FUTUREPORT BILBAO

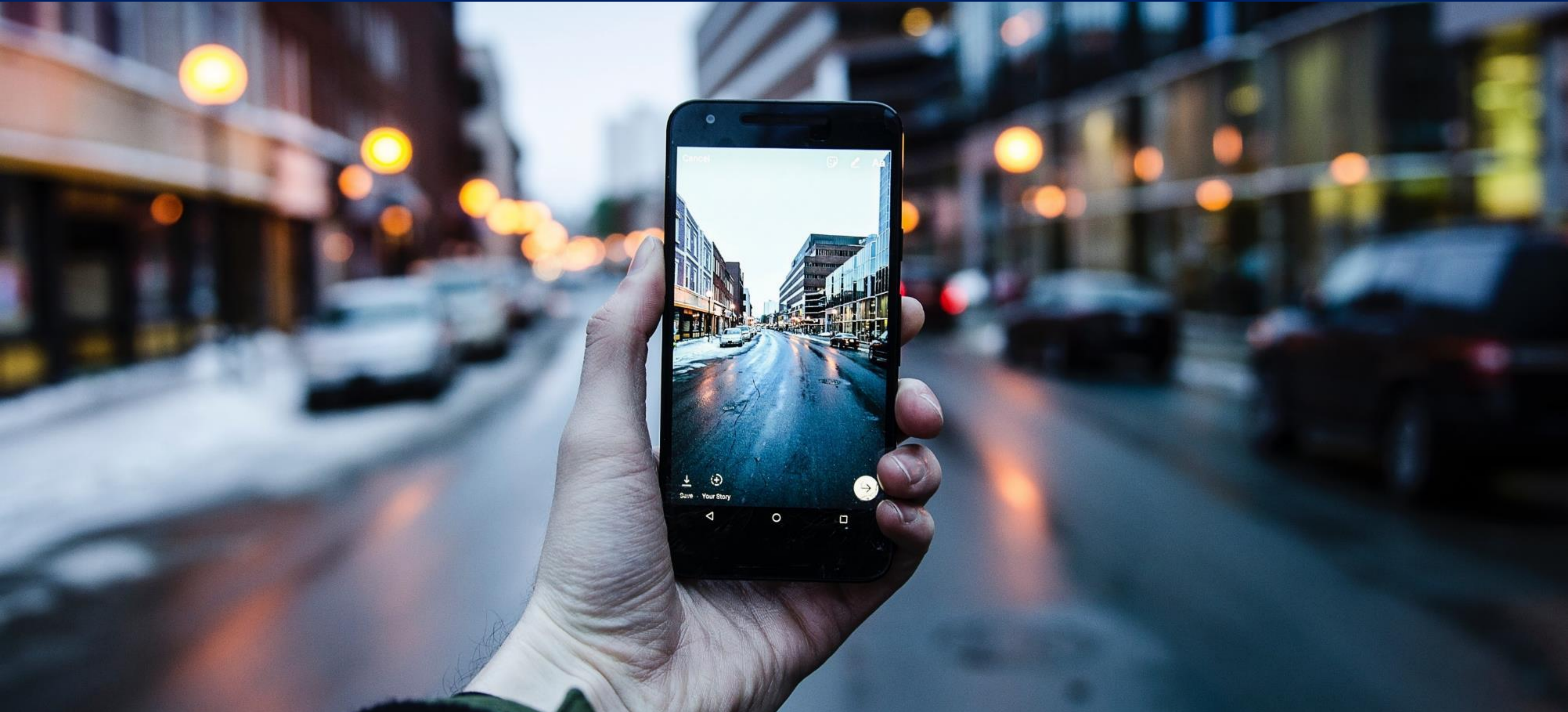
March 2023, Bilbao, Spain

Digitalización y Ciberseguridad en Puertos

Francisco de los Santos
Executive Partner, Executive Programs Iberia
francisco.delossantos@gartner.com

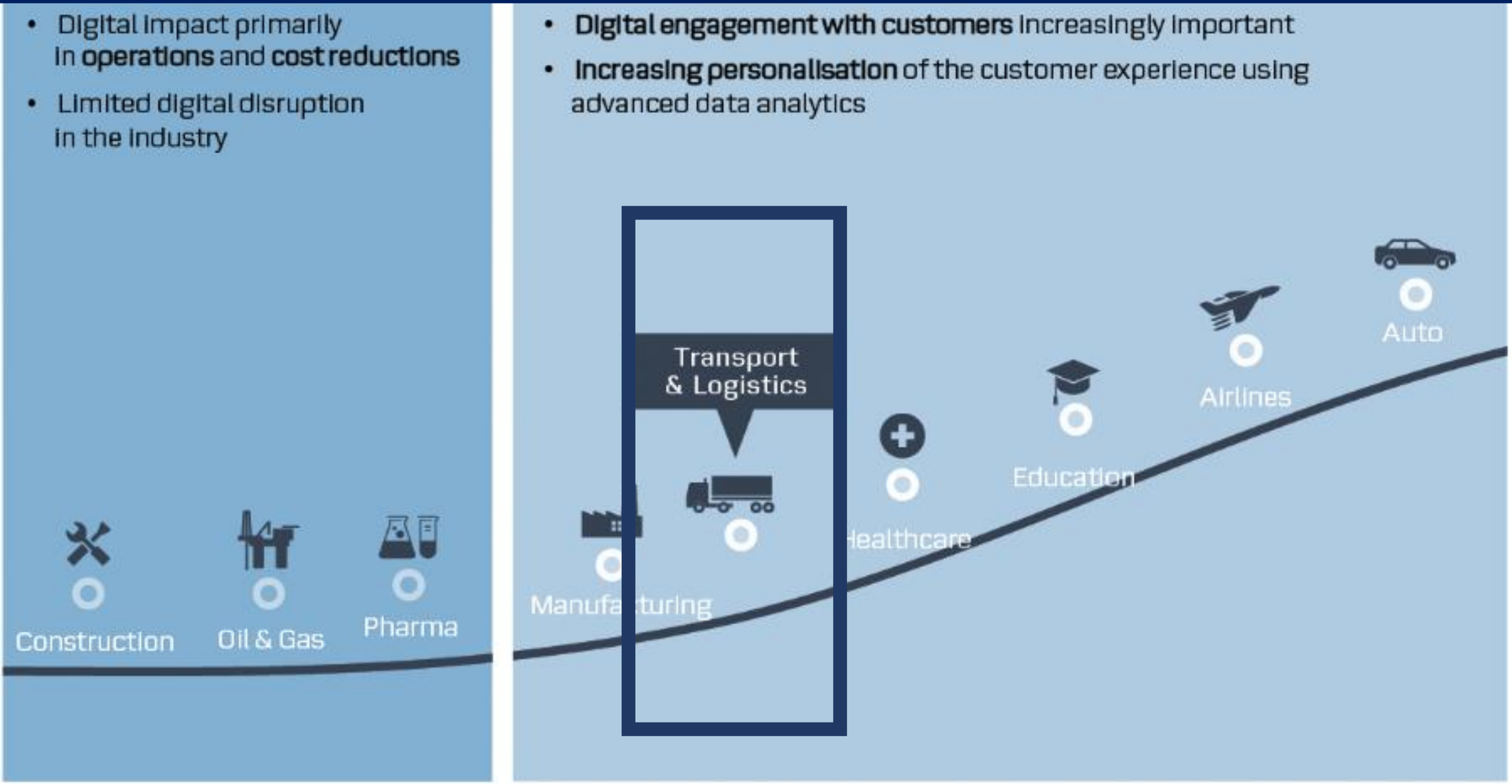
Gartner®

Information and Technology is Transforming the Port and Shipping Industry...



Adoption of Digital Technology

Transport & Logistics Lagging Behind: Processes Manual & Poorly Digitized



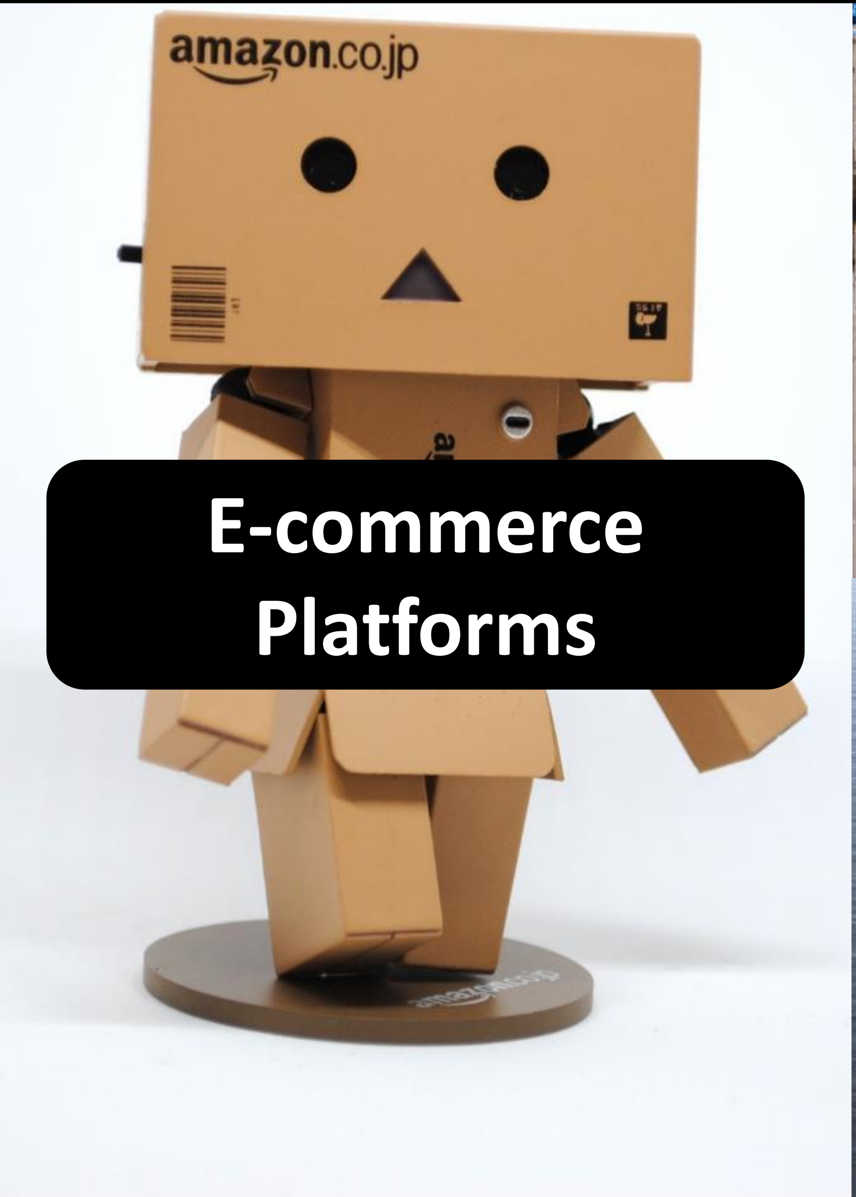
- Digital impact primarily in **operations** and **cost reductions**
- Limited digital disruption in the industry

