Generative AI, Predictive AI & the CISO

Frank Dickson
Group Vice President, Security & Trust

Why are we here?

1. Gen AI
2. Automation
3. Cybersecurity

Virtual/Augmented Reality

Direct to consumer platforms

ESG/Sustainability

Low code/no code technologies

Quantum Computing

Digital Sovereignty

Which of the following technology areas is top of mind for the C-Suite in terms of new investments for the next 12 months?

IDC

Defining Artificial Intelligence

Artificial intelligence comprises a grouping of machine-based technologies that perceive and synthesize data to infer information and insight to create systems that learn, reason, adapt, and self-correct.

Artificial Intelligence builds on itself

4 GENERATIVE AI

Learns from data and uses it to create artifacts that preserve a likeness to original data

3 PREDICTIVE AI

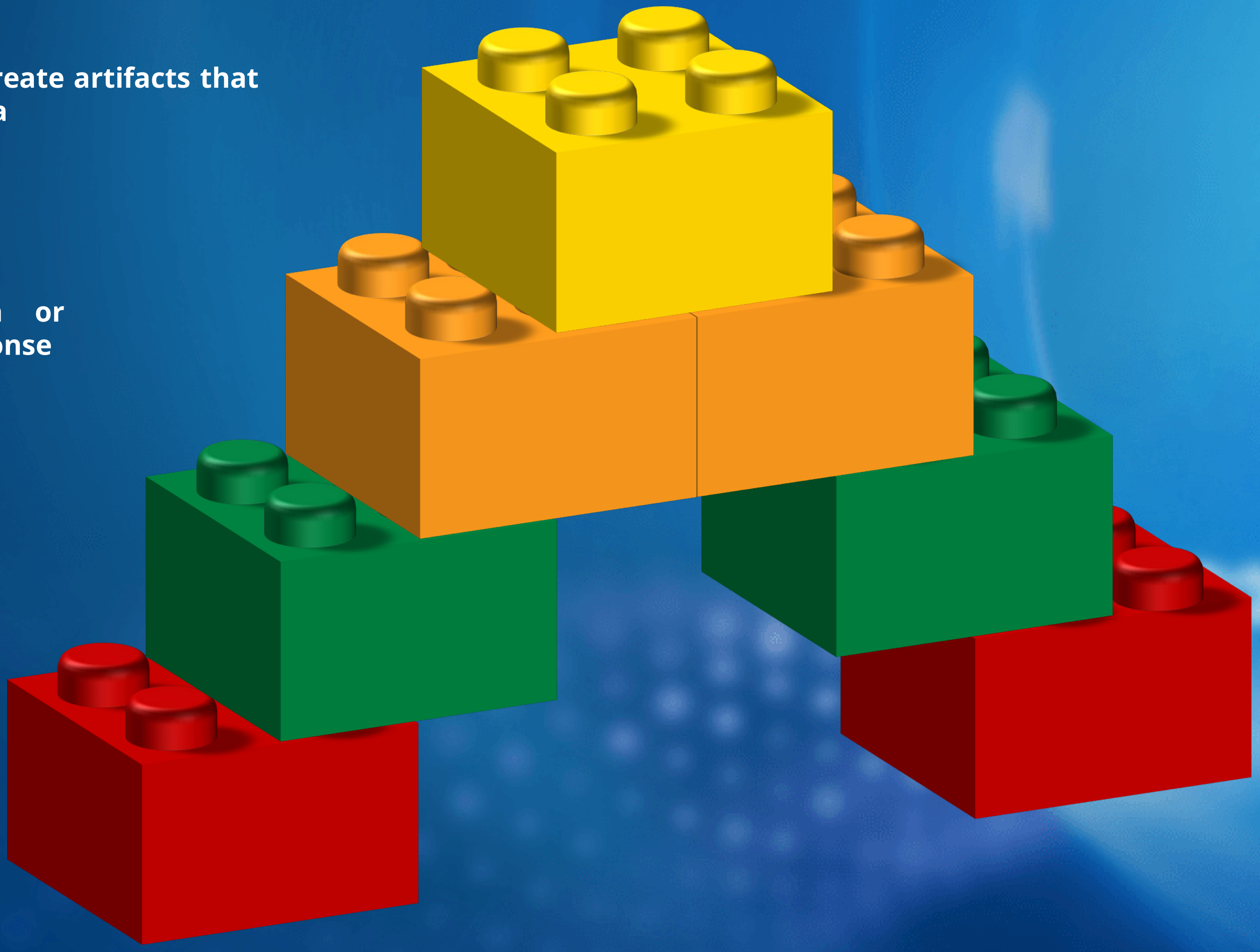
Analyzes existing data for prediction or automation, ie Blocking or Risk-based response

2 DEEP LEARNING

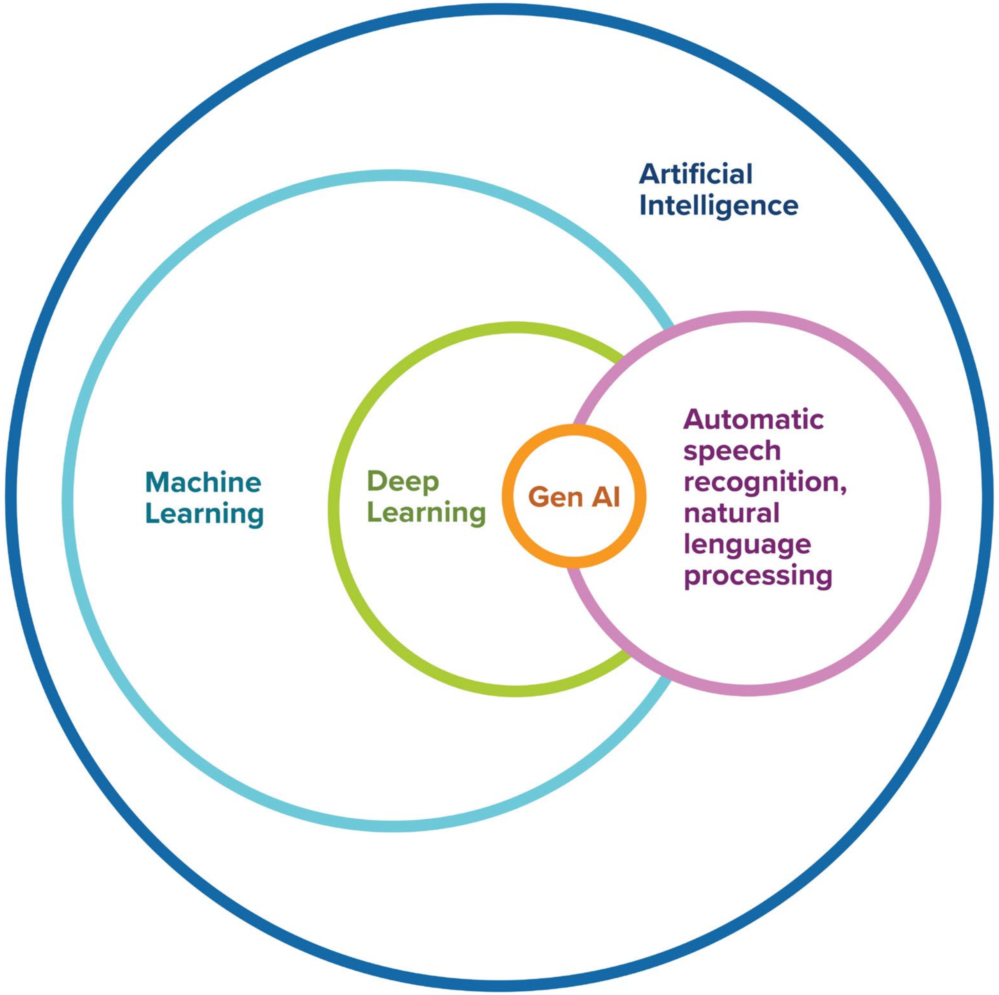
ML techniques that make computational multilayer neural networks feasible such as Convolutional neural networks

