


ARE EARLY MATURITY IN CYBERSECURITY OR A BRAND-NEW CYCLE? AN EXPLORATORY PERSPECTIVE

The Future of Digital is Highly Secure, But How Will We Get There?



DION HINCHCLIFFE (@DHINCHCLIFFE) 

VP & PRINCIPAL ANALYST

CONSTELLATION RESEARCH

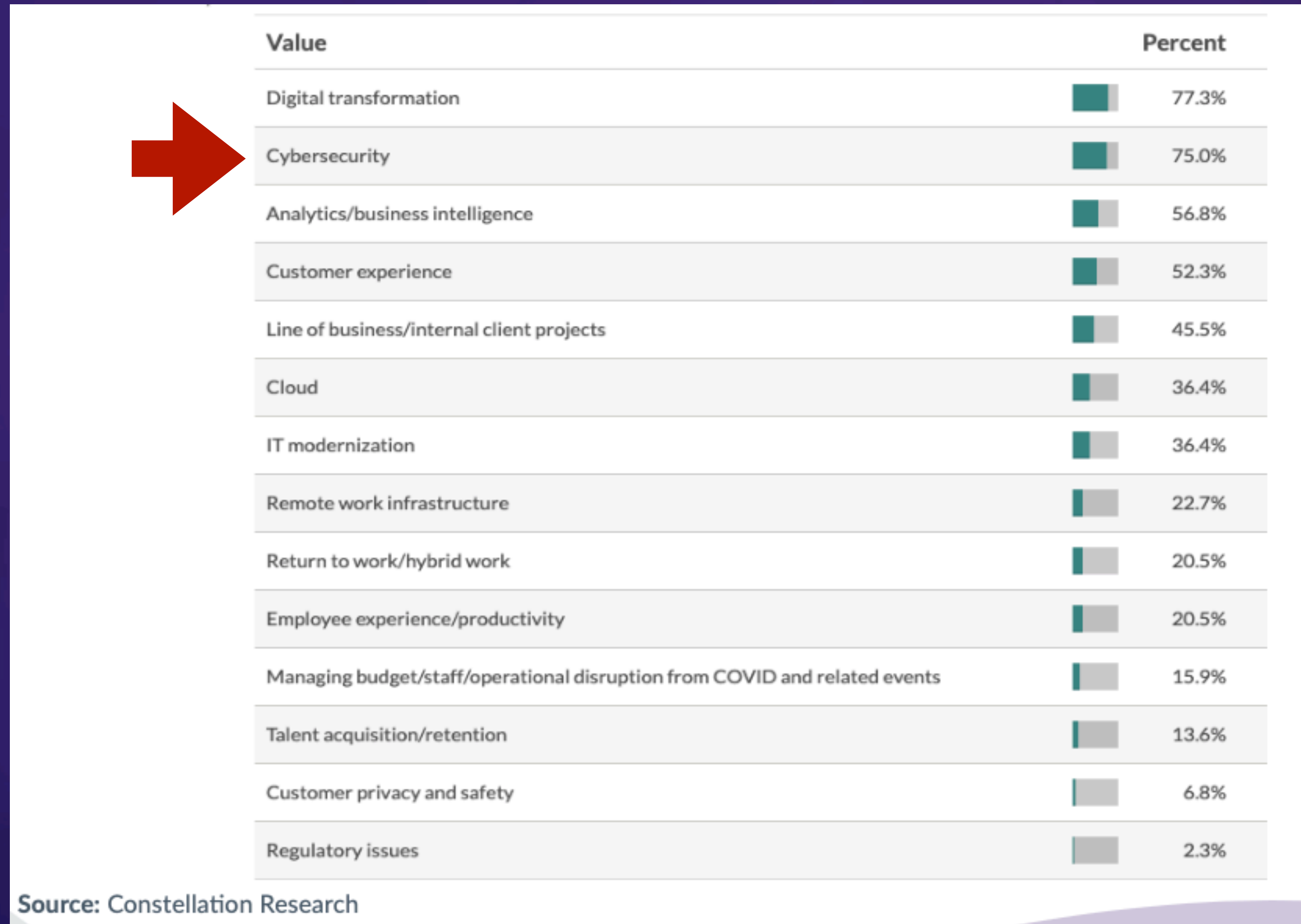
ZDNet

Executive Fellow, Tuck School of Business

dion@constellationr.com

Leading CIO Budget Priorities In the Last 18 Months

Top 100 CIOs in the World (My Pick)





State of Cybersecurity: The Key Trends

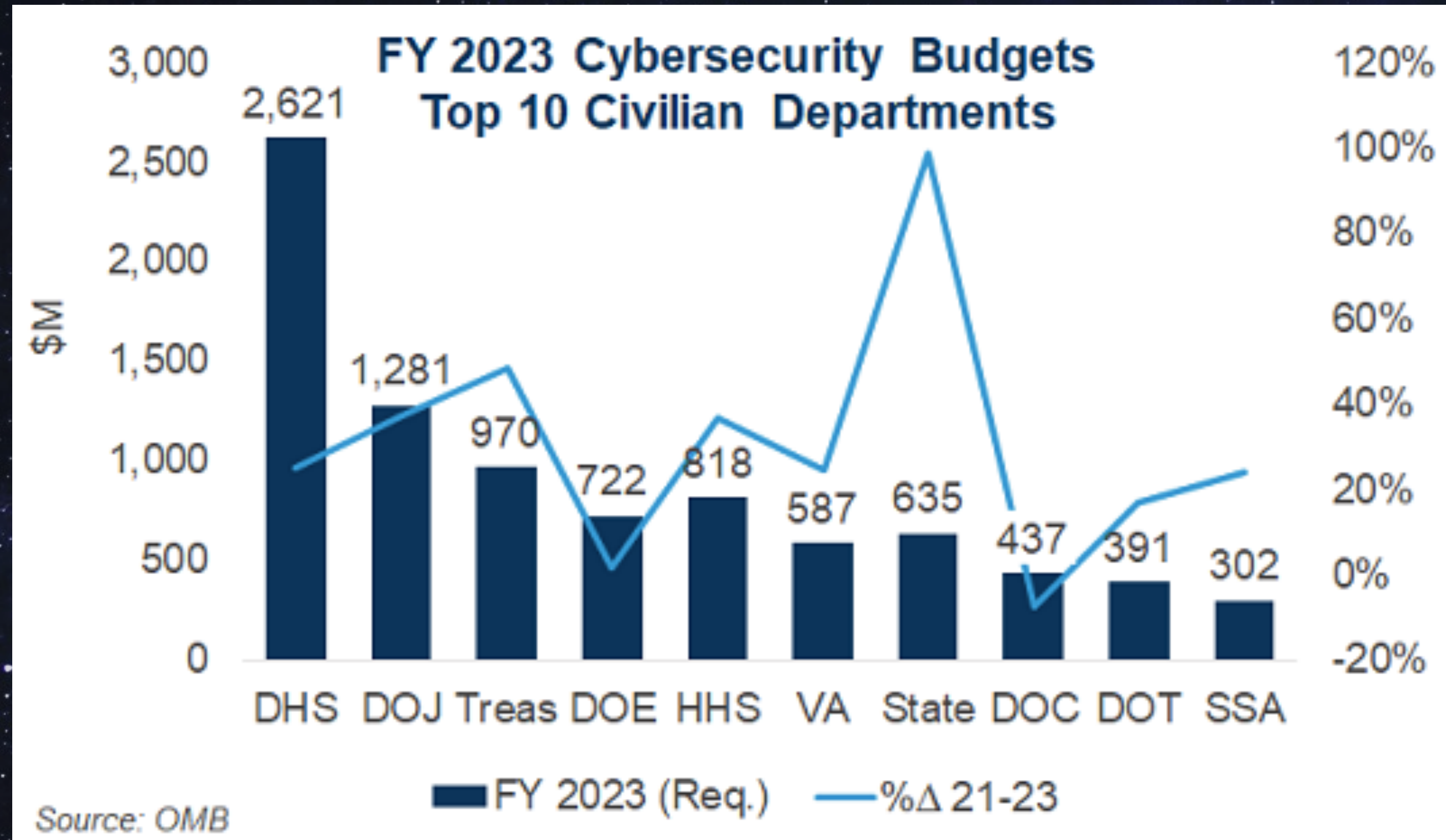
Today's Top Cyber Trends Are About Scale

