ACCESS & IDENTITY

How Not Deploying Zero Trust Data with AI May Risk Team Safety, Mission Failure

As AI transforms threat detection and response, securing the data that powers it is critical.

Patrick Miller, Steven Brown, Thomas Segars, Edward M. Levy

The Skinny

- **Faulty AI Can Lead to Wrongful Outcomes**—Robert Williams's wrongful arrest due to faulty facial recognition highlights the dangers of unverified AI data, raising critical concerns for security and law enforcement professionals.
- **Zero Trust (ZT) Is Essential for AI Security** – AI systems in security applications must operate on authenticated and verified data to prevent compromised decision-making, financial loss, and mission failure.
- **The Convergence of AI, ZT, and Digital Twins**—When combined with ZT principles, emerging technologies like Digital Twins offer enhanced threat detection, system optimization, and resilience in security environments.
- **Bad Data in AI Equals Bad Outcomes** – AI's effectiveness hinges on data integrity; untrusted data leads to systemic failures, legal risks, and reputational damage, reinforcing the need for ZT adoption.

Prologue: *A critical component of next-generation security is the adoption of Zero Trust Architecture (ZTA) for physical security*

equipment (PSE) and Operational Technology (OT) environments. As AI capabilities grow exponentially, ZTA greatly enhances and optimizes AI effectiveness; without ZT data, the risks are undoubtedly high. This is the second of our four-part editorial series.:

In January 2020, the Detroit Police Department wrongfully arrested Robert Williams based on a faulty facial recognition identification, accusing him of theft and ultimately resulting in a settlement. Though public details are scant, the lingering question for security, intelligence, and law enforcement professionals might be: Was the data contained in the algorithm authenticated and verified? In today's rapidly evolving digital landscape, artificial intelligence (AI) plays an increasingly vital role across all the domains that use technology to protect communities, businesses, and the homeland. From predicting cyberattacks to identifying potential physical threats, AI-driven systems reshape how organizations protect their assets and people.

Yet, alongside this promise comes a peril: the very data that powers these AI systems can become a vulnerability if not adequately trusted—meaning authenticated and verified—resulting in monetary loss, reputational damage, jeopardizing the safety of responding teams, risking mission failure, or worse.

In December 2024, Security Technology Executive magazine *SecurityInfoWatch* (SIW) partnered with Industry SMEs to launch a four-part series on Zero Trust and Zero Trust Architecture (ZTA), a

term the National Institute of Standards and Technology describes as “an enterprise cybersecurity architecture that is based on zero trust principles and designed to prevent data breaches and limit internal lateral movement.”

The first SIW article, titled “Strategies Emerging to Fill in the Physical Security Gaps with Zero Trust” provides a foundational understanding of the evolution of ZT, and highlights the need to redefine the “edge” for ZTA, even going so far as showcasing how some companies are leveraging technology to extend ZT to sensors, readers and beyond the camera lens to the scene itself. In this article, we explore the growing criticality of ZT data in AI systems and why ZT data is indispensable for enhancing security in an increasingly threat-laden world. The third article in the series will focus on the employment of Digital Twins and the use of ZTA and AI —the why and the how.

Artificial Intelligence without Zero Trust Data Is Ill-Fated

Artificial Intelligence has rapidly transformed numerous sectors, from healthcare and finance to education and transportation. Also at the forefront of this transformation is the security industry, replete with electronic security systems hosting state-of-the-art cyber security initiatives and physical security peripherals (sensors/readers/cameras), with vast amounts of data contained within the system and in data lakes, data warehouses and even process controls which feed Operational Technology (OT). As AI continues to evolve, the reliance on this data becomes increasingly

critical, and the adage rings true: **Bad/Untrusted Data In = Bad/Untrusted Data Out**. If trusted data is considered, well, utopia, then untrusted data should be regarded as *fait accompli,* and the resultant question is straightforward: "why would anyone run AI on data that is not Zero Trusted?"

The authors predict by 2030, ZT principles combined with AI and Machine Learning (ML), a core component of AI, will become the default standard for electronic security and video surveillance systems worldwide, enabling a new era of proactive and self-healing defense mechanisms. AI systems thrive on data and are trained on vast datasets to recognize patterns, make predictions, and generate insights. In the rapidly evolving domain of electronic security systems, the integration of AI and ML has unlocked unprecedented capabilities. From advanced video analytics and biometric authentication to predictive threat detection, AI and ML are redefining how security systems operate. However, the effectiveness and reliability of these technologies are predicated on the quality, security and actual reliability of the data which fuels them. To that end, ZT principles emerge as a cornerstone for safeguarding AI and ML in electronic security system environments.