1 MACHINE LEARNING

Subset of AI techniques that enable computer systems to learn without programing by a human



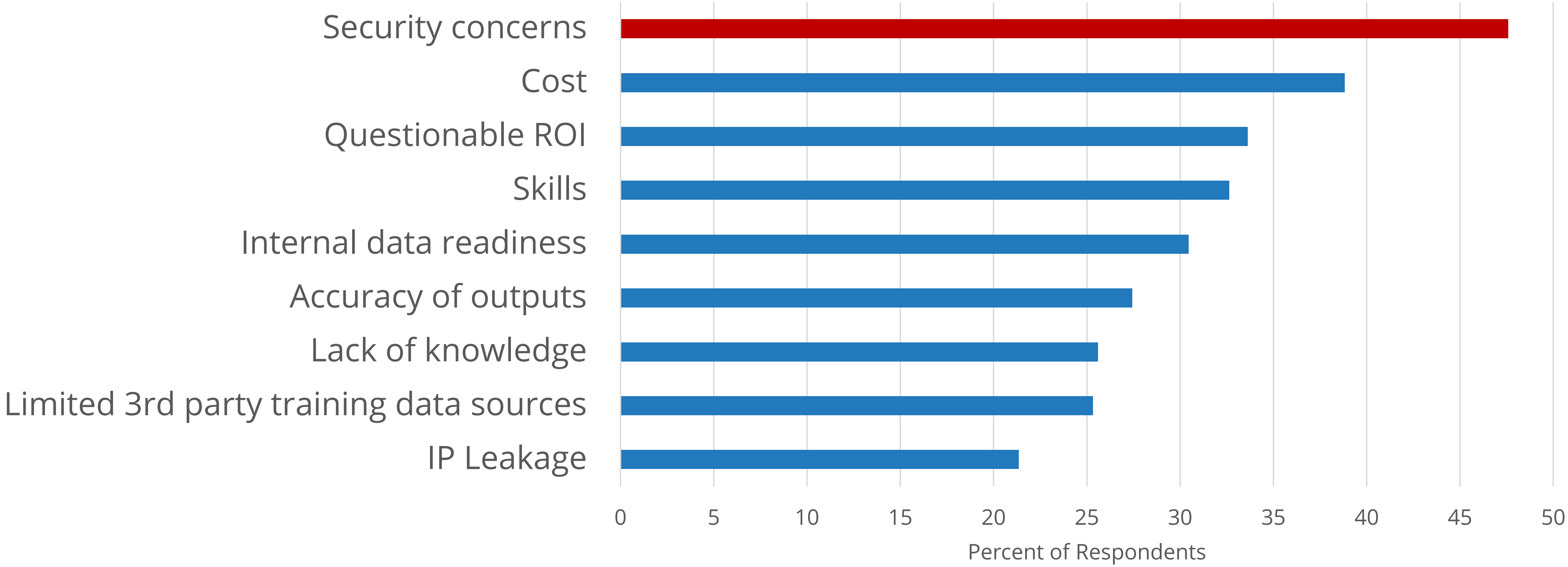
The flavors of AI have different applications and use cases.