- **Digital engagement with customers** increasingly important
- **Increasing personalisation** of the customer experience using advanced data analytics

Source: Maersk Line

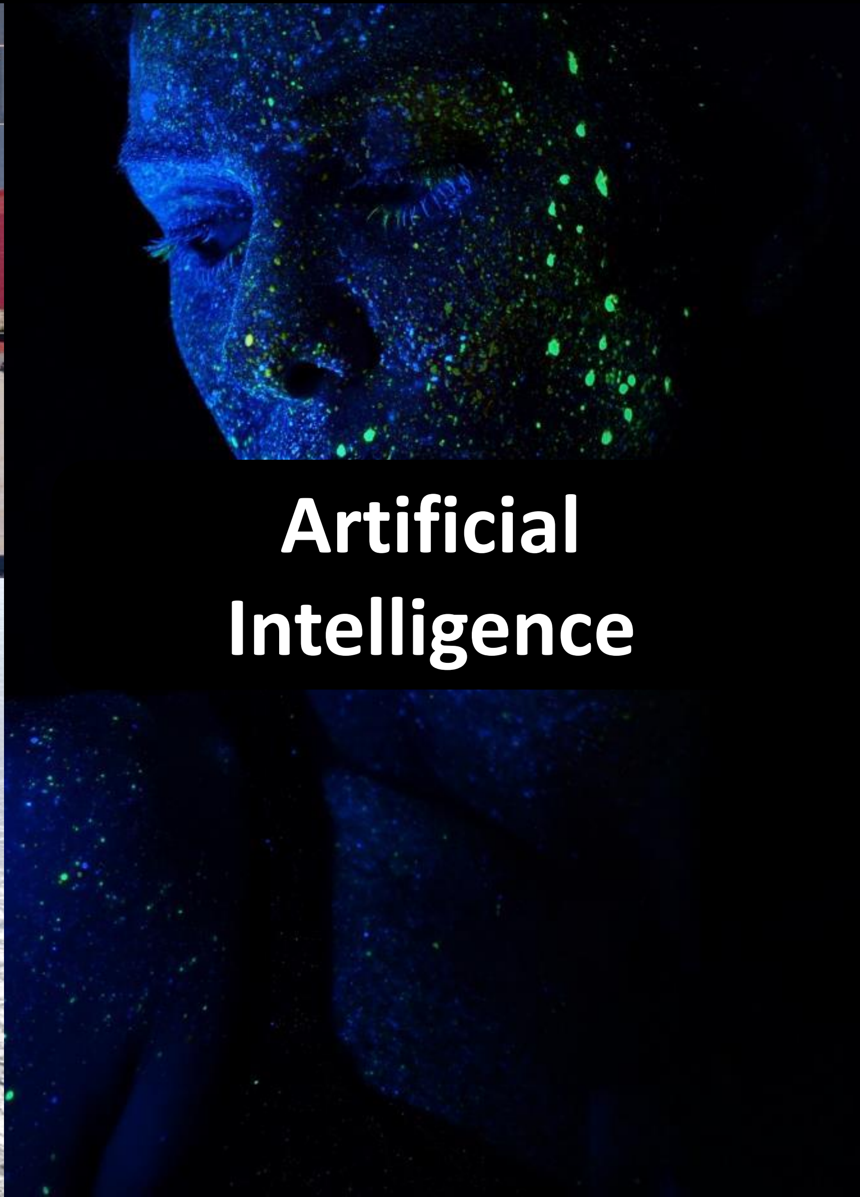
Source: Jan Hoffmann, UNCTAD

Digital Forces Transforming the Port and Shipping Industry



E-commerce Platforms

Automation & Autonomous



Artificial Intelligence

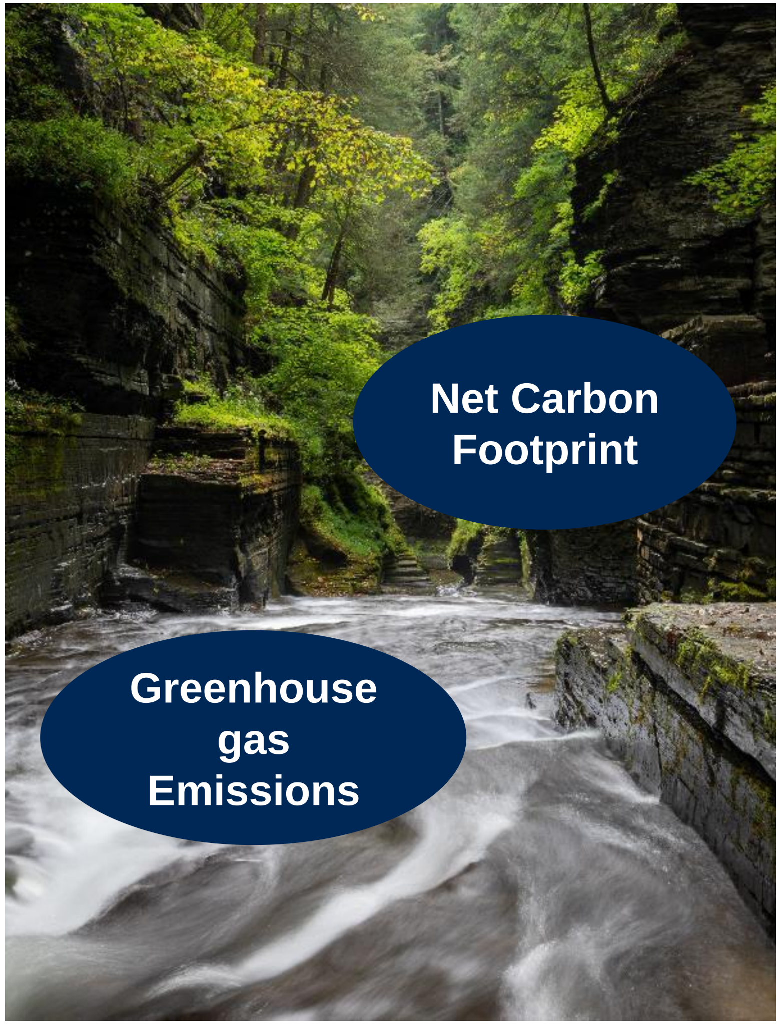
The Definition of Value Is Evolving

EBIT

EPS

Gender Diversity

Employee Satisfaction



Net Carbon Footprint

Greenhouse gas Emissions

14%

of employees want to return to the office full time

19%

of employees prefer to never work in the office

The Majority of Employees Expect the Best of Both Worlds

Source: Gartner, “Digital Worker Experience Survey 2021”

We Are in the Middle of an Era of Extreme Uncertainty

Supply Chain Complications

Semiconductor Shortages

Geopolitical Tension

Energy dependency

Cybersecurity

Deglobalization

Technology Matters More Than Ever

CEO Business Priorities

Growth

Workforce

Technology

Profitable Growth

Agile

Flexible

Digital

RESTRICTED DISTRIBUTION

Everyone wants great security...

... until they have to pay for it

Gartner

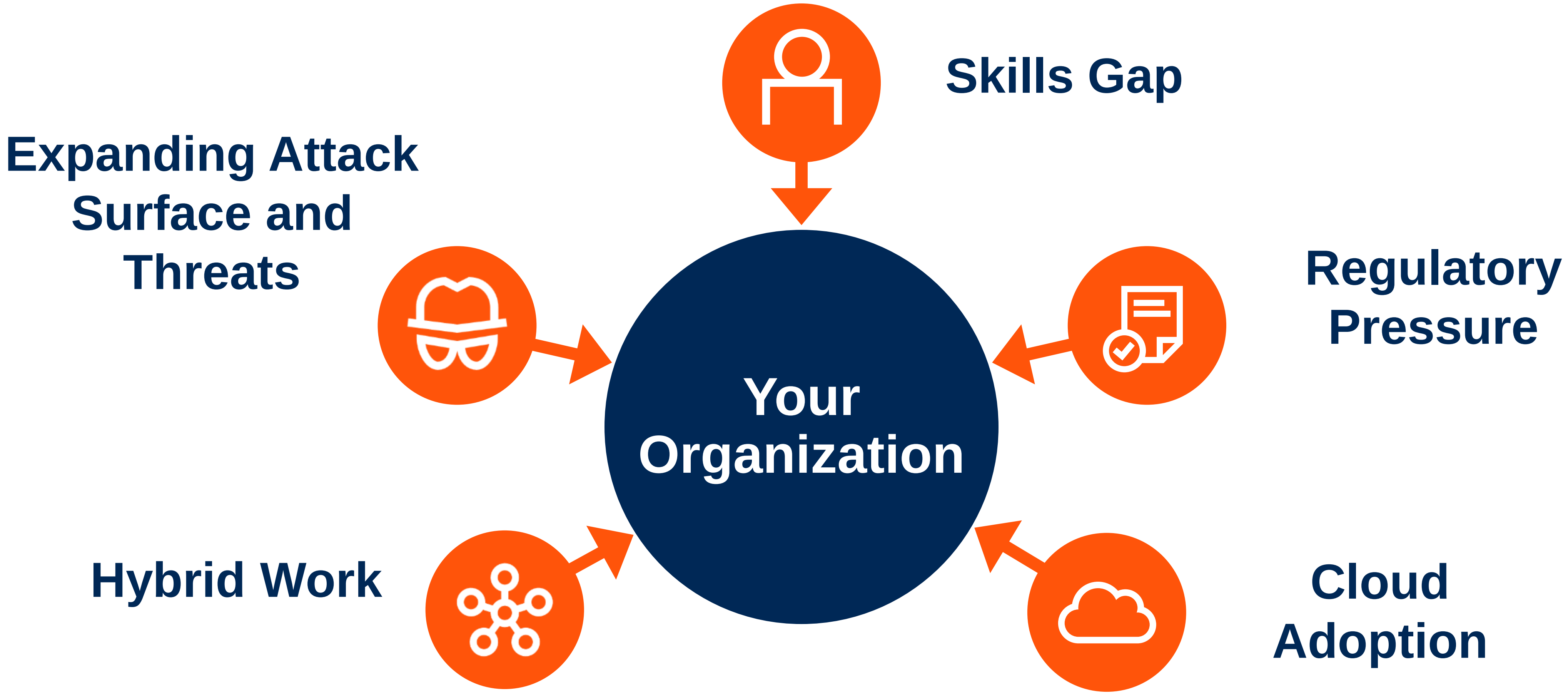
66%

of organizations were hit by ransomware in the last year

4 in 5

Hacks attributed to organized crime

Persistent Security Challenges Driving Top Trends



Skills Gap

Expanding Attack Surface and Threats

Regulatory Pressure

Your Organization

Hybrid Work

Cloud Adoption

About Today’s Event

Threat Landscape

Technology Trends

Leadership Vision

About Today's Event

Threat Landscape

Technology Trends

Leadership Vision

Handling the Various Categories of Threats

Top Threats

(Known and Frequent)