What is Zero Trust?

With the announcement of Executive Order 14028, *Improving the Nation's Cybersecurity*, in May 2021, the U.S. government cemented the importance of ZT for all echelons of the U.S. government spaces and private sector industry partners. The ZT security model is

founded on a simple yet powerful premise: **trust nothing and verify everything**. Unlike traditional security models, which rely on perimeter defenses, ZT assumes breaches can and will happen—to the extent that one should assume someone is already in your system. ZT also mandates continuous verification of identities, devices, and data, regardless of their origin.

Application of ZT in Data Security

Zero Trust principles emphasize:

- Authenticating and verifying data sources rigorously.
- Protecting data in transit and at rest using encryption and other safeguards.
- Continuously monitoring data access and usage to detect anomalies and unauthorized actions.
- Encrypted data pushed all the way to the edge.

AI Adoption Across Security Applications

The appeal of AI lies in its ability to process large amounts of data, identify patterns, and make predictions with unparalleled speed and accuracy. Subsequently, predictive analytics can help identify potential threats before they materialize, giving security, cyber, or incident-response teams a crucial edge. AI can significantly enhance security applications by efficiently analyzing complex data and identifying patterns that humans might miss. Consider the following example:

How many yellow trucks passed through perimeter zones 4-7 in the last six months? Did they stop? If so, at what time, for how long, and was there any associated zone activity (e.g., alarms or sensor anomalies) during those times? Has the organization verified the integrity of the zones in question to ensure continued operational reliability?

> *"The appeal of AI lies in its ability to process large amounts of data, identify patterns, and make predictions with unparalleled speed and accuracy. Subsequently, predictive analytics can help identify potential threats before they materialize, giving security, cyber, or incident-response teams a crucial edge."*

AI can quickly process and cross-reference this information, and more, flagging unusual patterns or behaviors. With continuous advancements, AI will not only perform these tasks faster but with

greater accuracy, enabling security teams to take prompt and informed actions such as deploying a response team to inspect suspicious activity in those affected zones.

AI is quickly becoming the backbone of many modern security initiatives and highlights the need for data purity through ZT principles. Physical security systems leverage AI for facial recognition, intrusion detection, and access control, while cybersecurity tools use AI to detect malware, identify anomalies, and mitigate threats in real-time. These capabilities enable organizations to act faster and more effectively than ever before—but only achieving the goal to the extent that data follows ZT principles. Other factors include:

1. ***Mitigating Security Threats****:* The use of non-ZT data exposes AI systems to myriad security risks, such as data breaches, tampering, and injection of malicious data. For example, adversarial attacks—where attackers subtly manipulate input data to deceive AI models—can compromise the performance and reliability of AI systems. ZT data protocols significantly reduce these risks by ensuring that only verified, authenticated and secure data is used in training and operations.

1. ***Ensuring Data Integrity and Quality****:* AI models are only as good as the data they are trained on and, again, **Bad Data In = Bad Data Out**. Biased, incomplete, or inaccurate data can lead to flawed models which produce unreliable or

discriminatory outcomes. ZT data emphasizes rigorous verification and validation of datasets, ensuring only high-quality data is used.

1. ***Protecting Privacy and Compliance****:* The handling of sensitive data, such as personal or health information, is governed by stringent regulations, including the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). Non-compliance can result in severe legal and financial repercussions.

1. ***Enhancing Ethical AI Development***: Ethical considerations are paramount in AI development. Instances of AI systems perpetuating bias, misinformation, or harm have sparked widespread concern. ZT data contributes to ethical AI by enforcing stringent data governance practices. ZT frameworks promote transparency and accountability in AI systems by ensuring data is accurate, unbiased, and ethically sourced.

1. ***Building Resilient AI Systems****:* AI systems must be resilient to adversities, including cyberattacks, data corruption, and operational disruptions. ZT data enhances resilience by implementing robust security measures and ensuring the continuous availability of clean, authenticated and verified data.

The Risks of Not Using Zero Trust Data in Artificial Intelligence

It should now be clear to the reader that ZT data on AI systems is the most credible pathway to data purity and, therefore, optimized efficiency and security—and is available today.