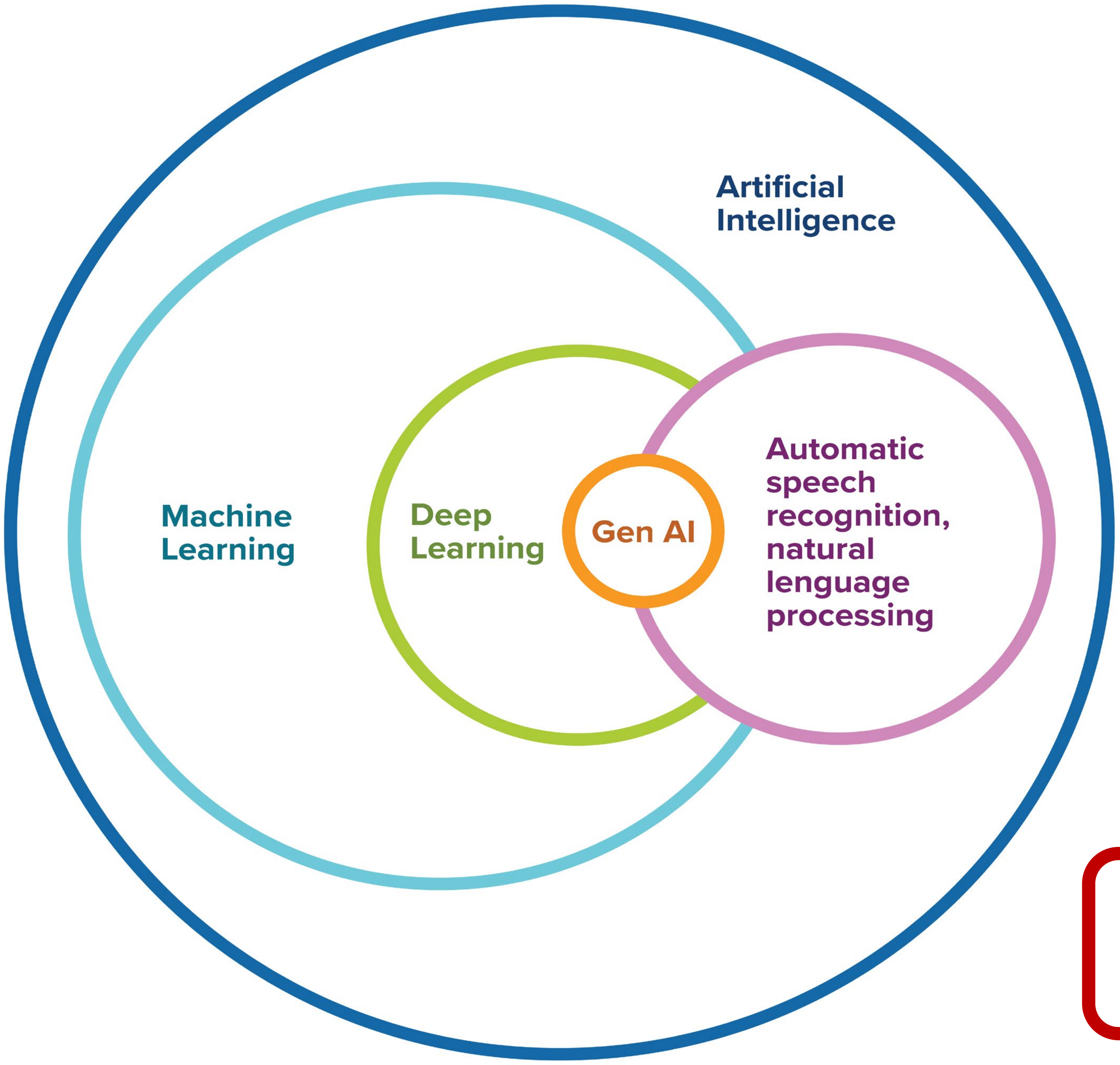
Concerns over AI

Should you be worried about Gen AI security?

What are the most important challenges your organization is facing (or anticipate will be facing) with implementing GenAI initiatives?



Source: WW C-Suite Tech Survey, IDC, August, 2023, n = 895


Artificial Intelligence
Machine Learning
Deep Learning
Gen AI
Automatic speech recognition, natural lenguage processing

Security AI Market Glance 1Q24

GenAI assistants

- BlackBerry
- Checkmarx
- cisco
- CROWDSTRIKE
- cybersixgill
- CYCLOPS
- druva
- elastic
- FLASHPOINT
- Google
- GURUCUL
- IBM
- Judy Security
- LIBERTY91
- FORTINET
- wipro
- LINEAJE
- Microsoft
- MixMode
- mobb
- NSFOCUS
- opentext
- paloalto NETWORKS
- Qualys
- RadiantSecurity
- Recorded Future
- REDCARBON
- rubrik
- SentinelOne
- splunk>
- STRIKEREADY
- BROADCOM
- sysdig
- tenable
- TREND
- VERACODE
- VERSA NETWORKS
- ZEROFOX
- ZEROFOX

Protecting Enterprise Data from AI Misuse

Content Control for AI Systems

- zscaler
- touch.io
- STRIKEREADY
- BigID
- CLOUDFLARE
- cyberhaven
- FORTRA
- FLASHPOINT
- GTB Technologies Data Security that Works
- GURUCUL
- Kobalt Labs
- LINEAJE
- Kobalt Labs
- next
- opentext
- Plurilock
- proofpoint.
- Skyhigh Security
- tenable
- ZEROFOX

Access Control for public GenAI Systems

- STRIKEREADY
- CALYPSOAI
- BigID
- CALYPSOAI
- code42
- credo ai
- Deasie
- onetrust
- cyberhaven
- FORTRA
- ExtraHop
- iboss
- opentext
- netskope
- THALES
- Plurilock
- portal26
- proofpoint.
- SAVVYCOM
- tenable
- ZEROFOX

Protecting AI Investments

Building Secure Models

- TIBCO
- AIShield Powered by Bosch
- Arthur
- CRANIUM
- digicert
- Kindo
- GURUCUL
- LAKERA
- preamble

Protecting AI Models

- TONIC
- HIDDENLAYER
- ADVERSA
- GURUCUL
- DeepKeep
- next
- MINDGARD
- PROTECT AI
- ROBUST INTELLIGENCE

Protecting AI model interfaces

- TROJAI
- f5
- BigID
- FLASHPOINT
- Akamai
- Skyhigh Security

Protecting AI Data Stores

- radware
- CYCLOPS
- COMMVAULT
- REDCARBON
- NetApp

Using GenAI in cybersecurity service delivery

- veeAM
- accenture
- BCG
- EY
- GURUCUL
- HCLTech
- pwc
- wipro

Talking to the Experts on Securing AI

"Sometimes you fight fire with fire;

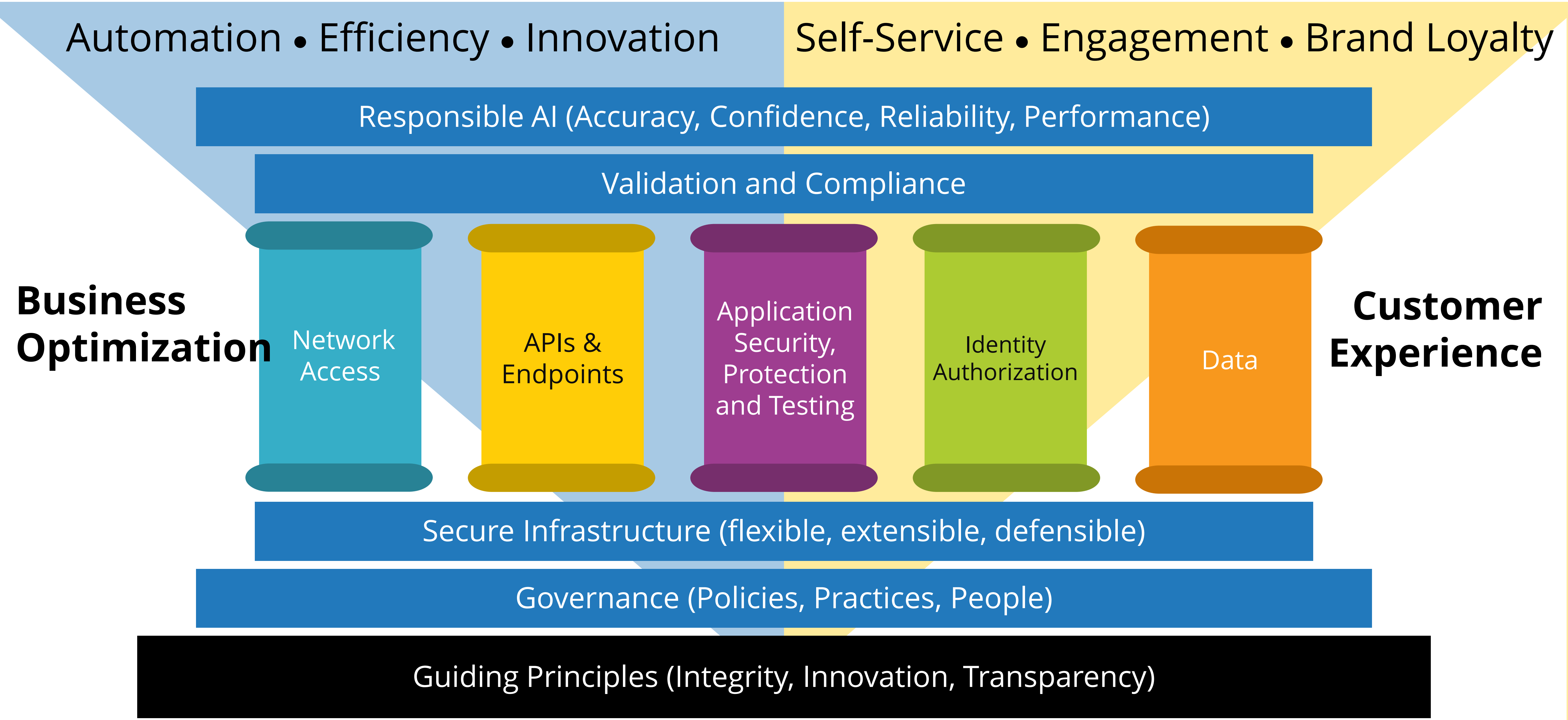
sometimes you fight fire with water."

