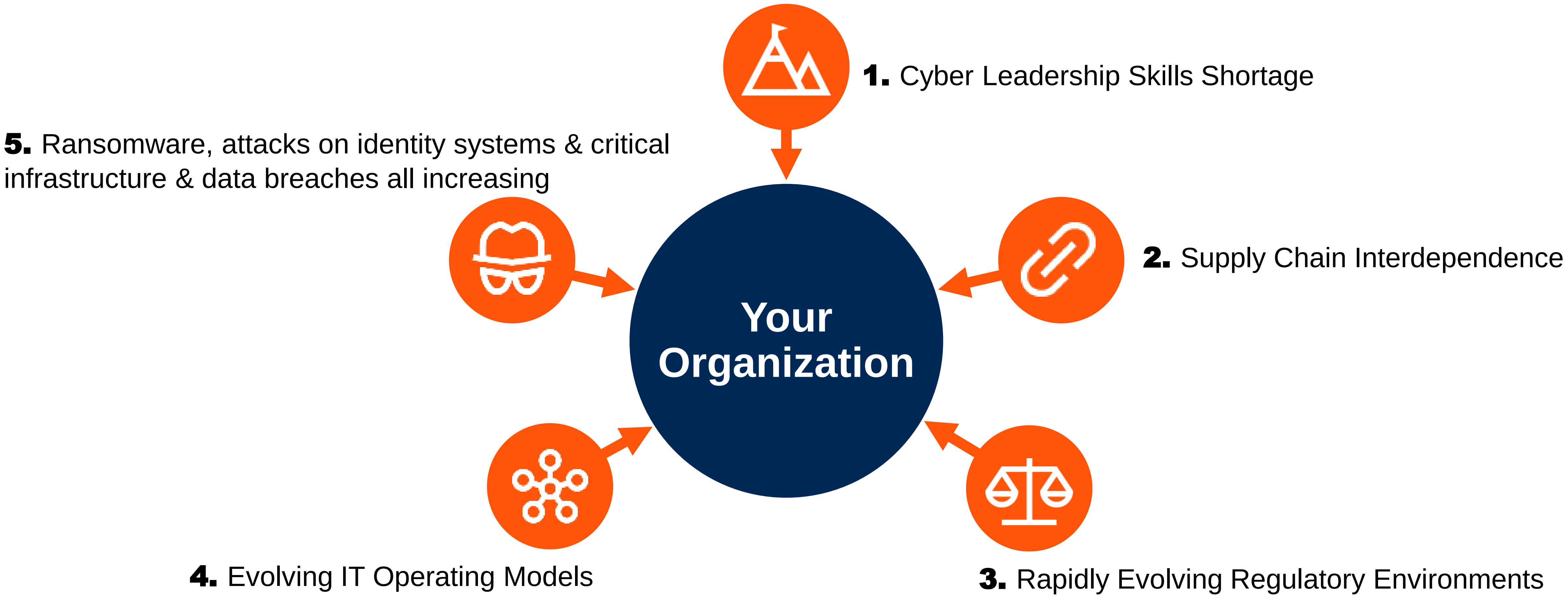
Cybersecurity Threats and Trends

E. Mastranza

VP Executive Partner
Security and Risk Management

Gartner®

Persistent Security Challenges



1. Cyber Leadership Skills Shortage

2. Supply Chain Interdependence

3. Rapidly Evolving Regulatory Environments

4. Evolving IT Operating Models

5. Ransomware, attacks on identity systems & critical infrastructure & data breaches all increasing

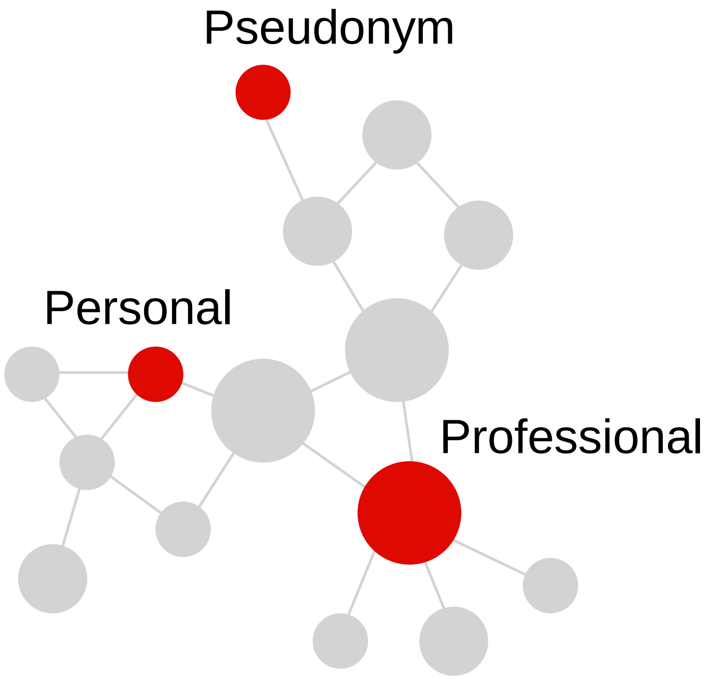
Predicts: Deepfakes for Social Engineering

In 2024,
15% of successful account takeover attacks will use deepfakes to socially engineer users to turn over sensitive data or move money into criminal accounts.

