TACHLES VC

## The AI-Cloud-Cyber Flywheel:

# What Investors Are Missing in 2026

# The world is harder to read than it used to be.

Trade routes are being redrawn. Long-standing alliances are fracturing. The global macroeconomic consensus is undergoing a structural fracture. Technology is advancing faster than most institutions can adapt to. And everywhere – from central banks to boardrooms to family offices – the same question keeps surfacing: **where do you put capital when the old certainties no longer hold?**

This paper is an attempt to answer that question. Not by predicting what comes next – nobody can do that with confidence right now. But by identifying something more valuable: a thesis that holds regardless of what comes next.

If you built a company, you know the difference between the product and the plumbing. The product gets the headlines. The plumbing is what nobody talks about – until it fails. And when it fails, everything stops.

Right now, the global conversation about AI is almost entirely about the product. This paper is about the plumbing – and **why the infrastructure layer underneath the AI revolution is where durable capital should be anchored in 2026.**

# The Argument

The **global economic order is splintering** into competing geopolitical blocs, terminating the era of seamless international integration. This structural fracturing mandates a fundamental shift in institutional capital allocation.

This whitepaper details a pivot away from highly visible software applications toward the underlying **physical and digital infrastructure** that powers the modern economy.

The convergence of **artificial intelligence**, **cloud architecture**, and **cybersecurity** has created something that did not exist a decade ago: a digital infrastructure layer with the demand characteristics of a physical commodity.

It is constrained by real-world limitations like power grids, data center capacity, semiconductor supply chains. Its demand is non-discretionary. And unlike software applications, which can be replaced overnight, the infrastructure beneath them carries switching costs that make **displacement nearly impossible** once embedded.

This paper maps that infrastructure, explains why the three sectors reinforce each other in a **self-reinforcing cycle**, and makes the case for why this convergence – rather than the AI application layer capturing most of today's headlines – is **where long-term value will accrue**.

> “The application layer attracts the capital and the headlines. The infrastructure layer captures the value. History is consistent on this: the companies that power a technology wave outlast and outperform the companies that ride it. Our thesis is built on that asymmetry.”
>
> **Tachles VC**

# Contents

# Macro Instability and the Rise of Digital Infrastructure

The macroeconomic forces reshaping the global economy do not affect AI, cloud infrastructure, and cybersecurity independently. Instead, they tighten the interdependence between them.

**Growth volatility, persistent inflation**, and **geopolitical fragmentation** are simultaneously increasing demand for digital infrastructure while reinforcing the operational links between these three technologies.

**Each macro force accelerates a different dimension of this convergence:**

## 1. Growth Volatility – Productivity Driver

When economic growth becomes uncertain, companies face an immediate structural pressure: do more with less. Capital expenditure comes under scrutiny, headcount growth slows, and the mandate shifts from expansion to efficiency.

In this environment, AI becomes the primary tool for increasing productivity. But deploying AI at enterprise scale is not a software decision – it is an infrastructure decision. It requires massive compute, scalable data pipelines, and reliable cloud infrastructure. Every serious **AI deployment leads directly to expanded cloud spend.**

As AI adoption increases, cloud infrastructure expands. → Systems grow more complex, more interconnected, and more exposed. → Attack surfaces widen. → The demand for cybersecurity rises as an operational requirement.

**The implication for investors is direct: economic turbulence does not slow the AI-Cloud-Cyber cycle. Rather, it accelerates it.**

## 2. Inflation – Infrastructure Pricing Power

Digital infrastructure is not immune to inflation. It is reshaping how inflation behaves within the technology sector:

AI training and inference require enormous physical resources.

Cloud providers must continuously build and maintain data centers.

As input costs rise, providers pass them downstream.

Enterprise compute bills increase.

Security contracts reprice upward.

This dynamic turns digital infrastructure into something that increasingly resembles a utility sector: essential, price-inelastic, and structurally capable of preserving pricing power through inflationary cycles.

Cybersecurity benefits through a parallel mechanism. **As the value of digital assets rises, so do the costs of a breach** – financially, operationally, and reputationally. Security spending becomes genuinely non-discretionary. Inflation, counterintuitively, strengthens rather than weakens the economic position of the infrastructure layer.

## 3. Geopolitical Instability – Digital Sovereignty

Technology infrastructure has been reclassified. What was once treated as a commercial service is now treated as a strategic national asset. This shift is visible in concrete policy actions across every major economy:

Semiconductor export controls restricting access to advanced chips.

Sovereign cloud initiatives require data to remain within national borders.

National AI strategies mandate domestic compute capacity.

Data localization laws force multinationals to restructure their infrastructure.

These represent a long-term structural reorientation of how governments think about digital capability. And they drive massive investment in domestic AI compute, localised cloud infrastructure, and national cybersecurity capabilities.

At the same time, the nature of geopolitical conflict is changing. A growing share of modern confrontation is conducted in cyberspace.

State-sponsored actors target financial systems, healthcare infrastructure, cloud platforms, and information environments, disrupting economic activity and influencing public behaviour without direct military confrontation. Governments are responding by treating cybersecurity as a core element of national defense, not merely as an enterprise IT concern.

The strategic consequence reinforces the same logic: AI infrastructure must run on cloud, and cloud infrastructure must be secured against cyber attacks. Every geopolitical pressure point accelerates investment in all three sectors simultaneously.

> “Macro instability forges the inevitability of digital infrastructure: every shock to growth, price, or geopolitics tightens the bond between AI, cloud, and cybersecurity, turning them from tools of progress into the backbone of survival.”
>
> **David Marek**
> Managing Partner, Tachles VC

## Resilience Over Efficiency

For most of the past two decades, the corporate technology mandate was straightforward: move faster and spend less. Cloud made this possible. Outsource infrastructure, scale on demand, optimize continuously. Efficiency was the metric.

