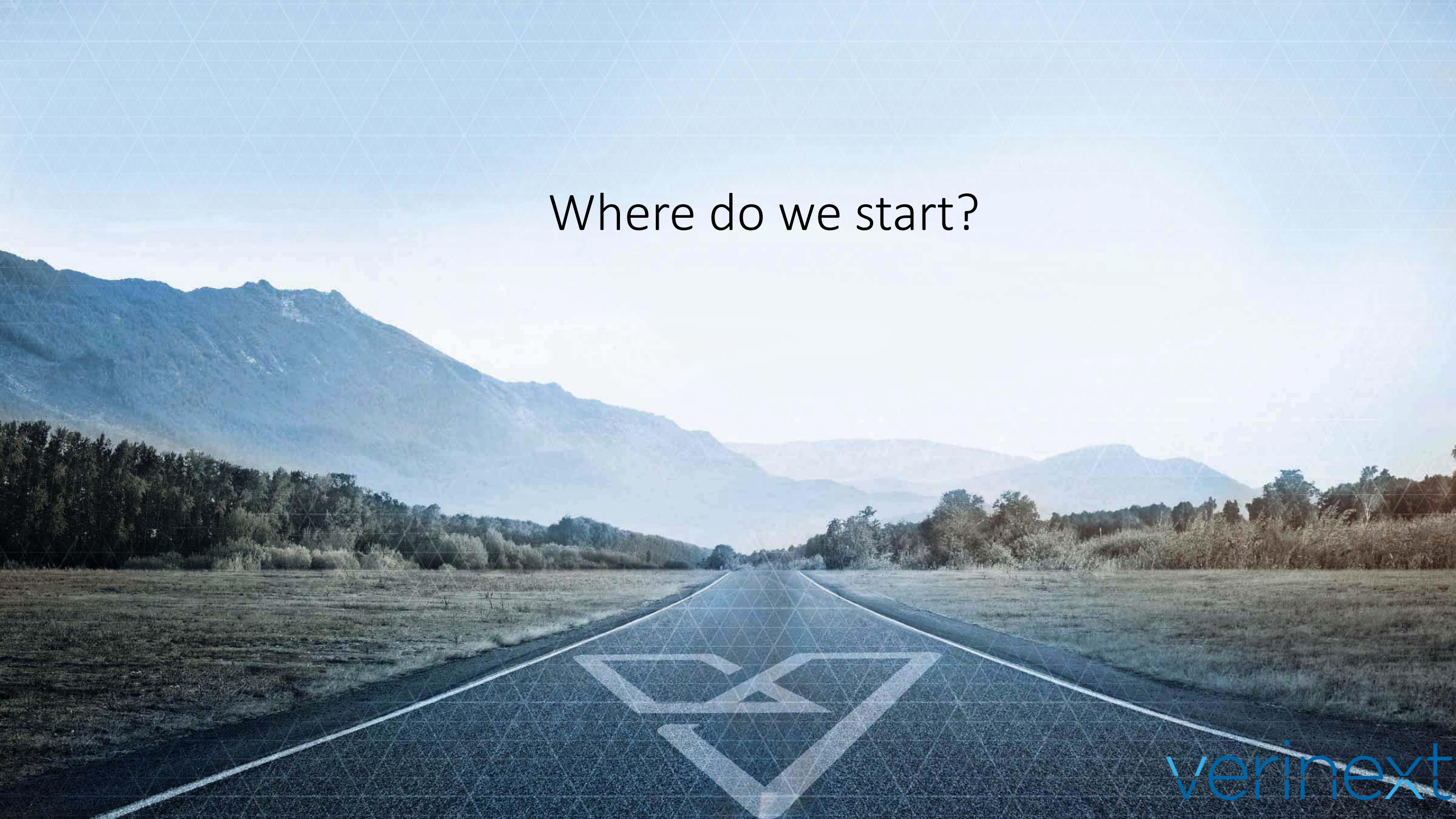
Session Abstract

Every day, we network-enable more aspects of our professional and personal lives. We make conscious decisions to adopt technologies in the pursuit of convenience or an apparent need to feel connected. Often the decisions are thrust upon us by employers, service providers or even those we've come to rely on in the physical world. Each step towards deeper and total connectivity comes with consequences; risks associated with our personal privacy, the security of our business and even our safety. In this session, we will explore the changes we've already allowed into our lives, where things are leading, and portents for personal, business and public security.

Session Abstract

- ❑ People want Automation. Automation enables & allows Freedom. Manual is bad
- ❑ Automation is giving rise to Large Language Models (LLM) & Artificial Intelligence (AI)
  - Automation is both the ingredients and often the output of AI
- ❑ The Cyber Threat Environment is already driven by AI. Our defense capability, visibility & speed is lagging.
- ❑ Ironically, now we usher in an era of:
  - Discovering our AI Systems & Understanding Vulnerabilities to / from
  - Protecting our own AI Systems
  - Defending from adversarial AI Systems

Where do we start?



