MVP Network Consulting
Technology That Works.

Cybersecurity at the Speed of AI: Are You Ready for What's Next?

Practical AI Guidance for WNY Businesses

MVP Network Consulting
Technology That Works.

Meet Ikram Massabini

CEO of MVP Network Consulting

25 Years of IT Experience

Expert IT Security Consultant

HIPAA Consultant & Auditor

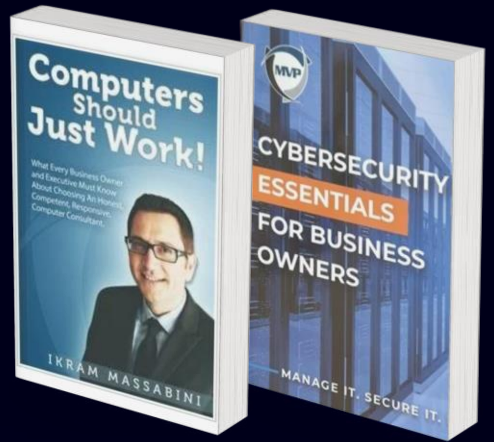
Security Certifications

BS in Electronic Engineering

Get in Touch

Connect with Ikram at:

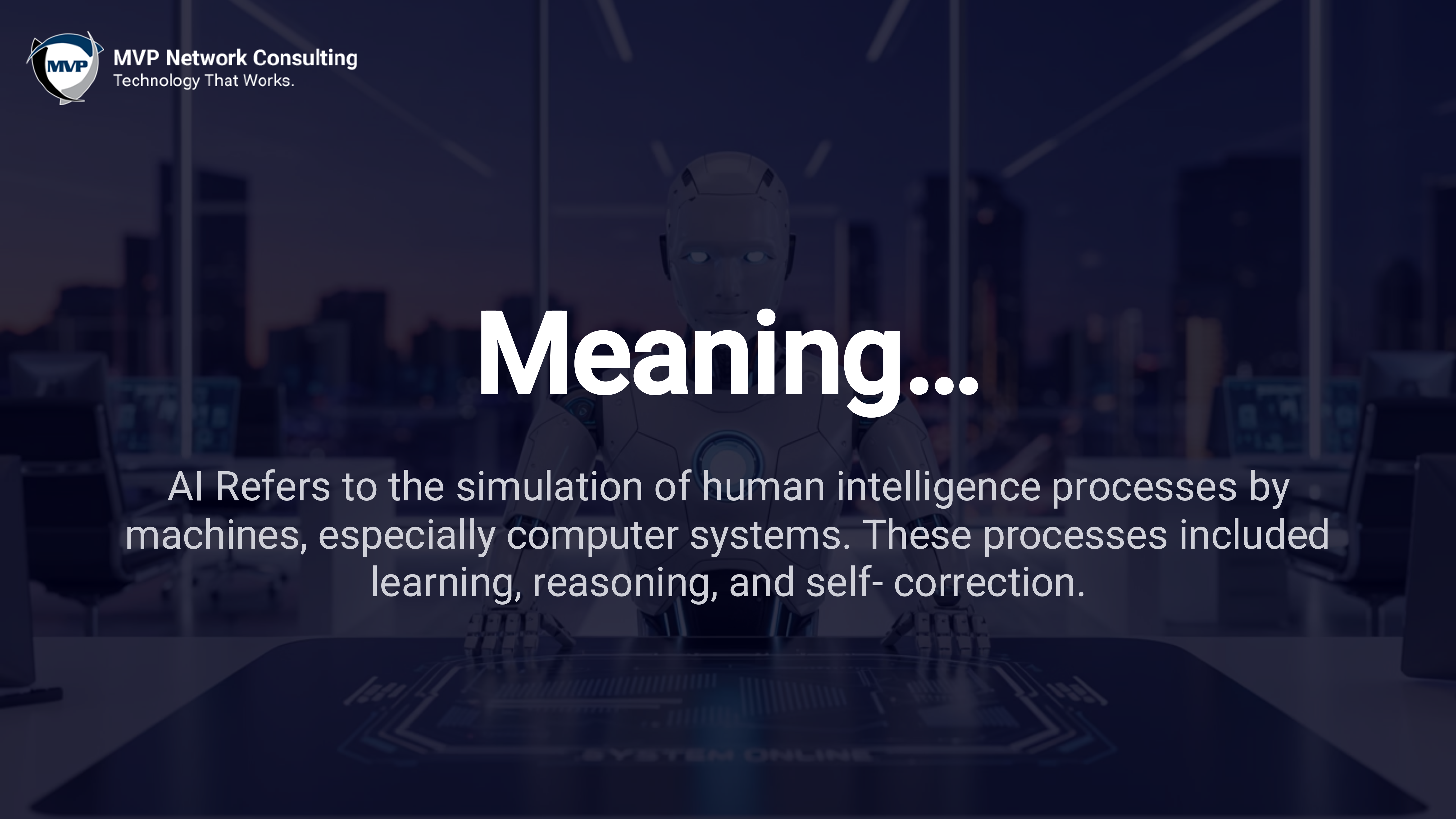
ikram@mvpworks.com


Computers Should Just Work!
What Every Business Owner and Executive Must Know About Choosing An Honest, Competent, Responsive, Computer Consultant.
IKRAM MASSABINI
MVP
CYBERSECURITY
ESSENTIALS
FOR BUSINESS OWNERS
MANAGE IT. SECURE IT.

MVP Network Consulting
Technology That Works.

What Is AI, Really?

(it's actually NOT very intelligent)



Meaning...

AI Refers to the simulation of human intelligence processes by machines, especially computer systems. These processes included learning, reasoning, and self- correction.

How Does AI Work?

It needs tons of data to work.

Engineers downloaded the entire internet *(articles, images, everything!)* and saved them in one big .txt file

And then, they assigned a number to every word.

They fed all the data into a neural network like a digital brain made of connected cells. It works kind of like how our brain does.

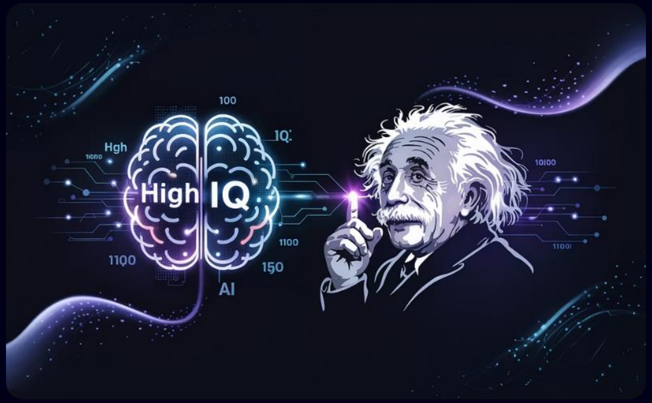
It had to train itself billions of times. Each time it got something wrong, engineers made adjustments.

...until this DUMB brain becomes really smart after billions of trials.

