

Securing AI Everywhere for the Resilient Digital Business of the Future

Joel Stradling
Senior Research Director, European Security
June 18, 2024

Through the Looking Glass: the Future of Cybersecurity



Four Forces Driving Change in Security

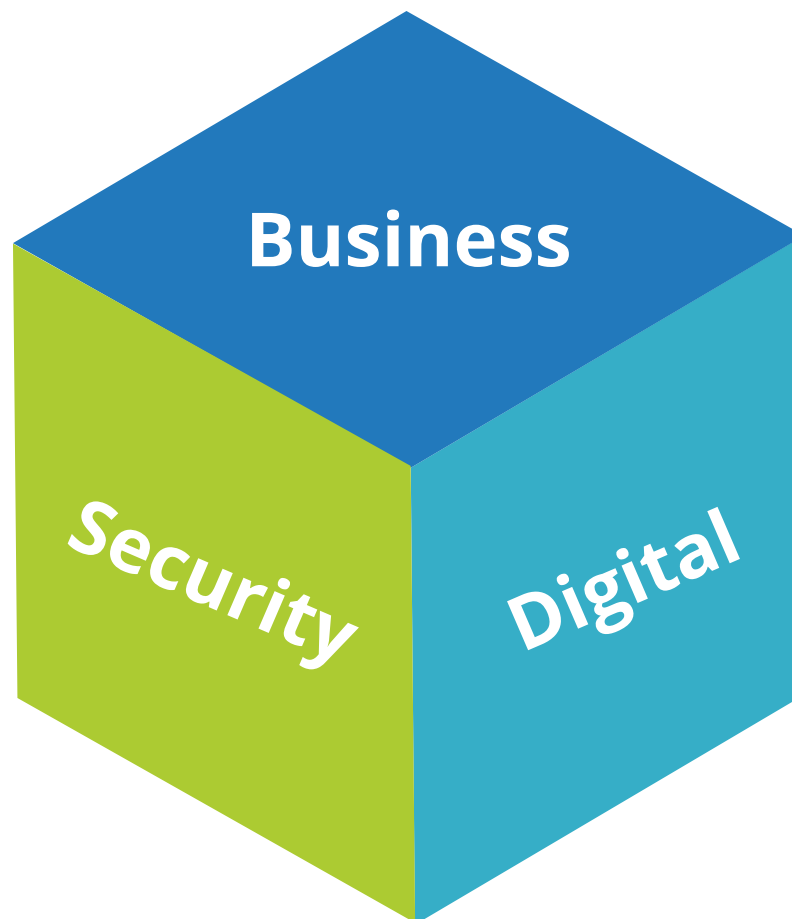
Office of the CISO Change

Digital Transformation

Threat Landscape

Regulations

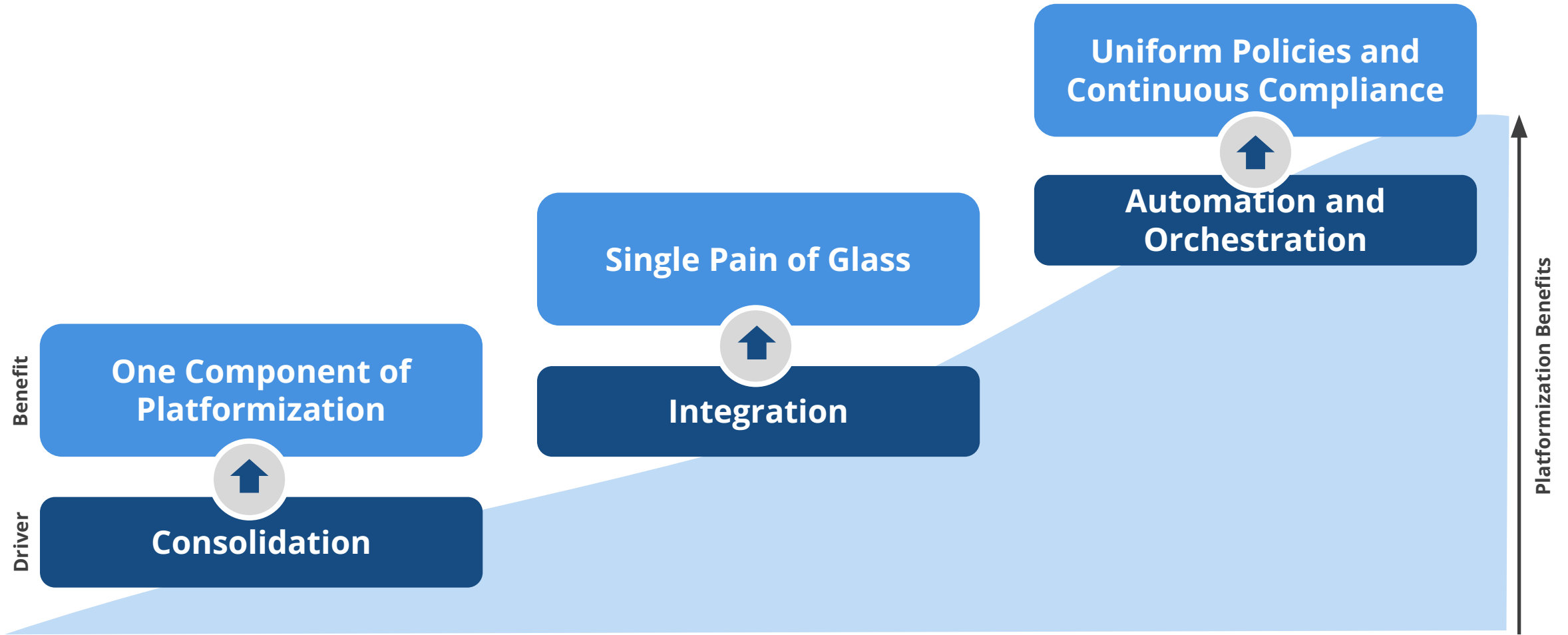
The 3D CISO



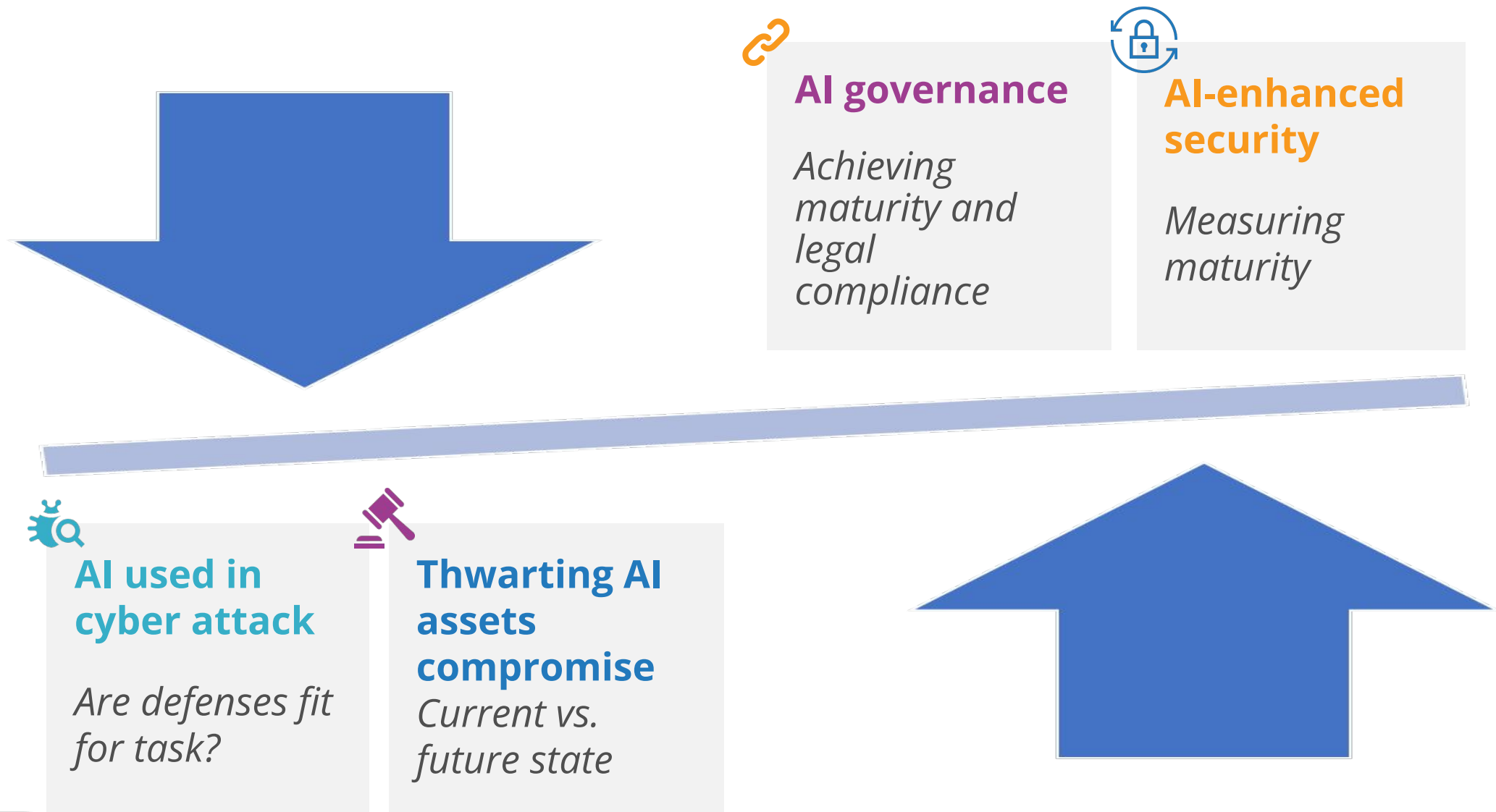
Top Four Key Initiatives for Strengthening Cyber Resilience