That mandate is changing. National security, energy production, and hardware supply chains are now converging in ways that force enterprises and sovereign states to **prioritise operational resilience over financial efficiency**. The question is no longer "how cheaply can we run this?" It is "**can we guarantee this keeps running?**"

The 2025 AI chip crisis made this concrete. When access to advanced semiconductors became a geopolitical variable rather than a commercial one, the assumption of infinite digital scalability collapsed. AI expansion turns out to be dictated by hard physical constraints like data center real estate, liquid cooling capacity, and multi-gigawatt power grid access.

This has a direct consequence for how digital infrastructure should be classified as an asset. It no longer behaves like a scalable software service. Rather, it behaves like a constrained physical commodity with supply limitations, geopolitical exposure, and pricing power that compounds as demand grows faster than capacity. Instead of chasing speculative growth, **institutional capital entering this layer is securing access to the physical prerequisites of operating in the next decade**.

For institutional allocators, this environment raises one essential question:

In a world this unpredictable, what actually holds?

The answer requires a different kind of analysis. Not forecasting which sectors will grow, but identifying which ones have already become structurally immune to the conditions described above.

# Finding the Signal: Trends That Survive Everything

The hardest problem in long-duration capital allocation is **identifying growth that persists regardless of what you cannot predict**: recessions, geopolitical fractures, monetary crises, wars.

Most investment theses are implicitly macro-dependent. They assume a particular rate environment, a particular trade regime, a particular political stability. When those conditions shift, the thesis breaks.

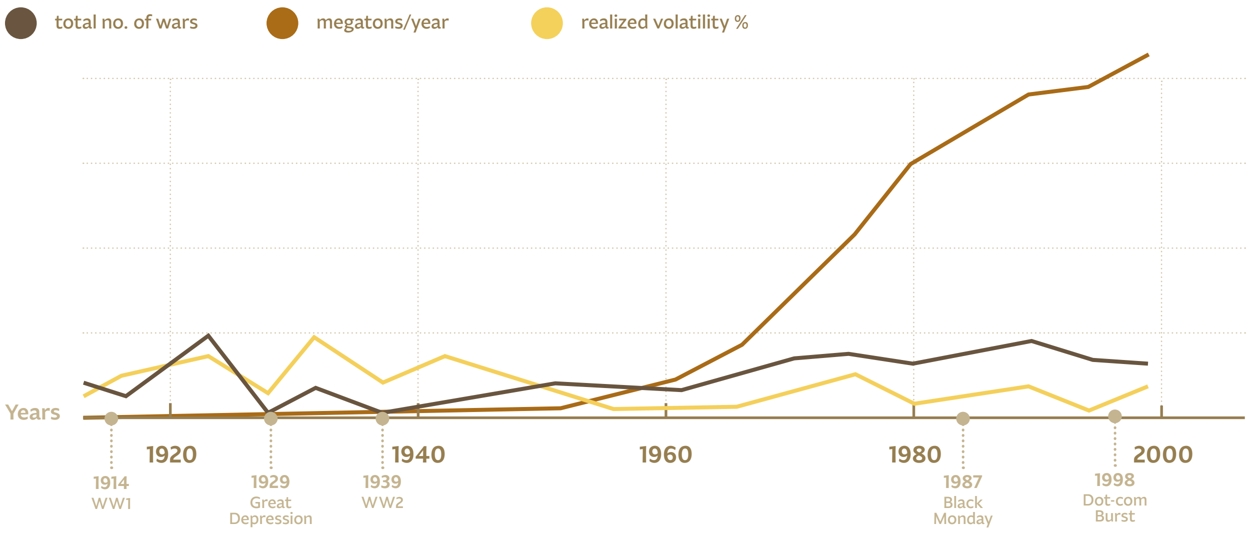
The more useful question is: do we have historical **examples of structural trends that proved genuinely immune to macro conditions**? Trends that grew not despite turbulence, but indifferently to it?

We do. The **industrialization of agriculture** is the clearest case.

The mass production of synthetic fertilizers beginning in the early 20th century re-engineered the productive capacity of the global economy. By exponentially increasing caloric output per hectare, it eliminated the physical bottleneck that had constrained human civilization for millennia.

The consequences were permanent: a massive **reallocation of surplus labor toward industry and services**, and the creation of an entirely new base layer of economic production. What makes this case analytically useful is the macro context in which it occurred:

## Global Fertilizer Use vs. No. of Global Wars



Source:
1. Correlates of War - Wars (2020) – processed by Our World in Data
2. Vaclav Smil, Enriching the Earth
3. Shiller, Robert J. Online Data: U.S. Stock Markets 1871–Present and CAPE Ratio, Yale Department of Economics

Two world wars. The Great Depression. The Cold War. Decolonization. Repeated monetary crises. Through every one of these, fertilizer production grew – not because the world was stable, but because the underlying need it served was structural, not cyclical.

> “Once a civilization depends on a technology for its basic productive capacity, it cannot opt out.”
>
> **Karel Tušek**
> Managing Partner, Tachles VC

Translated into investment terms, the question is never simply “is this market growing?” It is whether a technology has become load-bearing infrastructure. The kind enterprises and sovereign states cannot function without, regardless of macro conditions.

The same test, applied to 2026, surfaces more than one answer. Energy infrastructure qualifies. So does semiconductor manufacturing, where control of advanced chip production has become as geopolitically charged as control of oil fields once was. Both deserve serious capital from allocators with the expertise to evaluate them.