Evolving Phishing Techniques

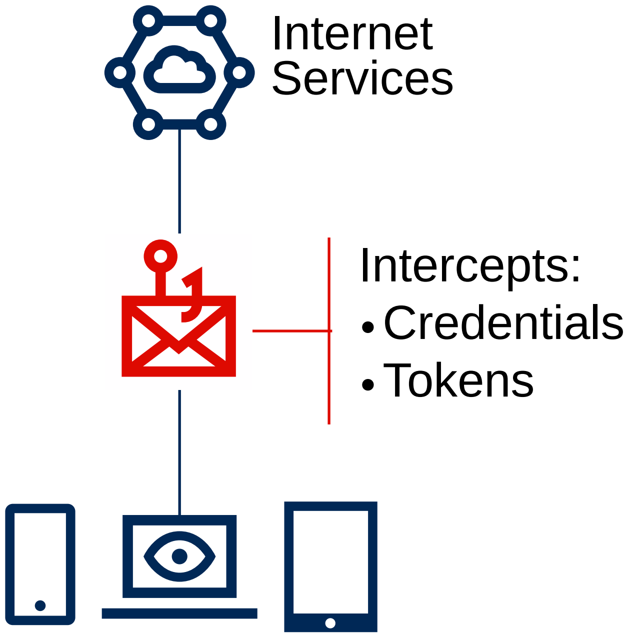
More Targeted

Cross-Platform Profiling



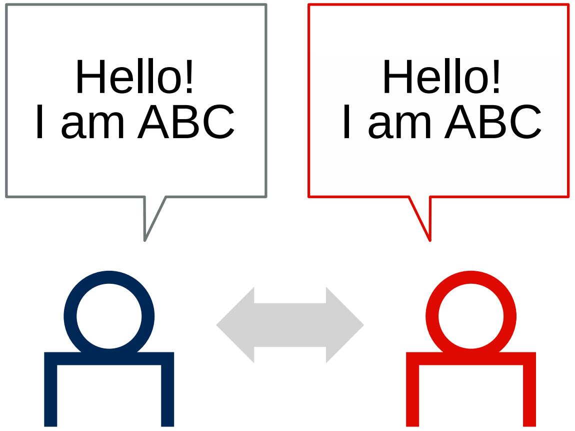
More Automated

Phishing as a Service



More Channels

Voice Impersonation



Source: Gartner

786244_C