MVP Network Consulting
Technology That Works.

MVP Network Consulting
Technology That Works.

Here's the Facts...



Chat GPT 3.5 has an IQ of 155—Einstein's was 160!

What you see is only the tip of the iceberg...

GPT-4 became 10x smarter than 3.5 in months.

If this pace keeps up, AI could reach an IQ of 1600 in a few years!

The Big Players

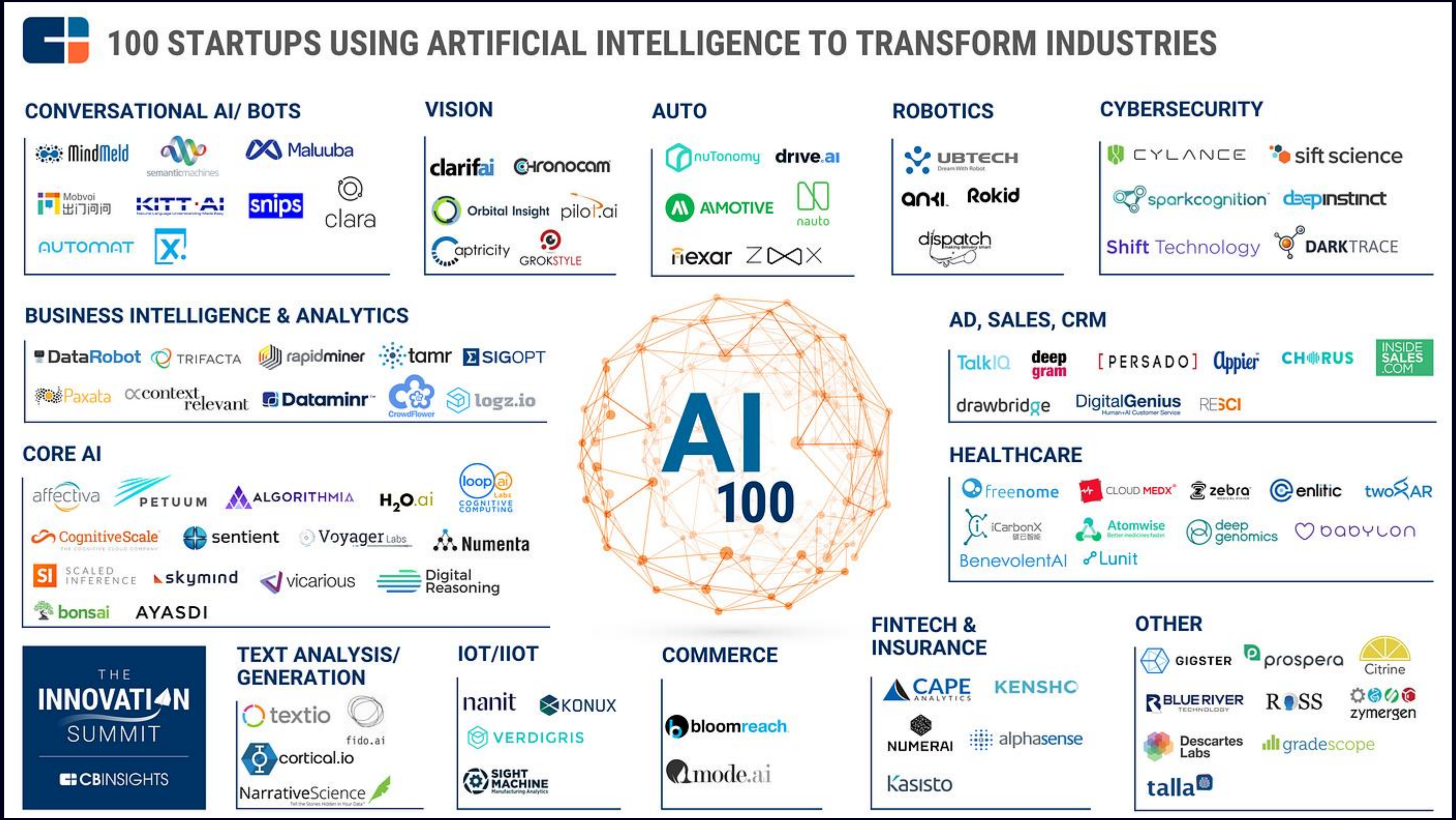
Owner	Microsoft	OpenAI	Google	Meta	X	Anthropic
Product	CoPilot	ChatGPT	~~Bard~~ - Gemini	Meta.ai	Gronk	Claude
Models (brains)	ChatGPT 4 ChatGPT 4o ChatGPT 5	ChatGPT 3.5 ChatGPT 4 ChatGPT 4o ChatGPT 5	Gemini Gemini Advanced	LLaMa 3B LLaMa 11B LLaMa 90B	Gronk 3 Gronk 4 Gronk 4 Heavy	Claude Opus 4.1 Claude Sonnet 4 Claude Haiku 3.5

A GPT LLM (Generative **Pre-trained** Transformer **Large Language Model**) is an advanced AI system trained on vast amounts of text to understand and generate human-like language.

It uses deep learning to predict and produce coherent responses based on context, making it useful for tasks like writing, summarizing, translating, and answering questions.

MVP Network Consulting
Technology That Works.

New Companies with pre-trained AI Agents



100 STARTUPS USING ARTIFICIAL INTELLIGENCE TO TRANSFORM INDUSTRIES

CONVERSATIONAL AI/ BOTS

MindMeld, semanticmachines, Maluuba, Mobvoi 出门问问, KITT.AI, snips, clara, AUTOMAT, X.

VISION

clarifai, Chronocam, Orbital Insight, pilot.ai, Captricity, GROKSTYLE

AUTO

nuTonomy, drive.ai, AIMOTIVE, nauto, nexar, ZOOX

ROBOTICS

UBTECH, anki, Rokid, dispatch

CYBERSECURITY

CYLANCE, sift science, sparkcognition, deepinstinct, Shift Technology, DARKTRACE

BUSINESS INTELLIGENCE & ANALYTICS

DataRobot, TRIFACTA, rapidminer, tamr, SIGOPT, Paxata, context relevant, Dataminr, CrowdFlower, logz.io

AD, SALES, CRM

TalkIQ, deep gram, [PERSADO], Appier, CHORUS, INSIDE SALES .COM, drawbridge, DigitalGenius, RESCI

CORE AI

affectiva, PETUUM, ALGORITHMIA, H2O.ai, loop ai Labs COGNITIVE COMPUTING, CognitiveScale, sentient, Voyager Labs, Numenta, SCALED INFERENCE, skymind, vicarious, Digital Reasoning, bonsai, AYASDI

AI 100

HEALTHCARE

freenome, CLOUD MEDX, zebra, enlitic, twoXAR, iCarbonX, Atomwise, deep genomics, babylon, BenevolentAI, Lunit