Shannon Murphy,

Global Security & Risk Strategist

Trend Micro

Identifying the issues associated with building out AI Trust



Automation • Efficiency • Innovation

Self-Service • Engagement • Brand Loyalty

Responsible AI (Accuracy, Confidence, Reliability, Performance)

Validation and Compliance

Business Optimization

Network Access

APIs & Endpoints

Application Security, Protection and Testing

Identity Authorization

Data

Customer Experience

Secure Infrastructure (flexible, extensible, defensible)

Governance (Policies, Practices, People)

Guiding Principles (Integrity, Innovation, Transparency)

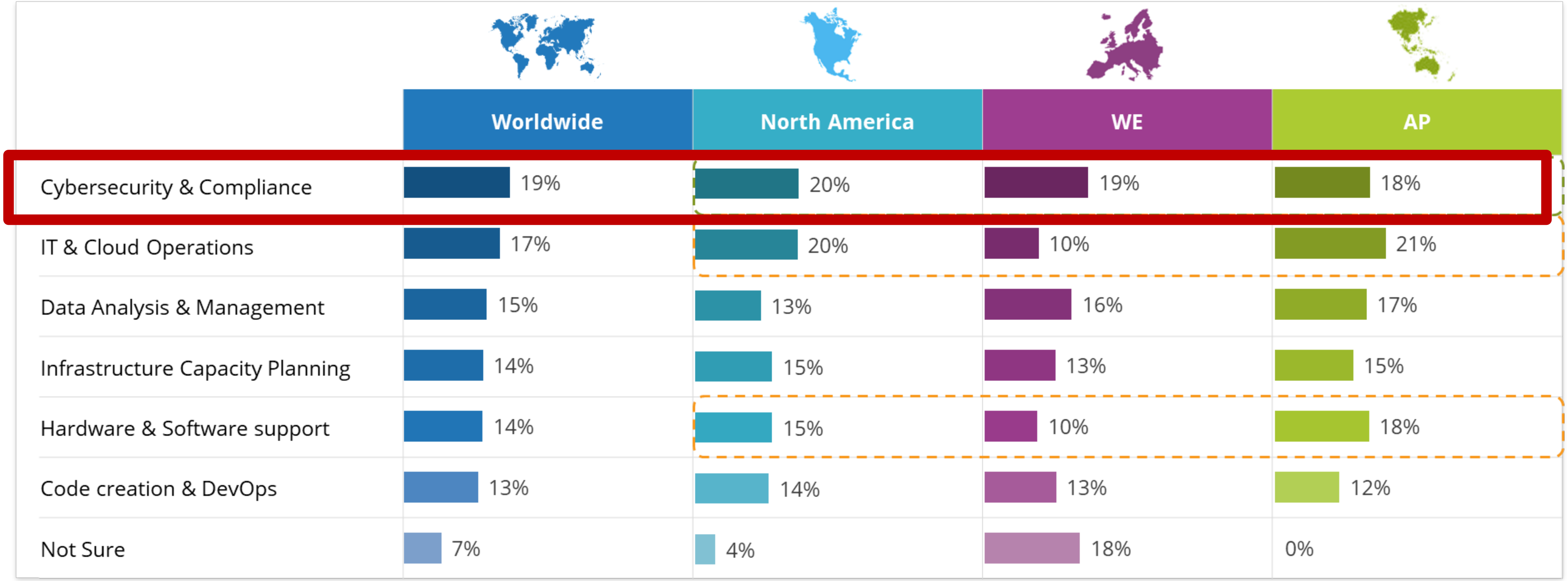
Getting Value from AI for Security

IDC Survey Spotlight

Artificial Intelligence (AI) will become the next evolution of business and IT and there is little to question about this; but how about cybersecurity? What will be the impact?

Philip Harris

Thinking about the organization in which you work, in which IT area do you think generative AI will have the most disruptive impact in the next 18 months?



	Worldwide	North America	WE	AP
Cybersecurity & Compliance	19%	20%	19%	18%
IT & Cloud Operations	17%	20%	10%	21%
Data Analysis & Management	15%	13%	16%	17%
Infrastructure Capacity Planning	14%	15%	13%	15%
Hardware & Software support	14%	15%	10%	18%
Code creation & DevOps	13%	14%	13%	12%
Not Sure	7%	4%	18%	0%

IDC #US51095722 (July 2023)
Source: Future Enterprise Resiliency & Spending Survey Wave 5, IDC, June 2023, N = 1,014.