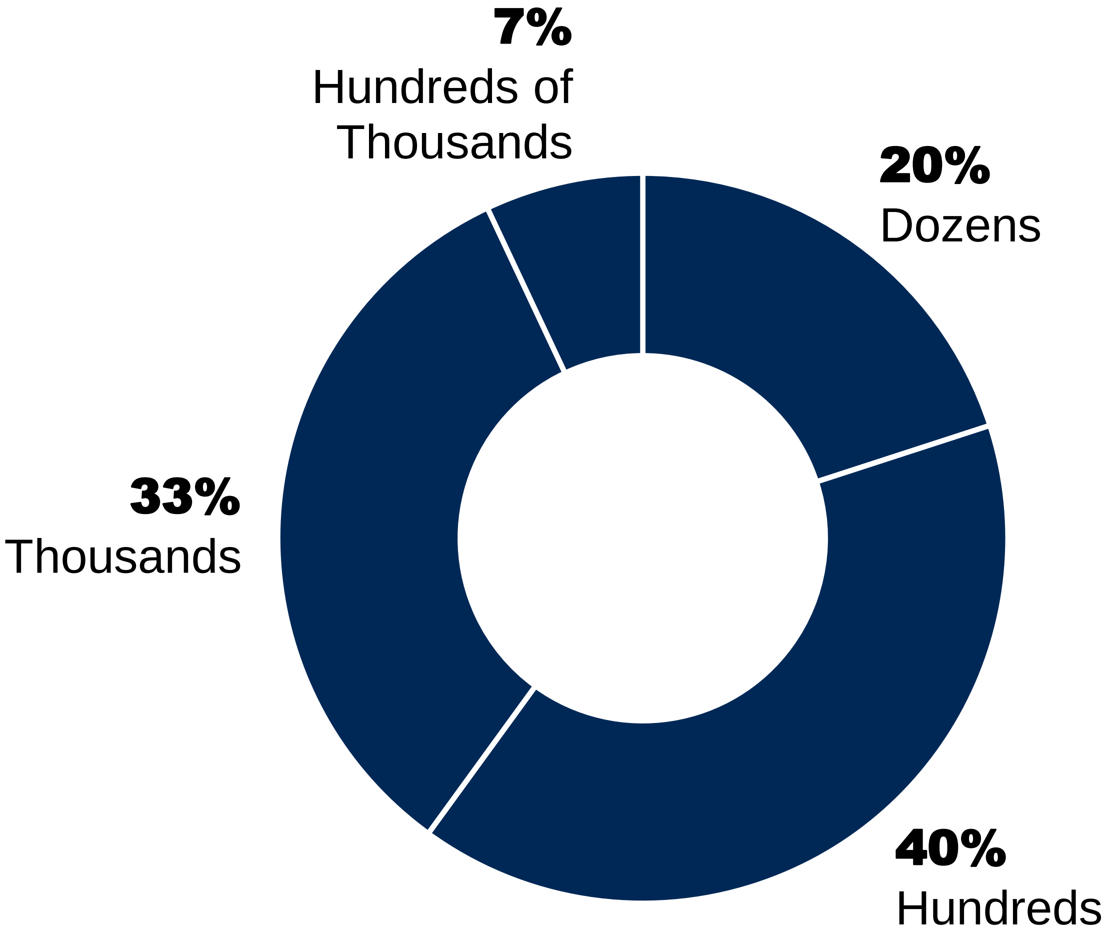
RESTRICTED DISTRIBUTION

Plenty of Models to Compromise and Attack

Number of AI Models Deployed to Date

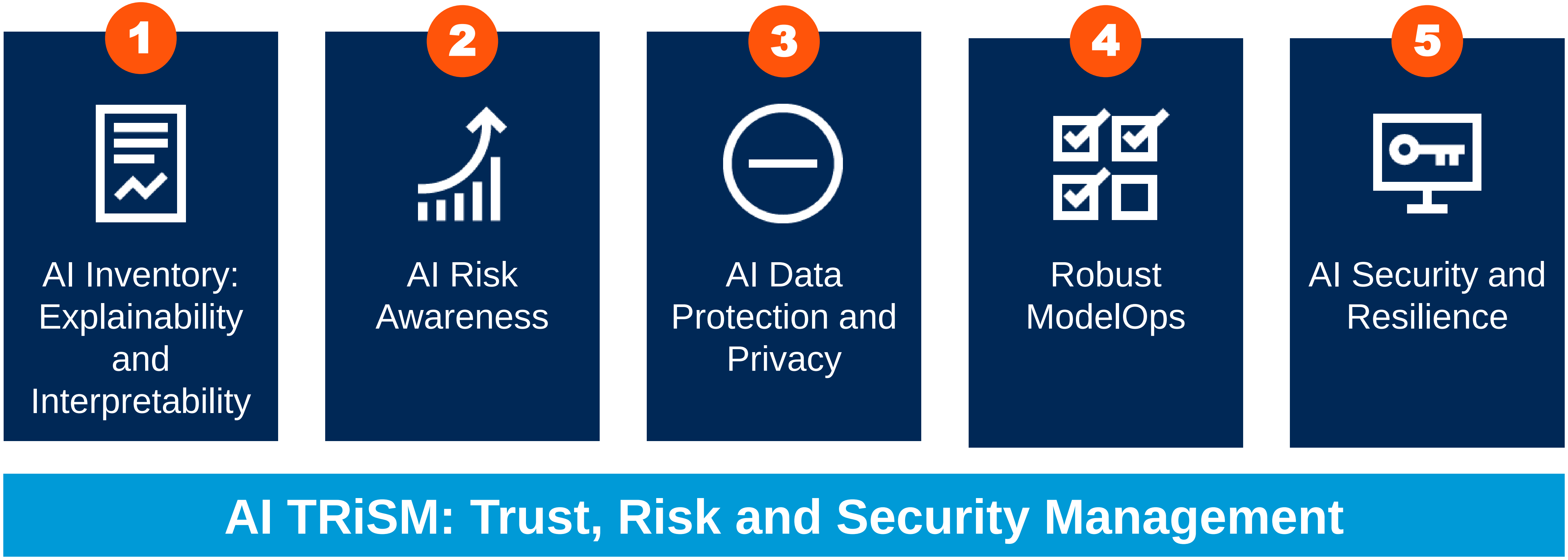
73%

of Organizations Have Hundreds or Thousands of Models Deployed