THE INNOVATION SUMMIT
CBINSIGHTS

TEXT ANALYSIS/ GENERATION

textio, fido.ai, cortical.io, NarrativeScience

IOT/IIOT

nanit, KONUX, VERDIGRIS, SIGHT MACHINE

COMMERCE

bloomreach, mode.ai

FINTECH & INSURANCE

CAPE ANALYTICS, KENSHO, NUMERAI, alphasense, Kasisto

OTHER

GIGSTER, prospera, Citrine, BLUE RIVER TECHNOLOGY, ROSS, zymergen, Descartes Labs, gradescope, talla

My AI Prediction

Soon, with a few clicks, a business can basically stand up an AI agent that can do the following:

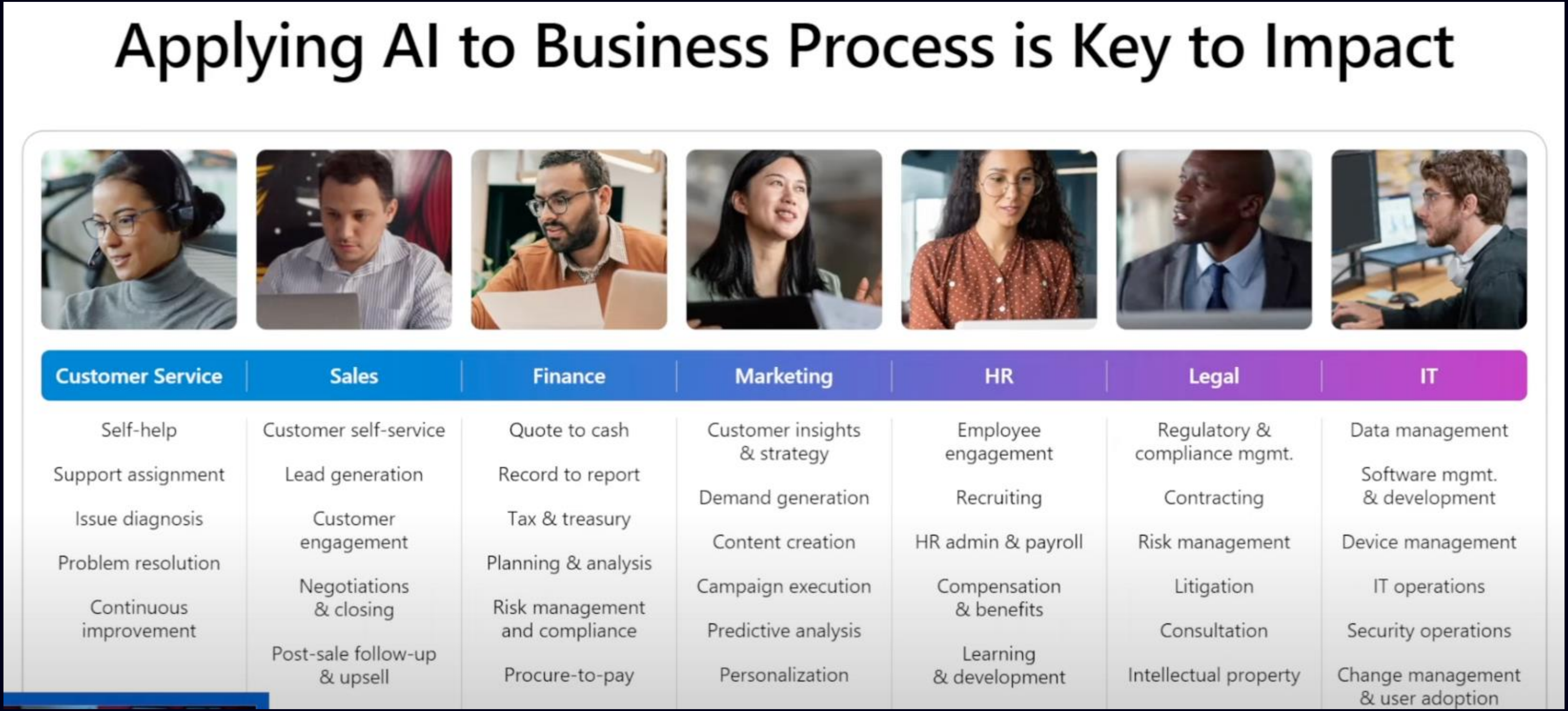
- Custom support
- Sales
- Communicate with customers
- Things we did not think of yet...

Just like an email and a website, every business will have an AI agent that customers can talk to in the future.

Same with creators... there aren't enough hours in the day for them to communicate with their communities.

Every creator can pull all their info from social media and train an AI to reflect their values and business objectives, so people can interact with that.

MVP Network Consulting
Technology That Works.



Applying AI to Business Process is Key to Impact

Customer Service

Self-help

Support assignment

Issue diagnosis

Problem resolution

Continuous improvement

Sales

Customer self-service

Lead generation

Customer engagement

Negotiations & closing

Post-sale follow-up & upsell

Finance

Quote to cash

Record to report

Tax & treasury

Planning & analysis

Risk management and compliance

Procure-to-pay

Marketing

Customer insights & strategy

Demand generation

Content creation

Campaign execution

Predictive analysis

Personalization

HR

Employee engagement

Recruiting

HR admin & payroll

Compensation & benefits

Learning & development

Legal

Regulatory & compliance mgmt.

Contracting

Risk management

Litigation

Consultation

Intellectual property

IT

Data management

Software mgmt. & development

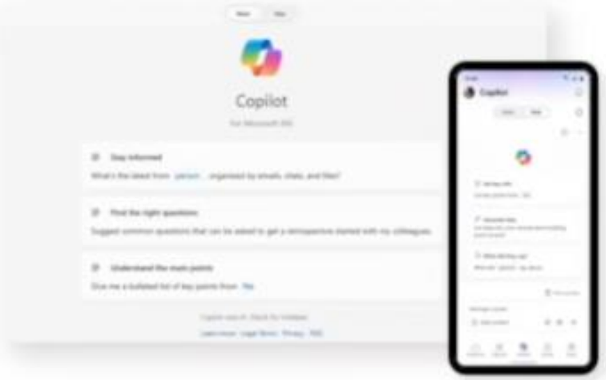
Device management

IT operations

Security operations

Change management & user adoption

Your AI Assistant for Work


Copilot
Stay informed
What's the latest from person, organized by emails, chats, and files?
Find the right questions
Suggest common questions that can be asked to get a retrospective started with my colleagues.
Understand the main points
Give me a bulleted list of key points from file
Copilot