Either in Growth, Fragmentation, or Reductionism



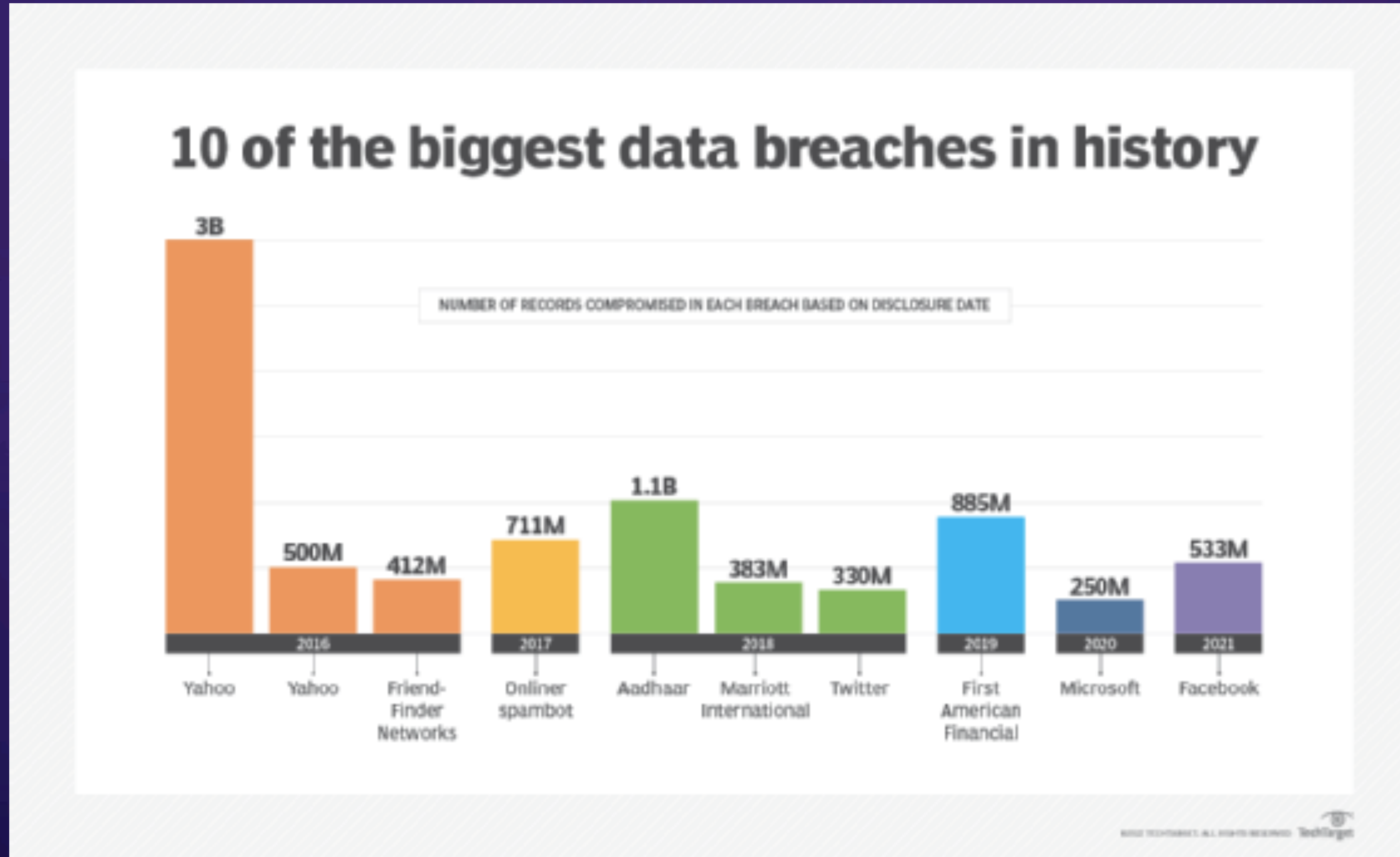
Cyberdefense Budgets Are Unsustainable

Existing Processes Cannot Continue Much Longer



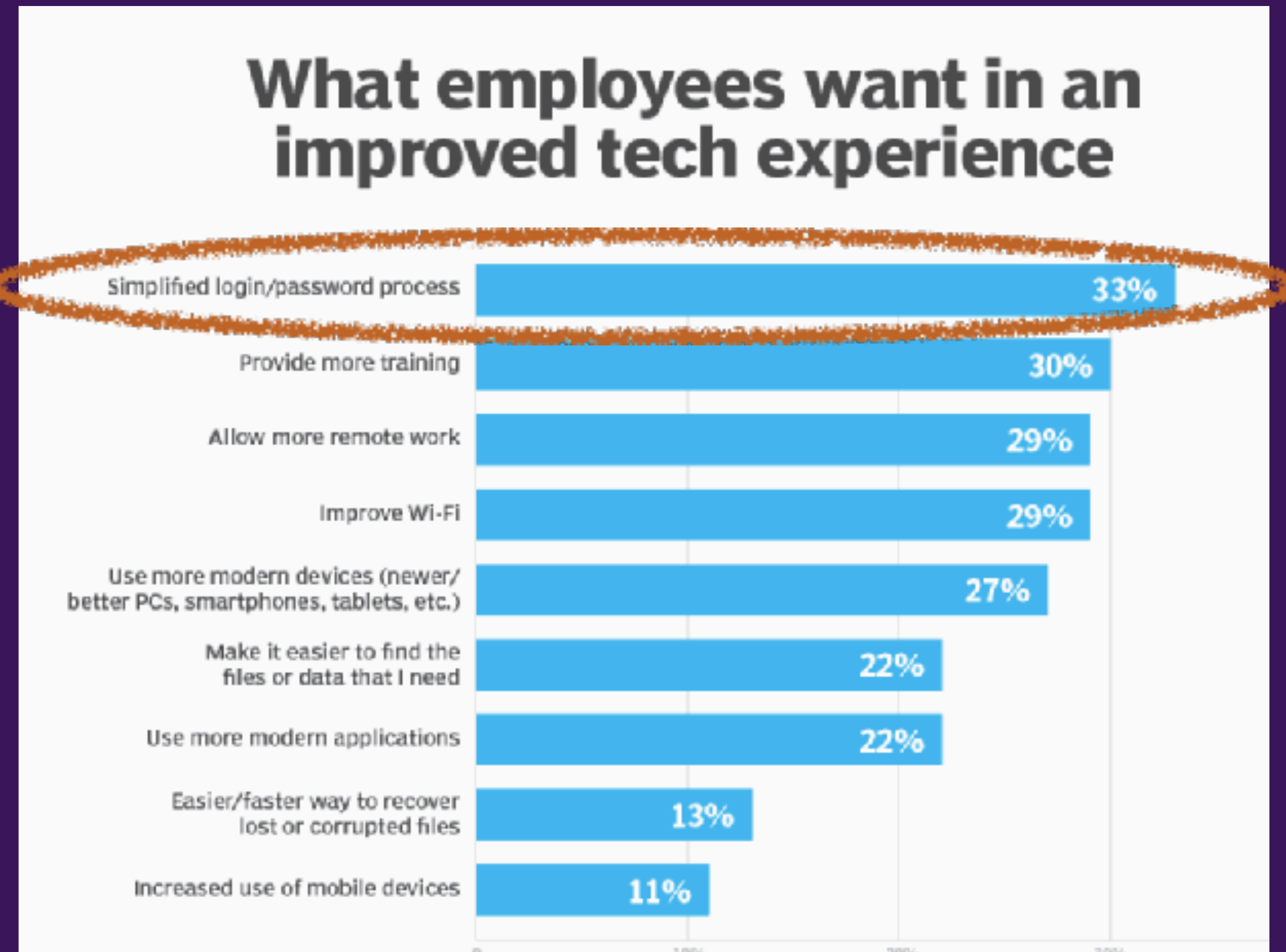
The Stakes Keep Growing

As Do the Exploits



The Security Experience Today Is Lacking

- Now the top hindrance of the digital workplace today
- Security Must Be Effective without Killing Usability of IT
- Invest in security experience design and validation