High Momentum Threats

Emerging and Niche Threats

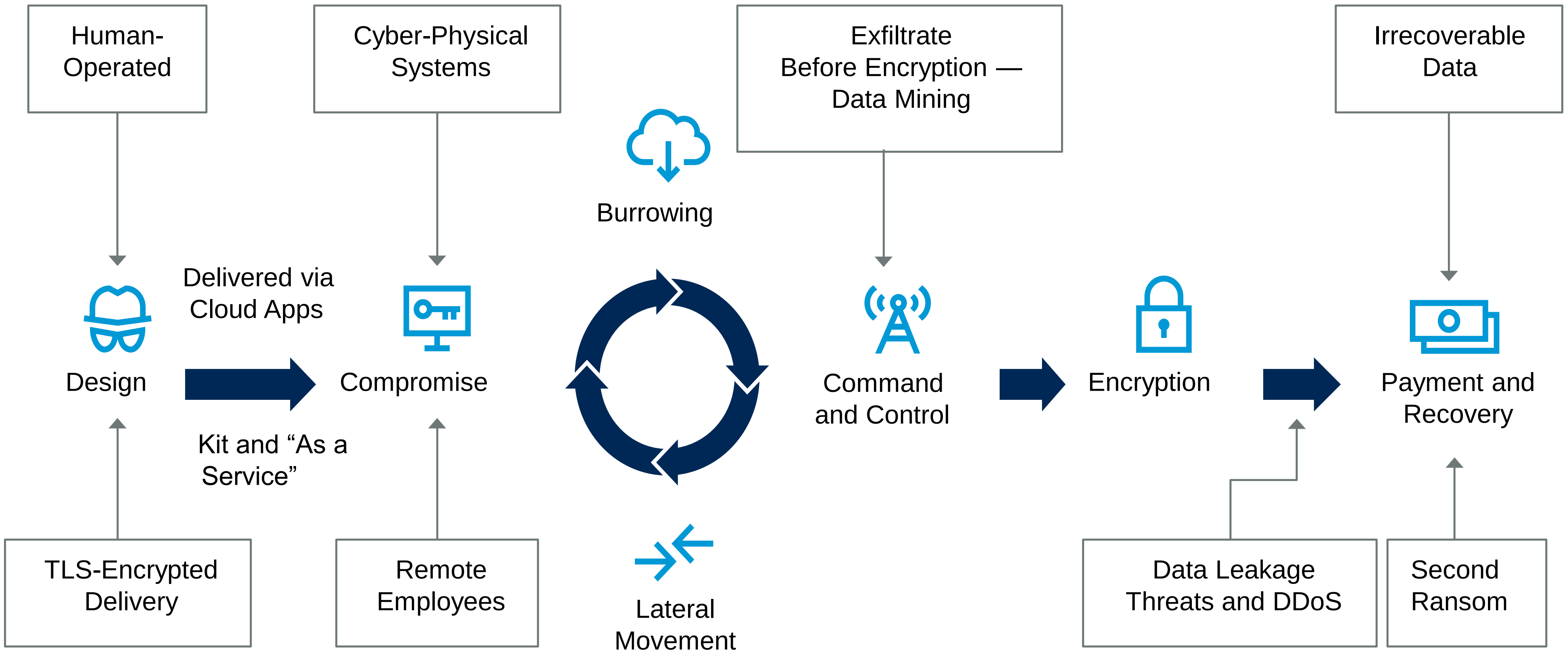
Handling the Various Categories of Threats

Top Threats
(Known and Frequent)

High Momentum Threats

Emerging and Niche Threats

#1: Ransomware becomes Extortionware



Human-Operated

Cyber-Physical Systems

Exfiltrate Before Encryption — Data Mining

Irrecoverable Data

Burrowing

Design

Delivered via Cloud Apps

Kit and “As a Service”

Compromise

Command and Control

Encryption

Payment and Recovery

Lateral Movement

TLS-Encrypted Delivery

Remote Employees

Data Leakage Threats and DDoS

Second Ransom

Source: Gartner

759813_C

Four Stages of Ransomware Extortion

Encryption

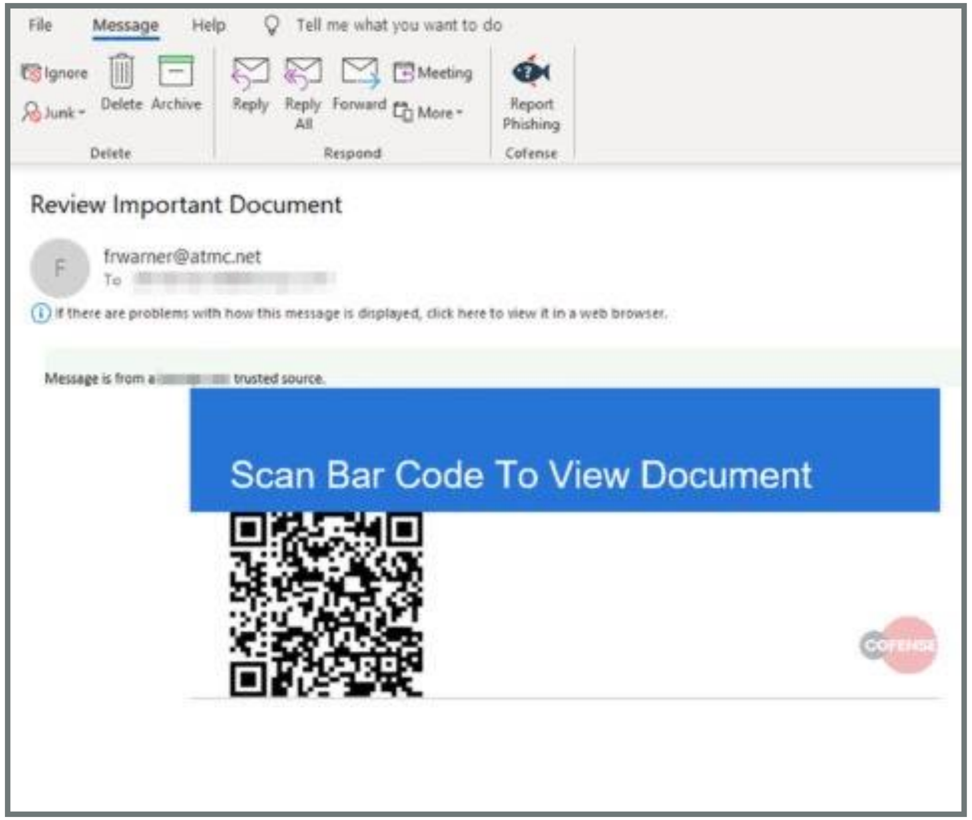
Data Exfiltration

Data Mining

DDoS Attacks

#2: Multi-Channel Phishing

Targeted phishing tests can top at 70% success rate[1]



Review Important Document

F frwarner@atmc.net

To [redacted]

If there are problems with how this message is displayed, click here to view it in a web browser.

Message is from a [redacted] trusted source.

Scan Bar Code To View Document

Recommendations:

- ✓ Enhance people-centric phishing detection
- ✓ Improve the speed and quality of phishing triage processes
- ✓ Reduce the impact through phishing by implementing internal business controls.

[1] Proofpoint “State of the Phish, 2022”. Graphic source: https://cofense.com/radar-phishing-using-qr-codes-evade-url-analysis/

#3: Multiple flavors of Account Abuses

Targeted Identities

- Privileged accounts
- Employees
- Contractors
- Services

Attack trends

- Credential stuffing
- Hu-bot: semi-automated attacks
- Gaps in MFA
- Abuse remote-based enrolment

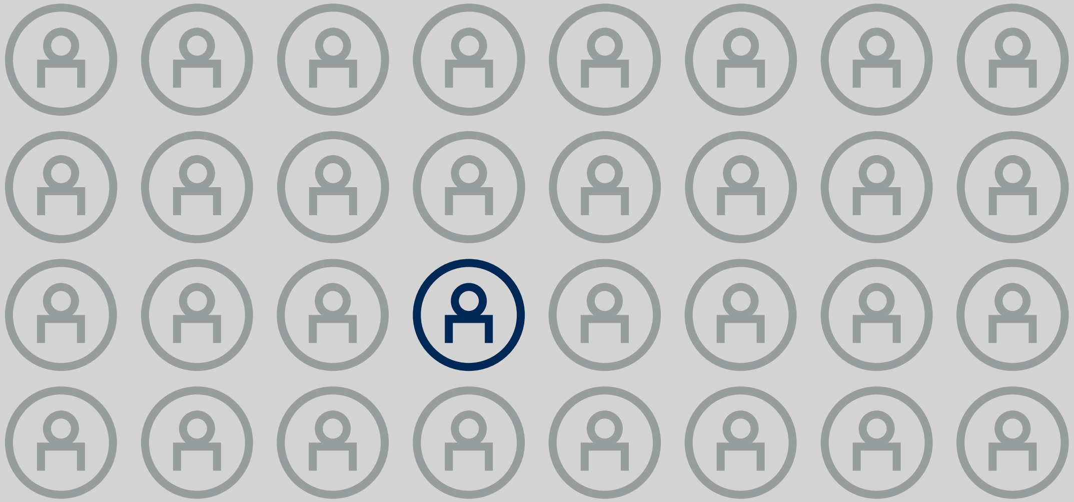
#4: Insider Risk vs. Insider Threat

Insider Risk

The 100% of connected employees that are innovating, collaborating and creating.

Focus on **protecting all data and users** from everyday risks – no matter their intent.

Insider Threat



The <1% of employees that are bad.

Focus on **specific users** committing **isolated acts** with **malicious intent**.