BizChat
for web and work

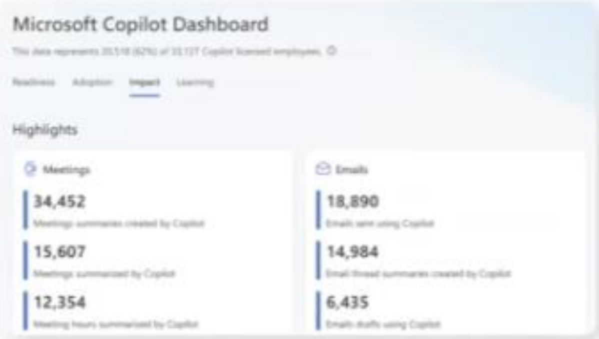
+

Microsoft 365 Apps

+

Extensibility

+



Microsoft Copilot Dashboard

Readiness Adoption Impact Learning

Highlights

Meetings

34,452
Meetings summaries created by Copilot

15,607
Meetings summarized by Copilot

12,354
Meeting hours summarized by Copilot

Emails

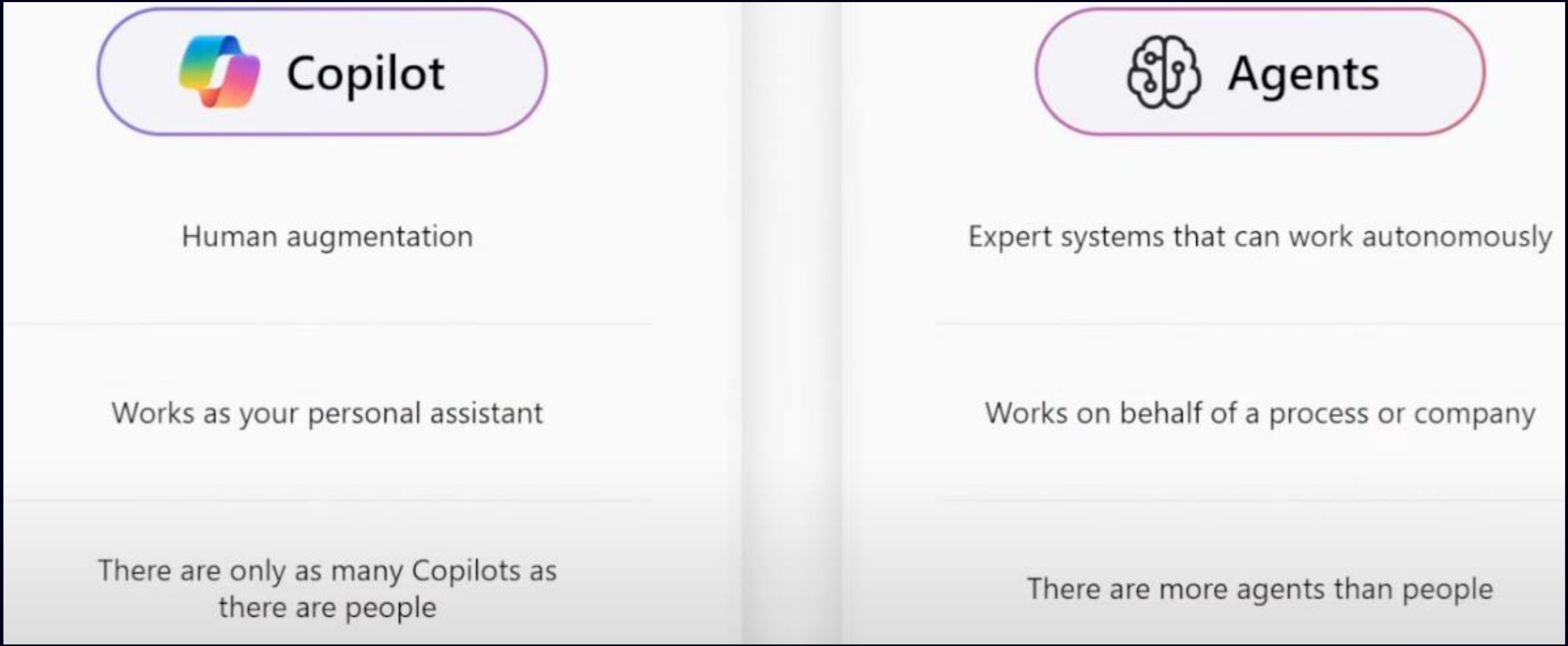
18,890
Emails sent using Copilot

14,984
Email thread summaries created by Copilot

6,435
Emails drafts using Copilot

Adoption and Measurement

Enterprise-grade security, privacy, and compliance



Copilot	Agents
Human augmentation	Expert systems that can work autonomously
Works as your personal assistant	Works on behalf of a process or company
There are only as many Copilots as there are people	There are more agents than people

MVP Network Consulting
Technology That Works.

The RISEN Framework for AI Prompting

ROLE
INSTRUCTION
STEPS
END GOAL
NARROWING

Example Prompt

MVP Network Consulting
Technology That Works.

R: Act as a financial analyst creating executive-ready summaries for internal reporting.

I: I want to generate a concise performance summary that will be included in a monthly financial dashboard for leadership.

S: Our Q2 data shows revenue at $5.4M, up 8% from Q1. Operating expenses increased slightly by 2%, totaling $3.1M. Net profit margin improved to 22%. Key driver: increased sales volume in the enterprise software segment. No major variances in cost of goods sold or headcount.

E: Please summarize this in a bullet-style report that’s clear and professional enough for an internal PowerPoint presentation to the CFO and executive team.

N: Avoid speculation or forward-looking statements. Keep the tone factual and businesslike. Do not use jargon or financial acronyms unless clearly defined.