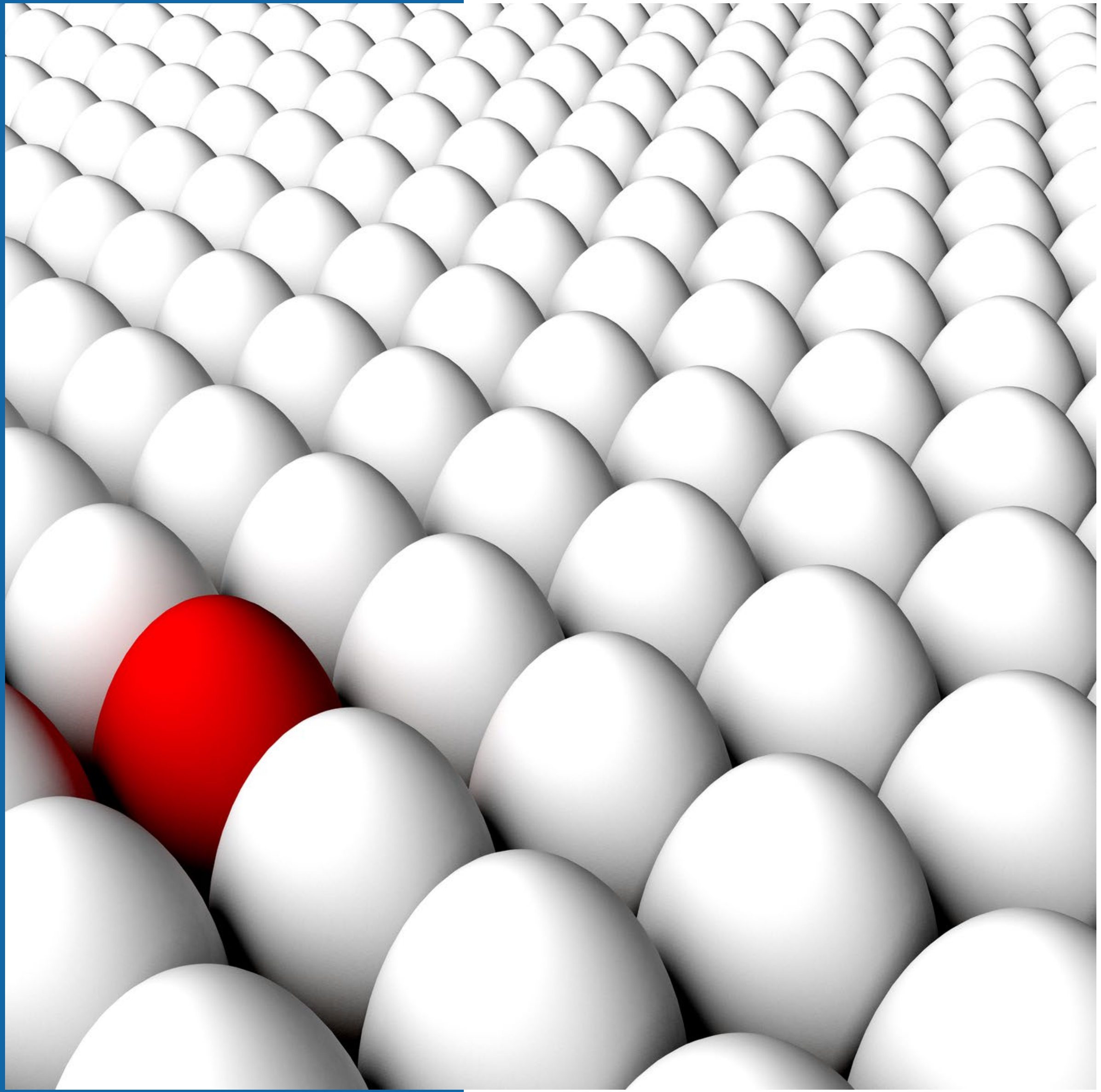
Cybersecurity Challenges in 2024

Digital First & Complexity

Staff Shortage

Threat Landscape

Compliance



Artificial intelligence is not particularly smart.

- Machine learning illuminates patterns.
- AI automation applies patterns.
- AI really leverages existing knowledge but cannot create new constructs; essentially, it does not "think."

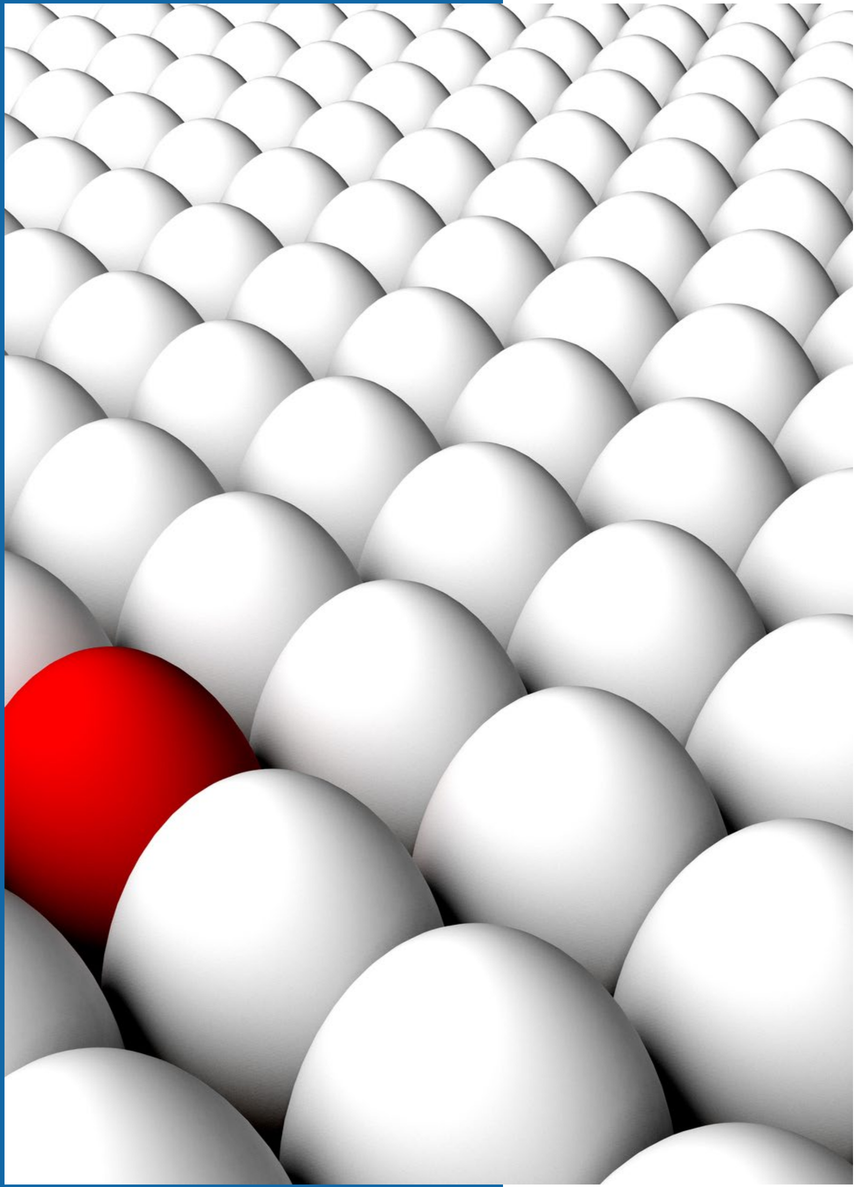
AI Narrowed to the Use Case of Cybersecurity

AI is the application of applied statistics to solve cybersecurity problems.

Artificial intelligence as providing advisory, enhanced service, and semiautonomous cybersecurity defense functionality based on a range of structured and unstructured data, including logs, device telemetry, network packet headers, and other available information.

The goal is to

- create analytics platforms that capture and replicate the tactics, techniques, and procedures of the finest security professionals;
- democratize the traditionally unstructured threat detection and remediation process; or
- complete a range of near-real-time automated detection and response techniques that theoretically can be replicated, but by the time the security professional completed the task, it would be far too late.



It's Not About the AI; It's About the Data

Data is the enabling infrastructure for security AI.

Data Framework Structures

- AI needs structure to be able to look at the data at scale.
- MITRE ATT@CK framework.

Data Management

- Data has weight. Security data has a lot of weight.
- Data weight has become a competitive differentiating tool.