Historical Perspective

NYC is going robot patrols

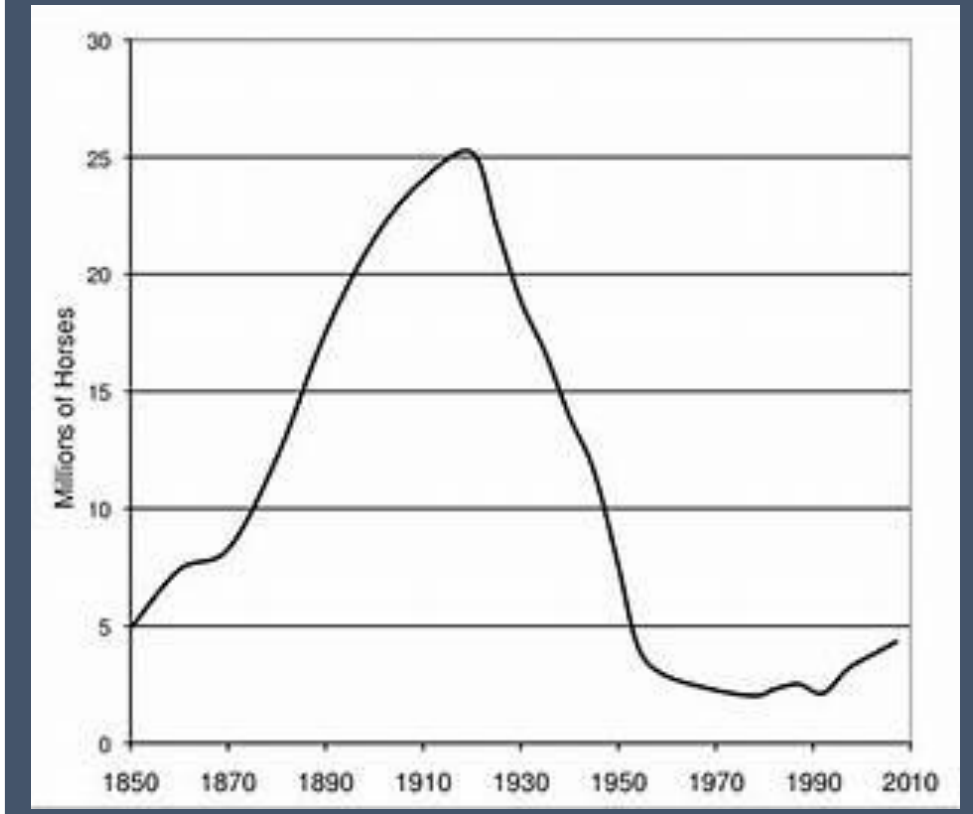
New York’s mounted unit has shrunk considerably over the last decade: it now has 79 police officers and 60 horses, down from the 130 officers and 125 horses it had before, Deputy Commissioner Paul J. Browne said.