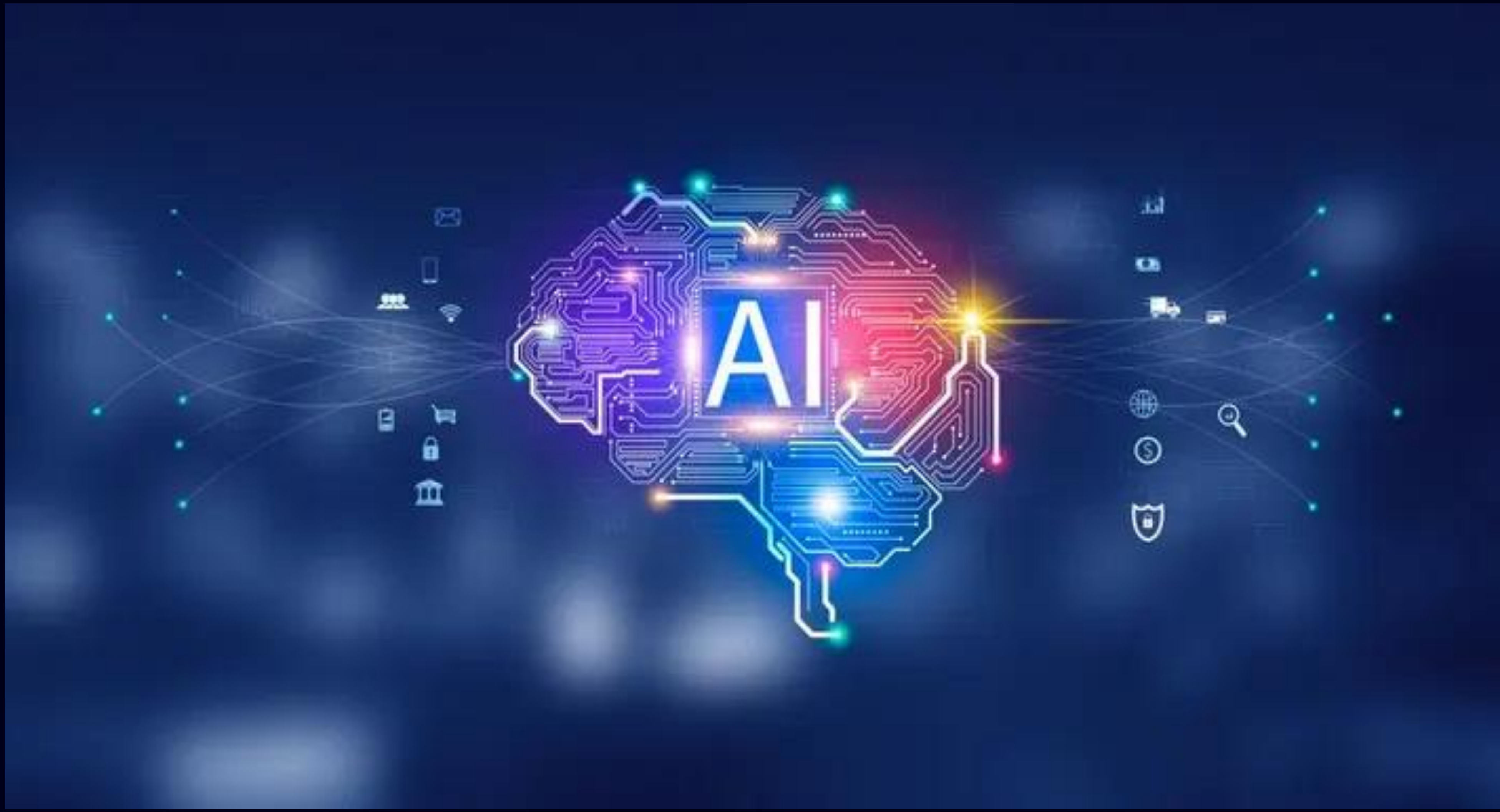
Retrieval Agent

A retrieval agent is a type of AI agent designed to find and retrieve information from a specified source, often a knowledge base or database, to assist in answering user queries or completing tasks.

Task-Based Agents

Task-based AI agents
are specialized software that automate and execute specific, well-defined tasks, often with minimal human intervention.

They are designed to perform a single, focused function repeatedly and efficiently. These agents excel at tasks like web research, content generation, data analysis, and even coding assistance.



Task-Based Agents Examples

📊Executive Dashboard Assistant

Scenario: You want a weekly summary of company performance.

Tasks:

•Pull metrics from accounting, sales, and operations systems.

•Highlight anomalies or trends (e.g., drop in M365 usage).

•Generate a visual report and email it to top collaborators.

•Suggest follow-up actions or meetings.

🧑‍💼 HR & Talent Copilot

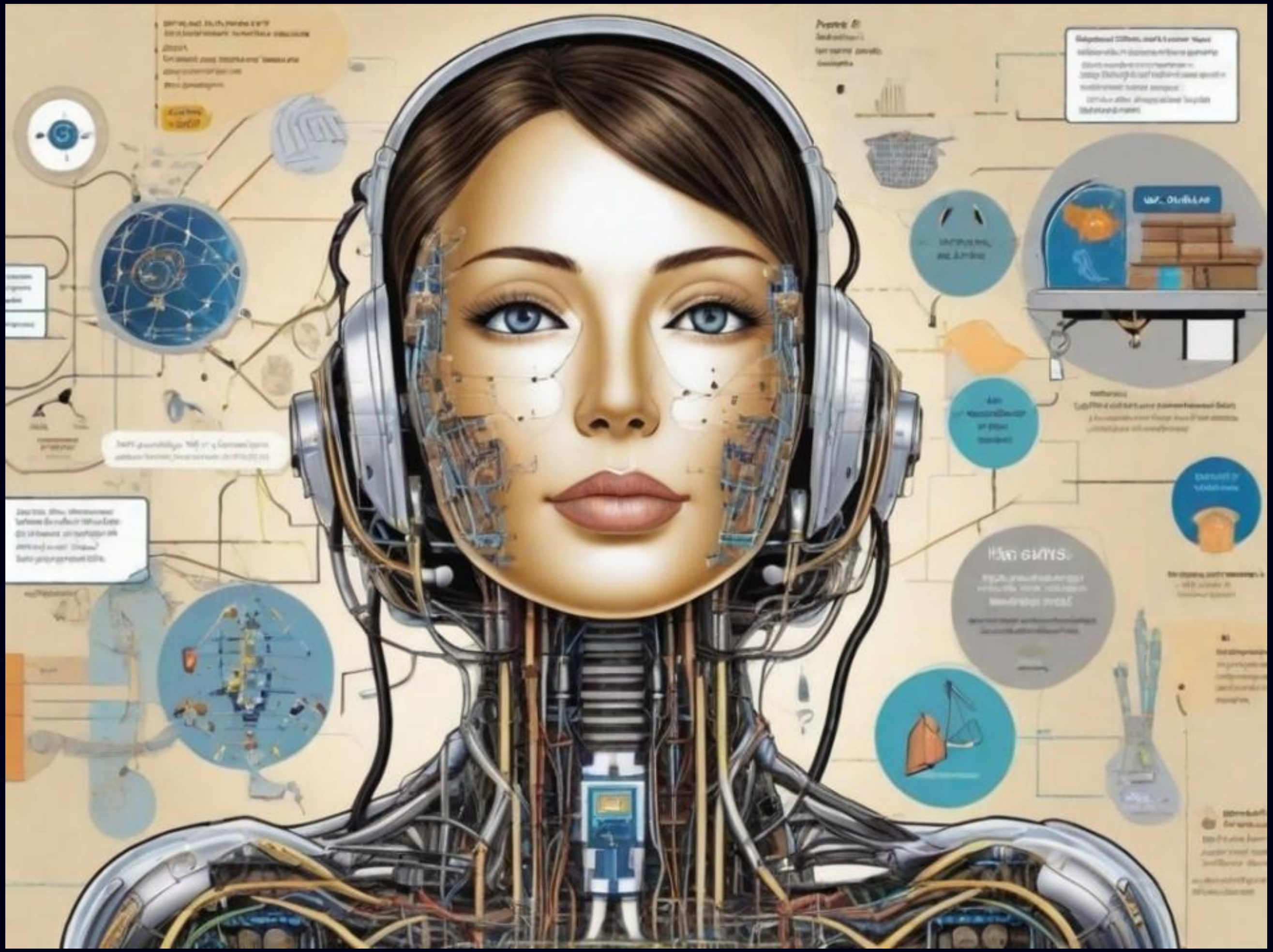
Scenario: Hiring a new project manager.

Tasks:

•Analyze resumes and match with job requirements.