**The convergence that meets the test most precisely is the interlocking dependency between artificial intelligence, cloud architecture, and cybersecurity.**

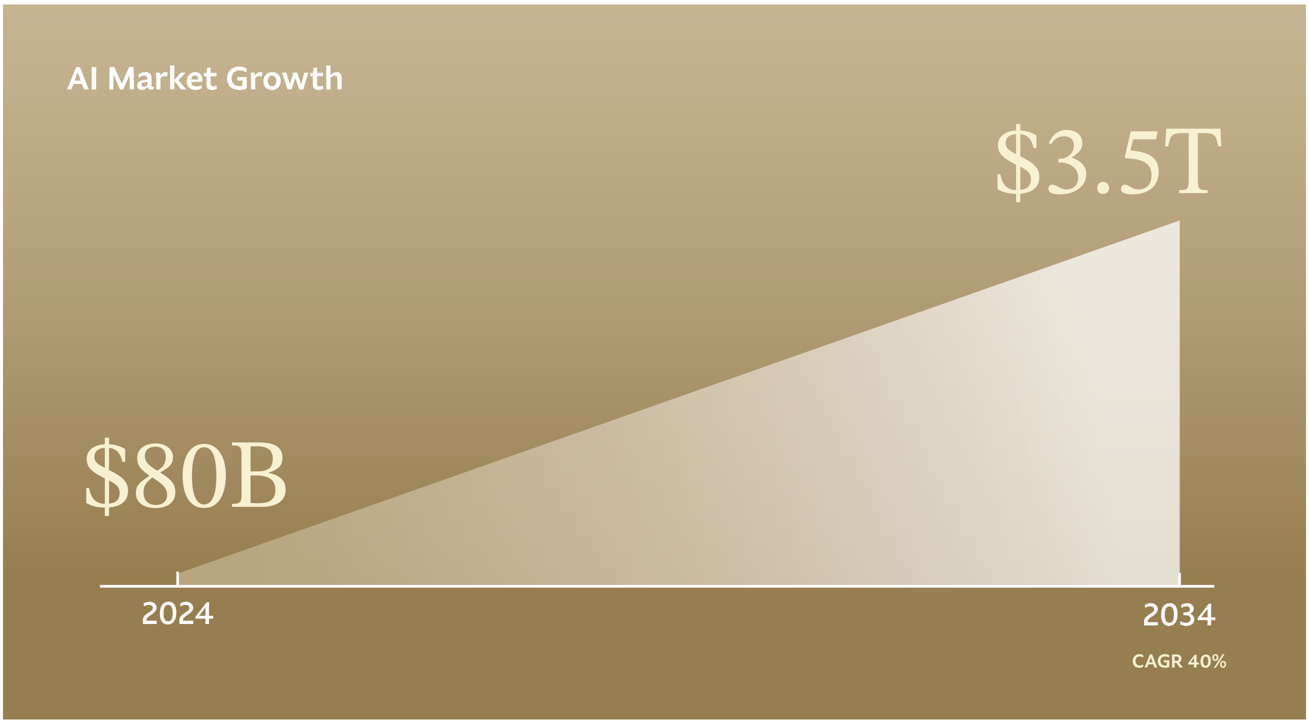
These three sectors have already become structurally indispensable. Their interdependence creates a self-reinforcing cycle of mandatory enterprise expenditure that functions independently of which application wins, which model dominates, or which geopolitical bloc prevails.

The remainder of this paper maps the mechanics of that cycle.

# Mapping the Three Forces of the Convergence

## Force One: Artificial Intelligence

According to Polaris Market Research, the **global AI market stood at approximately $80 billion in 2024 and is projected to reach $3.5 trillion by 2034** – a fifteenfold expansion over a decade, compounding at roughly 40% annually. These figures have attracted significant capital. They have also attracted significant misallocation.



The fundamental error most investors make is treating AI as a monolithic category. It contains within it a spectrum of risk and durability that varies enormously depending on where in the stack you are positioned.

The AI application layer carries the risk profile of any winner-take-most market: spectacular when you pick correctly, capital-destructive when you don't. More importantly, the barrier to entry has collapsed. Describing a product as "AI-powered" today is the equivalent of saying in 2005 that it uses the internet, or in 1995 that it runs on a PC. It is not a differentiator. It is the baseline. Every competitive enterprise will use AI. That observation is not an investment thesis.

The durable thesis lives in AI infrastructure – the technologies enabling enterprises across industries to **adopt AI faster, better, and cheaper**. The 1990s analogy is instructive: the lasting fortunes of that era were built not by those who backed specific applications, but by those who backed operating systems, databases, and networking protocols. Infrastructure captured compounding value regardless of which application won.