n = 324; Base: Using AI (S08), Excludes Unsure
Q13A: How many AI models has your organization deployed to date?
Source: 2021 Gartner AI in Organizations Survey

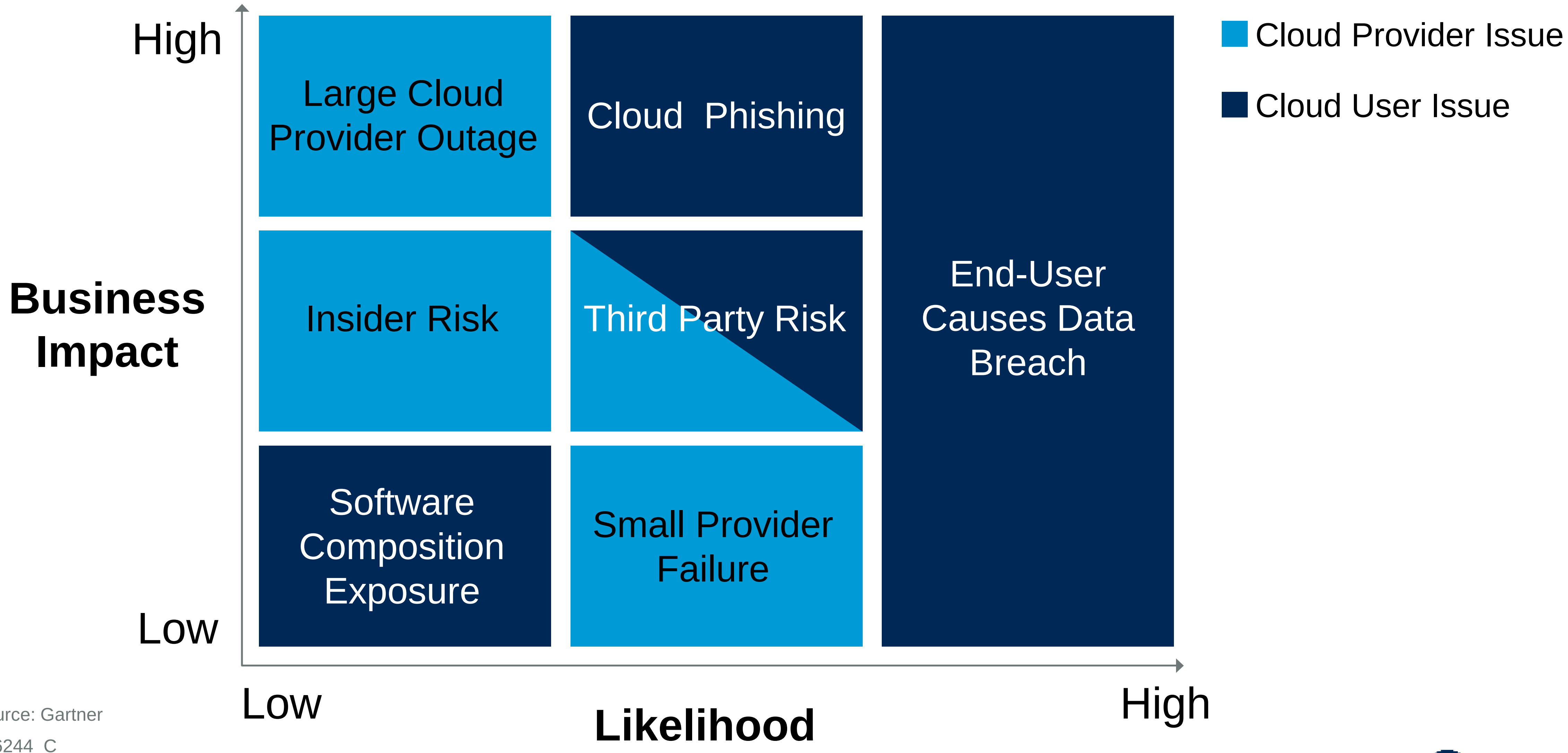
Top 5 Priorities for Securing AI Applications