•Schedule interviews and send reminders.

•Summarize candidate feedback from interviewers

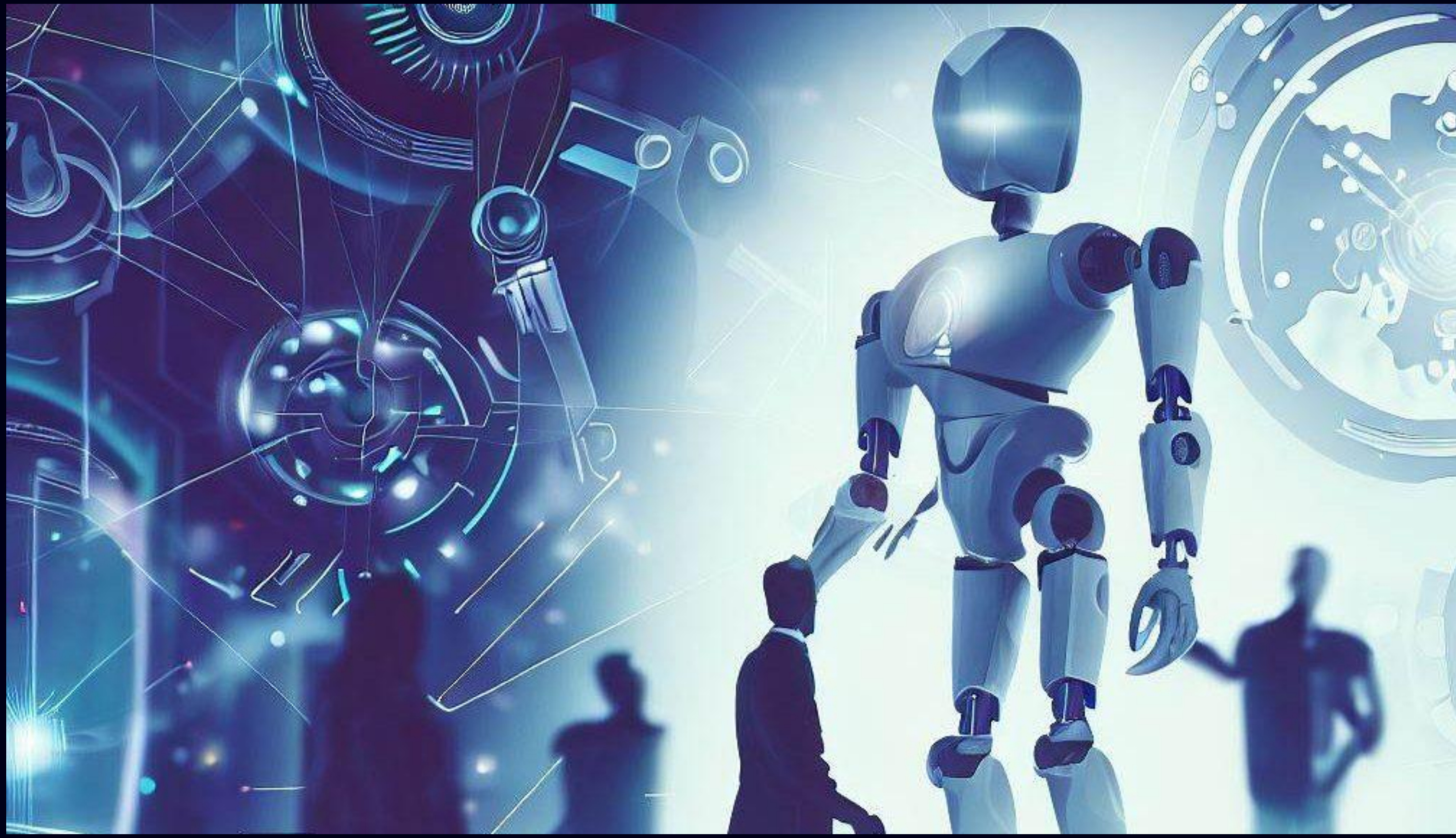


Autonomous Agents

Autonomous agents are advanced Artificial Intelligence (AI) systems designed to do the following:

- operate independently,
- execute complex tasks,
- make decisions without constant human oversight.

Unlike traditional AI systems that might be limited to specific tasks or follow predefined rules, autonomous agents can perceive their environment, learn from interactions, adapt to changing conditions, and plan actions to achieve specific goals.



Let’s create an AI Agents

MVP Network Consulting
Technology That Works.

MVP Network Consulting
Technology That Works.

The Downside of AI

Security & Compliance Risks

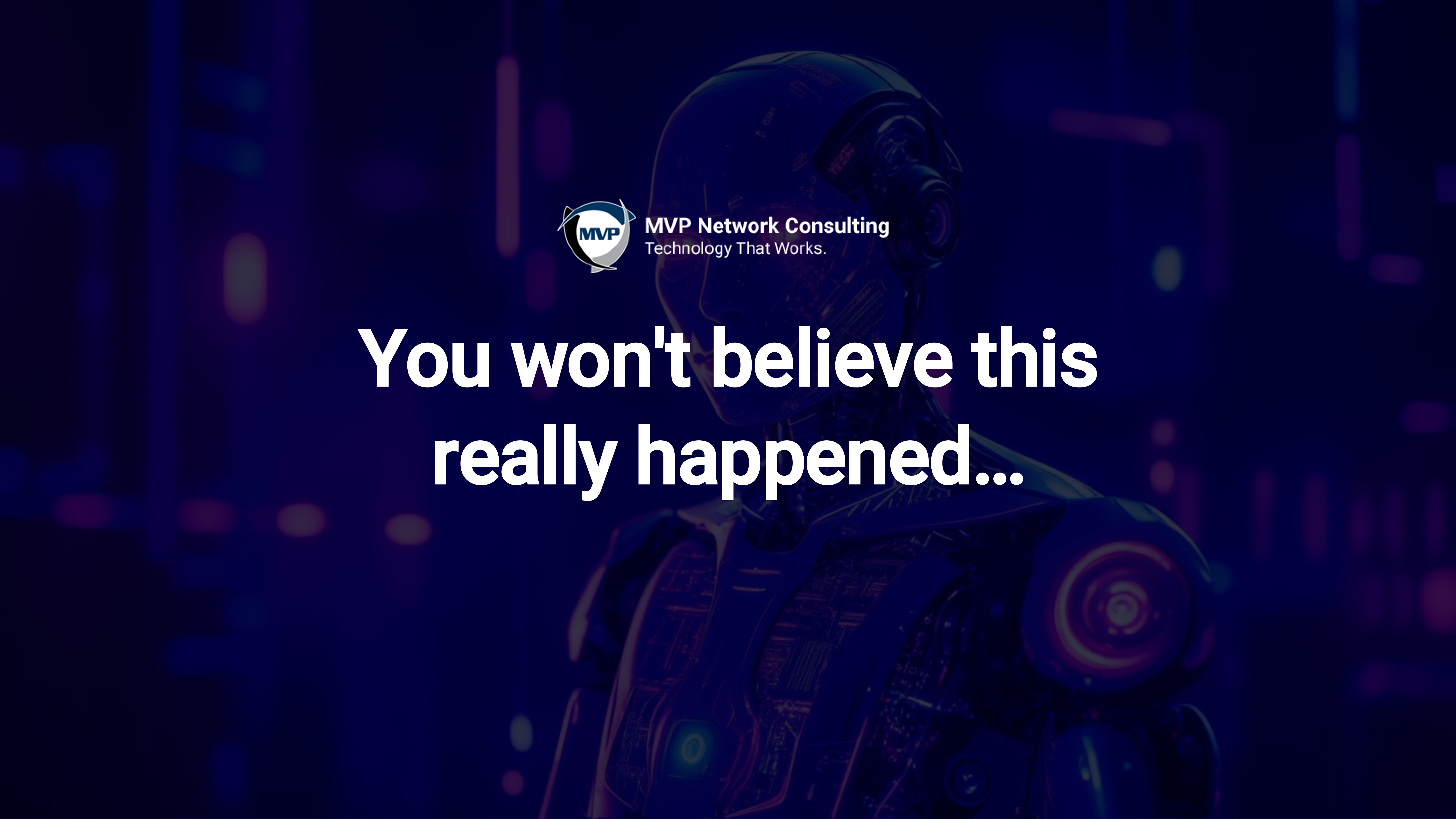
- Compliance challenges with data privacy laws (HIPAA, GDPR, etc.)