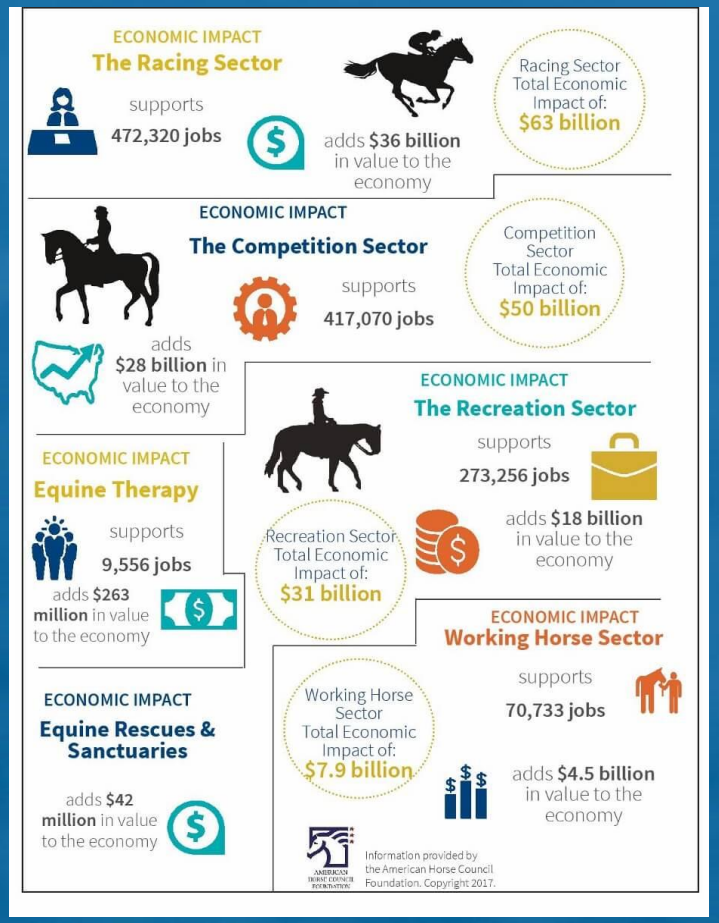
So, Two Horses Were Chatting…

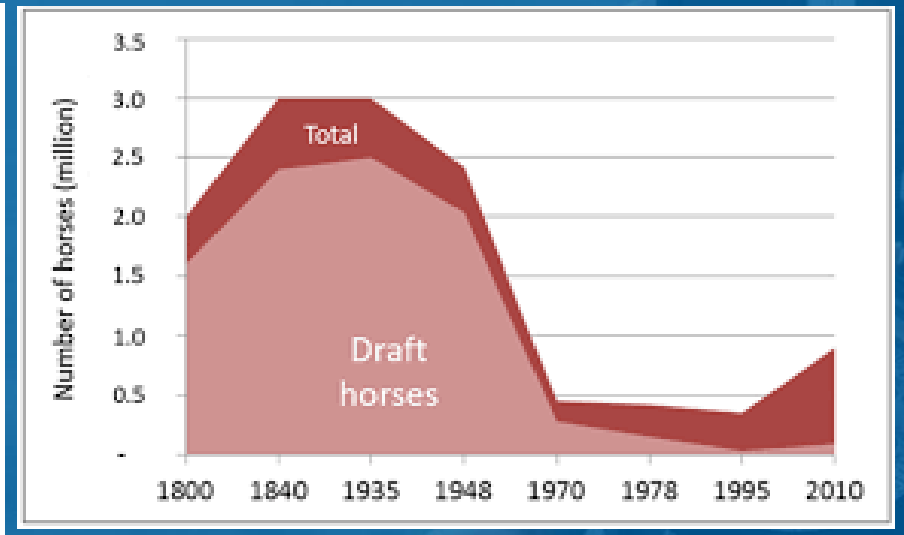
26m

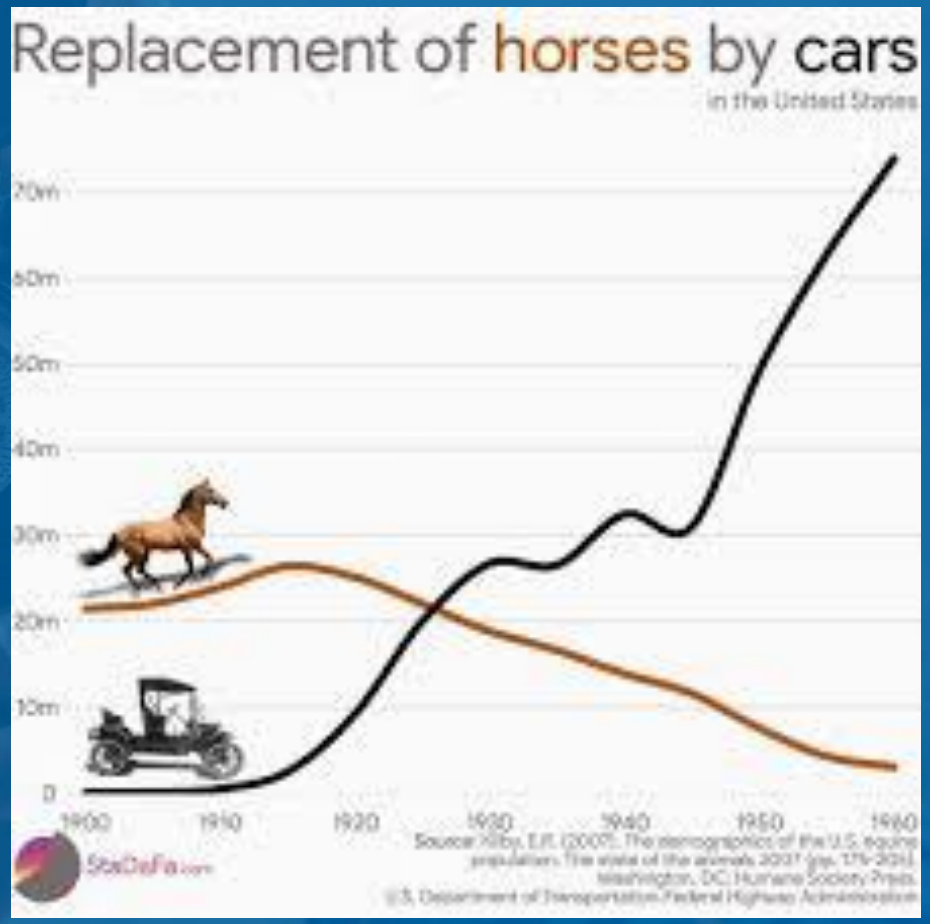
5m

US Horse Population