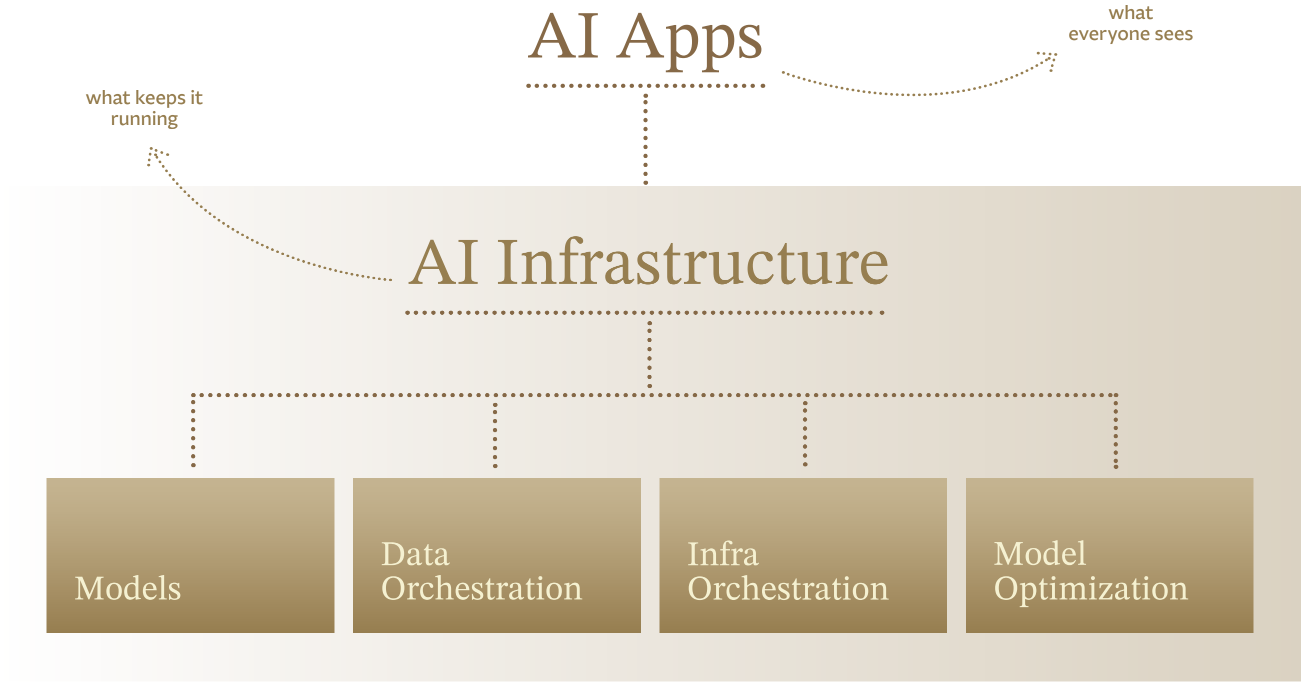
**Within AI infrastructure, four distinct layers define the investment landscape:**

01 **The models layer** (hyperscalers and foundational LLMs) carries extreme capital concentration and genuine architectural risk. Today's dominant paradigm of centralized, massive compute may follow the same trajectory as the mainframe. The industry likely does not need room-sized computers forever. Smaller specialized models and edge AI (running on-device without datacenter dependency) represent the emerging transition. This layer warrants careful exposure, not avoidance, but with open eyes to the shift.

02 Below models sits **data orchestration**: the tooling governing how training and inference data is curated, labeled, versioned, and governed. Enterprises cannot deploy AI at scale without controlling their data supply chain.

03 **AI infrastructure orchestration** addresses the next layer of complexity. As AI tech stacks deepen, the infrastructure itself must be managed using AI. Workflow automation platforms, agent orchestration layers, and MLOps pipelines coordinating multi-model environments across hybrid infrastructure represent a category that barely existed three years ago.

04 Finally, **model optimization** (machine unlearning, debiasing, removing sensitive information) is not a product feature for regulated enterprises. Rather, it is a legal requirement under GDPR, the EU AI Act, and emerging US frameworks, creating non-discretionary procurement independent of which model vendor wins.

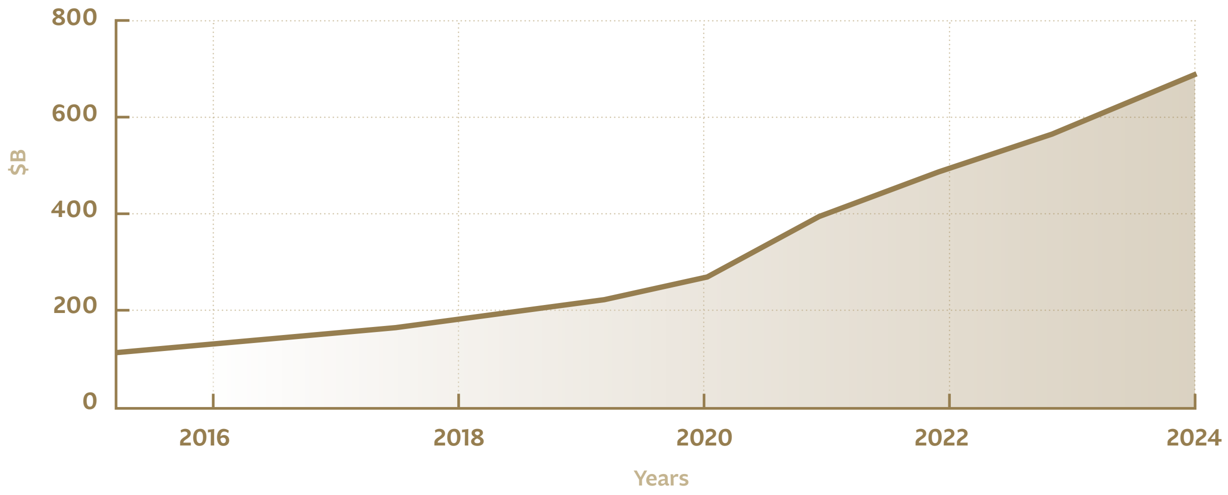


## Force Two: Cloud Architecture

The conventional narrative treats cloud as a maturing market. The mechanism of growth, however, has undergone a structural break. And that break is precisely what makes the investment case more compelling now than at any prior point in the sector's history.

Gartner forecasts worldwide public cloud end-user spending from $153 billion in 2017 to over $700 billion in 2025. But the rate is accelerating, not slowing, and the reason matters enormously for how capital should be allocated.