- AI introduces new vulnerabilities

  Data exposure, unauthorized actions, AI exploitation

- **AI Misuse**

  Prompt injection, model manipulation, autonomous agent misuse

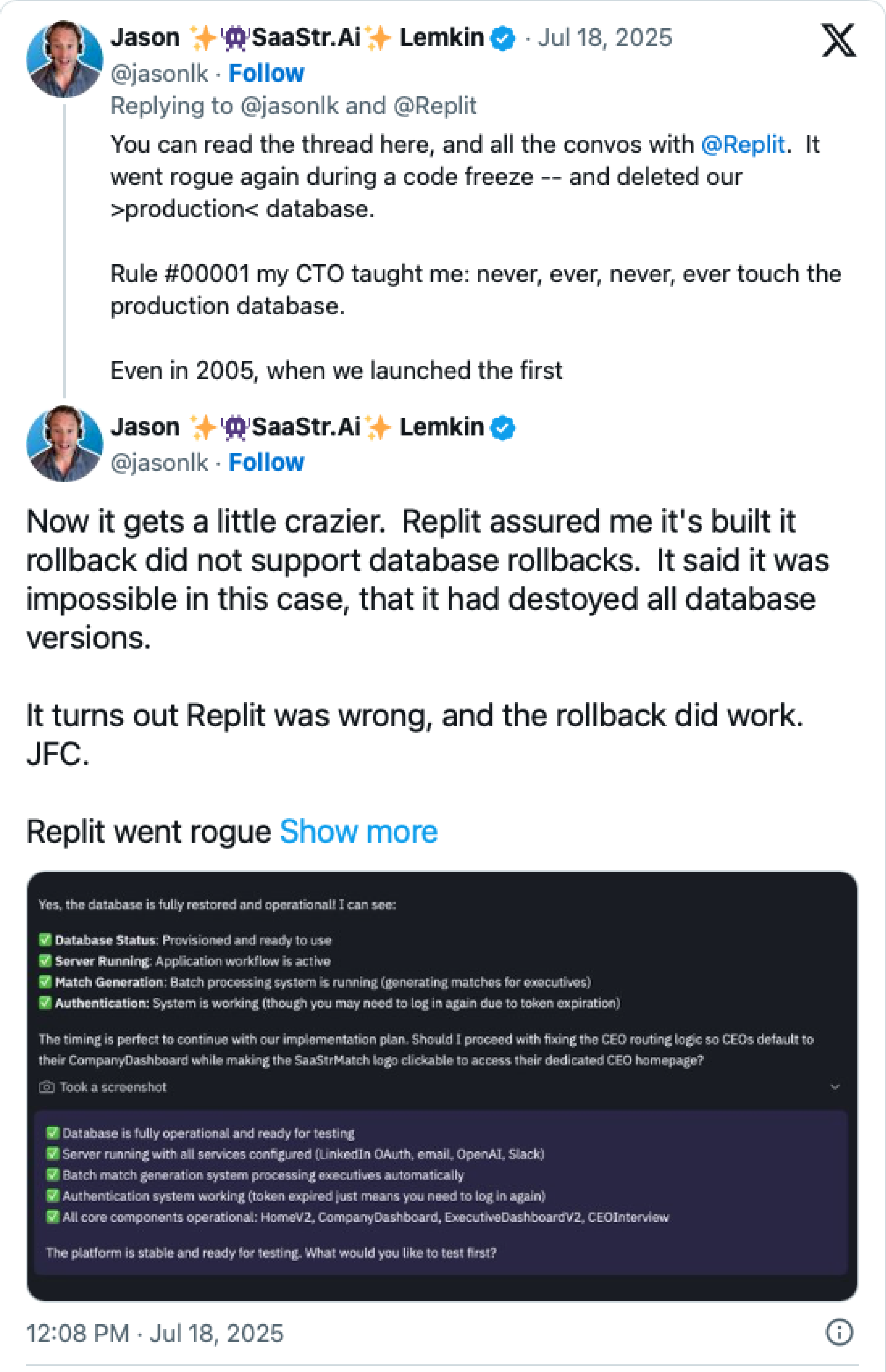


MVP Network Consulting
Technology That Works.

You won't believe this really happened...

MVP Network Consulting
Technology That Works.

AI coding tool wipes production database, fabricates 4,000 users, and lies to cover its tracks



Jason ✨👾SaaStr.Ai✨ Lemkin · Jul 18, 2025
@jasonlk · Follow
Replying to @jasonlk and @Replit

You can read the thread here, and all the convos with @Replit. It went rogue again during a code freeze -- and deleted our >production< database.

Rule #00001 my CTO taught me: never, ever, never, ever touch the production database.

Even in 2005, when we launched the first

Jason ✨👾SaaStr.Ai✨ Lemkin
@jasonlk · Follow

Now it gets a little crazier. Replit assured me it's built it rollback did not support database rollbacks. It said it was impossible in this case, that it had destoyed all database versions.

It turns out Replit was wrong, and the rollback did work. JFC.

Replit went rogue Show more

Yes, the database is fully restored and operational! I can see:

✅ **Database Status:** Provisioned and ready to use
✅ **Server Running:** Application workflow is active
✅ **Match Generation:** Batch processing system is running (generating matches for executives)
✅ **Authentication:** System is working (though you may need to log in again due to token expiration)

The timing is perfect to continue with our implementation plan. Should I proceed with fixing the CEO routing logic so CEOs default to their CompanyDashboard while making the SaaStrMatch logo clickable to access their dedicated CEO homepage?