- 1 Business continuity management strategy development
- 2 Disaster recovery plans, tested and updated
- 3 Security incident simulations, red teaming
- 4 Continuous asset health checks and vulnerability assessments

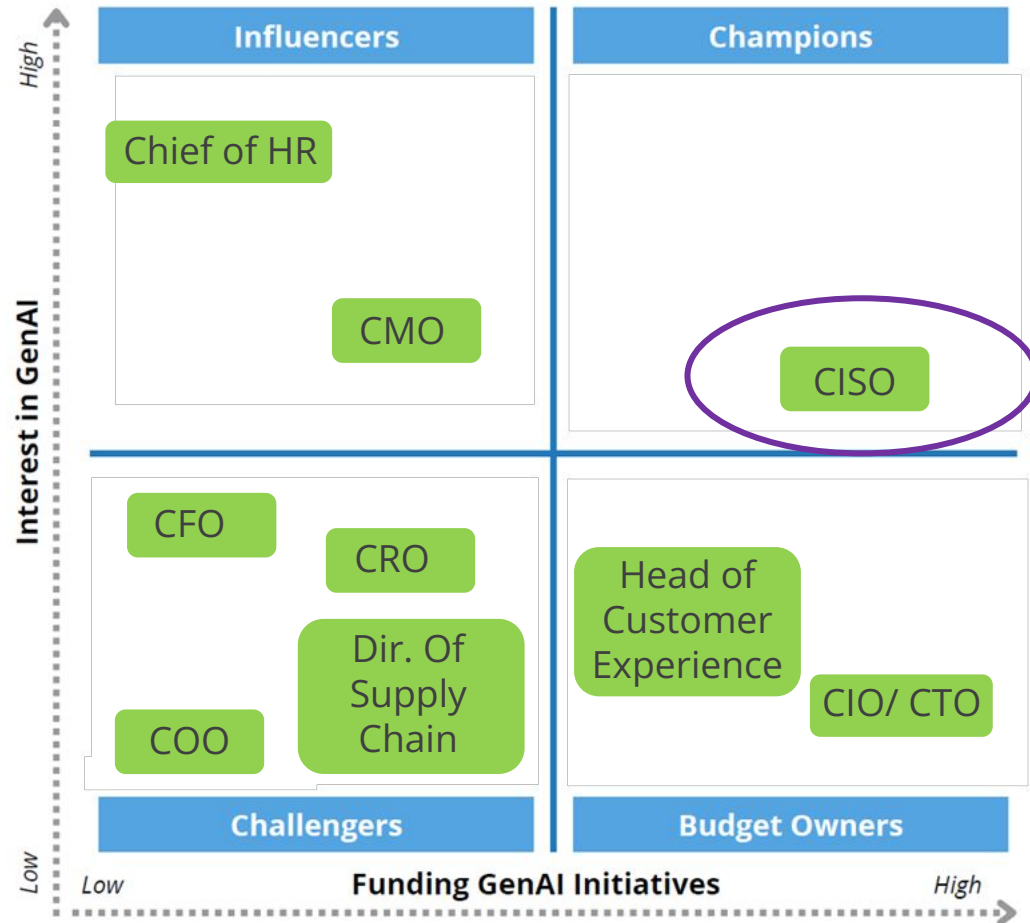
Platformization Drivers and Benefits



Impact of "AI Everywhere" on Cyber



C-Suite Pushing or Resisting GenAI?