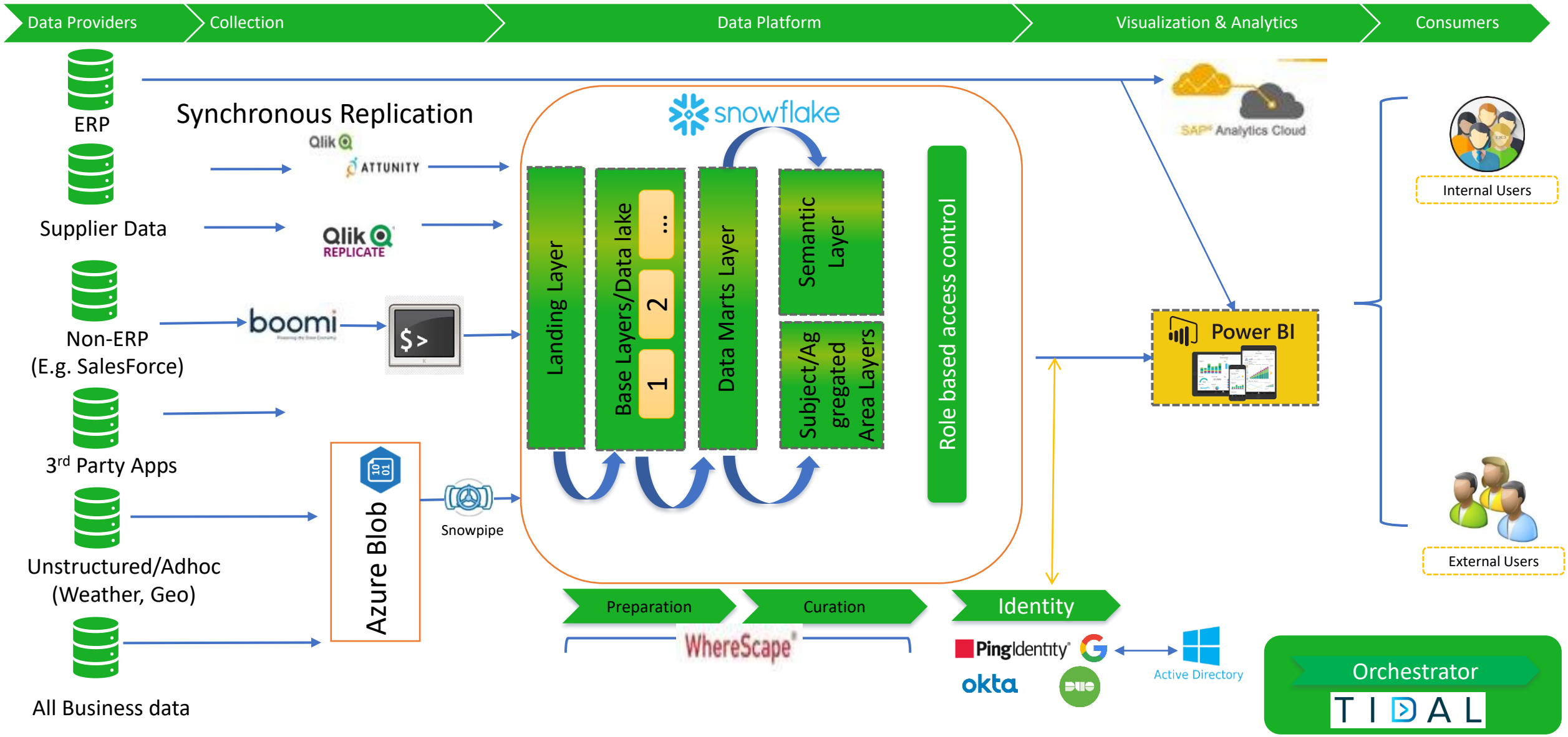


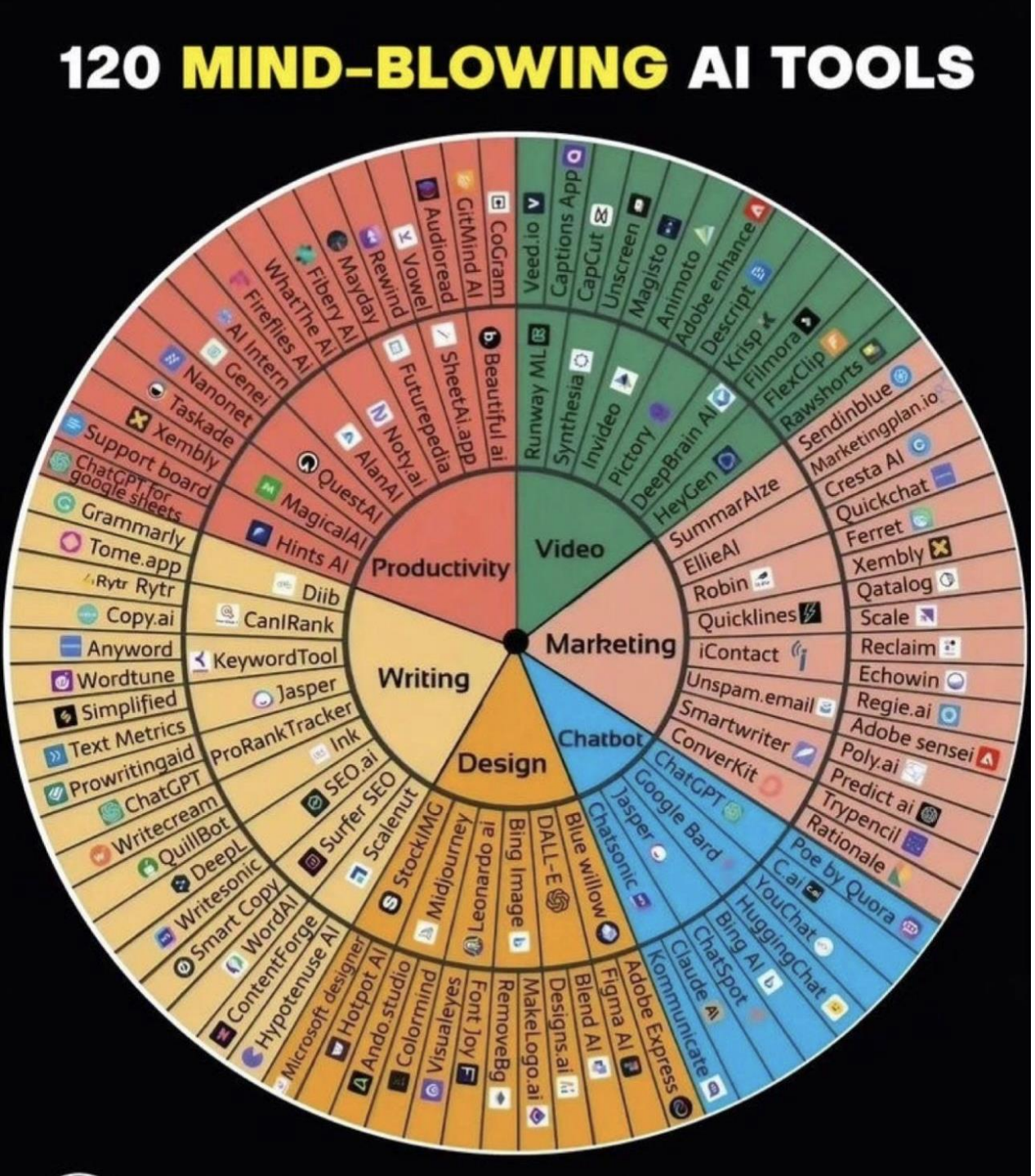


Horse Population & Models

Large Language Model in Architectural Concept