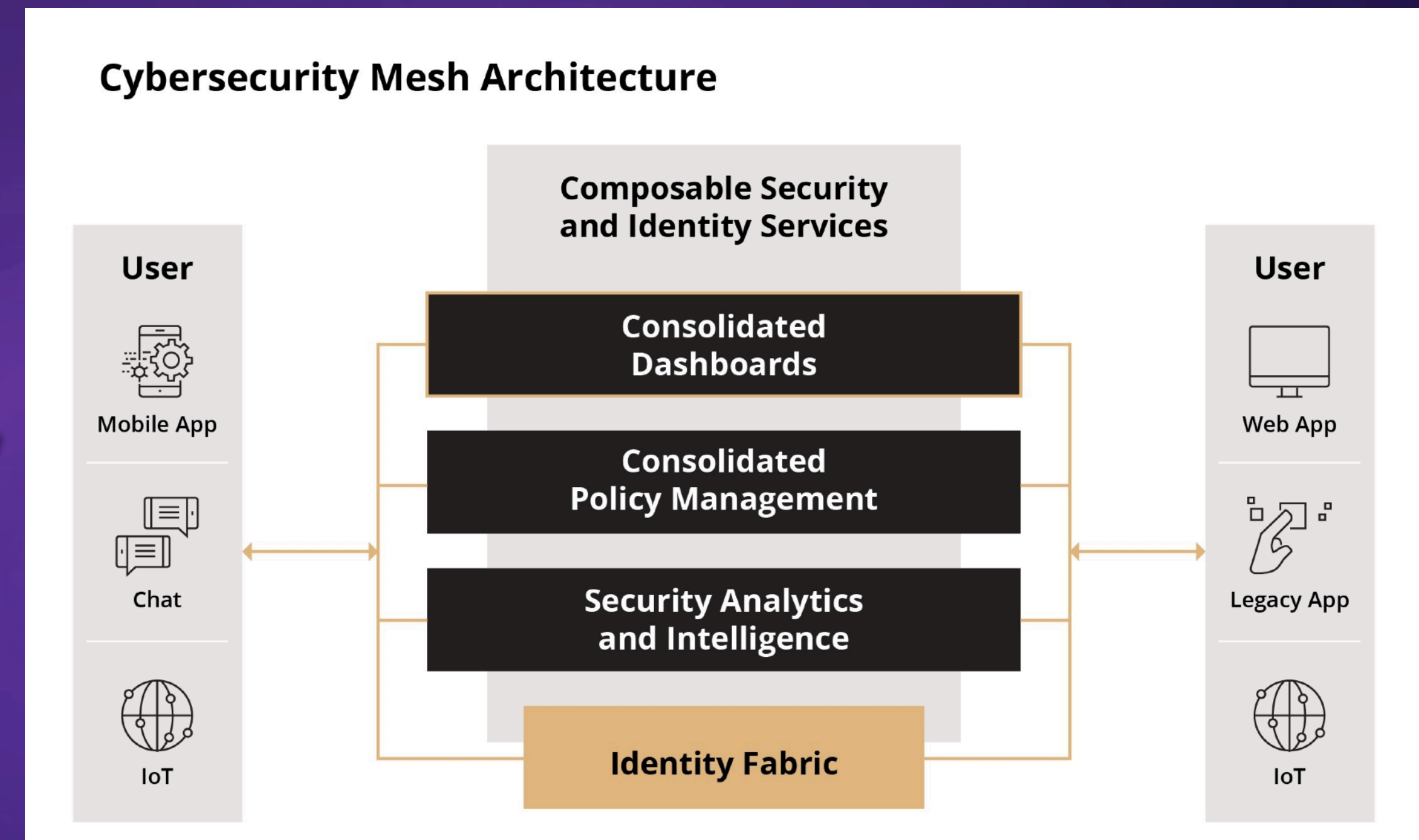
Cybersecurity Trend: Privacy Laws

- **Will restrict and direct the personal information of 70% of the world's population by end of 2023**
 - GDPR (EU)
 - PIPEDA (Canada)
 - CCPA (California)
 - APPI (Japan)
 - LGPD (Brazil)
 - PDPA (Singapore)
 - PDPA (Thailand)
 - PDPB (India)
- **The laws have vast reach and scope that affect cybersecurity delivery**
- **Orgs are increasingly unable to avoid complying with them, even in other countries**
- **Automating privacy management is the only real practical solution**
 - **Cybersecurity offerings must comply with these and automate their enforcement**
- **Recommendation: Standardize security capabilities using GDPR as a base, and then adjust for individual jurisdictions.**



Cybersecurity Trend: Mesh Architectures

- Organizations must now support a variety of cybersecurity technologies in different places
- They need a flexible security solutions that work together and complement each other.
- The concept of cybersecurity mesh extends to cover identities inside and outside the traditional security perimeter
- It brings these together to create a holistic view of the organization.
- A mesh approach also helps improve security for remote work.
- These demands will drive adoption in the next two years.
- Recommendation: Communicate clearly how cybersecurity solutions easily fit into and proactive support a mesh architecture.



Cybersecurity Trend: Consolidation

- Cybersecurity department are seeking to reduce the complexity in their landscape
- Consolidation and optimization has become a major trend
- By 2023, 30% of companies will have these cybersecurity services from one vendor:
 - Secure Web Gateway (SWG)
 - Cloud Access Security Brokers (CASB)
 - Zero Trust Network Access (ZTNA)
 - Firewall As A Service (FWaaS)
- Data point: Security teams today often manage dozens of tools.
- But they plan to consolidate to fewer than 10 by 2023.
- Recommendation: Either become very co-existent and/or offer a growing suite of services.



By 2023, 30% of orgs will have core cybersecurity services from one vendor. By 2026, it will be 45% of orgs.

Cybersecurity Trend: Risk Ratings



By 2025, 65% of orgs will use cyber risk ratings in their standards contracts.

- Cybersecurity is poised to become a top risk determinate in 3rd party transactions
- Buyers and investors have begun using cybersecurity risk as a key risk factor in assessing opportunities.
- Increasingly, organizations look to cybersecurity risk during business deals, including mergers and acquisitions and especially vendor contracts.
- The result is more requests for data about a supplier or partner's cybersecurity program via questionnaires or security ratings/assessments.
- Recommendation: Provide data and ratings about overall risk reduction that your offering provides

Cybersecurity Trend: Ransomware Regulation

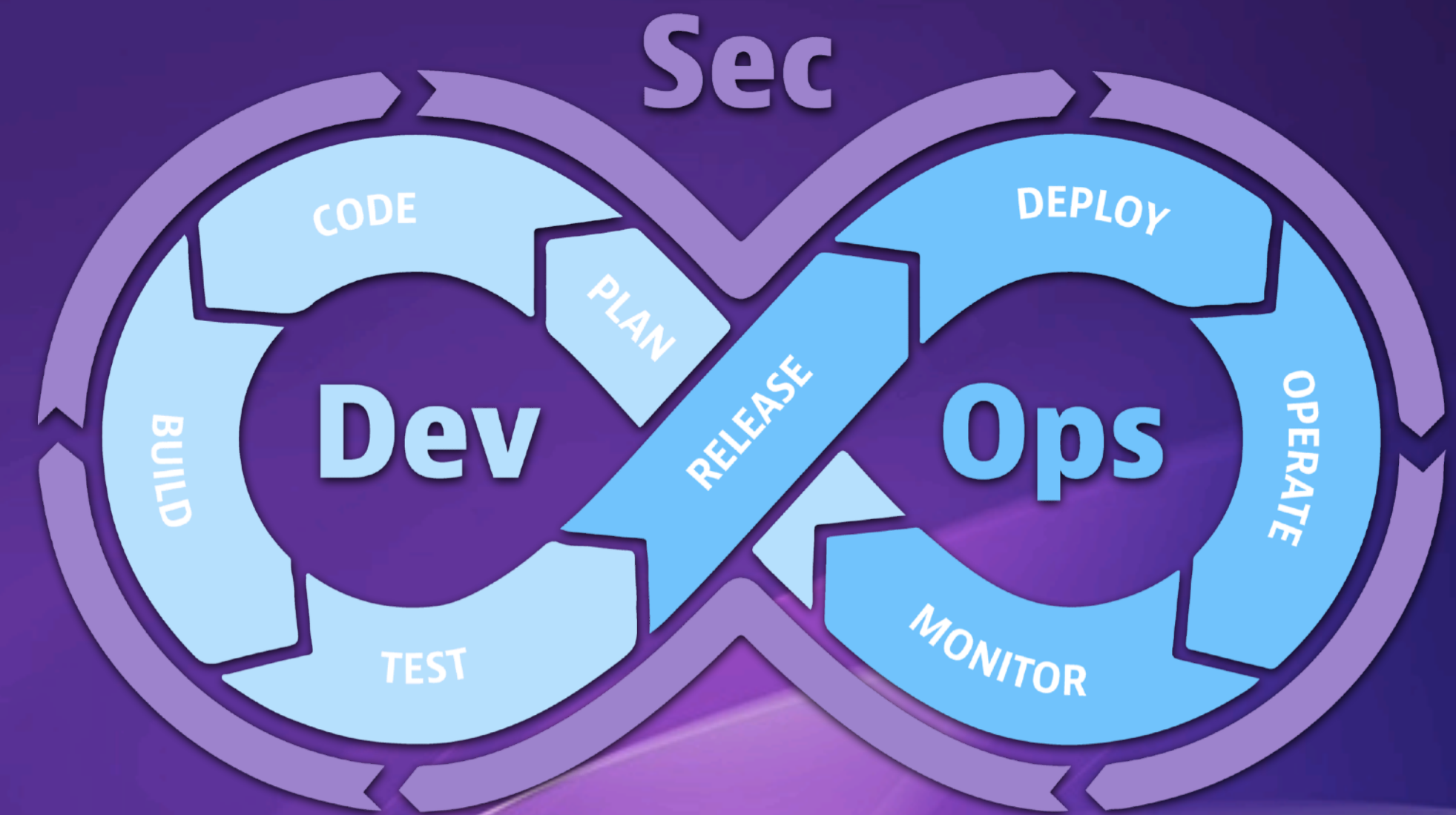
- **Most developed nations will soon have ransomware patent regulations.**
- **Given the mostly unregulated cryptocurrency market, there are ethical, legal and moral implications to paying ransoms,**
- **By 2025, there will be regulations for ransomware payments, fines and negotiations**
- **Security experts should expect a more aggressive crackdown on payments especially.**
- **This will further drive demand for ransomware solutions that cannot be easily compromised.**



Ransomware regulations will rise to 30% of countries by the end of 2025, compared to less than 1% in 2021.