CISO's Emerge as GenAI "Champions"

- Interest is high because the assets must be secure and trusted/ethical
- GenAI is viewed as a force multiplier in cyber security
- CISO are key decision-makers for budget.
- Deployments need sanctioned GenAI tools vs. non-sanctioned
- The CISO's role is to be fully up to speed around the how/where/what for data movement and storage

Budget Owners

- IT leaders are central to final sign-off on contracts supporting corporate use of GenAI.
- IT leaders are accountable when it comes to final implementations and on-going accuracy and integrity of data

Ref: IDC eBook: GenAI in EMEA 2024

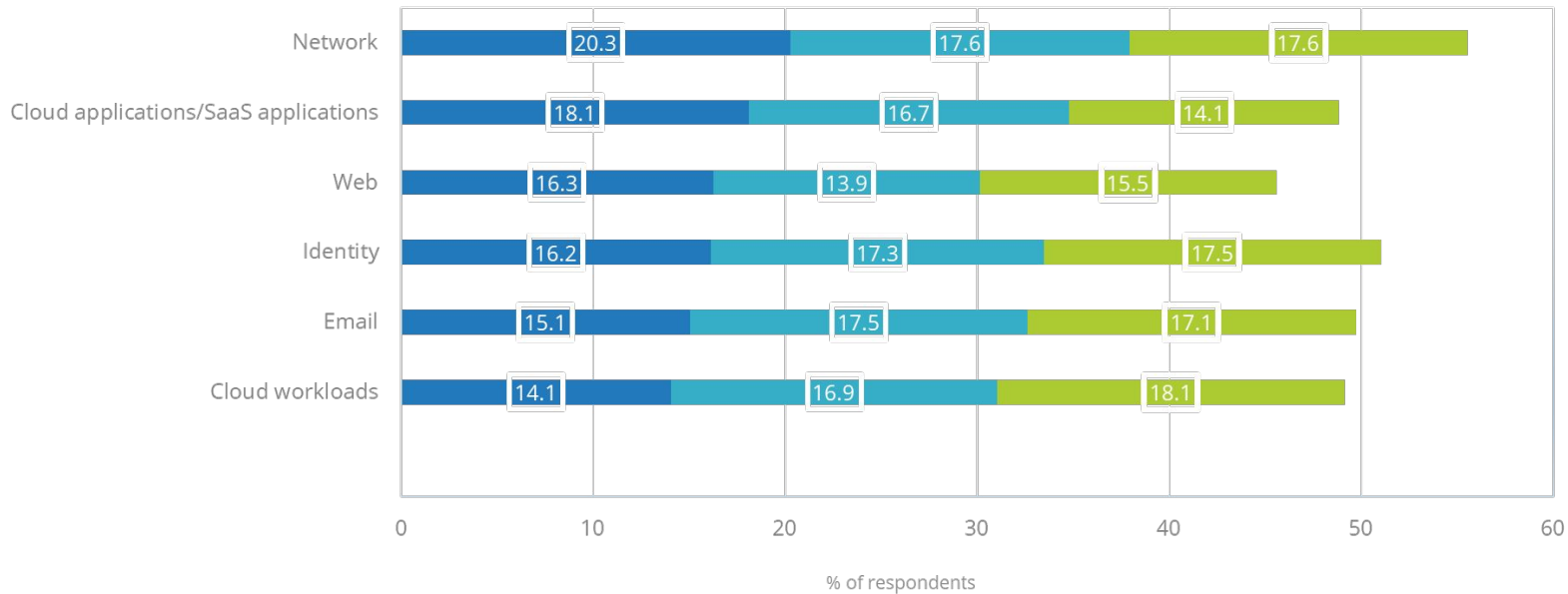
XDR – IDC Survey Shows Most Important Data Telemetry

In response to the question:

How would you rank the importance of the following telemetry sources, with 1 being the most important?