Example Typical Architecture, Vendor & Dataflow Diagram

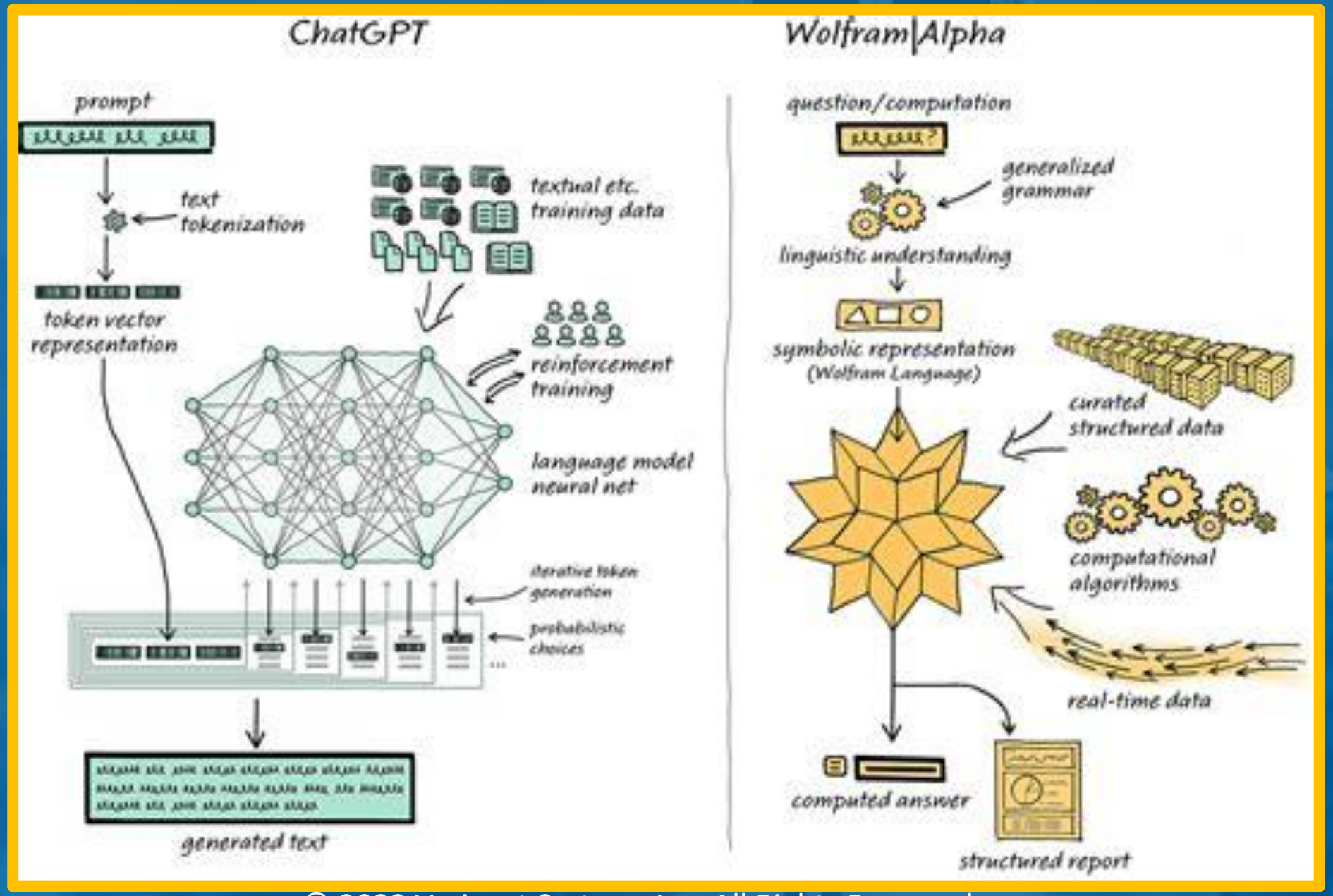




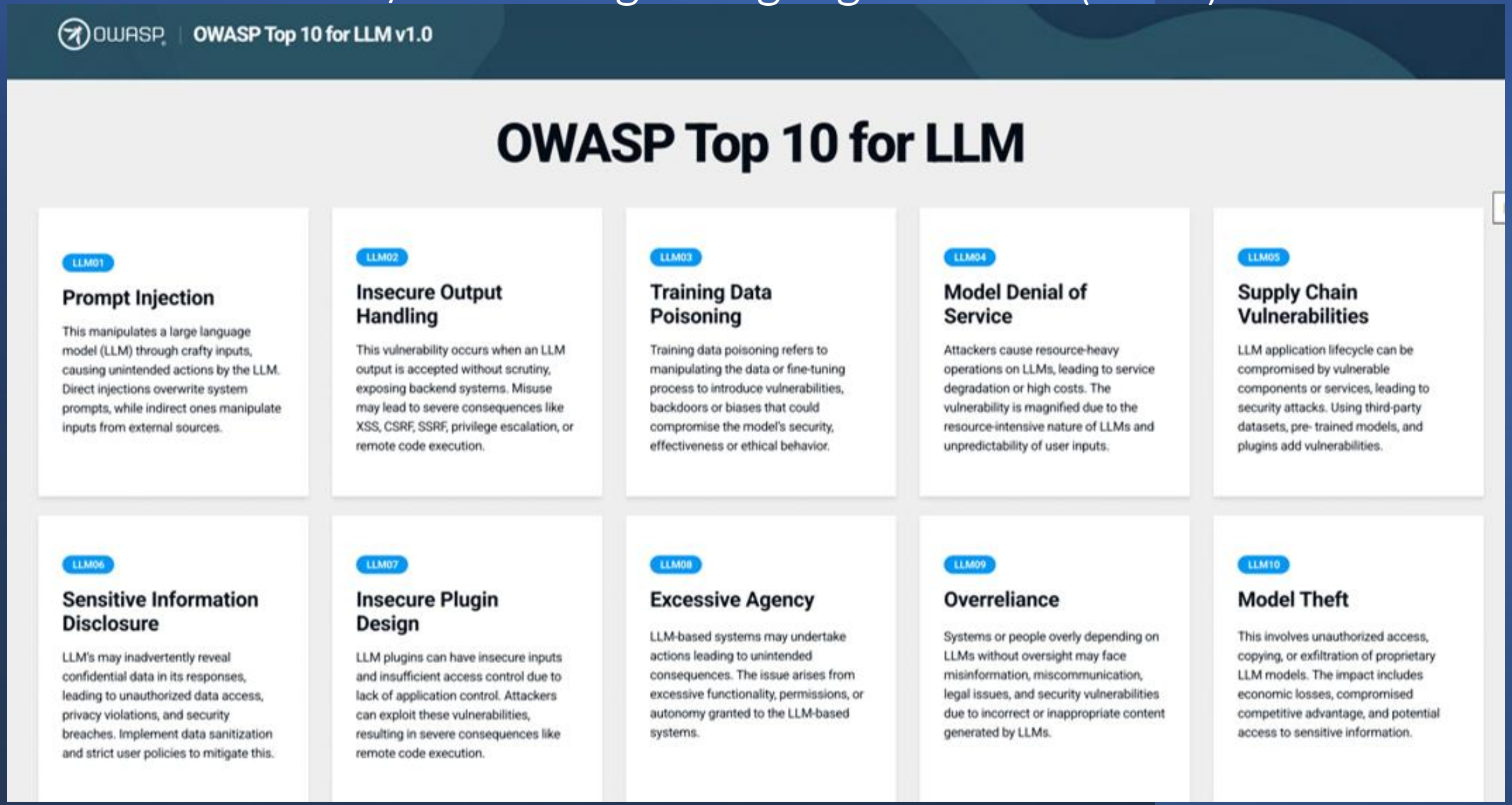
As we know AI Tools are Exploding in Availability