Cybersecurity Trend: Cyber Innovation

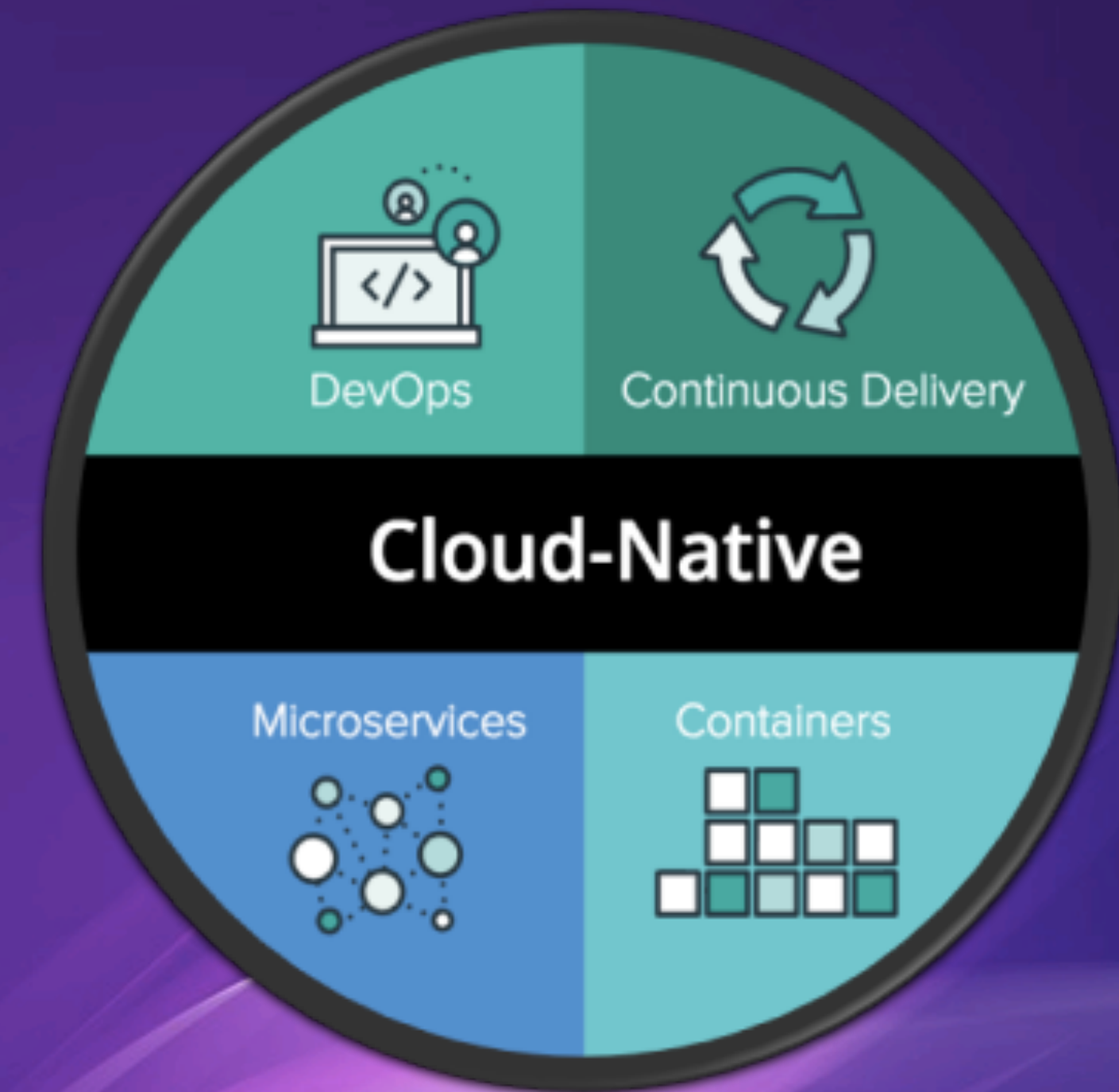
- Cybersecurity restrictions and controls are increasingly seen as broadly inhibiting tech innovation and digital transformation.
- DevSecOps is the latest battleground where the rapid pace of agile processes is often running aground by introducing security-first processes from the outset.
- Cybersecurity solutions are now urged to focus on enabling innovation and not hindering it.
- Recommendation: Use automation and AI (especially static verification) to make the DevOps chain run much more efficiently and accelerate the dev, test, deploy cycle, not slow it down.



DevSecOps is credited with accelerating incident detection (95%) and response (96%) efforts. 22% of organizations today are adopting the practice.

Cybersecurity Trend: Cloud-Native

- As the world moves broadly to cloud-native architectures, especially Kubernetes and microservices, cybersecurity vendors must extend their envelope to include them.
- Cloud-native is poised to be the main definitive future architecture of the Internet and IT.
- But C-N is complex and sophisticated in operations. This requires specific solutions to address how it works.
- Recommendation: Cybersecurity solutions must offer specific ways to make security cloud-native applications easier, simpler, and faster, *inherently*.



30% of orgs report they are cloud-native today. 37% report they will be cloud-native by 2025.

Cybersecurity Trend: Operational Resilience



Organizations will seek to co-locate operational resiliency with cybersecurity, with 20% of large orgs attempting it by 2025.

- Orgs will experiment with co-locating organizational resilience operations with cybersecurity operations (SOCs).
- Goal: To navigate and survive coincident threats from cybercrime, privacy law violations, disease outbreaks, severe weather events, civil unrest and political instability.
- The effort is to create an integrated capability that can effectively response quickly to global and regional events.
- Recommendation: Have a specific point of view and thought leadership that shows how a cybersecurity solutions fits into emerging operational resilience centers.

Cybersecurity Trend: Bad Actors Fight back

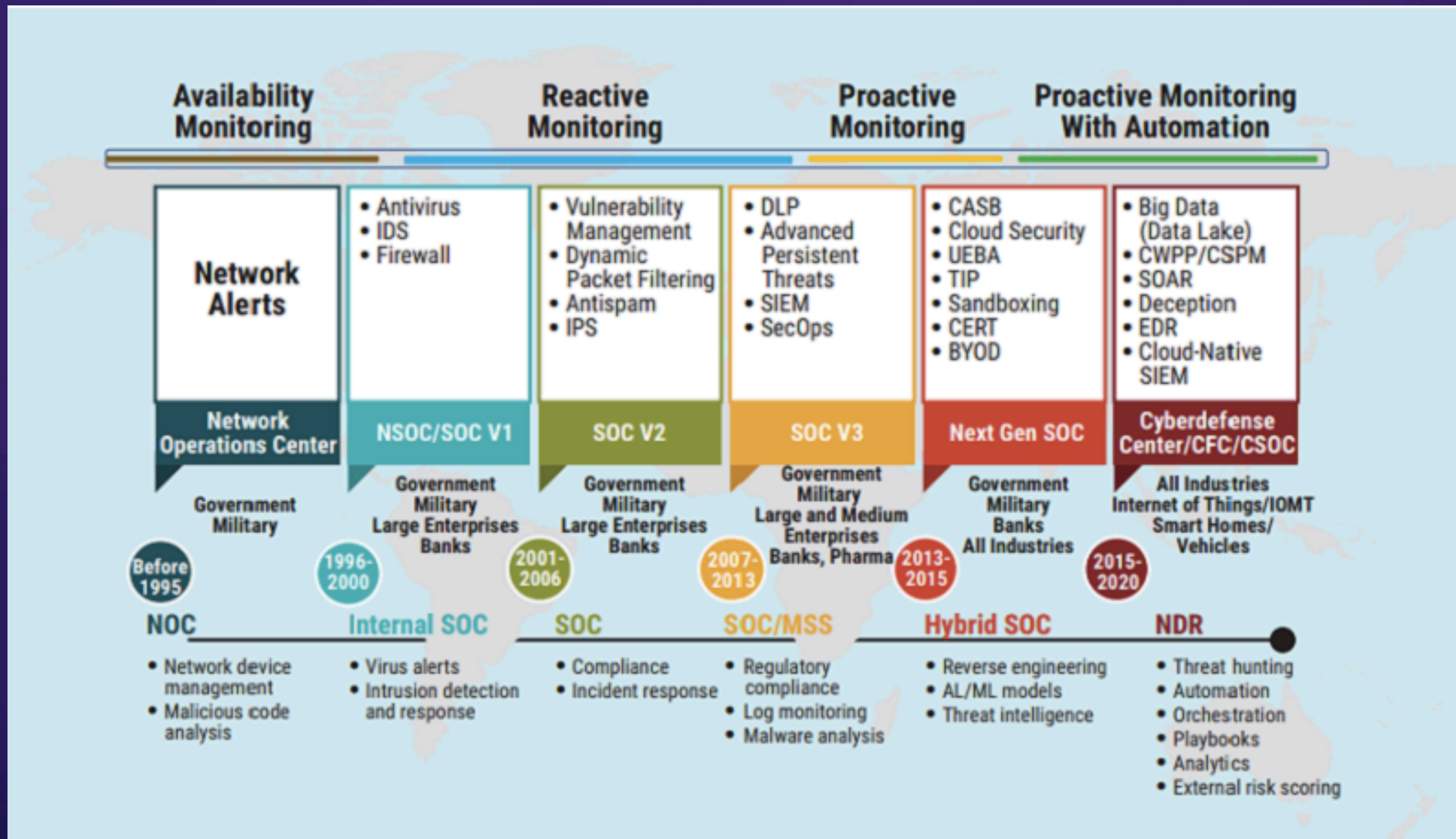


By 2022, 65% of businesses have endured some sort of ransomware attack, resulting in a loss of significant amounts of revenue for their organization.