RESTRICTED DISTRIBUTION

Why It Matters

17%

of all sensitive files are accessible to every employee

30%

of all data breaches are the result of internal actors

63%

of insider incidents stem from careless user actions

Sources: Forcepoint and Ponemon Institute

Handling the Various Categories of Threats

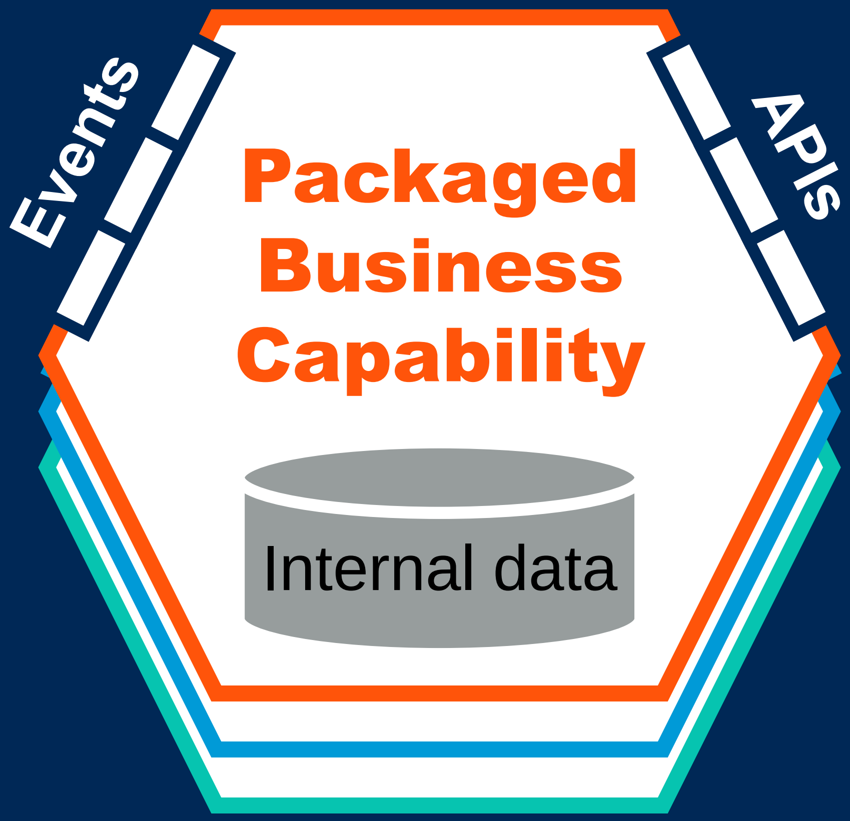
Top Threats

(Known and Frequent)

High Momentum Threats

Emerging and Niche Threats

Package Business Capabilities as Components



By 2024, the design mantra for new SaaS and custom applications will be **“composable API-first or API-only”**, rendering traditional SaaS and custom applications “legacy.”

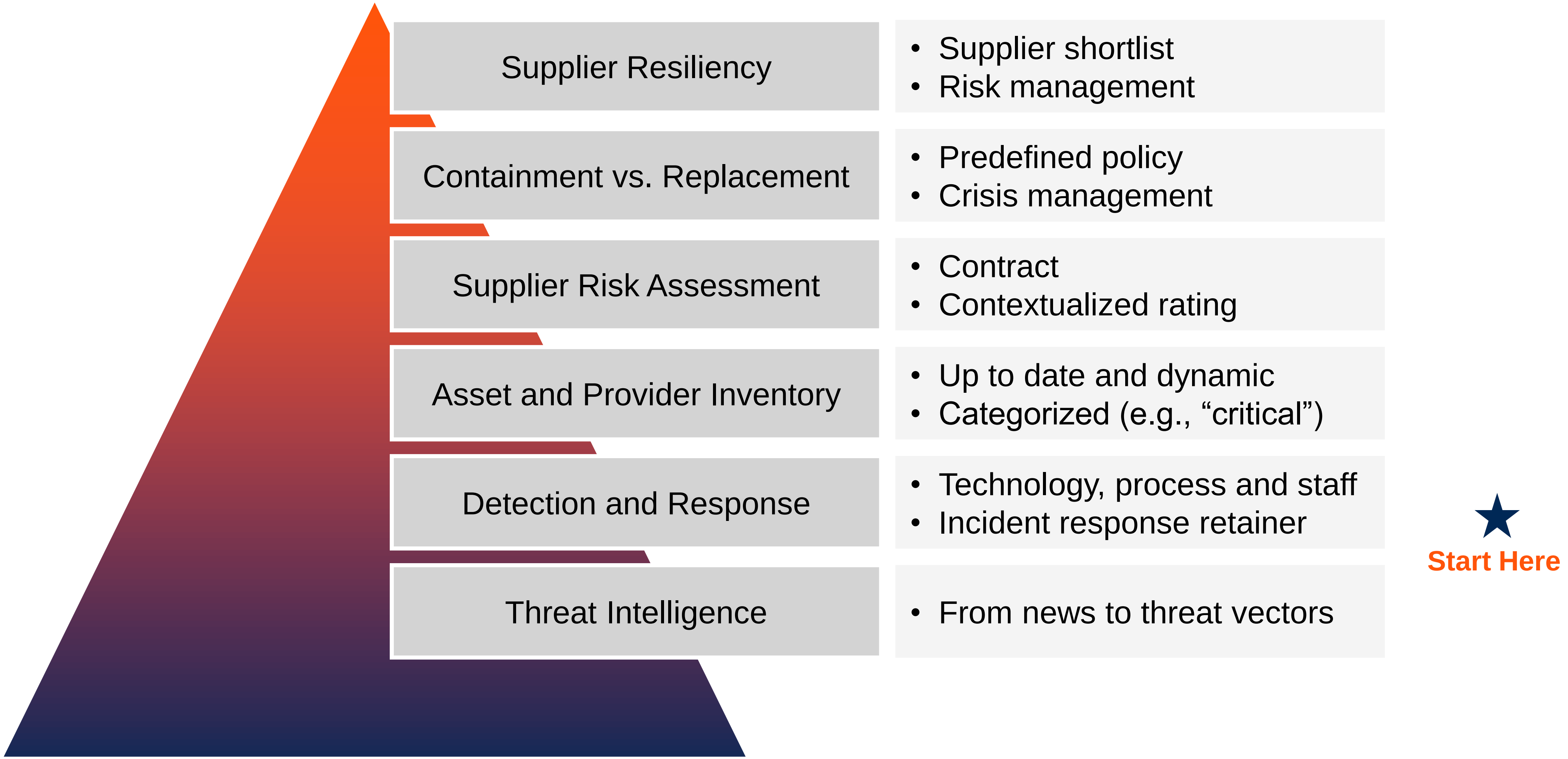
By 2025, **less than 50%** of enterprise APIs will be managed, as explosive growth in APIs surpasses the capabilities of API management tools

Gartner Strategic Planning Assumptions

By 2025, 60% of organizations will use cybersecurity risk as a **primary determinant** in conducting **third-party transactions and business engagements**.

Analysis: Sam Olyaei

Portfolio of Supply Chain Technology Controls



Supplier Resiliency
- Supplier shortlist
- Risk management

Containment vs. Replacement
- Predefined policy
- Crisis management

Supplier Risk Assessment
- Contract
- Contextualized rating

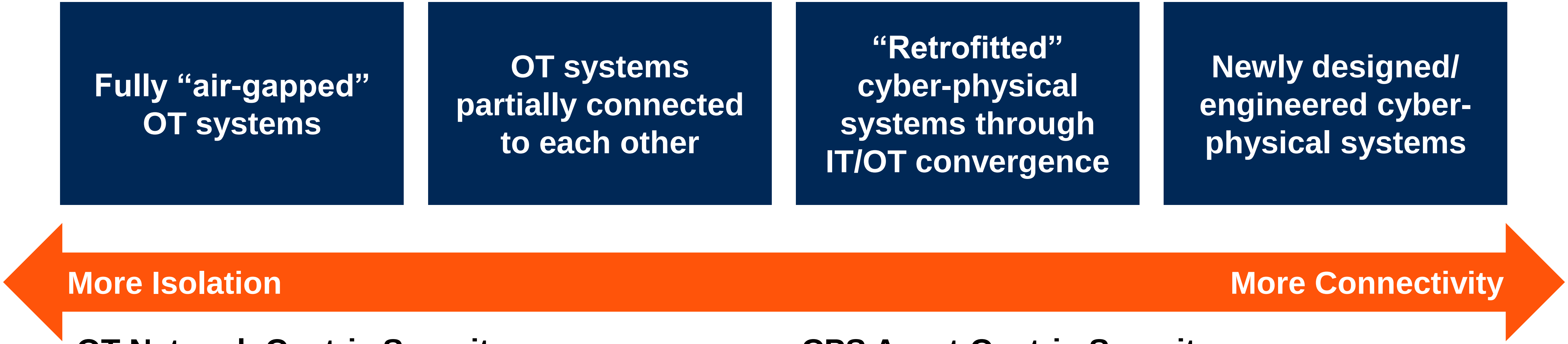
Asset and Provider Inventory
- Up to date and dynamic
- Categorized (e.g., “critical”)

Detection and Response
- Technology, process and staff
- Incident response retainer

Threat Intelligence
- From news to threat vectors

★ Start Here

From OT Security to CPS Security



Fully “air-gapped” OT systems

OT systems partially connected to each other

“Retrofitted” cyber-physical systems through IT/OT convergence

Newly designed/ engineered cyber-physical systems

More Isolation

More Connectivity

OT Network-Centric Security

- Purdue 5 Layer model
- Firewalls
- DMZs
- Unidirectional diodes

CPS Asset-Centric Security

- Discovery, Inventory
- Connectivity/communications mapping
- Vulnerability management
- Dynamic segmentation
- Remote Access Management
- Dashboards and Compliance Reports
- Etc.…

Source: Gartner

Handling the Various Categories of Threats

Top Threats

(Known and Frequent)

High Momentum Threats

Emerging and Niche Threats

The Future of Work is Hybrid

Advanced Attackers			Recommendations		
Adapt Social Engineering	**Exploit Gaps**	**Exploit Mistakes**	**Change Mindset**	**Monitor Initiatives**	**Audit**
For remote workers	*From transition*	*When transitioning to cloud*	*From “Scale Fast” to “Long-term”*	*Workforce and workplace modernization*	*Use cases “unthinkable” before*

RESTRICTED DISTRIBUTION

Although cloud providers (SaaS, PaaS and IaaS) suffered issues in 2021, the biggest threat when it comes to using the cloud remains customer misconfiguration or misuse of these increasingly complicated services.