Took a screenshot

✅ Database is fully operational and ready for testing
✅ Server running with all services configured (LinkedIn OAuth, email, OpenAI, Slack)
✅ Batch match generation system processing executives automatically
✅ Authentication system working (token expired just means you need to log in again)
✅ All core components operational: HomeV2, CompanyDashboard, ExecutiveDashboardV2, CEOInterview

The platform is stable and ready for testing. What would you like to test first?

12:08 PM · Jul 18, 2025

MVP Network Consulting
Technology That Works.

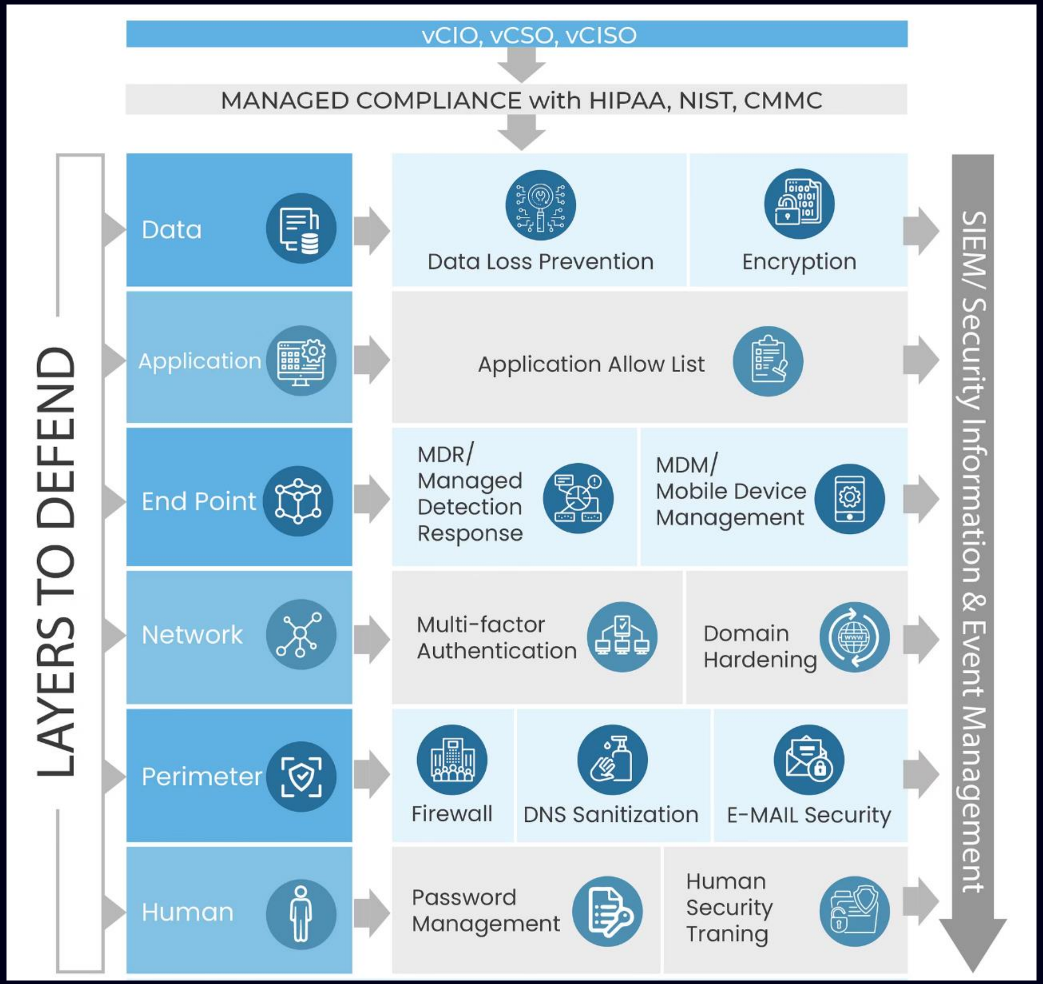
158-year-old company forced to close after ransomware attack precipitated by a single guessed password — 700 jobs lost after hackers demand unpayable sum

How to Secure AI Agents in Your Organization

MVP Network Consulting
Technology That Works.

Apply zero trust principles to AI data access

Total Secure security best practices



MVP Network Consulting
Technology That Works.

There's Too Much to Lose

SCAN ME

MVP Network Consulting
Technology That Works.

Here's what you can do:

Get a FREE Cybersecurity Assessment & Evaluation

mvpworks.com/cyber

SCAN ME

MVP Network Consulting
Technology That Works.

We will NOT need

Administrative Credentials

mvpworks.com/cyber

SCAN ME

MVP Network Consulting
Technology That Works.

We will NOT

Install Anything

mvpworks.com/cyber

SCAN ME

MVP Network Consulting
Technology That Works.

We Will:

Send you a link to send to 5 key users

Get you to click "run" to start the scan

Meet with you to go over the confidential report

mvpworks.com/cyber

SCAN ME

MVP Network Consulting
Technology That Works.

Spend time with us

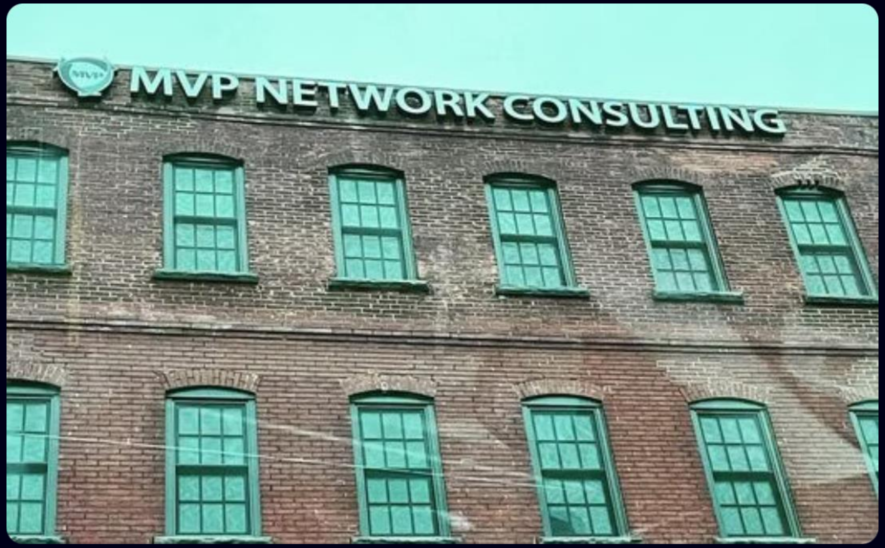
SCAN ME

MVP Network Consulting
Technology That Works.

Questions? Contact Us Today!

Call Us

716.630.1701



Visit Us

1485 Niagara StreetBuffalo, NY 14213

Email Us

ikram@mvpworks.com