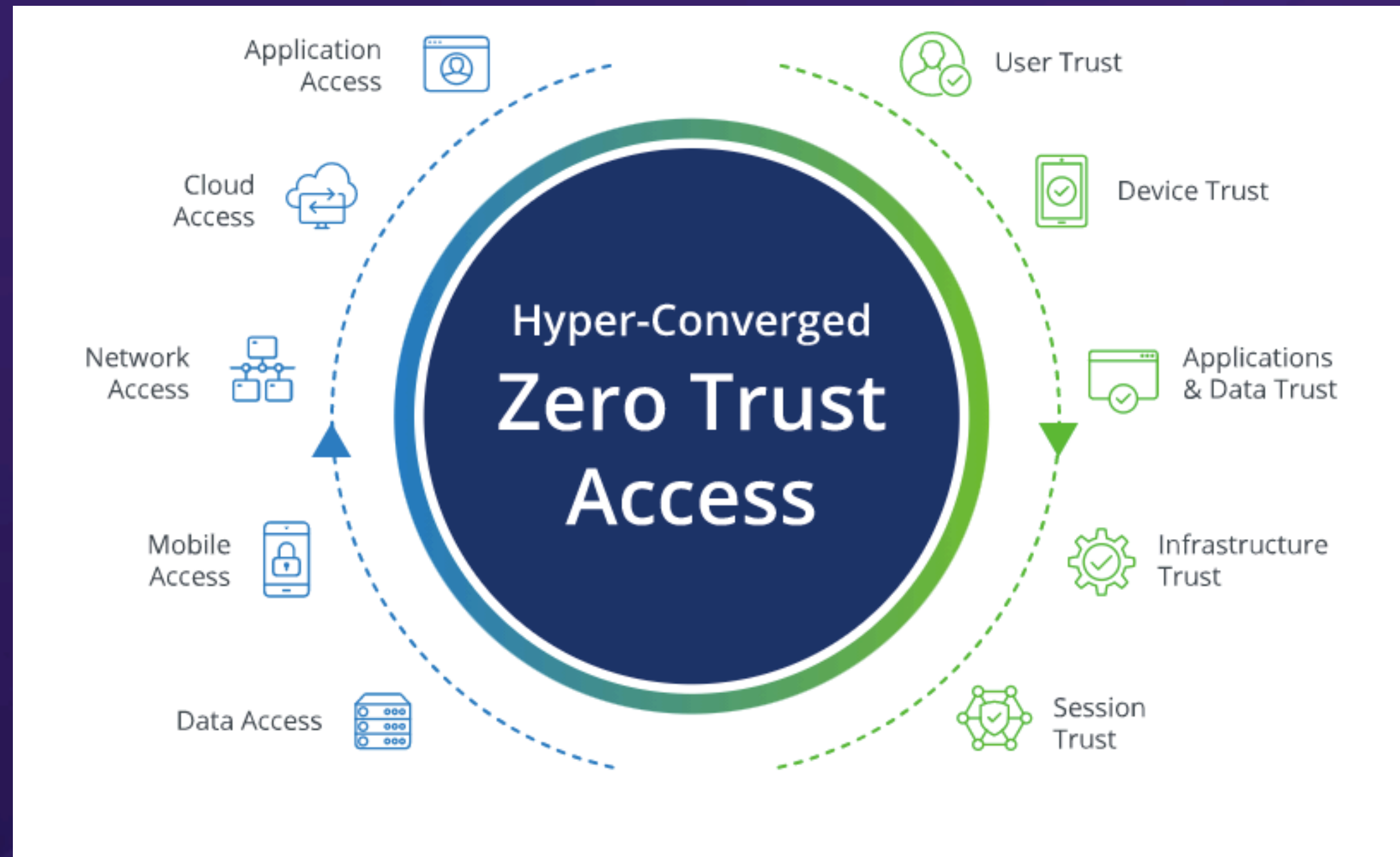
- Attacks against multi-factor authentication schemes, ransomware gangs productizing their own stacks, and upgrading their TTPs.
- AI-powered exploits, remote work attacks, and massive DDOS farms have emerged in 2022 to become major new vectors.
- Nation-states continuing funding certain cyber groups and making the problem larger, faster.
- Recommendation: Communicate broadly with customers and the market about how cybersecurity offerings are keeping pace, and hopefully exceeding the rate of change.

The Evolution of the SOC

The State of the Art Becomes "Excessively" Sophisticated



Cybersecurity Trend: Rethinking the Network Stack -> Zero Trust

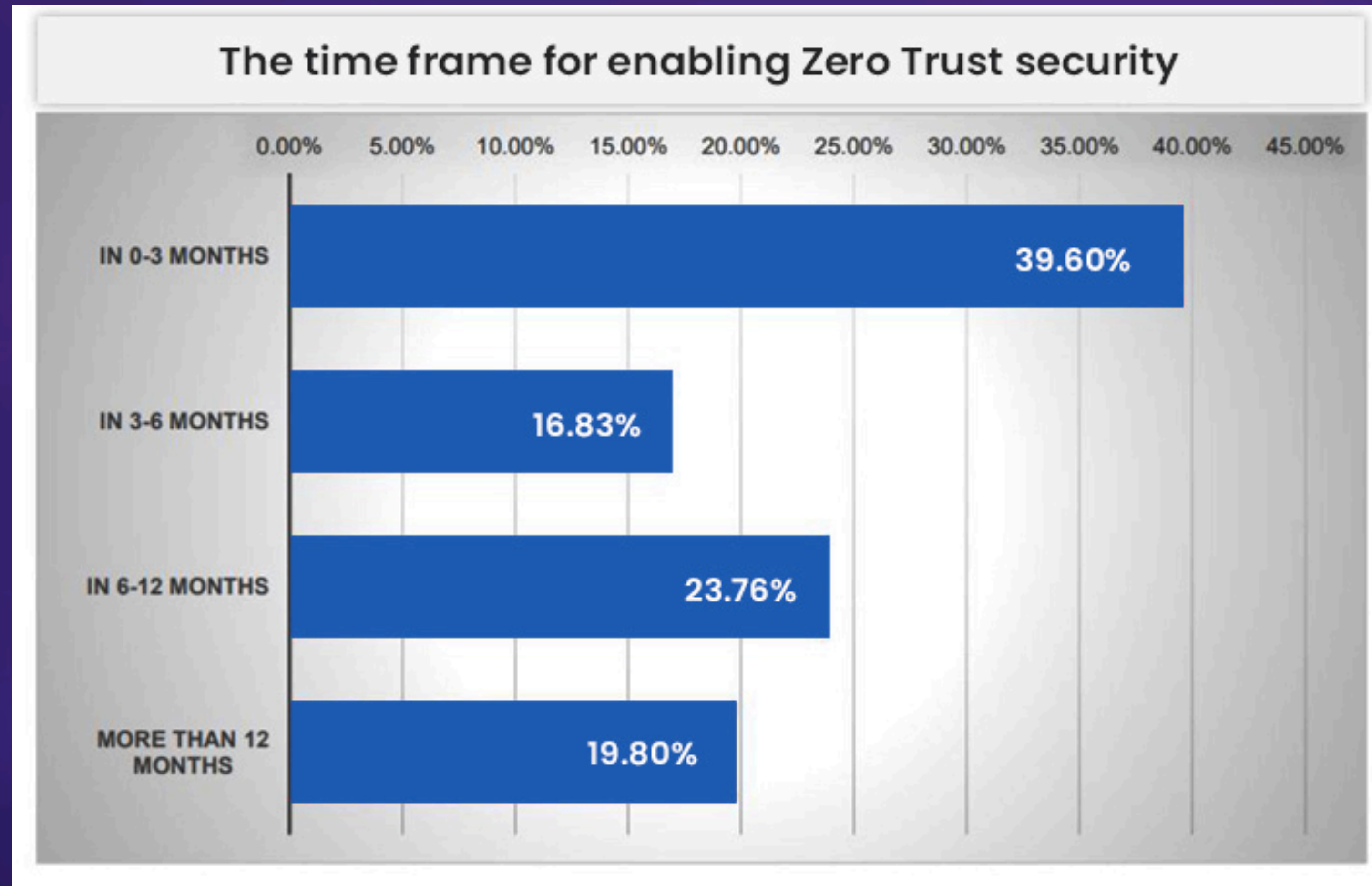


A hyper-converged zero trust network stack will emerge to industry consensus in the next 3 years.

- As Zero Trust has emerged a pre-eminent overarching approach to cybersecurity, the reality is still that network devices will connect with anything by default.
- The proliferation of IoT and IIoT devices has made the problem much worse.
- Simply put, many are now seriously considering rethinking TCP/IP so that all network devices — and only network devices that use an opt-in list — will function on a corporate network.
- This will require a new network stack that is fundamentally zero trust by default.
- Recommendation: Rapidly follow industry initiatives that will update the aging network stack to be fully Zero Trust.