1. AI Inventory: Explainability and Interpretability
2. AI Risk Awareness
3. AI Data Protection and Privacy
4. Robust ModelOps
5. AI Security and Resilience

AI TRiSM: Trust, Risk and Security Management

Threats on Cloud Assets



High

Business Impact

Low

Large Cloud Provider Outage

Cloud Phishing

Insider Risk

Third Party Risk

End-User Causes Data Breach

Software Composition Exposure

Small Provider Failure

Low

Likelihood

High

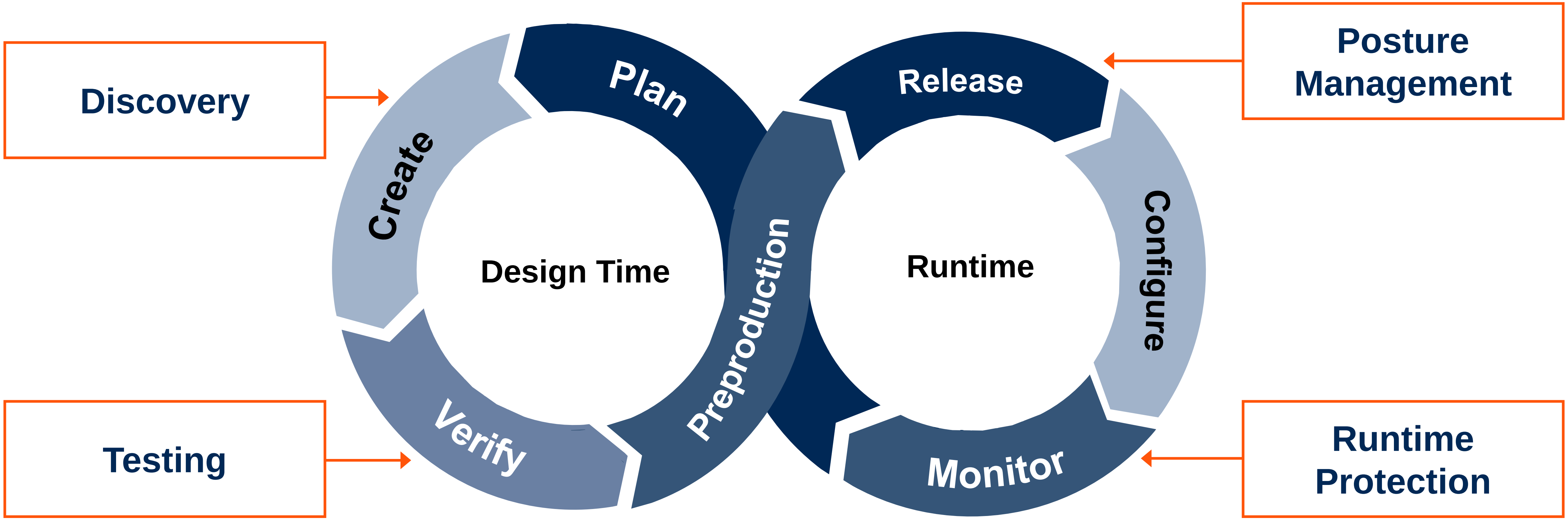
🟦 Cloud Provider Issue

■ Cloud User Issue

Source: Gartner

786244_C

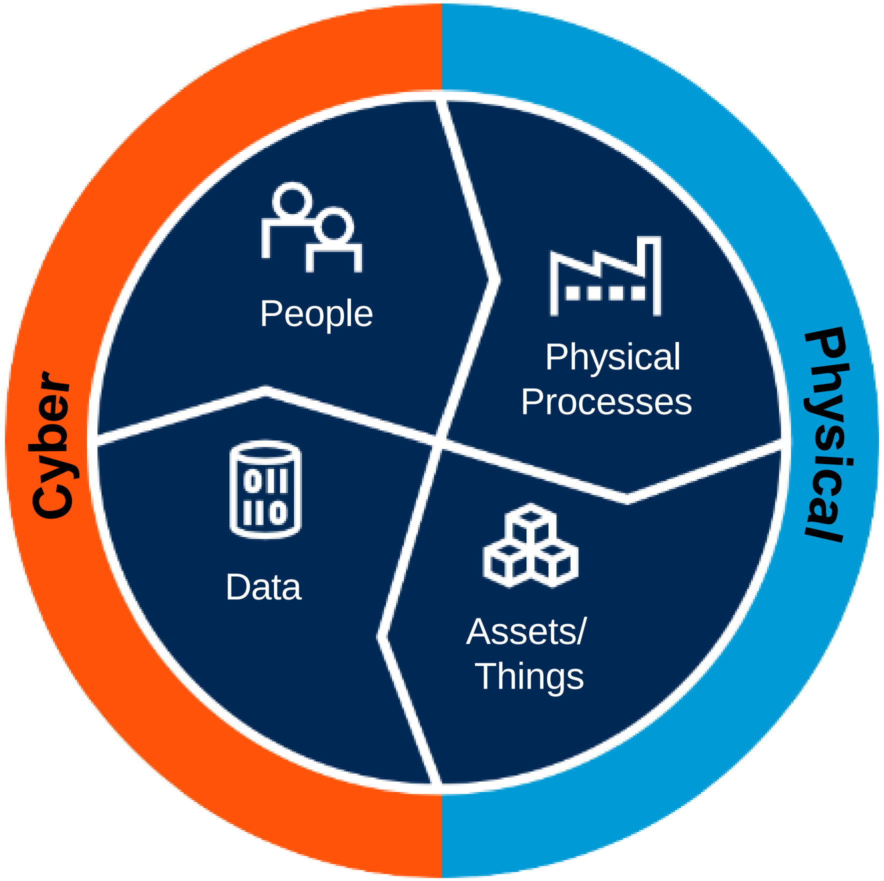
API Security Requires More than Runtime Controls



