongoing game of CIP security. While ZT is anything but a panacea, the framework mitigates the consequences of compromise. It enables prompt detection and remediation for everything from OT devices to Digital Twins, data centers, and connected security personnel. The CONOPS will lay out the case for adoption to hedge against current and future threats while enhancing system effectiveness, mission success, and team safety.

About the Author

Steven Brown | Vice President for Strategy & Business Development at Prometheus Security Group Global (PSG).

Steven Brown is Vice President for Strategy & Business Development at Prometheus Security Group Global (PSG). He is a critical infrastructure security expert and USAF veteran with 23+ years of operations, strategy, policy, design, and implementation experience securing critical infrastructure and strategic assets worldwide.

PSG provides unified security solutions specializing in software and hardware for video surveillance, access control, intrusion detection, and cyber security. PSG's open architecture, zero trust, scalable, reliable security solutions are entrusted to protect the United States' most sensitive strategic assets along with critical missions, facilities, and people around the world.

About the Author

Thomas Segars | Founder and President of Foursquare Security Solutions, LLC,

Thomas Segars is a retired United States Air Force Colonel with over 32 years in physical security, nuclear security, law enforcement, and anti-terrorism. After completing his final active-duty post in June 2024 as the Director of intelligence,

Strategic Plans, and Requirements for the Air Force Installation and Mission Support Center in San Antonio, Texas, Thomas launched a consulting company, Foursquare Security Solutions, LLC, and provided independent security consulting services. Thomas has a bachelor's degree in criminal justice from the University of Georgia, a master's degree in human resources development from Webster University, and a Master of Strategic Studies from the United States Army War College. He is also a Federal Bureau of Investigation National Academy Session 263 graduate with a Department of Defense Counter Insider Threat Professional certification.

About the Author

Jason Beers | independent consultant

Jason Beers is an independent consultant specializing in strategy, policy, and government engagement across several fields, currently advising Prometheus Security Group Global regarding Fed-Gov Zero Trust. Jason is a retired Air Force officer with experience in law enforcement, physical security, technology integration and organizational design. In his final assignment, he was the Deputy Director of Logistics, Engineering, and Force Protection for Air Force Special Operations Command and an advisor to the Air Force Director of Security Forces.