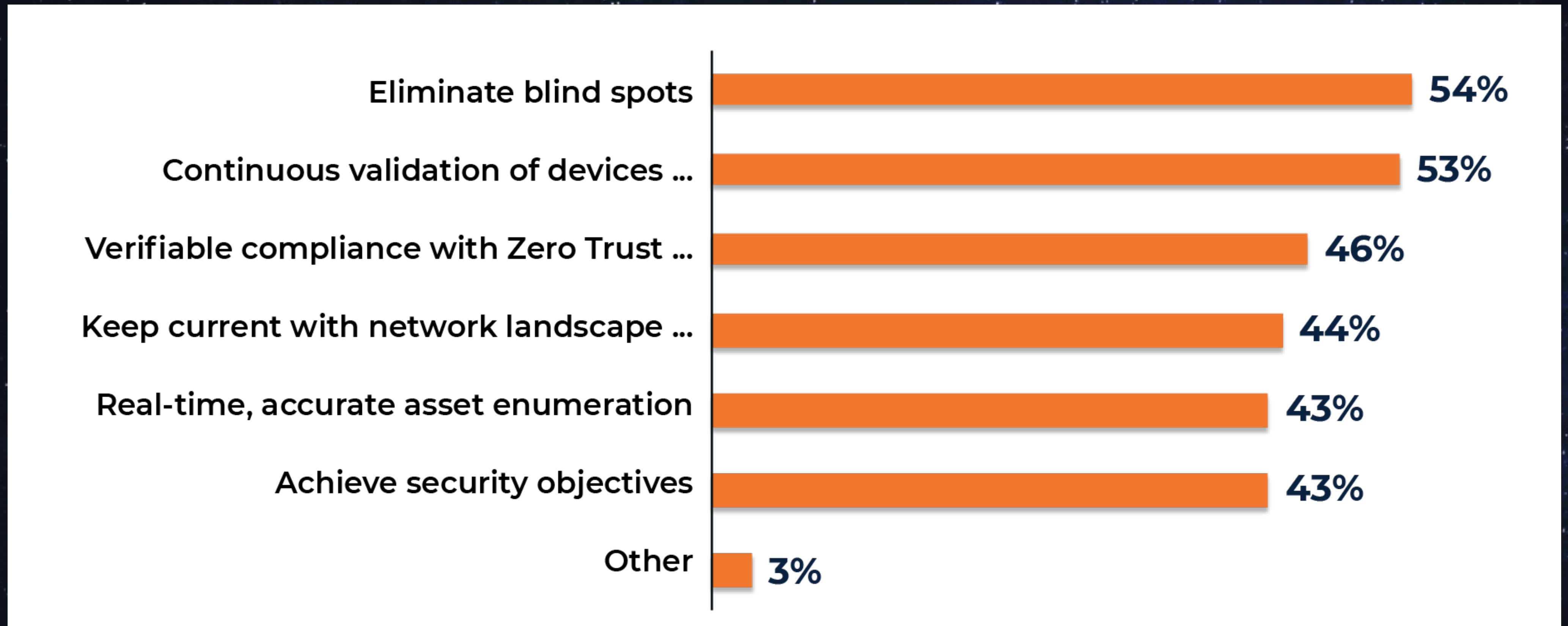
Timeline to Zero Trust

80% of Organizations Are Committed Long Term



What Is Zero Trust Really? And Is It Enough?

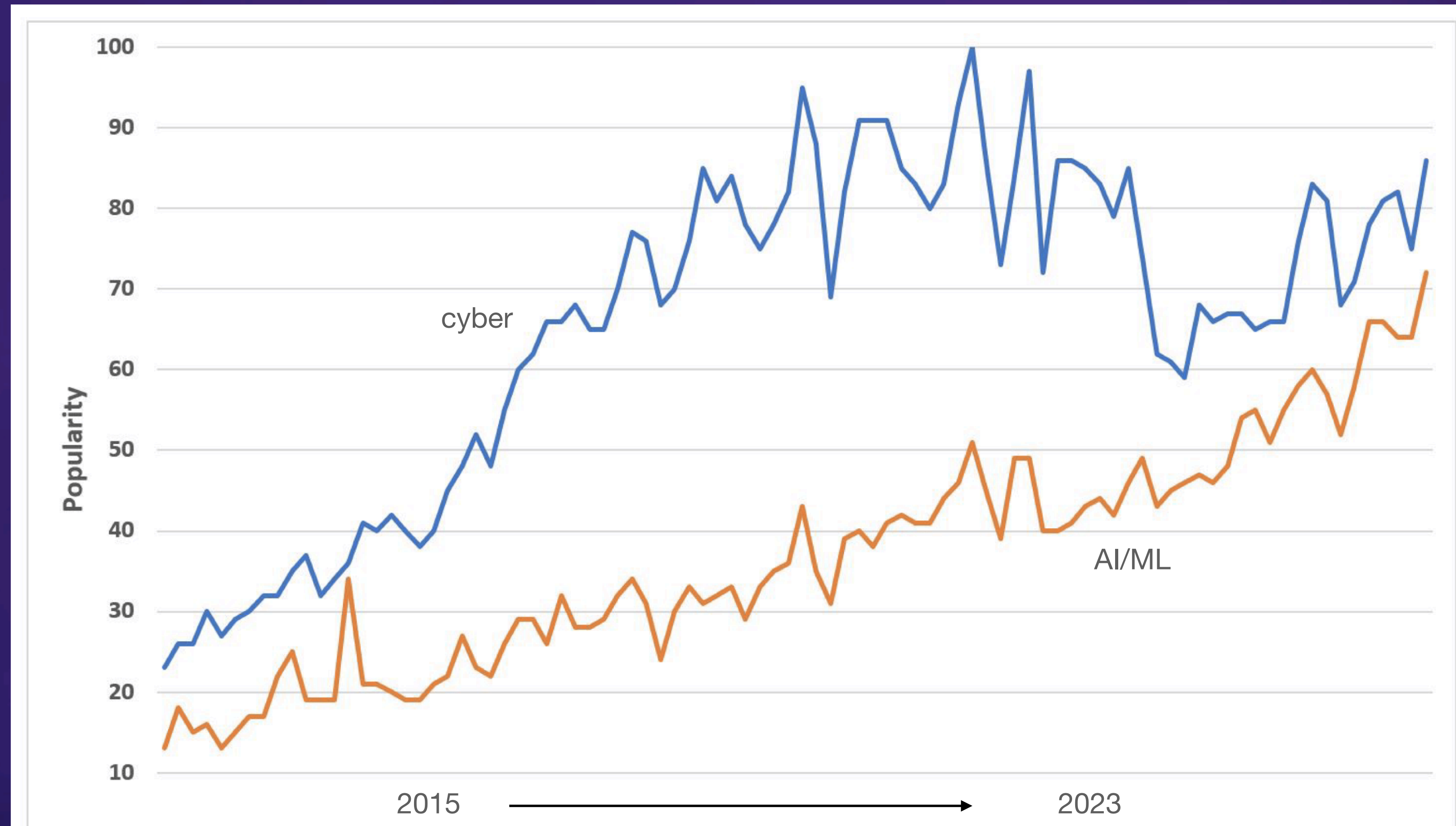
Analysis: The Practice Is Comprehensive Enough To Form an End State



Source: 2023 Gigamon Survey on What Orgs Are Doing to Implement Zero Trust

There is An Undeniable Pattern in the Trends

Long Term Machine Learning Trends vs. Cybersecurity



Source: Google

Cybersecurity Trend: AI-Based Cyber Operations

- **Cybersecurity attacks and incidents can increasingly not be fought by hand.**
- **Automation is coming using ML and AI to systematically automate cyber operations.**
- **AI can fight hundreds to thousands of incidents per day. Soon per hour.**
- **It can even remediate many of the incident without human supervision.**
- **AI Cyber Operations is becoming part of a broader trend know as AIOps.**
- **Recommendation: Cybersecurity vendors must increasingly automate all aspects of their product suites to detect and remediate cyber incidents to the 90% level by 2025.**



AIOps growing by 15% a year to a \$12 billion industry by 2025. AI Cyber Ops will be fully half of that industry.

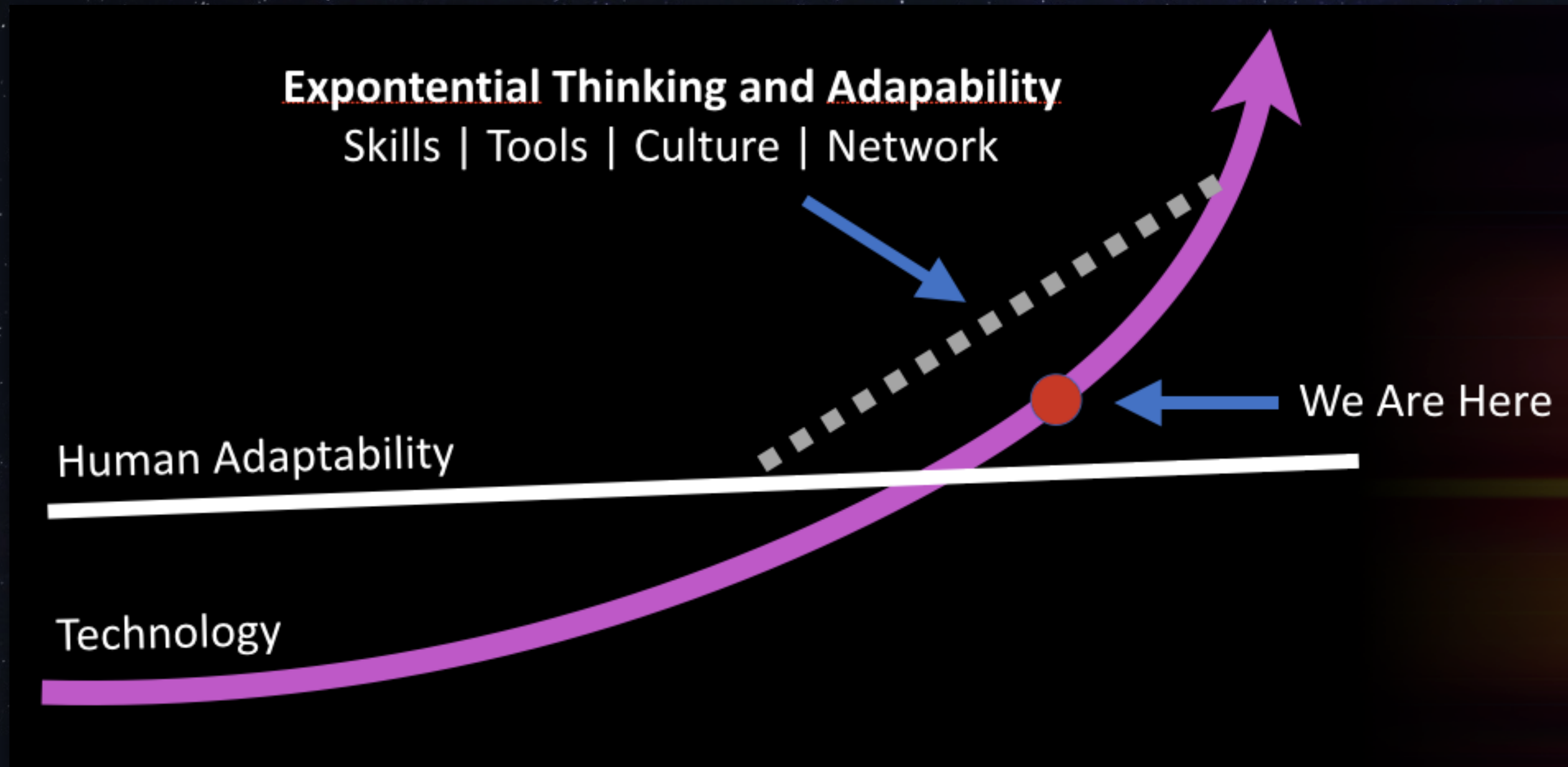
Decentralization of Everything is Arriving...