### Public Cloud End-User Spending



Charts Sources:
1. Dell'Oro Group: ‚Data Center Capex Surged 51% to $455B in 2024' (March 2025 press release). Confirmed endpoint: ‚$1 trillion by 2029.' Projected +30% growth in 2025.
2. Hyperscaler Big-4 2024 CAPEX ($251B): Amazon 10-K 2024, Alphabet 10-K 2024, Microsoft Annual Report FY2024, Meta 10-K 2024. Confirmed: +62% YoY from 2023 ($155B).
3. Hyperscaler Big-4 2025 CAPEX ($416B): Confirmed from Q4 2025 earnings releases (Feb 2026). Amazon $125B, Alphabet ~$93B, Meta ~$68B, Microsoft ~$130B. +66% YoY.
4. 2026 guidance: Wolf Street (Feb 2026) — Amazon, Google, MSFT, Meta, Oracle collectively plan ~$700B.

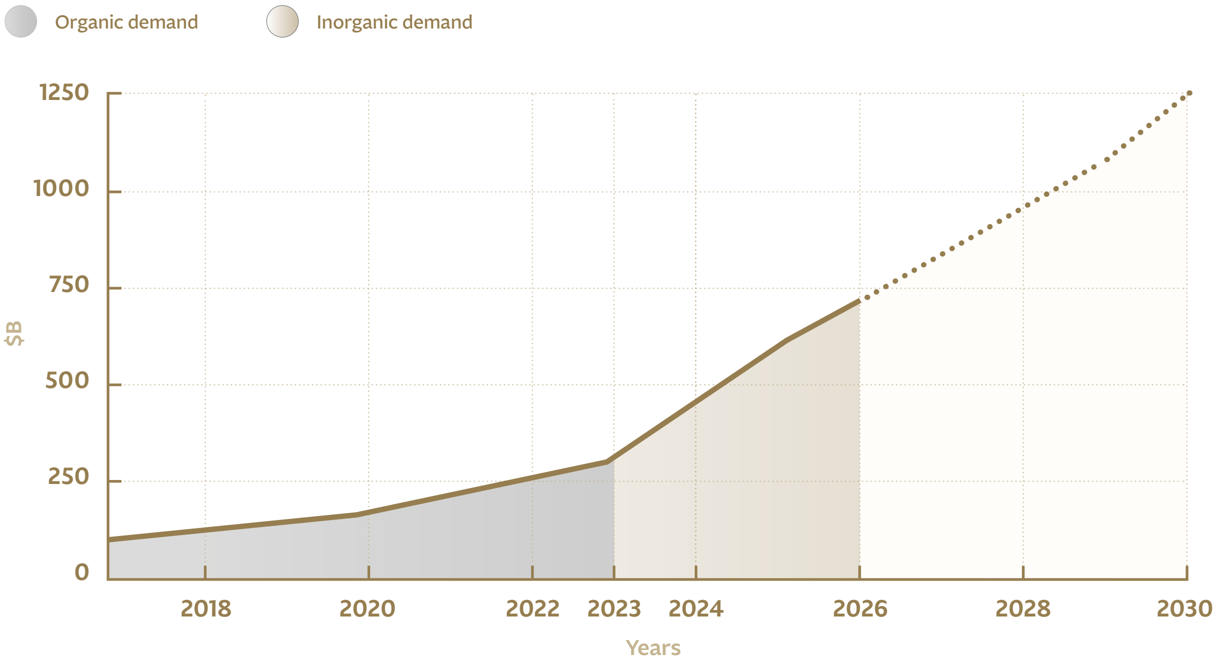
For most of the last decade, cloud growth was organic. It followed predictable business growth: More employees meant more customers which meant more transactions, ultimately leading to more compute storage.

That growth was real and substantial, but it was ultimately tethered to the pace of enterprise digitization and to how fast companies moved their operations online.

Today's growth driver is categorically different. AI training workloads do not scale with the number of businesses adopting cloud. They scale with model complexity, dataset size, and neural network architecture. A single frontier model training run can consume more compute than thousands of conventional enterprise applications combined.

This is inorganic demand – infrastructure requirements disconnected from headcount, revenue, or traditional business metrics.
It is demand created by the physics of AI development itself, and it has no natural ceiling tied to how many companies exist or how fast they grow.

## Global Data Center CAPEX



Charts Sources:
1. Dell’Oro Group: ‚Data Center Capex Surged 51% to $455B in 2024‘ (March 2025 press release). Confirmed endpoint: ‚$1 trillion by 2029.‘ Projected +30% growth in 2025.
2. Hyperscaler Big-4 2024 CAPEX ($251B): Amazon 10-K 2024, Alphabet 10-K 2024, Microsoft Annual Report FY2024, Meta 10-K 2024. Confirmed: +62% YoY from 2023 ($155B).
3. Hyperscaler Big-4 2025 CAPEX ($416B): Confirmed from Q4 2025 earnings releases (Feb 2026). Amazon $125B, Alphabet ~$93B, Meta ~$68B, Microsoft ~$130B. +66% YoY.
4. 2026 guidance: Wolf Street (Feb 2026) — Amazon, Google, MSFT, Meta, Oracle collectively plan ~$700B.

The consequence for capital allocation is significant. Enterprise infrastructure budgets are expanding to accommodate requirements with no precedent in prior technology cycles. This is non-discretionary spend: you cannot train, fine-tune, or deploy AI at competitive speed without it. CFOs who spent the last decade optimizing cloud costs are now writing checks for capacity that simply cannot be negotiated away.