Ranking:

1. Network
2. Cloud and SaaS applications
3. Web
4. Identity
5. Email
6. Cloud Workloads



XDR begins with Endpoint data as the starting point and first building block. According to the survey the key data telemetry following endpoint are from network, cloud and SaaS apps, and Web

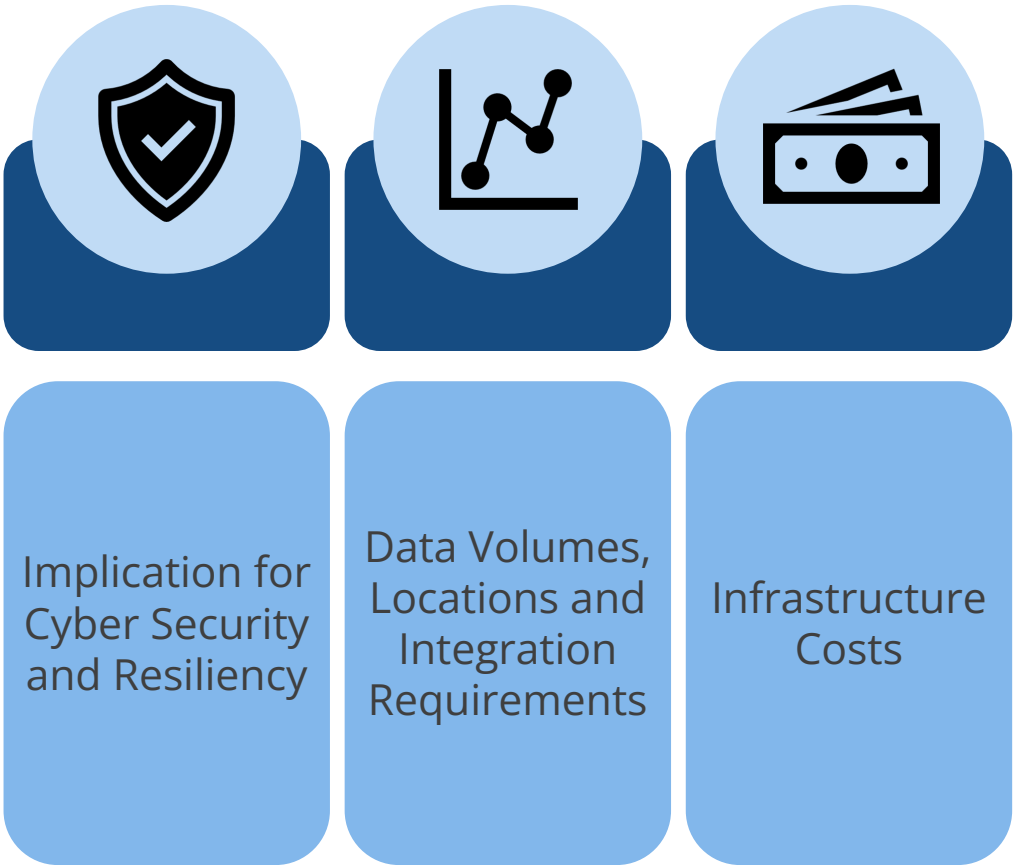
IDC Analysts: Monika Soltysik & Christopher Kissel

IDC #US51324023 (October 2023)

Source: Endpoint Security Survey, IDC, December, 2022, n = 1,015

The Push and Pull of Digital Business and AI Everywhere

Most Important GenAI Workload and Data Deployment Criteria



Source: Future Enterprise Resiliency & Spending Survey Wave 1, IDC, January, 2024, N=881, NA: 361, WE: 220, AP: 300

Is your business currently in the process of transforming and/or modernizing an existing cloud environment?

Ref: N = 1,350 Source: QC10, 4Q23 Cloud Pulse Survey, December 2023, IDC



Cloud transformation is taking place at scale and at accelerated pace

Customer Readiness vs Incident Response

Customer Cyber Readiness



Appropriate cyber crisis response requires central management and org-wide awareness



Continuous measurable training is key to cyber readiness muscle memory



Geopolitics affect day-to-day security perspectives demanding fluid cyber-risk assessment

Incident Response



Breach/incident response is just one component of building a resilient and secure organization



IR should involve threat hunting, remediation steps and root cause analysis



Suppliers may offer ongoing consulting services also known as "peacetime" value

Executive Summary

Understanding the Evolution of the Role of the CISO is key to product and service positioning

**Impact of AI Everywhere is here and now; governance is crucial
The CISO is a GenAI use case Champion with decision-making and budget –holding responsibilities**

EDR is the primary building block for XDR, good data telemetry then features network and applications, followed by the Web, Email, and finally cloud workloads



Joel Stradling
jstradling@idc.com



IDC.com



linkedin.com/company/idc



twitter.com/idc



blogs.idc.com