The Structure of IT and Cybersecurity Is Profoundly Impacted

- Decentralization is coming
- Open movements to broadly decentralize technology, the Internet and business, making it more trusted and private
- Everything in the IT stack, and beyond
- Including personal identity, data, media, services, applications, transactions, cybersecurity, and even finance and money
- Crowdsourcing, cloud, blockchain and other decentralized tech underpinning
- Fundamentally centered around local fit for purpose
- Flying under the IT and business radar
- Leading edge is Web3
 - Massive economic (tens of billions of \$ a day in transactions) and wild tech innovation activity
 - \$2 trillion market right now



Technology: Exponential Thinking and Methods Now Required



Understanding Exponential Tech Change Helps Us Prepare

Enabling Us to Anticipate the Nearly Unlimited Value Potential

1 **Insight:** The Value of Digital is Driven by Power Laws That Pay Off Big Downstream

2 **But Most Organizations Only Change Linearly, or Logarithmically at Best**

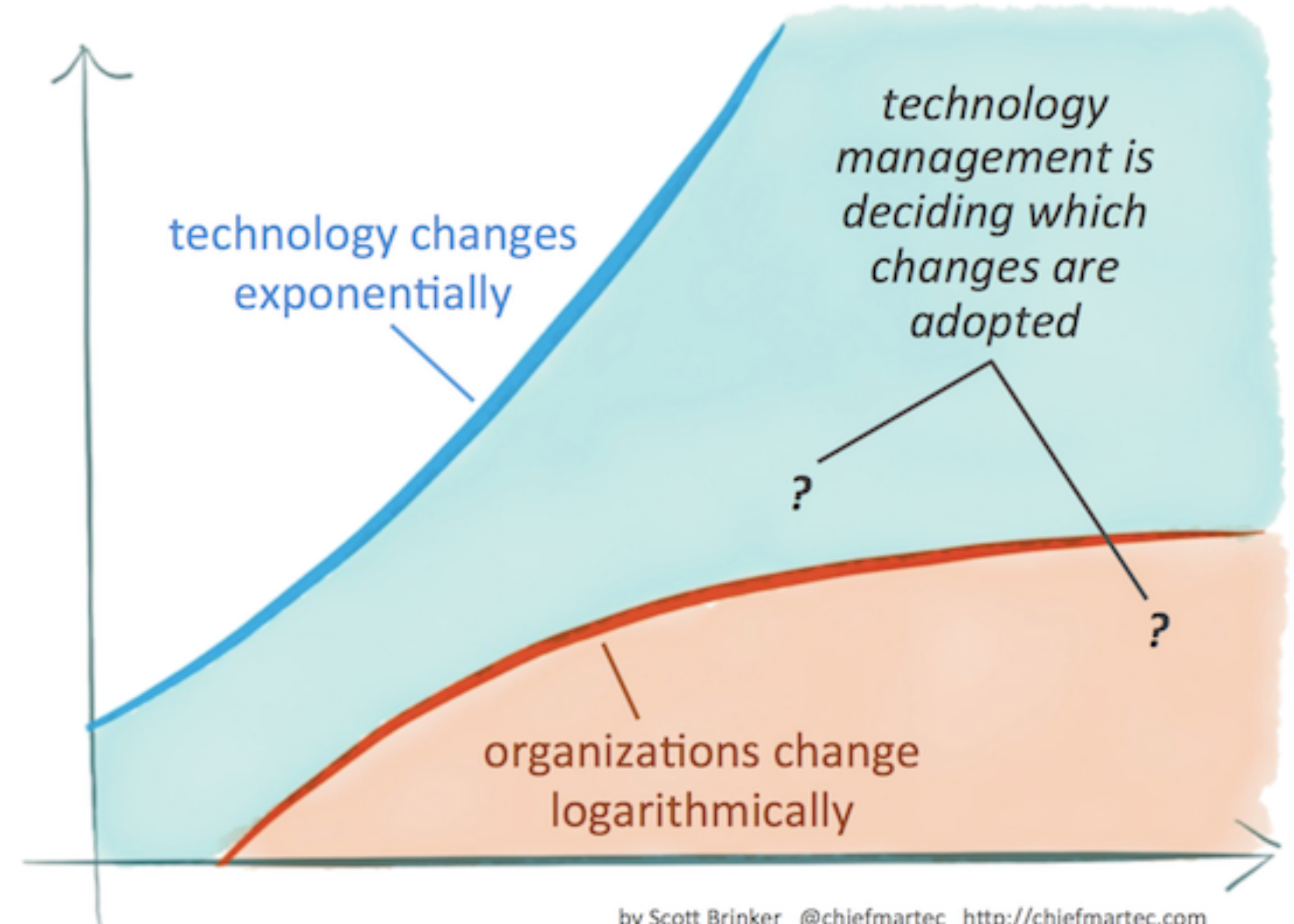
Technology	Average cost for equivalent functionality	Scale
3D printing	\$40,000 (2007) to \$100 (2014)	400x in 7 years
Industrial robots	\$500,000 (2008) to \$22,000 (2013)	23x in 5 years
Drones	\$100,000 (2007) to \$700 (2013)	142x in 6 years
Solar energy	\$30 per kWh (1984) to \$0.16 per kWh (2014)	200x in 20 years
3D LIDAR Sensors	\$20,000 (2009) to \$79 (2014)	250x in 5 years
DNA genome seq	\$10,000,000 (2007) to \$1,000 (2014)	10,000x in 7 years
BCI neuro devices	\$4,000 (2006) to \$90 (2011)	44x in 5 years
Full body med scan	\$10,000 (2000) to \$500 (2014)	20x in 14 years

Source: "Exponential Organizations"