Data Curation

- Curating heterogeneous data sets to create data homogeneity to enable analysis is an inhibitor.
- Restructuring data takes time and costs money.
- The value of standards
  - Structured Threat Information Expression (STIX)
  - Trusted Automated eXchange of Indicator Information (TAXII)
  - Open Cybersecurity Schema Framework (OCSF)

Considerations in Leveraging AI

"With great power comes great responsibility."

Hallucinations and the Role of the Analyst

- Creating value requires context
- AI/ML will not now or likely ever be fully trustworthy

Data Security and Privacy Risks

Input/Content Manipulation/Bias

Efficacy/Seed Set

Spoiling the Milk

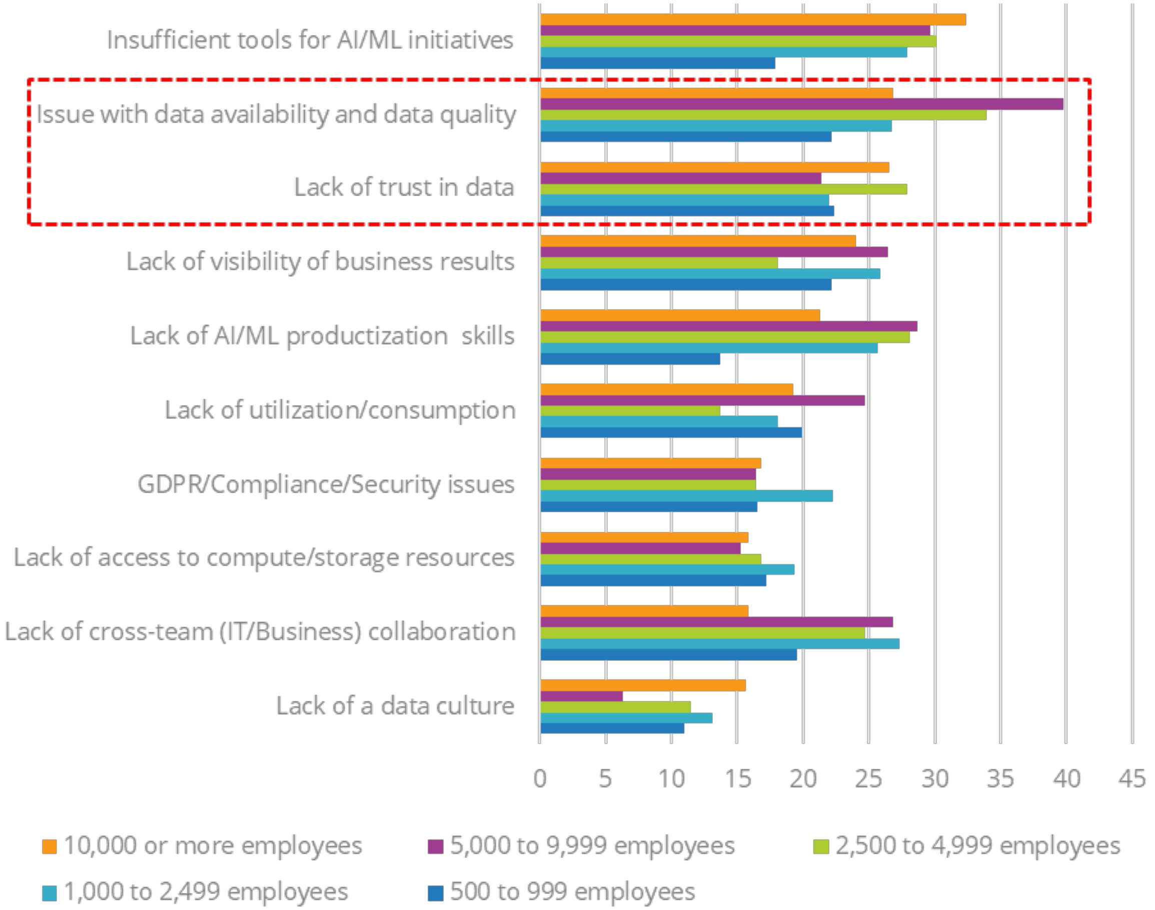
IDC Survey Spotlight

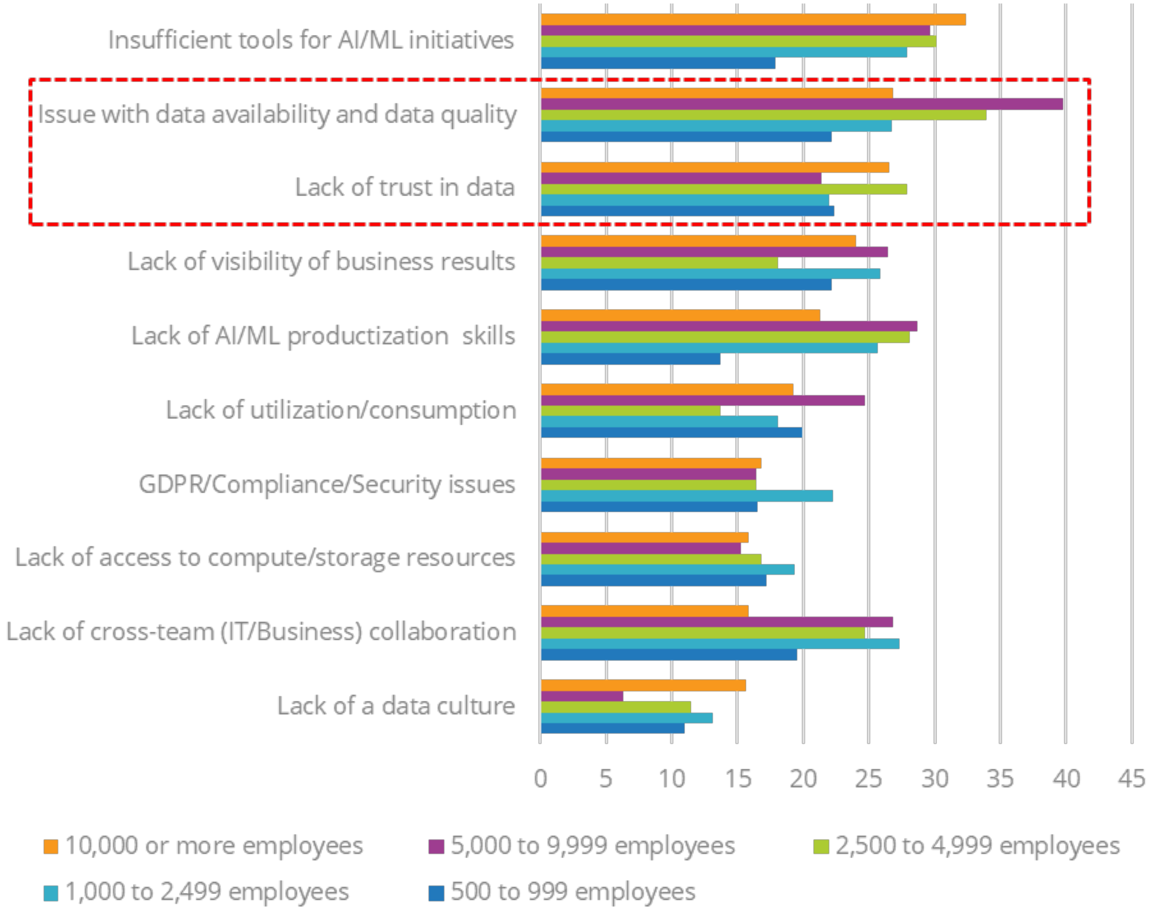
Does the lack of trust in data for AI/ML initiatives differ based on the size of business or role within the organization?