RESTRICTED DISTRIBUTION

Gartner

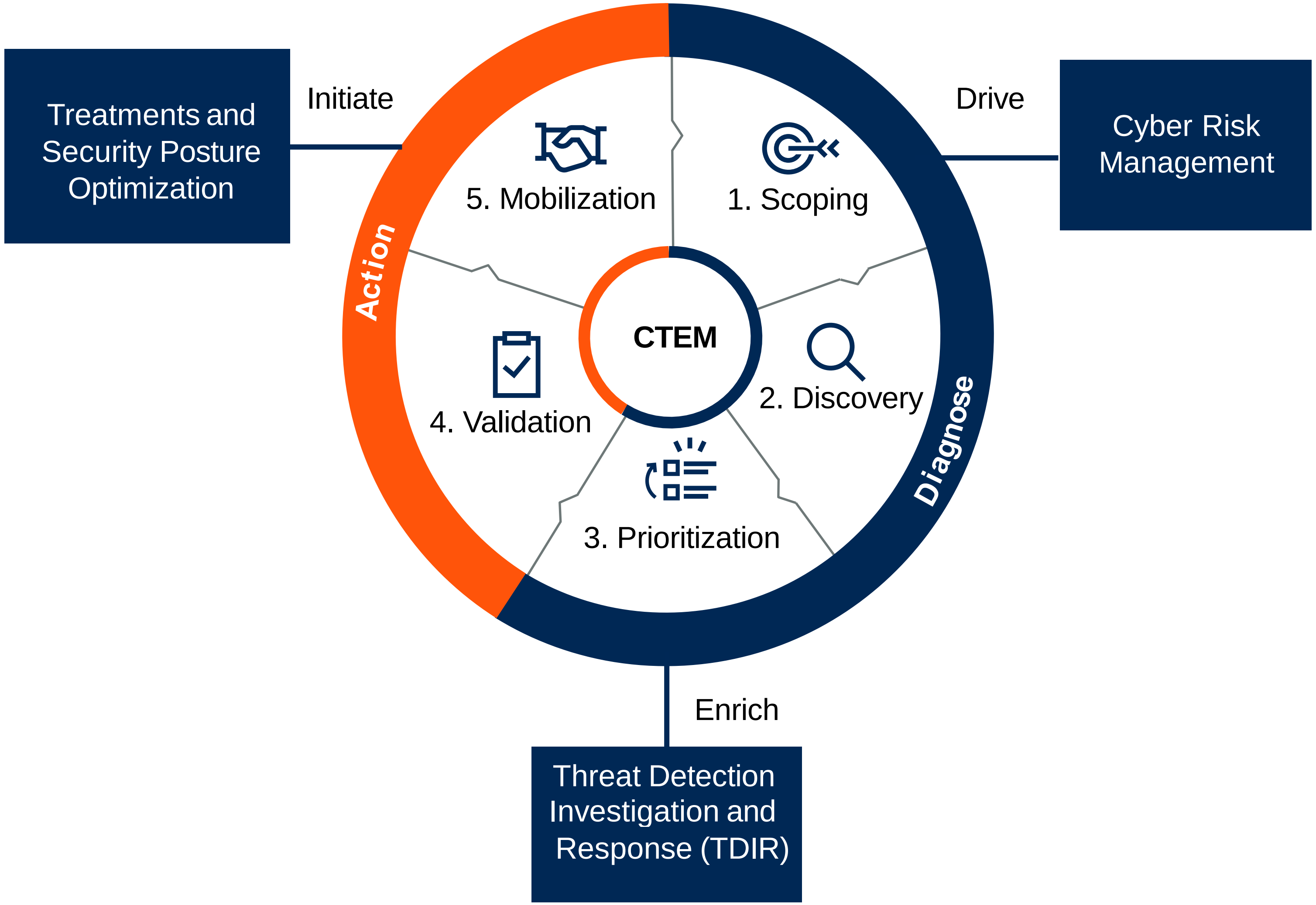
Cyber Physical Systems: Get Ready for Different Threats



Drones	Physical Infrastructure	Humans
Temperature, Humidity, Light Levels, etc.	Time	Location GPS/GIS

RESTRICTED DISTRIBUTION

Continuous Threat Exposure Management (CTEM)



Source: Gartner 779535_C

Gartner

Top Cybersecurity Trends for 2023-2024

Responsive Ecosystems

- Threat Exposure Management
- Identity Fabric Immunity
- Cybersecurity Validation

Restructuring Approaches

- Cybersecurity Platform Consolidation
- Cybersecurity Operating Model Transformation
- Composable Security

Rebalancing Practices

- Human-Centric Security Design
- Enhanced People Management
- Increasing Board Oversight

Sustainable Balanced Cybersecurity Programs

Source: Gartner

Key Recommendations

- ✓ Avoid declining effectiveness against top threats by monitoring and adapting to microtrends
- ✓ Prepare for the most likely high momentum threats where current posture lags behind attackers.
- ✓ Plan for uncertainty through investment in resilience rather than specific defensive postures.