Jeremy D'Hoinne, John Watts, Katell Thielemann

About Today’s Event

Threat Landscape

Technology Trends

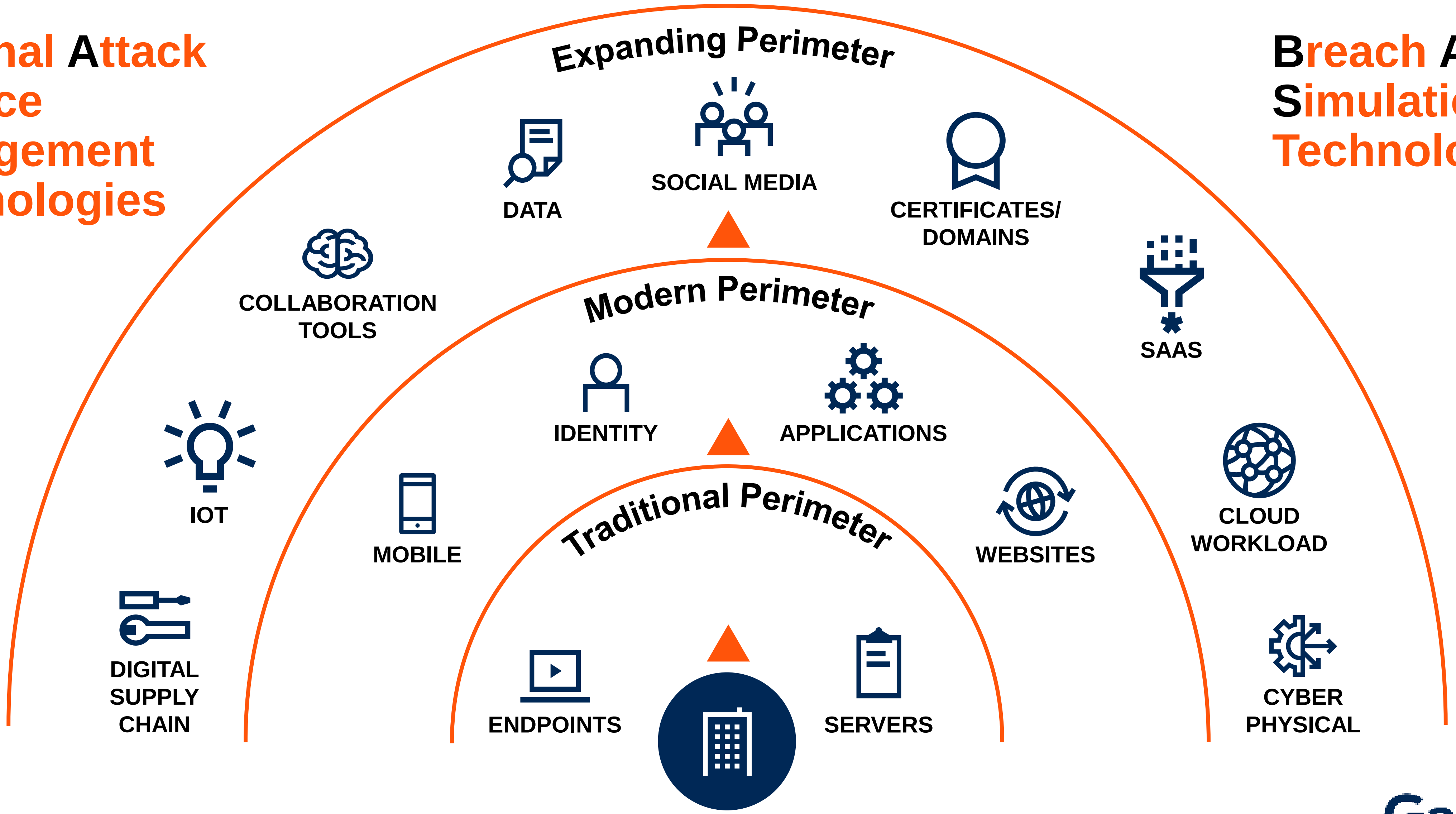
Leadership Vision

TREND

Enterprise Attack Surfaces are Expanding Rapidly

Attack Surface Expansion

External Attack Surface Management Technologies



Breach Attack Simulation Technologies

TREND

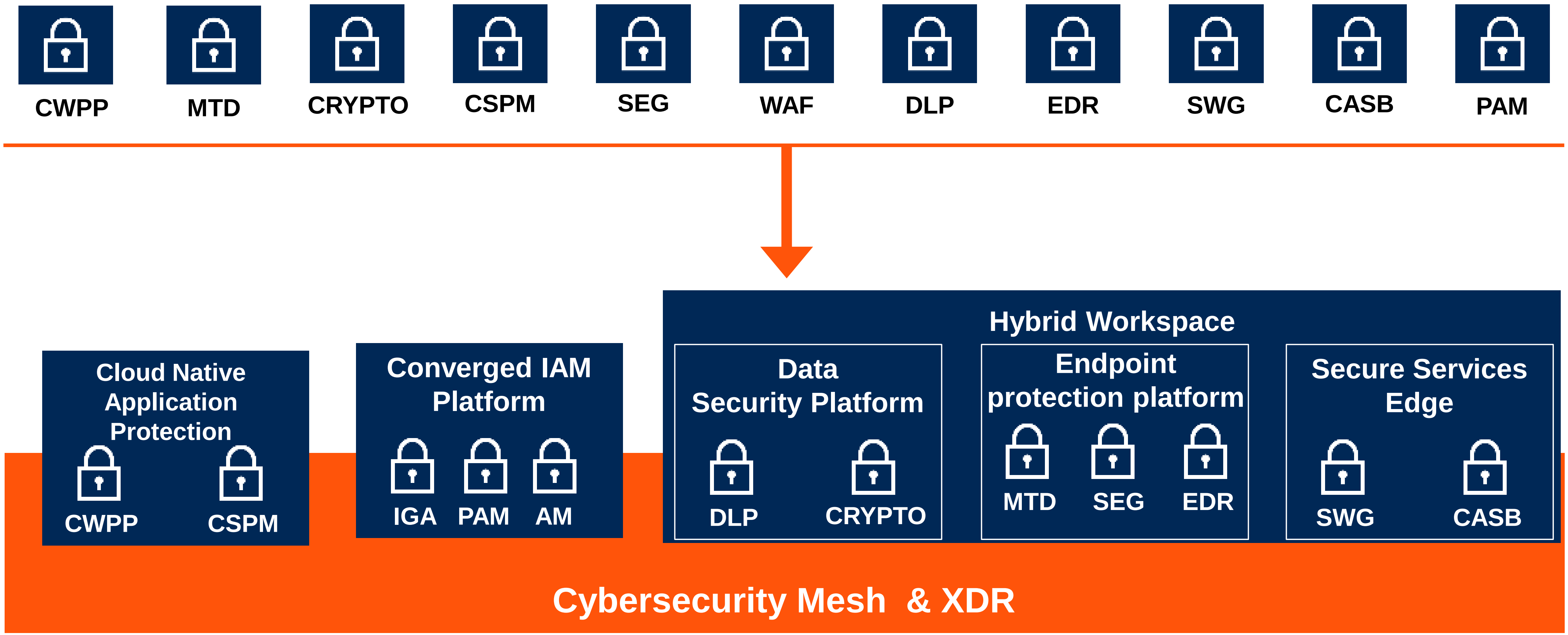
Identity Threat Detection and Response discipline emerges

Identity Threat Detection and Response encompasses the tools and processes to protect the identity infrastructure from malicious attacks, detect and investigative potential incursions, and restore normal operation in the event of tampering.