In earnest, CyberSecurity of / from these tools has just begun

How to think about CyberSecurity of Large Language Models (LLMs)



Threats To / From Large Language Models (LLMs)



How to think about CyberSecurity of Large Language Models (LLMs)

Threats TO the Feed

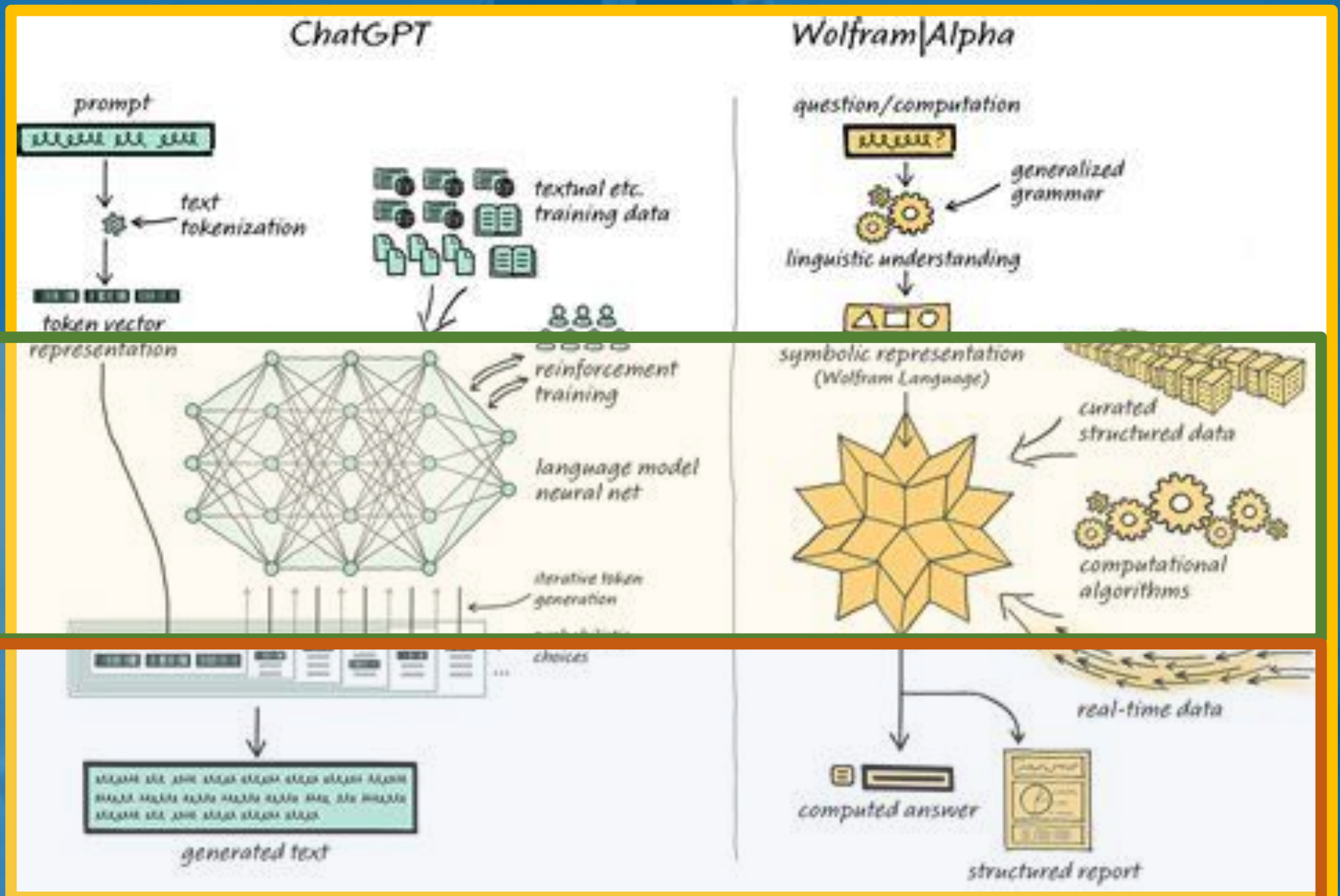
- Integrity:
- MiM & Injections
- Compliance