However, the authors acknowledge some may not yet be ZT disciples or practitioners and indulge this population next with some risks to consider for organizations using non-ZT data on AI systems, but not before revealing another apropos Sun Tzu quote, where the famous Chinese General says, “If ignorant both of your enemy and yourself, you are certain to be in peril.” Consider the following risks:

1. ***Compromised Data Leads to Systemic Failures***: AI systems relying on untrusted data are prone to systemic errors,

which enable attackers to manipulate outcomes and render electronic security systems ineffective.

2. ***Unchecked Bias Erodes Public Trust:*** Failure to implement ZT data allows biases to persist in AI models, leading to discriminatory practices and undermining confidence in security solutions.
3. ***Adversaries Exploit Unprotected AI Pipelines:*** Without ZT, malicious actors can poison data pipelines, introducing vulnerabilities that compromise the integrity of critical security applications.
4. ***Non-Compliance Risks Financial and Legal Consequences:*** Organizations that neglect ZT principles risk non-compliance with privacy and security regulations, facing hefty fines and reputational damage.
5. ***Data Breaches Accelerate Threat Proliferation:*** Using unverified data increases the likelihood of breaches, enabling attackers to weaponize compromised systems for broader security exploits.
6. ***Untrusted Data, poor quality data, or data compromised*** through malicious intent could lead to an organization's incorrect response protocols, flawed decision-making, improper data segmentation, unnecessary expenditures, mission failure, and more.

Implementing Zero Trust Data in AI Security Systems

Best Practices for Organizations

1. ***Use Only ZT Data****:* Ensure OT data sources from edge devices employ ZT data and store the data in cyber-secure data lakes and/or data warehouses.
2. ***Continuous Monitoring and Validation****:* Implement tools that validate data sources and continuously monitor anomalies.
3. ***Data Encryption and Masking***: Use encryption to protect data at rest and in transit and mask sensitive information to reduce exposure risks.
4. ***Access Limitation****:* Apply the principle of least privilege to ensure that only authorized individuals and systems can access critical data.
5. ***Threat Mitigation***: Implement robust threat detection capabilities and response options for internal and external threats. Employees with nefarious intentions or agendas can do as much damage, if not more, than external actors seeking to hack, exploit, delegitimize, or even bankrupt a company in short order.
6. ***Policies and Governance****:* As discussed in the first article in this series, organizations must develop data governance frameworks, continuously train employees on company policies, and regularly audit and refine in-place security measures and processes.

Emerging Trends

The convergence of AI and ZT is paving the way for new possibilities. Blockchain technology, for example, offers a

decentralized method for verifying data provenance, while advances in quantum computing promise to enhance encryption capabilities. As advancements continue, a next-generation technology dubbed Digital Twins (DT) reinforces the need for organizations to have ZTA and can help shield a company's OT system.

Digital Twins are increasingly used in security environments to aid in modeling and simulation, enhancing surveillance, threat detection, system optimization, and response strategies. By creating a DT—a virtual representation of physical security systems, facilities, assets, and other OT—organizations can improve their ability to monitor, analyze, and respond to potential threats. In this sense, DTs are poised to become central to smart security systems, especially in high-value industries like critical infrastructure and banking. This teaser provides a short synopsis on DTs; tune in to the third SIW article in this series for a deeper dive into DTs, modeling and simulation, and how they can improve the security landscape—including better safety for responding teams and enhanced mission success.

Encryption Solutions

Five key considerations for tackling Zero Trust

Mark Cassetta

Cybersecurity

Seven critical requirements true zero trust authentication solutions should meet

Jasson Casey

Access & Identity

What Zero Trust Means for Physical Security Systems

Jason Beers

Conclusion

Integrating ZT data principles with AI systems is not just the best practice but a necessity. As AI reshapes how organizations detect and respond to threats, the integrity and security of the data fueling these systems are paramount. From mitigating security risks, ensuring data quality, aligning with regulatory compliance, and enhancing ethical AI development, ZT data frameworks form the cornerstone of resilient and trustworthy AI applications.

The message is clear: **Bad Data In = Bad Data Out**, and the industry must use ZT data to avoid the *fait accompli*. Organizations that fail to implement ZT data in their AI systems are setting themselves up for inevitable security breaches and operational disruptions that may not be recoverable. Leaders and stakeholders must ask themselves whether they will accept the consequences of using untrusted data...or commit to the righteous path of integrating ZT principles. The choice between a secure, ethical, and high-performing AI system or one destined for failure hinges on this critical decision—and directly impacts the utilization and effectiveness of DTs. Neglecting ZT principles could compromise the efficacy of AI systems, leading to reputational damage, significant

financial and legal repercussions, risk to personnel, or even systemic mission failures.