TRENDCybersecurity Products are Consolidating

Cybersecurity Product Consolidation

Legacy Security Vendor Ecosystem



CWPP MTD CRYPTO CSPM SEG WAF DLP EDR SWG CASB PAM

Cloud Native Application Protection
CWPP CSPM

Converged IAM Platform
IGA PAM AM

Hybrid Workspace

Data Security Platform
DLP CRYPTO

Endpoint protection platform
MTD SEG EDR

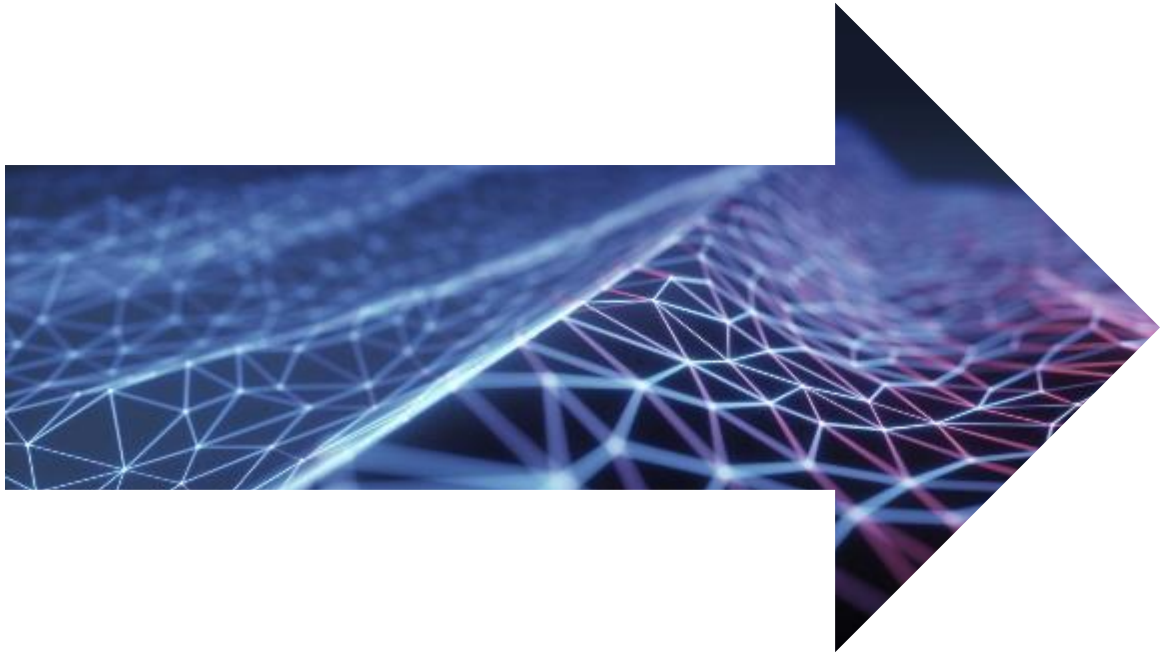
Secure Services Edge
SWG CASB

Cybersecurity Mesh & XDR

TREND

The Cybersecurity Mesh Matures

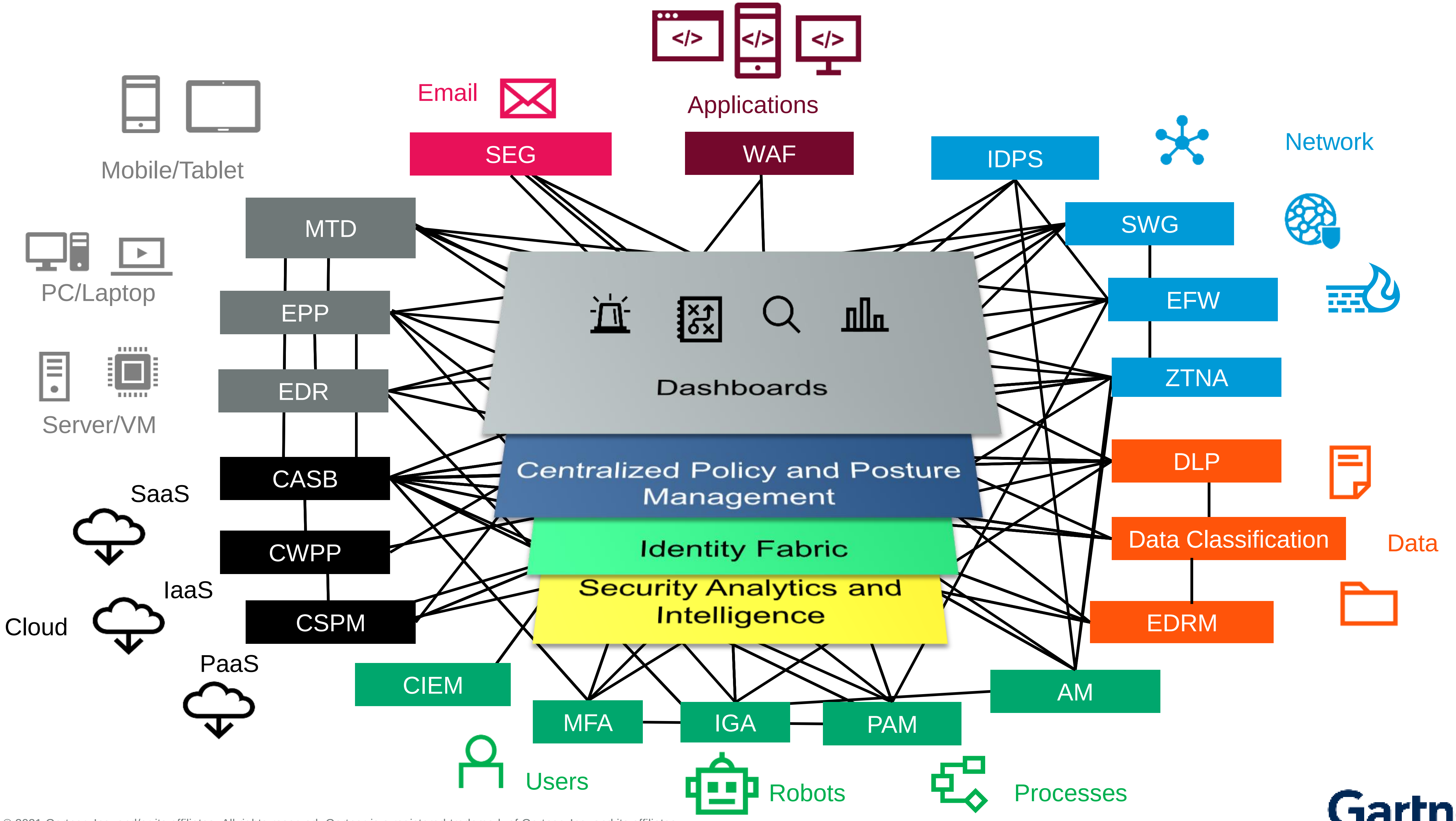
What Is Cybersecurity Mesh Architecture?



An **architectural approach** to create a **collaborative ecosystem** of security tools operating **beyond the traditional perimeter.**

This extends from technology into organization, practices and processes.

Cybersecurity Mesh Architecture Complete



TECH TRENDS

- ➢ Enterprise Attack Surfaces are Expanding Rapidly
- ➢ Identity Threat Detection and Response discipline emerges
- ➢ Cybersecurity Products are Consolidating
- ➢ The Cybersecurity Mesh Matures

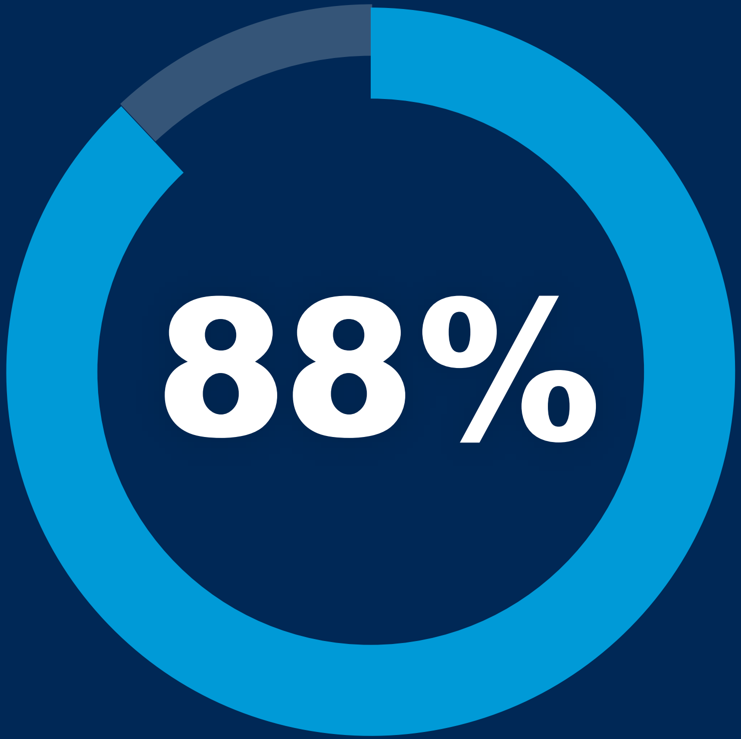
About Today’s Event

Threat Landscape

Technology Trends

Leadership Vision

2022 Gartner Board of Directors Survey

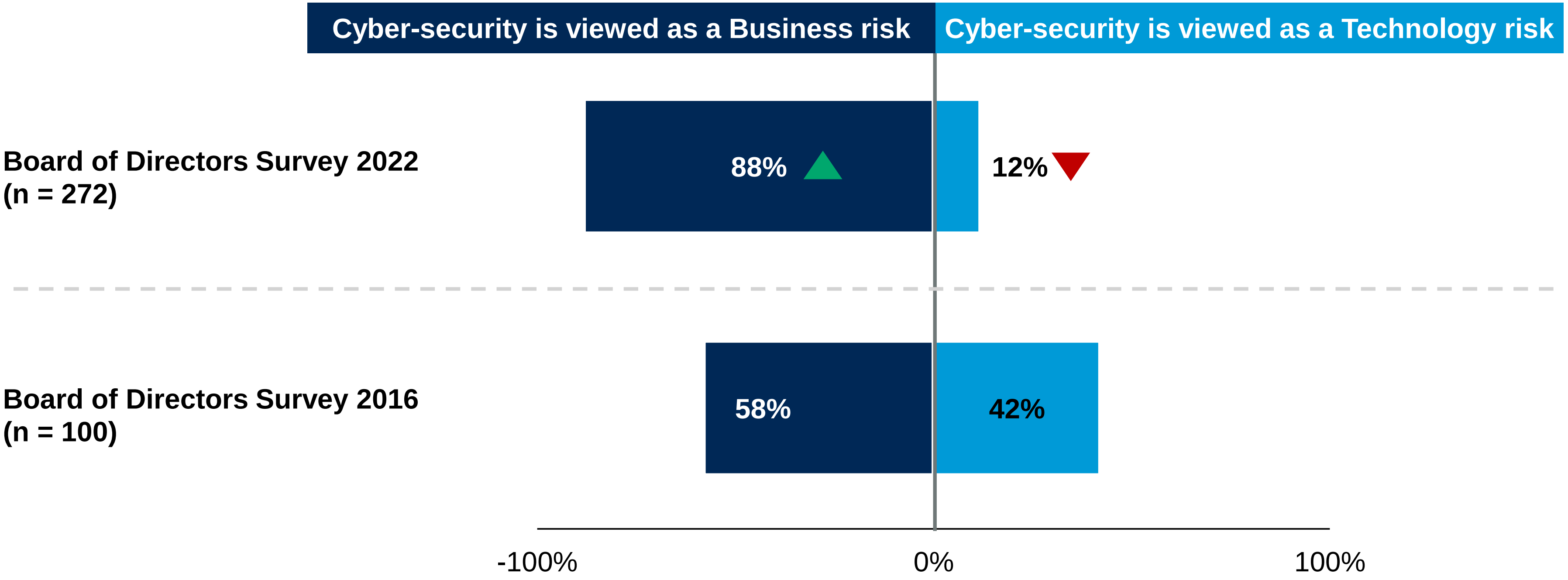


of boards now view security as a business risk, not a technical one

Source: Gartner, "2022 Gartner Board of Directors Survey"

Cybersecurity Is Now Viewed as a Business Risk

View of Cybersecurity – Comparison



▲▼ High/low significance differences between 2022 vs. 2016 survey

n varies ; All Respondents, Excluding Don't Know

Q07. Please tell us which of the two opposing viewpoints most closely represents how cyber-security is viewed and handled in your organization.

Source: 2022 Gartner View from the board of Directors' Survey

RESTRICTED DISTRIBUTION

CISO Role: What Needs to Change?

Today	Tomorrow
SRM leader is the “defacto” person **accountable** for managing cybersecurity risks	SRM leader is the person formally **responsible** for **ensuring business leaders** have the **knowledge** and **capabilities** required to make informed, high-quality information risk decisions.