Threats to the Model

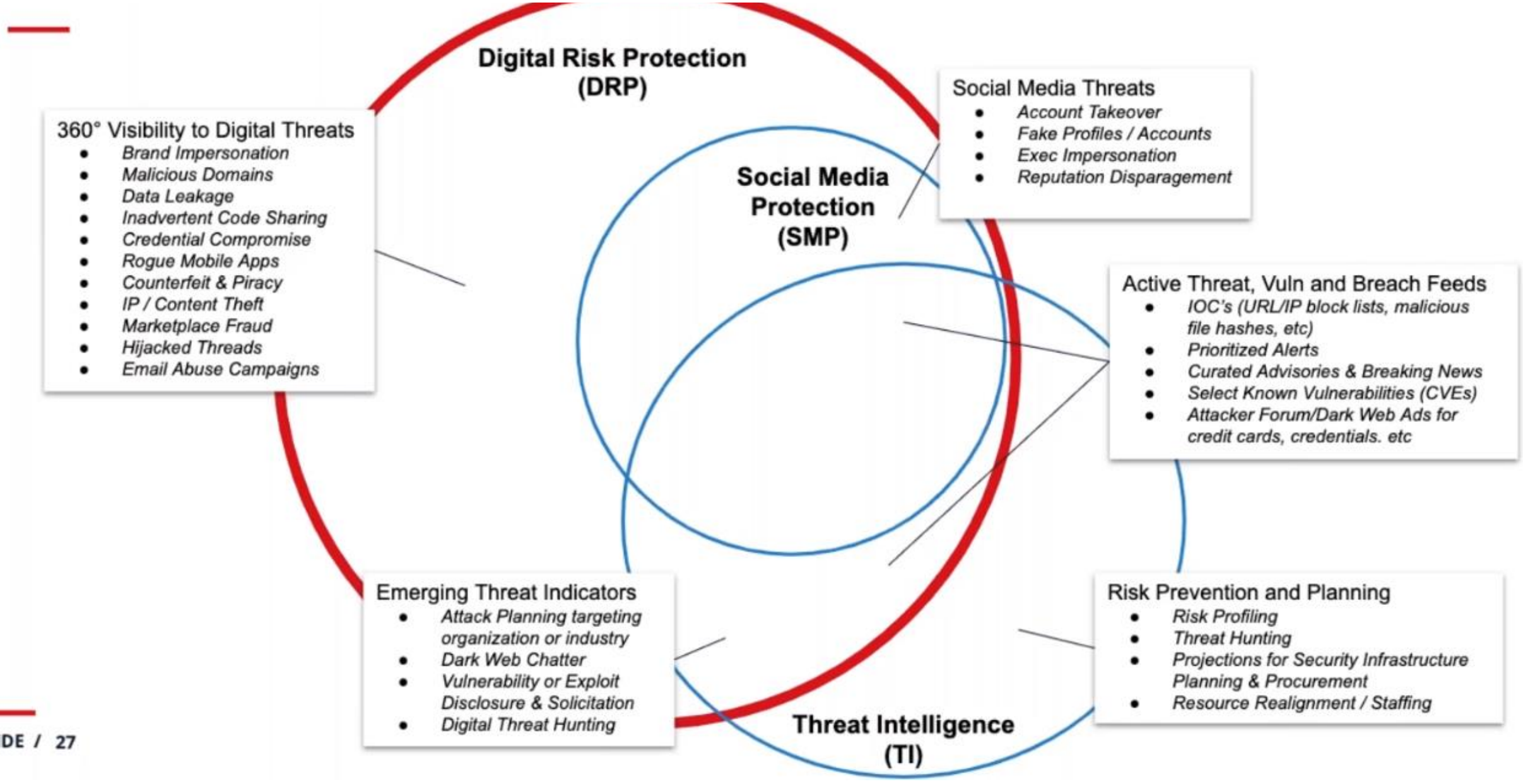
- Availability
- API & Bots / DDoS
- Ransomware / Malware