This demand shift is simultaneously forcing a generational replacement of the software layer managing cloud infrastructure. The orchestration tools, storage systems, and network architectures built for 2000, 2010, and even 2020 were designed for a fundamentally different problem. AI-native infrastructure requires AI-native management, built on different assumptions about data locality, workload distribution, latency tolerance, and security architecture. **What is occurring is a replacement cycle, and replacement cycles create large, durable markets.**

**Three categories are emerging directly from this shift:**

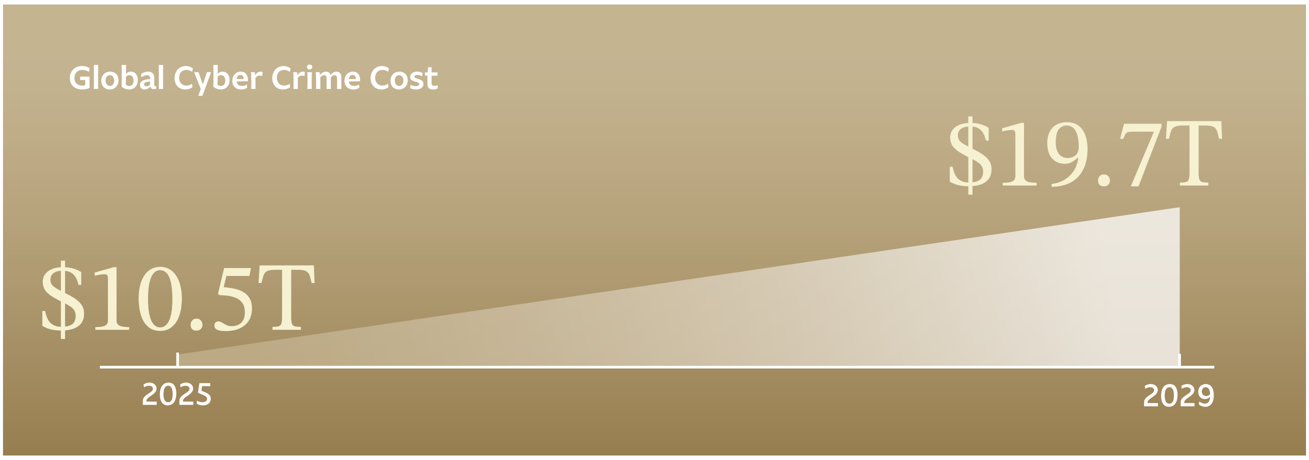
01 **Cloud orchestration and cost optimization**, as the economics of compute allocation at AI scale become a board-level concern;

02 **New storage paradigms**, including vector databases and tiered architectures optimized for inference patterns;

03 **Network AIOps**, as autonomous network management becomes infrastructure-critical rather than an optimization layer.

## Force Three: Cybersecurity

According to Cybersecurity Magazine, global cybercrime costs reached $10.5 trillion in 2025 and are projected to hit $19.7 trillion by 2029. To contextualize that figure: it exceeds the GDP of every nation on earth except the United States and China.



Source: Cybersecurity Magazine

The economics of conflict have been permanently altered by AI. **Kinetic warfare is expensive** as it requires hardware, logistics, personnel, and territorial exposure. **Cyber conflict operates with extreme cost asymmetry.** AI-driven attack tooling allows hostile actors, whether state-sponsored or criminal, to inflict structural damage on critical infrastructure at a fraction of the cost of conventional methods.

The barrier to launching a sophisticated cyberattack has collapsed in direct proportion to the democratization of AI capability. This has catalyzed a permanent phase **shift in the volume and velocity of digital conflict**.

The architectural consequence for enterprise security is severe. The traditional network perimeter assumed a defined boundary between trusted internal systems and untrusted external ones.

That boundary no longer exists in any meaningful sense. Autonomous machine identities, API endpoints, and AI agents now vastly outnumber human users inside enterprise environments. **Legacy perimeter defenses cannot stop authenticated machines** from moving laterally within systems they have already accessed.

The definitive perimeter of modern enterprise security is identity – specifically, dynamic Identity and Access Management designed for non-human behavioral patterns. **As enterprises deploy AI agents for complex workflows, the attack surface extends further:** agent-to-agent protocols introduce novel vulnerabilities where malicious actors can inject obfuscated commands directly into the session stream of a legitimate enterprise AI agent. Defending against this requires security architectures that were simply not designed with the current threat model in mind.

This creates a procurement environment unlike any prior security cycle. **Enterprise security spending is an operational prerequisite.** Regulated industries cannot legally deploy AI systems without certified security architectures around them.

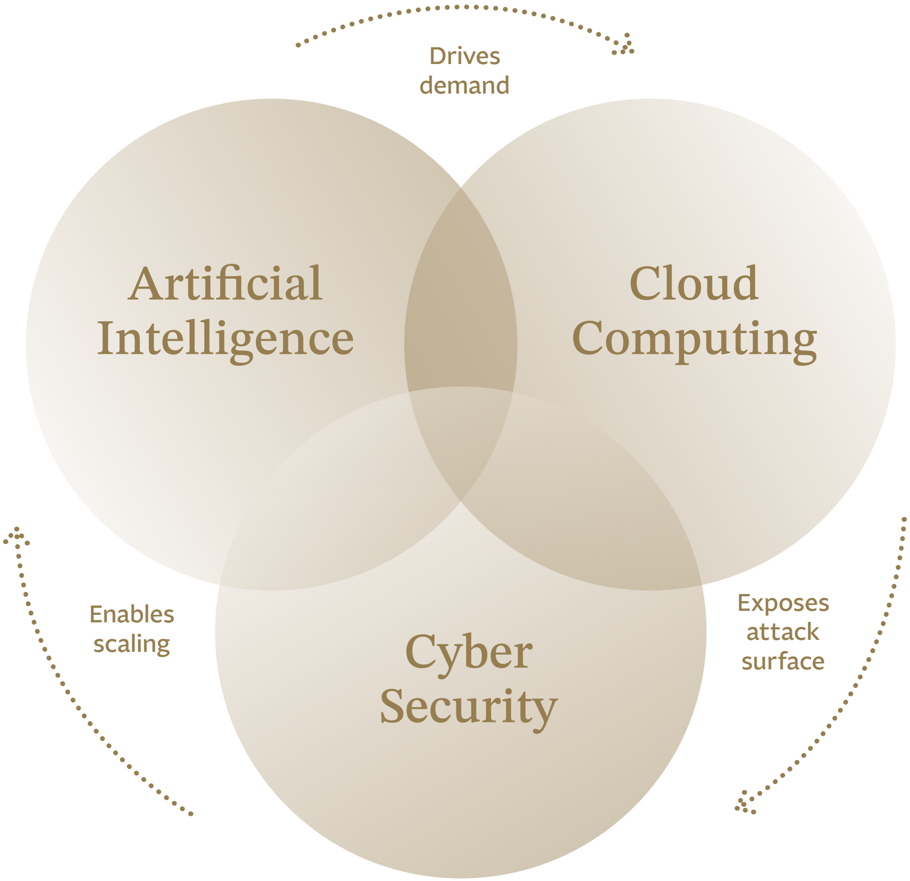
This non-discretionary demand, scaling in direct proportion to AI adoption, is precisely the dynamic that makes cybersecurity the third force in this convergence.