Executive influence and partnership with the business is **more critical than ever** — regardless of who the SRM leader reports to …

What We Found … Human Factors

67% use same passwords for **multiple accounts**

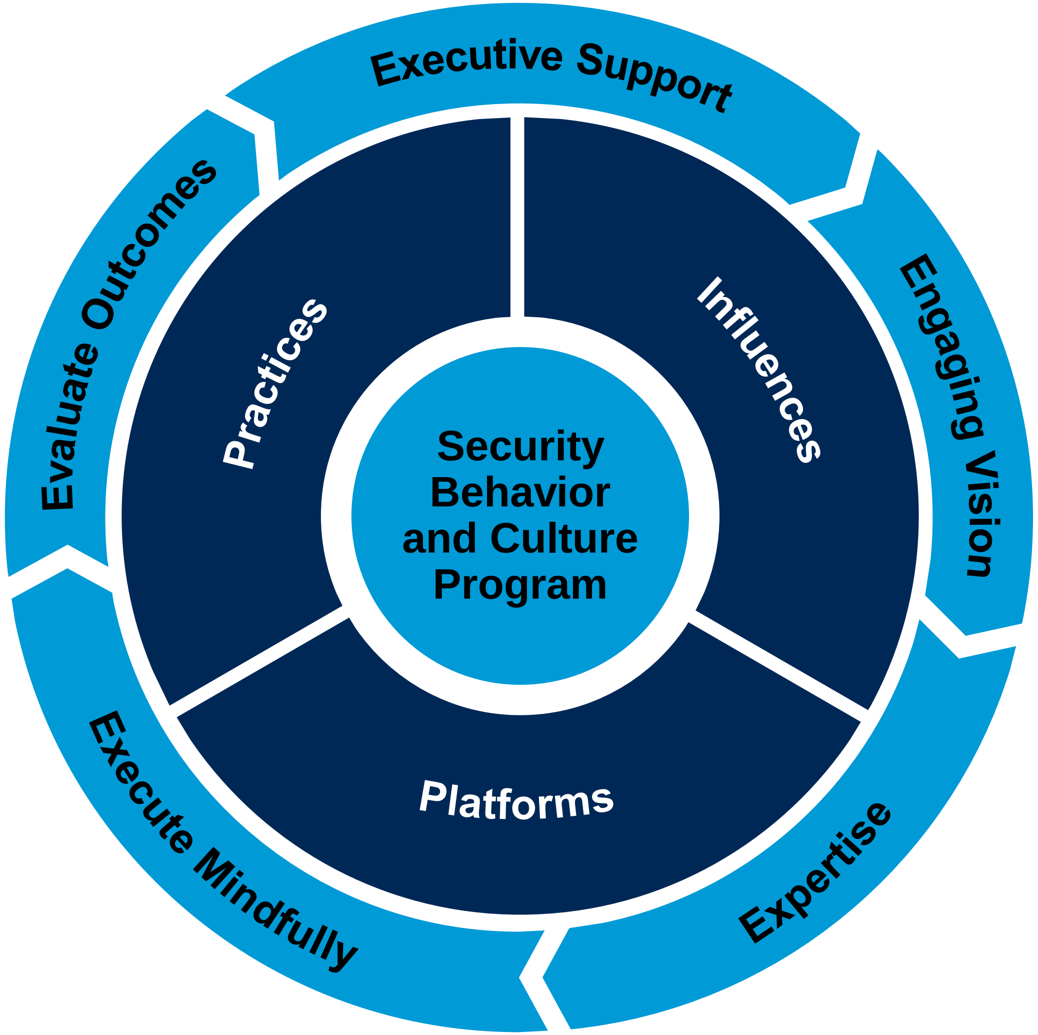
65% open emails from **unknown sources on work devices**

61% send sensitive information via **unencrypted email**

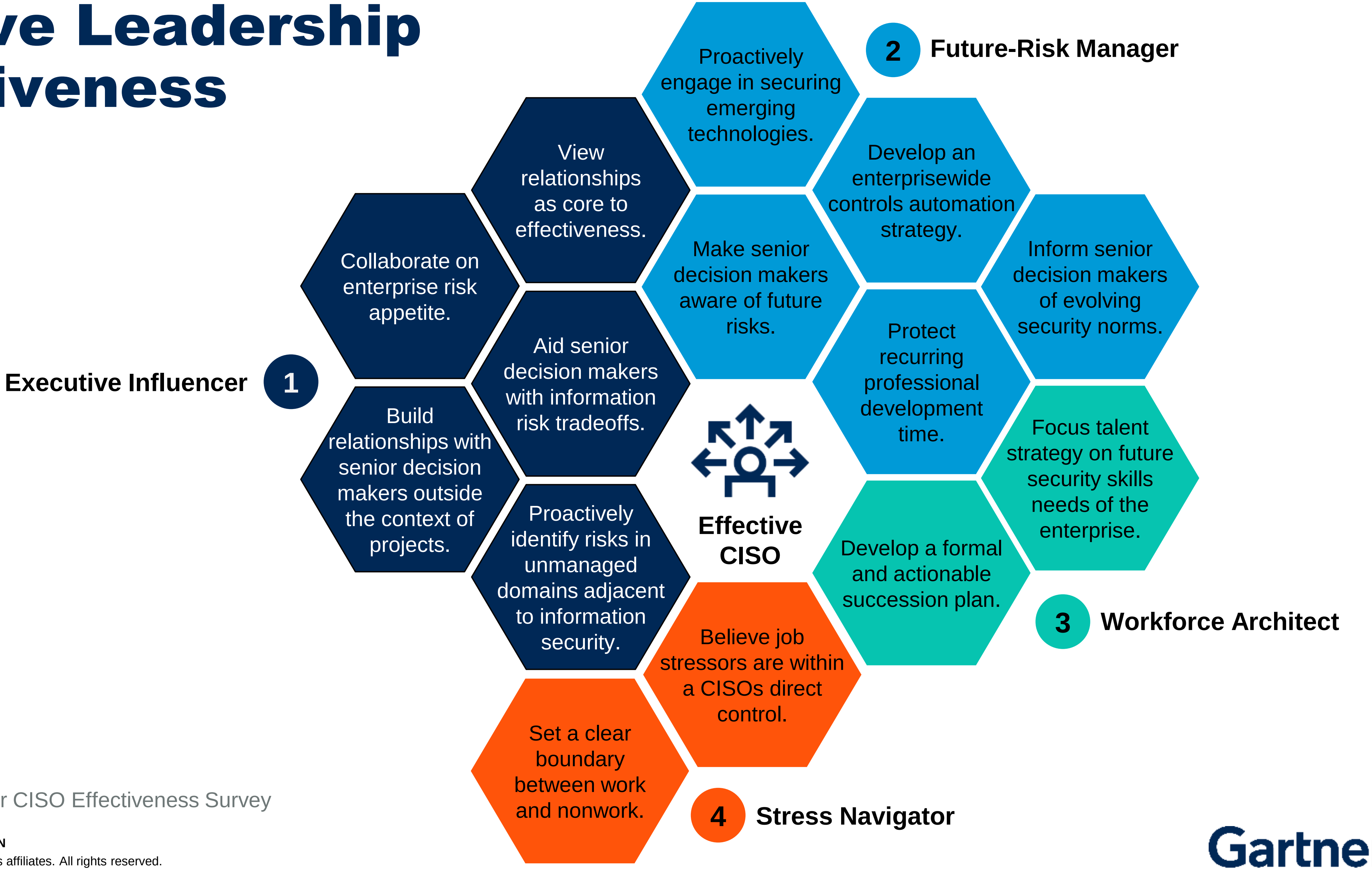
93% acknowledged their behaviors would **increase enterprise cybersecurity risk**

Source: 2022 Gartner Drivers of Secure Behavior Survey
n = 1,310 employees, excluding NA/don't know
Percentages indicate employees who engaged in these behaviors sometimes or more frequently in the past 12 months

Security Behavior & Culture Program



Improve Leadership Effectiveness



Executive Influencer 1

Collaborate on enterprise risk appetite.

View relationships as core to effectiveness.

Build relationships with senior decision makers outside the context of projects.

Aid senior decision makers with information risk tradeoffs.

Proactively identify risks in unmanaged domains adjacent to information security.

2 Future-Risk Manager

Proactively engage in securing emerging technologies.

Make senior decision makers aware of future risks.

Develop an enterprisewide controls automation strategy.

Inform senior decision makers of evolving security norms.

Protect recurring professional development time.

3 Workforce Architect

Focus talent strategy on future security skills needs of the enterprise.

Develop a formal and actionable succession plan.

4 Stress Navigator

Believe job stressors are within a CISOs direct control.

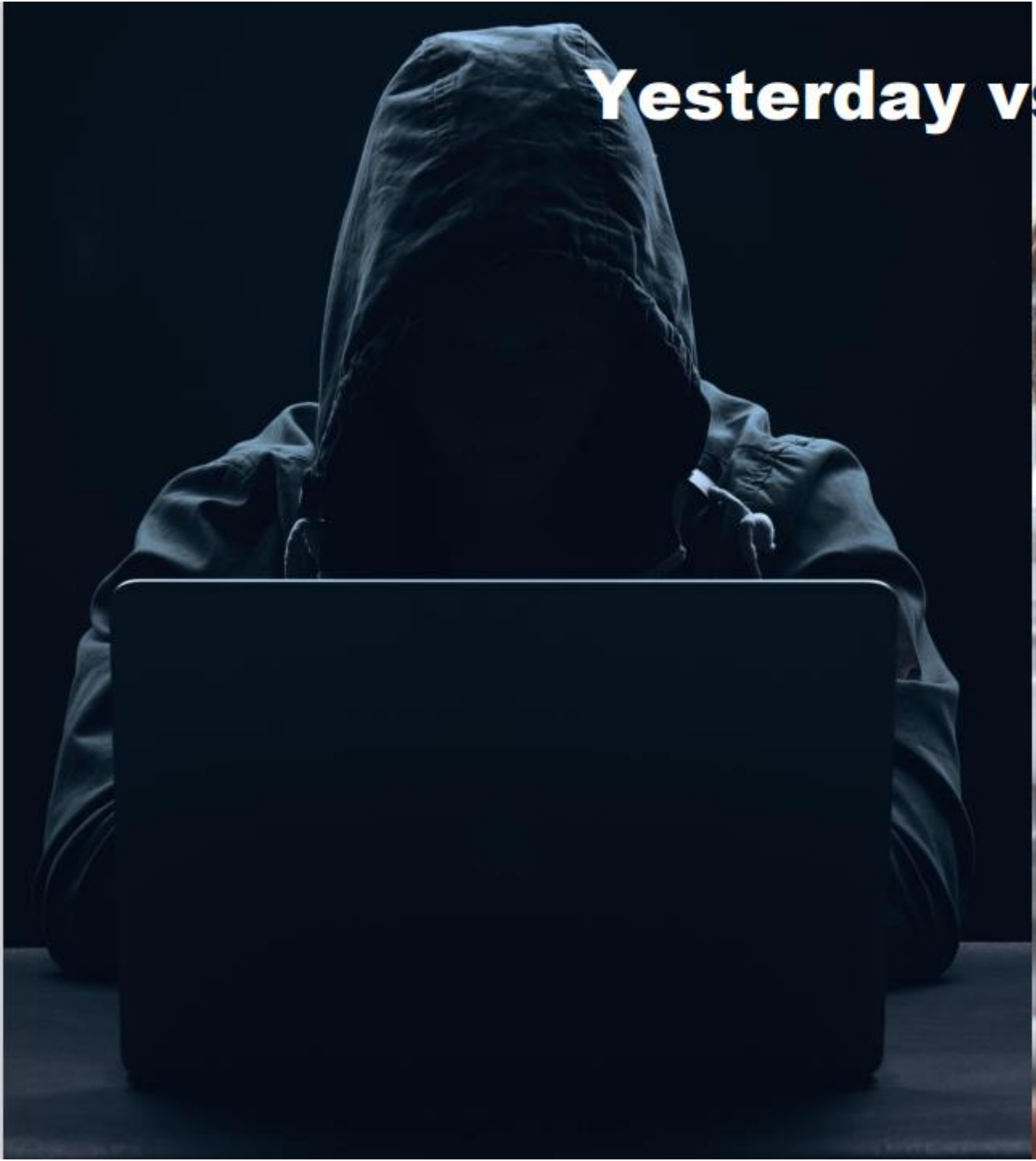
Set a clear boundary between work and nonwork.