Grace Trinidad

Michelle Abraham

Which of these are significant challenges to maximizing the value of your organization’s AI/ML initiatives?



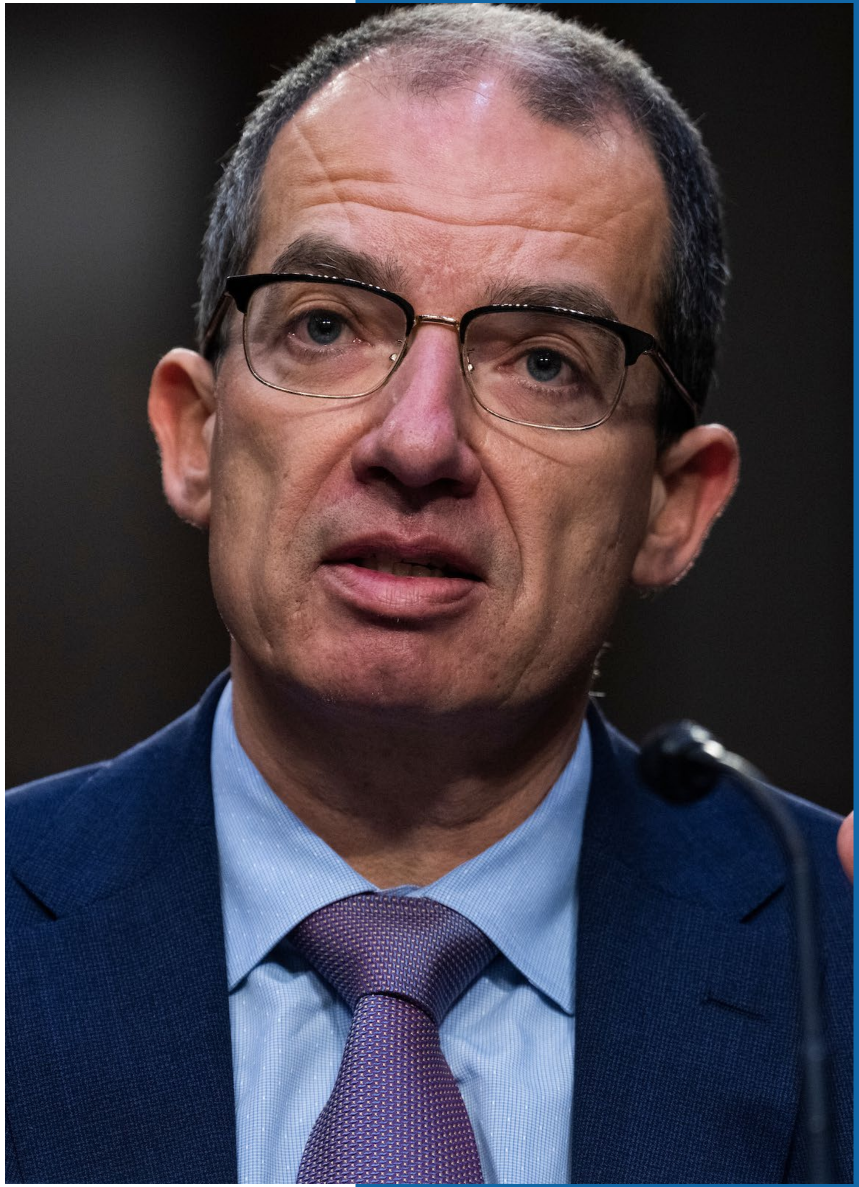


IDC #US50732423 (May 2023)
Source: Future Enterprise Resiliency & Spending Survey Wave 2, IDC, March, 2023, n = 952

Don’t believe me?

Moderna CEO Stéphane Bancel

We developed a ChatGPT for Moderna called M chat (because we don’t want to teach the rest of the planet the things we are learning with our data). We’re using it for pattern writing, contract writing. We are loading up all of our sensitive data.



https://www.semafor.com/article/09/13/2023/moderna-ceo-on-ais-potential-to-cure-cancer?utm_source=tldrnewsletter

Trust in how the vendor will use my data is the top consideration for the C-Suite when evaluating potential gen AI tech partners.

Most important - Please rank these factors in importance when you are evaluating potential generative AI technology partners. (Rank 1)