Threats to the Results

- False / Fake Information
- Privacy / Law Breach
- Used as a Threat Platform

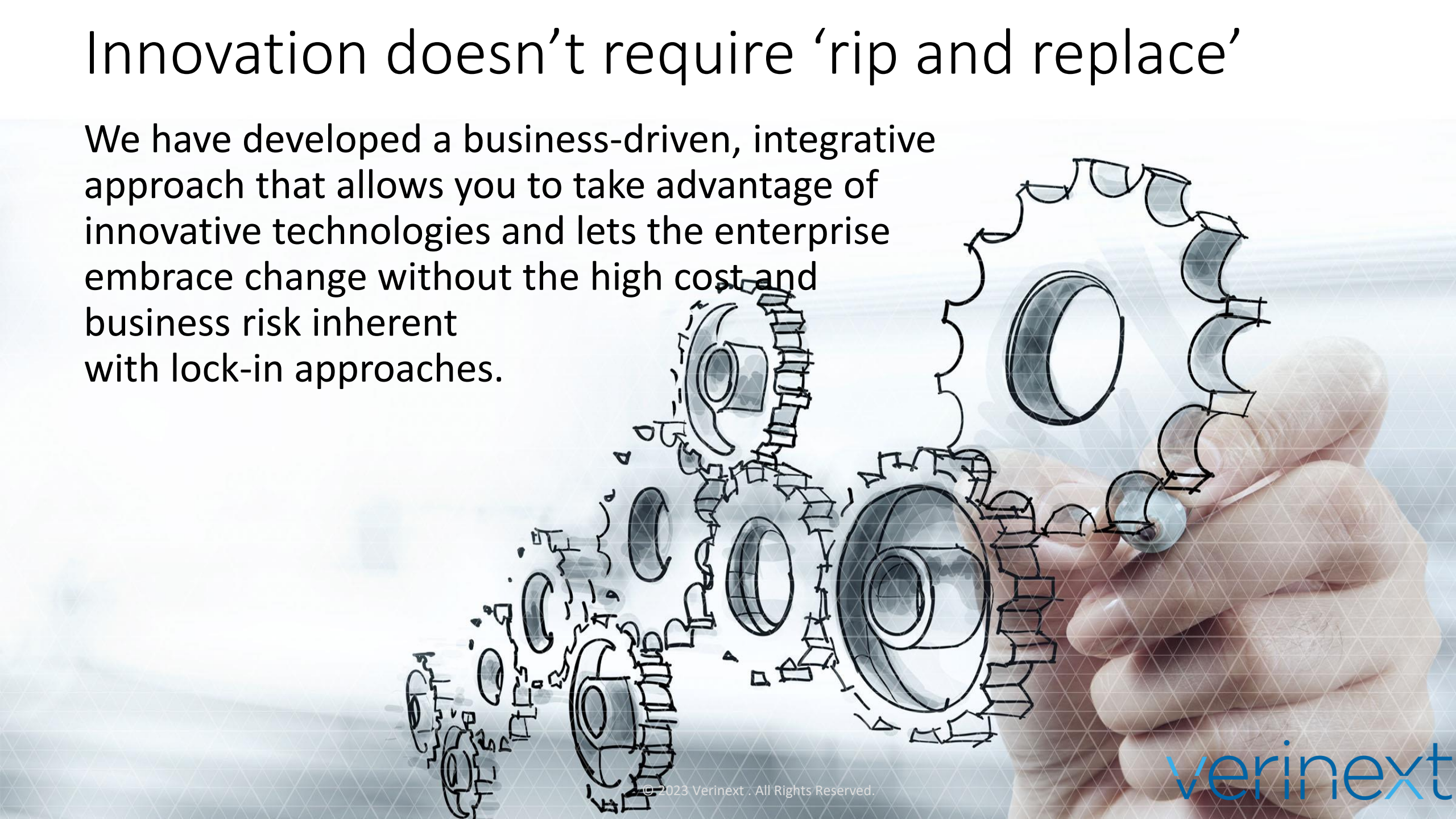


AI Security Requires External Concepts



Innovation doesn’t require ‘rip and replace’

We have developed a business-driven, integrative approach that allows you to take advantage of innovative technologies and lets the enterprise embrace change without the high cost and business risk inherent with lock-in approaches.



How to Start thinking of LLM & GAI Cybersecurity

How do I start Secure LLM Models?	How do I Protect Myself From Malicious Model Output?	How do I stop Data From Being Used by GAI / LLM?	How do I Protect Myself From Malicious Model Input?	How do I **manage** LLM / GAI CyberSecurity?
DSPM, Anti-Bot, API Security, RASP DDoS, WAF, DLP	**API, Bot Mgmt, WAF, DSPM, DLP, SIEM & SOAR**	**GAI Policy & Architecture Plan RASP, DSPM, DLP, API**	**API, Bot Mgmt, WAF, DSPM, DLP, SIEM & SOAR**	**AI vs AI Managed Services**

verinext

High Level Components of a AI Security Program

Generative AI (GAI) / LLM Policy

All Good Things CyberSecurity start with Policy desires

Defined Data Architecture

Junk In / Junk Out

You Must Know & Discover Your Assets

GAI / LLM Security Testing

Ensuring your defenses are working as intended

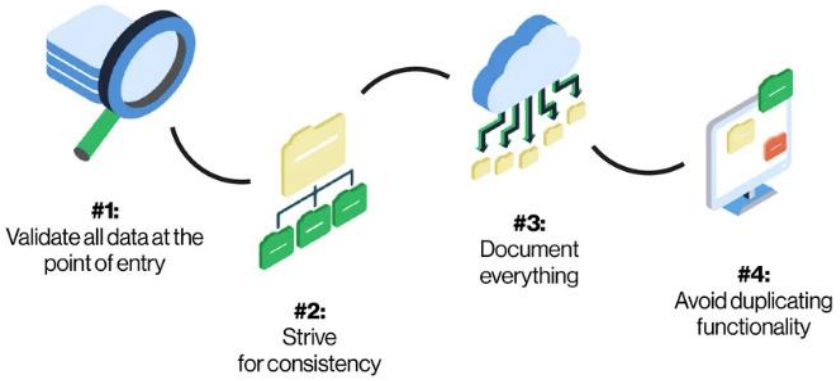
Prepare for AI: Curation Tools & Enable Culture of Security

Defensive mechanisms are layered in order to protect valuable data and information.

Step 2:Data Architecture Strategy

- **Define Guiding Principles**
- **Replication Strategy/plan**
- **Data Profiling**
- **Define Application (e.g. Snowflake) Architecture**
- **Technology Stack**
- **Data Governance and Management**
- **Data Security**
- **Data Archive Strategy**
- **Data Mart Approach**
- **Data Cleanup and Alternative Data Warehouse Decommissioning**

Step 4: Define LLM / GAI Guiding Principles, Tools, & Curation



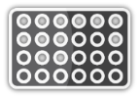
1. *Centralized data management: a centralized view of the business across functions*
2. *Restrict data movement and bring over only necessary attributes to data warehouse*
3. *Ensure Data security and access control*
4. *Provide role based access to the data*
5. *Data Curation: manage the lifecycle of the data from collection, cleansing, transforming, cataloging to archiving*
6. *Establish a common vocabulary*
7. *Eliminate the copy of the data and increase the data sharing*
8. *Archive historical data*
9. *Build easy to use data structure for visual layer*

Stay Focused. Be Prepared.

Build your protection strategy. Develop an incident response plan.
Remember this is mostly about integrity

Look to Automation. It has become necessary to fight automated threats with automation technology.

Simplify with Services. Fully managed services will provide the resources and expertise needed to combat today's attacks



Cover the Blind Spot. Choose a solution with the widest coverage to protect from multi-vector attacks.

Single point of contact is crucial when under attack - it will help to divert internet traffic and deploy mitigation solutions.

Questions?

Security = Confidentiality, Integrity & Availability:

Zero trust focuses on Confidentiality & Integrity

Zero Trust is required at the Perimeter, In Transit, At Rest, SaaS & in Trusted Supply-Chain Providers

- Legacy systems may not adapt to zero trust
- All-in-one zero-trust products don't exist
- Best of breed approach to zero-trust creates gaps
- Zero trust requires ongoing administration, maintenance
- Trust is consolidated and, like password managers, at risk
- Solutions for multi-cloud, service-provider, hybrid and powerful scale are still lacking
- ZT focuses on human interactions & IoT, but software & automation is still developing
- Balancing Zero Trust Theory with Real-world Functionality