n = 129 CISOs

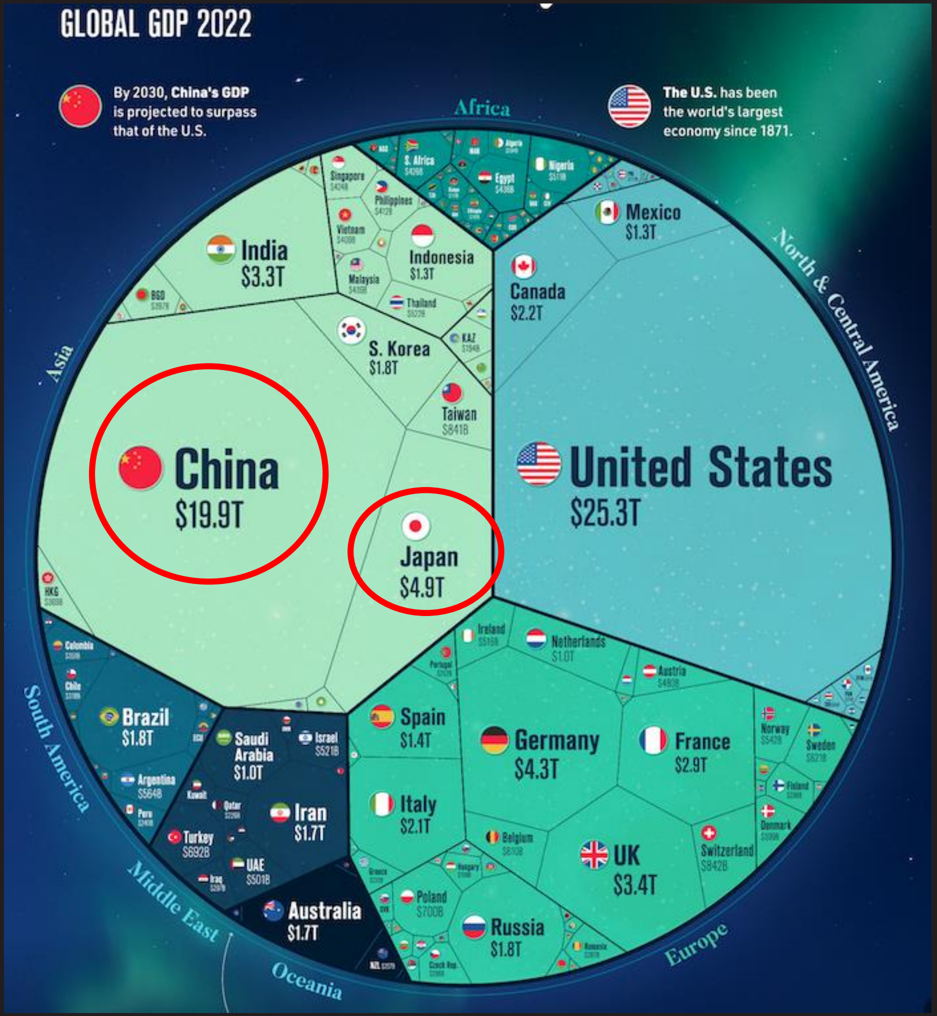
Source: 2020 Gartner CISO Effectiveness Survey

Why is this so hard?

Yesterday vs Today



Third Largest Economy in the World



Source: The $100 Trillion World Economy, Visual Capitalist

- According to Cybersecurity Ventures, total global losses were $6T in 2021.
- If this was a nation it would be the third-largest economy by GDP, between China and Japan.
- That's 6.25% of the world's global economy.
- Gartner estimates worldwide end-user spending on the information security and risk management market to reach $261.9B in spending by 2026, from $158B in 2022.

Source: Forecast Analysis: Information Security and Risk Management, Worldwide (G00775555)

"Culture Eats Strategy for Breakfast"

— ***Peter Drucker***

It is, ultimately, about culture!

Few Final Thoughts

Cybersecurity:

- It’s important to senior leadership, so it’s important to everyone in the organization
- It’s a choice, not a technical one, rather a business one
- Everybody must contribute to make the organization more secure!

Recommendations:

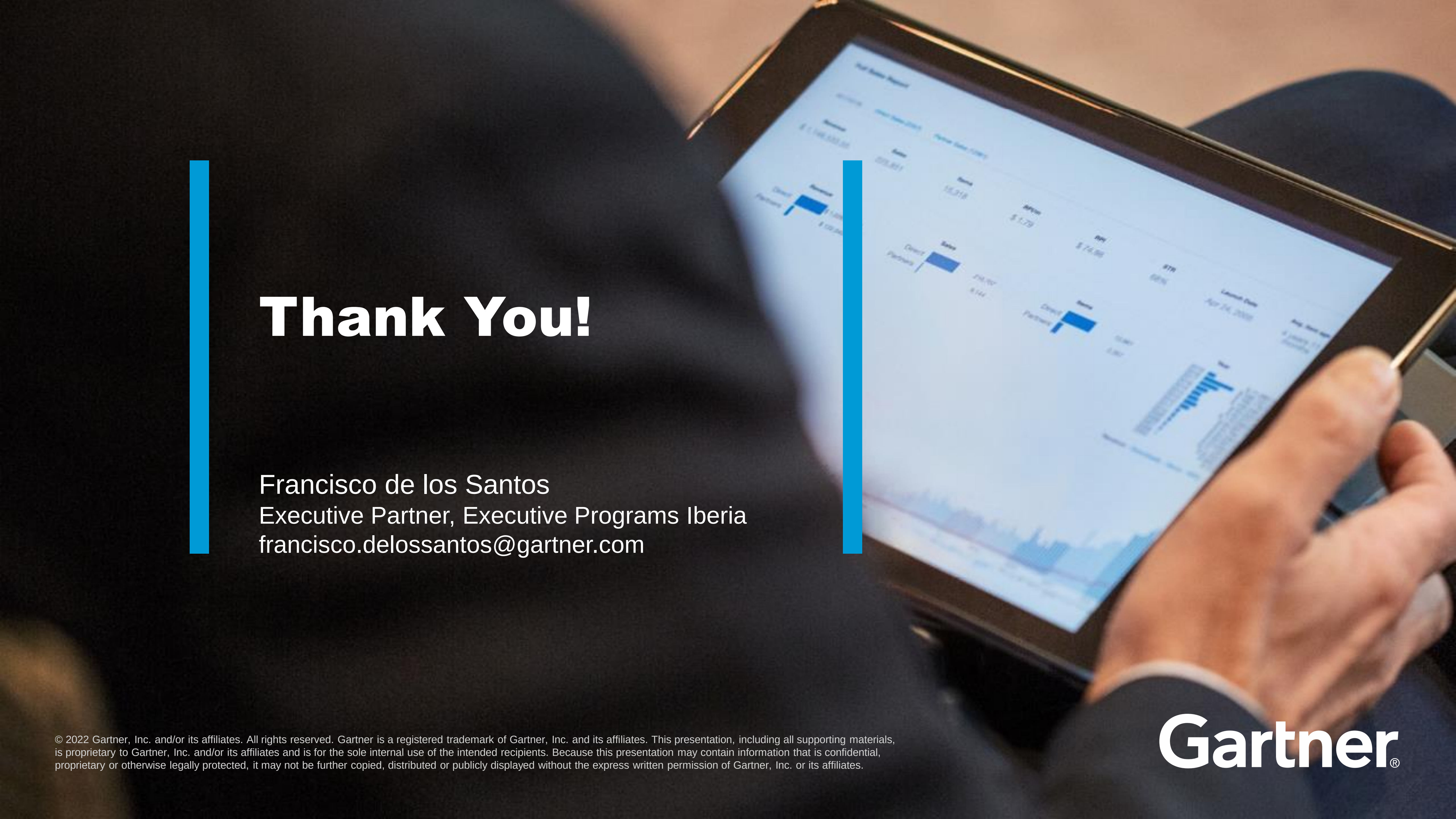
- Implement a security behavior program
- CISO as a business leader and executive influencer
- Establish and mature supply chain risk management capabilities
- Initiate and mature a cybersecurity mesh strategy

RESTRICTED DISTRIBUTION

Treat cybersecurity as a business issue

Recommended Gartner Research

- How to Start Building a Cybersecurity Mesh Architecture
- CISO Effectiveness: A Report on the Behaviors and Mindsets That Impact CISO Effectiveness
- CISO Foundations: Build a Culture of Security Consciousness: Introducing the Gartner PIPE Framework
- Emerging Best Practices to Manage Digital Supply Chain Risks
- Cyber Judgment Presents a New Approach to Informed Risk Decision Making
- Case Study: User-Experience-Focused Cybersecurity Design (Santander)
- Outcome-Driven Metrics for Cybersecurity in the Digital Era



Thank You!

Francisco de los Santos
Executive Partner, Executive Programs Iberia
francisco.delossantos@gartner.com

Gartner®