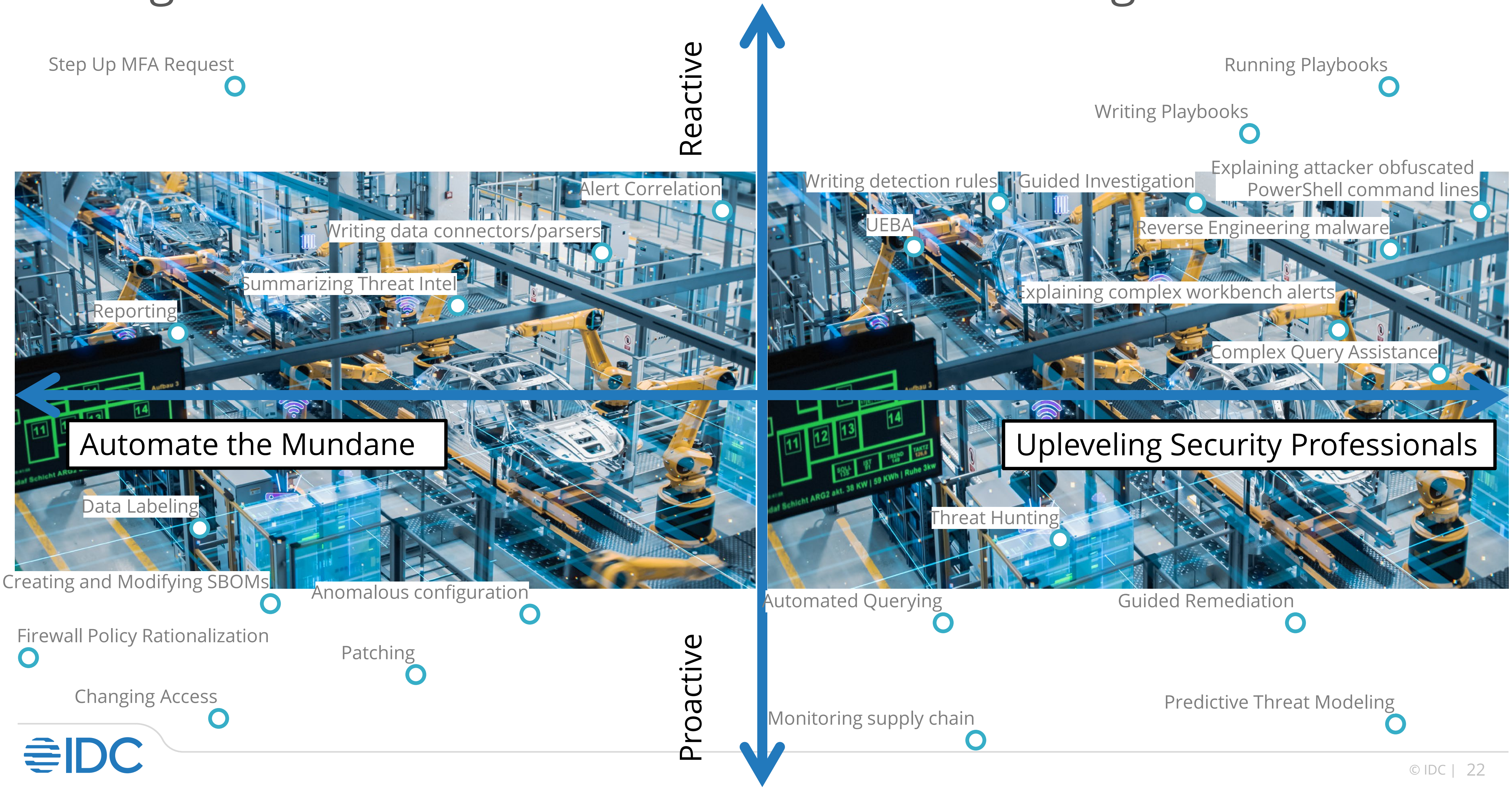
#1 **Trust in how the vendor will use my data**

#2 Accuracy of generated content

#3 Deliver measurable business outcomes

n = 895
Source: IDC Worldwide C-Suite Tech Survey, August 2023

Getting Value from “not that smart” Artificial Intelligence



Reactive

Proactive

Automate the Mundane

Upleveling Security Professionals

Step Up MFA Request

Alert Correlation

Writing data connectors/parsers

Summarizing Threat Intel

Reporting

Data Labeling

Creating and Modifying SBOMs

Anomalous configuration

Firewall Policy Rationalization

Patching

Changing Access

Running Playbooks

Writing Playbooks

Writing detection rules

Guided Investigation

Explaining attacker obfuscated PowerShell command lines

UEBA

Reverse Engineering malware

Explaining complex workbench alerts

Complex Query Assistance

Threat Hunting

Automated Querying

Guided Remediation

Monitoring supply chain

Predictive Threat Modeling

IDC

10 Concerns that You Better Understand

10 Concerns that You Better Understand

Benefit

Must explain EXACTLY what you do
- Reduces mean-time-to-detect?
- Satisfies NIST 800-53 requirements?

Offering

Understand technology arc for 2-3 years
Company, service, platform, point-product, feature

Scability

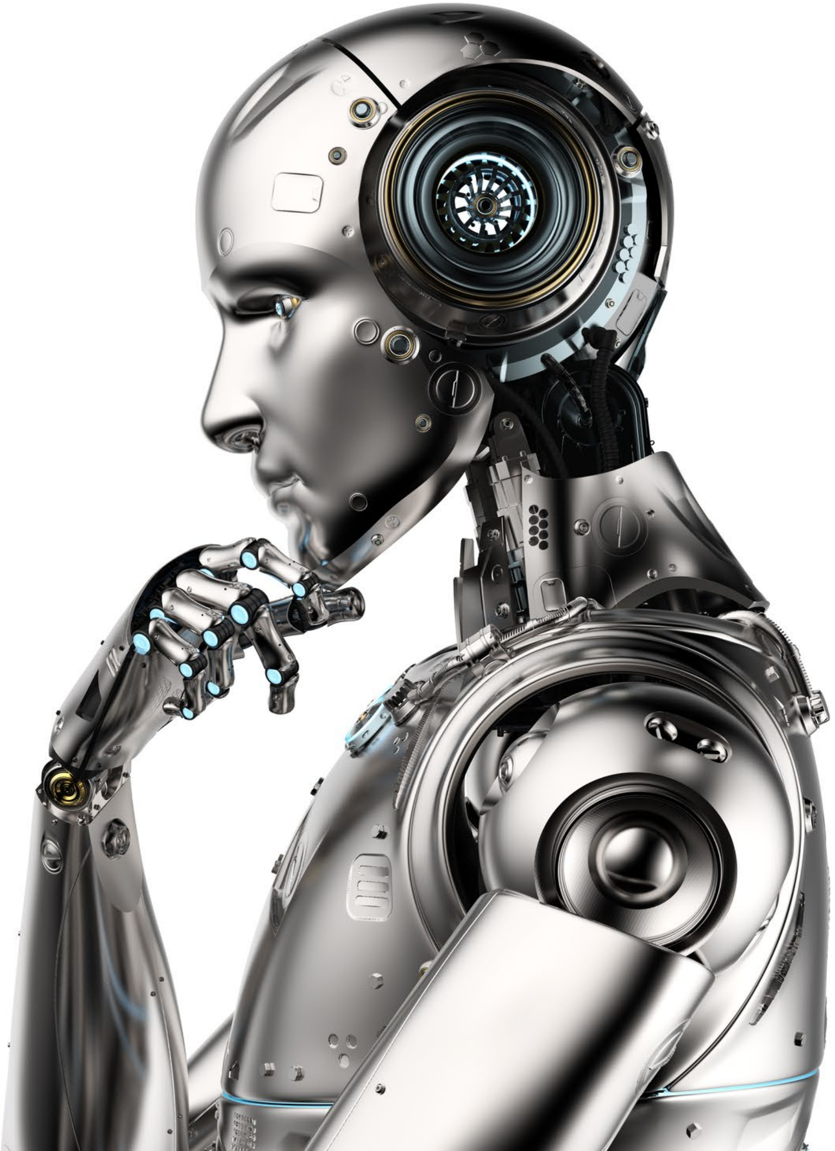
What happens at capacity?

Usability

Low code, no code usability

Support

What ancillary support will be included? Install? API? Maintenance?



Future Proof

Proprietary or open stack?
Both!

Where is my data?

Complexity

Solve problems that I create for myself
Buyers want fewer security vendors

Time to Value

Demonstrate ROI, defined by metrics!
- Time to detect under 1 hour?
- Payback in 4 months?

Frank Dickson
fdickson@idc.com
https://www.linkedin.com/in/frankdickson/
@fdickson777

IDC.com linkedin.com/company/idc twitter.com/idc blogs.idc.com

IDC