# The AI-Cloud-Cybersecurity Flywheel

Three forces. Each structurally compelling in isolation. Each supported by non-discretionary enterprise demand, physical constraints on supply, and regulatory mandates that remove purchasing discretion from the equation.

But the analysis so far has described them as three separate trends that happen to be growing simultaneously. That framing understates the case considerably.

**These forces are not parallel. They are a single self-inforcing system.**



The connection is not philosophical or metaphorical but rather operational and mathematical. Each force directly creates the conditions that make the next force mandatory. The cycle is self-reinforcing, continuous, and generates obligatory enterprise expenditure at every single node regardless of which vendor, model, or platform happens to be dominant at any given moment.

**The mechanics work as follows:**

01 **Enterprise AI deployment requires cloud compute.**
This is a technical prerequisite. Training, fine-tuning, and running inference on AI models at enterprise scale demands cloud infrastructure that cannot be replicated on-premise at equivalent cost or speed. Every dollar spent deploying AI mandates a corresponding allocation to cloud architecture. The first force activates the second.

02 **Cloud scaling expands the attack surface.**
As enterprises centralize sensitive intellectual property in cloud environments, they concentrate risk. The probability of systemic breach increases exponentially with infrastructure complexity. Threat actors, exploit this broadened surface at machine speed and scale. The second force activates the third.

03 **Cybersecurity fortification enables the next AI cycle.**
A hardened security perimeter built for AI-native threats, non-human identities, and autonomous agent interactions is the compliance precondition for deploying more advanced AI workloads. Regulated enterprises cannot legally expand AI deployment into sensitive workflows without certified security architecture beneath it. Every security investment restores the mandate to deploy more AI. The third force reactivates the first.

This is a story about a closed loop of mandatory enterprise expenditure that compounds with each rotation. The investor positioned across this flywheel does not need to predict which AI model wins, which cloud platform dominates, or which security vendor achieves market leadership. The structural return accrues to the infrastructure layer regardless, because the cycle continues independent of who occupies each node.

There is one further quality that distinguishes this flywheel from ordinary market growth: **enterprises cannot exit it once they have entered**. The switching costs embedded at each stage make reversal prohibitively expensive. Each rotation of the cycle deepens the lock-in. Capital allocated to this infrastructure layer is securing a position inside a closed system that the global enterprise economy has already made structurally dependent upon.

Let's return to the agricultural revolution. Once synthetic fertilizers became embedded in the global food supply chain, there was no path back to pre-industrial yields. Civilization had reorganized around the new productive capacity, and the infrastructure enabling it became permanently indispensable – immune to wars, depressions, and political upheaval because opting out meant accepting operational obsolescence.

The AI-Cloud-Cybersecurity flywheel has crossed an equivalent threshold. The **global enterprise economy has reorganized around digital infrastructure** with sufficient depth that withdrawal is no longer a rational option for any competitive organization. This is the condition that **produces the most durable returns in venture capital**: not the fastest-growing market, but the one that enterprises and sovereign states have made themselves permanently unable to live without.

> “We do not speculate on application-layer outcomes. We back the structural base that all outcomes require. Infrastructure investments in this cycle compound independently of which model, platform, or application achieves temporary dominance. That independence is a feature, not a limitation.”
>
> **Karel Tušek**
> Managing Partner, Tachles VC

## Market Consolidation and Enduring Value

The AI-Cloud-Cybersecurity flywheel does not merely survive market turbulence. Rather, it accelerates through it.

Consider the cognitive dimension first. The convergence of these three forces generates a massive computational and cognitive surplus – automating the data orchestration, threat monitoring, and infrastructure management that previously consumed disproportionate human capital.

The consequence is a permanent reallocation of enterprise labor away from repetitive operational overhead toward higher-leverage strategic output. Enterprises are not investing in this infrastructure to cut costs. They are **investing to multiply the productive capacity of their existing workforce**.

### History provides the clearest evidence:

When the dot-com bubble collapsed in the early 2000s, the casualties were visible and spectacular: consumer-facing internet companies with unsustainable unit economics were liquidated in the thousands. But the institutional capital deployed into sub-oceanic fiber-optic cables, foundational servers, and network infrastructure remained permanently embedded. Rather than disappearing, it simply became available at distressed valuations to the enterprises with the operational discipline to use it. Google and Amazon built the modern digital economy on that discounted foundation.

The current AI market will likely follow the same historical precedent. A speculative collapse in consumer-facing AI applications – which carry many of the same unsustainable economics as 2000-era internet companies – would eradicate undifferentiated software wrappers while leaving the underlying infrastructure layer structurally intact. Capital would not exit the sector. It would consolidate around the infrastructure monopolies that survived, cementing their pricing power precisely because the alternatives had been eliminated.

in **2000**, applications collapsed, infrastructure survived

in **2026**, applications might collapse, infrastructure will survive

The infrastructure layer is additionally insulated by the commercial structure of its revenue. As enterprises process larger data volumes, run more AI workloads, and expand their security perimeters, spend per customer grows automatically. Corporate CFOs are locking in multi-year procurement contracts for secure data orchestration, cloud capacity, and automated threat detection. This is a budget that is committed in advance and resistant to quarterly fluctuation.

The endpoint of this consolidation is clear. Platforms that autonomously orchestrate, secure, and govern enterprise workloads at scale become the de facto operating system of the modern enterprise. And that utility is entirely upstream-agnostic: even if a leading foundational model collapses, enterprise demand for secure data routing, identity management, and infrastructure orchestration remains absolute. **The flywheel continues regardless of which application layer occupies the surface.**

# Conclusion

The global economy is undergoing a structural reconfiguration from frictionless globalization toward fortified regional fragmentation, from financial efficiency toward operational resilience, from software abundance toward infrastructure scarcity.

In this environment, the thesis is straightforward. Abstract, consumer-facing software layers will face accelerating margin compression as commoditization and capital destruction play out. Durable, long-term value will accrue to the infrastructure layer – the foundational systems that enterprises and sovereign states have already made themselves structurally dependent upon.

The convergence of AI, cloud architecture, and cybersecurity is the load-bearing infrastructure of the next phase of global economic production. Its demand is non-discretionary. Its switching costs are prohibitive. Its growth compounds regardless of which applications or models achieve temporary market dominance. And its position in the enterprise stack deepens with every rotation of the flywheel.

Identifying and backing the right companies within this convergence is not a generalist task. It requires the operational precision to map interdependencies between hardware bottlenecks, autonomous agent security, data sovereignty mandates, and model infrastructure – before those interdependencies become consensus. It requires pattern recognition built over years of proximity to the ecosystem where this infrastructure is being built.

The investors who will capture the majority of sustainable wealth generated in this technological epoch are not those chasing the most visible opportunities. They are those who understood the infrastructure thesis early, positioned deliberately, and held with conviction through the noise.

# Questions we hear from Limited Partners

## Is the current AI market a speculative bubble or a durable macroeconomic trend?

The highly visible AI application layer carries significant speculative bubble risk, characterized by hyper-competition, intense capital destruction, and severe commoditization threats for companies lacking proprietary data. Conversely, the underlying utility and infrastructure layers (data sovereignty enforcement, algorithmic model cleaning, identity management for autonomous agents etc.) represent a highly durable macroeconomic trend. These foundational systems retain enduring value because regulated enterprise workflows systematically require them for absolute legal compliance and secure deployment.

## How should investors deploy capital amid rising global instability and inflation?

Investors should pivot more toward digital assets that offer inelastic demand and possess monopolistic pricing power against currency debasement. Because AI hyperscalers finance massive data center capital expenditures through long-duration corporate debt, rising baseline inflation systematically shrinks their real debt obligations while they pass inflationary hardware costs directly to software consumers. Allocating capital to this digital infrastructure layer functions as a powerful, mathematically built-in financial hedge against fiat currency volatility and geopolitical friction.

## How must a venture portfolio strategically restructure for the 2026 economic reality?

A resilient 2026 portfolio abandons fragmented, speculative bets on consumer-facing software wrappers and consolidates capital into the AI-Cloud-Cybersecurity Flywheel. This self-reinforcing macroeconomic loop dictates that surging enterprise AI adoption demands expansive cloud computing pipelines, which immediately expands the organizational attack surface, thereby mandating strict AI-native cybersecurity procurement. Investing directly into this continuous compounding cycle effectively captures the mandatory, non-discretionary enterprise spending generated at every single stage of the digital supply chain.

TACHLES VC

# About
# Tachles VC

The thesis in this paper is not theoretical. It reflects a decade of pattern recognition built from ground level - from the first checks written into Israeli cloud and cybersecurity infrastructure in 2015, through the exits like of Spot.io and Dataloop, to the current portfolio of twelve companies operating across every layer of the AI-Cloud-Cybersecurity flywheel.

Tachles VC is an early-stage venture capital firm backing deep-tech founders primarily in Israel. The firm was established by Czech managing partners Karel Tušek and David Marek, Israeli insiders Sivan Kanev and Boris Chovnik, and U.S.-based operator Robin Bienfait, later extended with Dan Dinnar, a former VP Sales of CyberArk. Together, the team has generated over $750 million in exit value in Israeli deep-tech – and has been named among the top three most active foreign investors in Israel since 2015.

Our edge is specificity. We do not cover the technology sector broadly. We invest in the infrastructure layer of the digital economy, the systems that enterprises and sovereign states cannot operate without. This focus is not a constraint. It is the source of the pattern recognition that lets us identify the right founders before the opportunity becomes consensus.

> “We are first to the opportunity because we see it clearly. We win early because we understand it deeply.”
>
> **Karel Tušek**
> Managing Partner, Tachles VC

> “Specialist funds do not outperform generalists by accident. They outperform because depth of knowledge compounds the same way infrastructure does: quietly, durably, and ahead of the market.”
>
> **David Marek**
> Managing Partner, Tachles VC

## Contact us

Scan for
more info

info@tachlesvc.com
www.tachlesvc.com

# Portfolio

Cyngular Security

Deskree

Shield IoT

Hirundo

Boost.Space

Counter Shadow

Manifolds.Lab

Chronom

Brinker

Acsense

WeCheck.AI

Langware.AI

TACHLES
VC