<http://www.slideshare.net/vangeest/exponential-organizations-h>

@dw2

**The Payoff of Power Laws
(Like Moore's Law) Over Time**

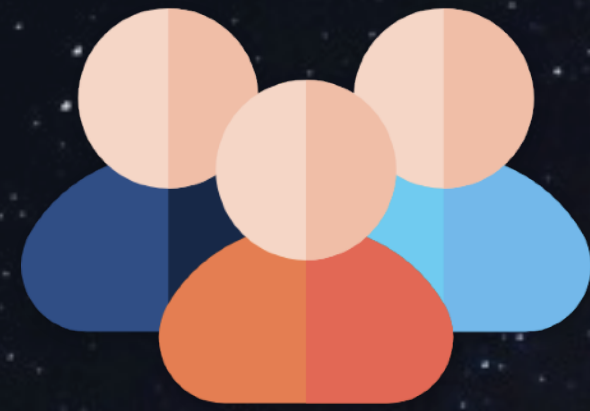


by Scott Brinker @chiefmartec <http://chiefmartec.com>



State of Cybersecurity: The Evolution of Core Practices

A Comprehensive Analysis: The Cyber Domains



Users



**Apps &
Workloads**



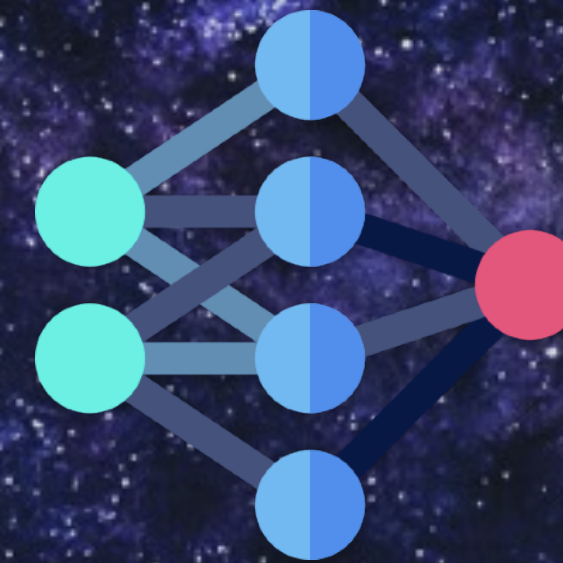
Devices



Data



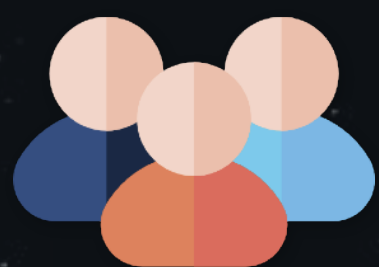
**Automation &
Orchestration**



Network



Analytics



Users



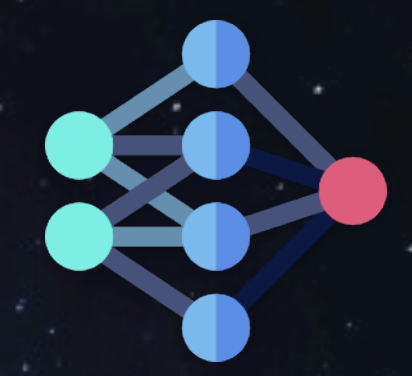
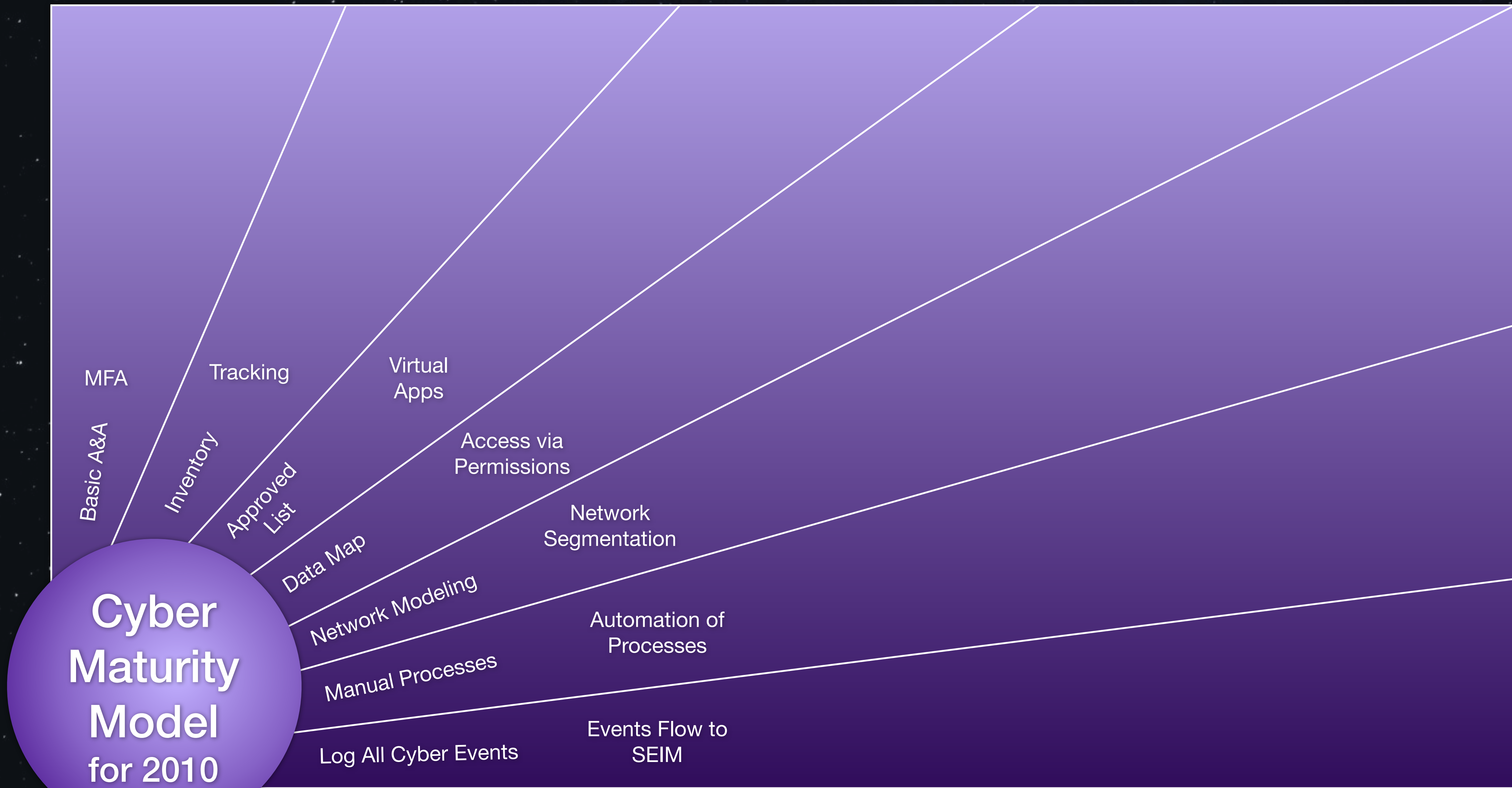
Devices



Apps & Workloads



Data and Payloads



Network



Automation & Orchestration



Analytics

1 Initial

2 Basic

3 Intermediate

4 Advanced



Users



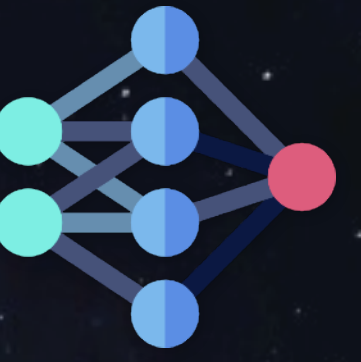
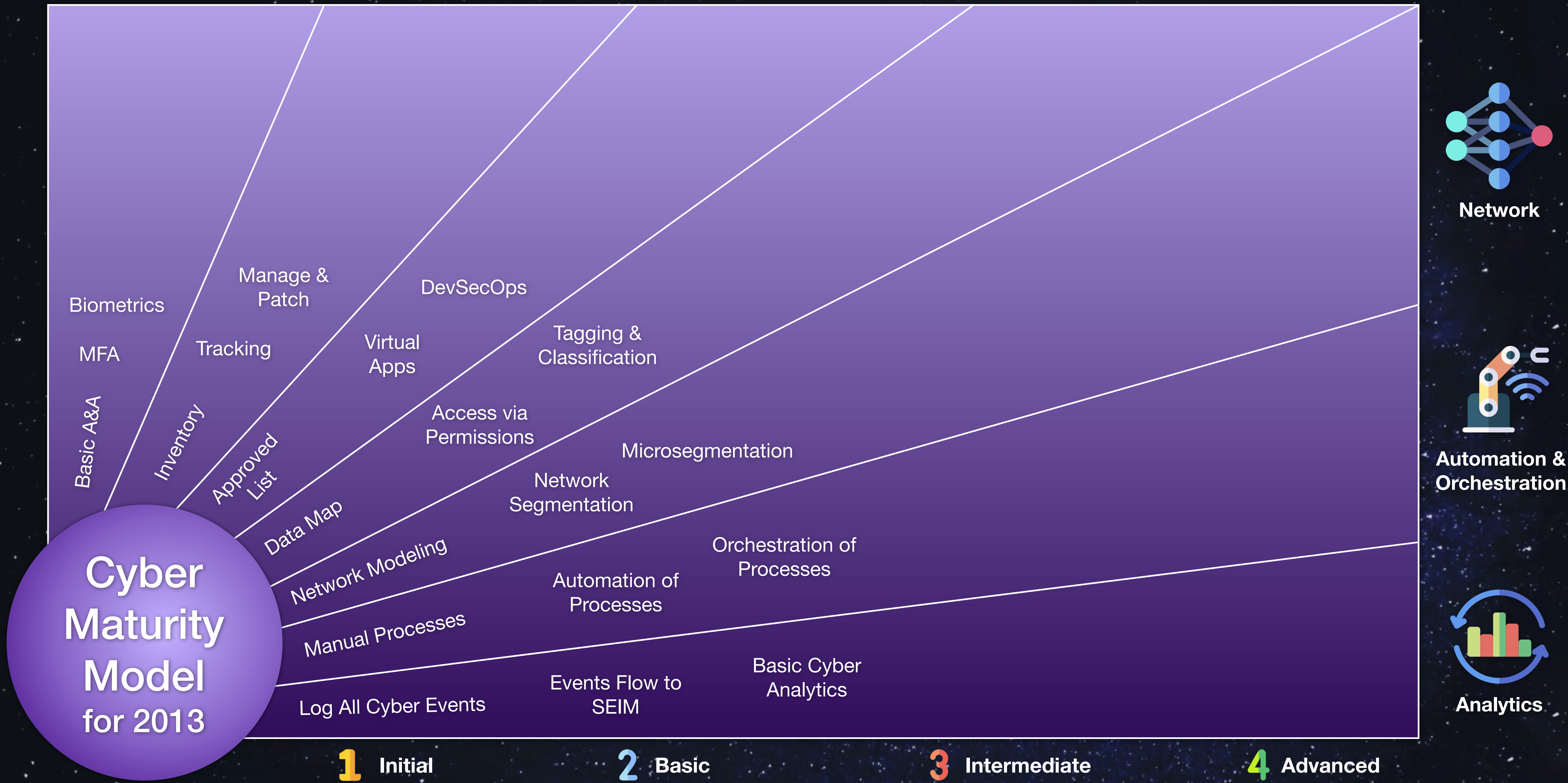
Devices



Apps & Workloads



Data and Payloads



Network



Automation & Orchestration



Analytics

1 Initial

2 Basic

3 Intermediate

4 Advanced



Users



Devices

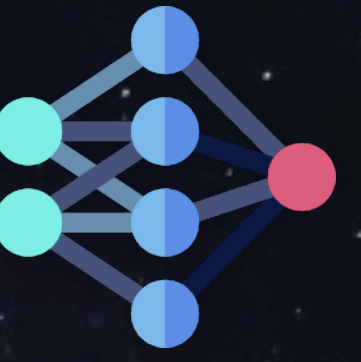
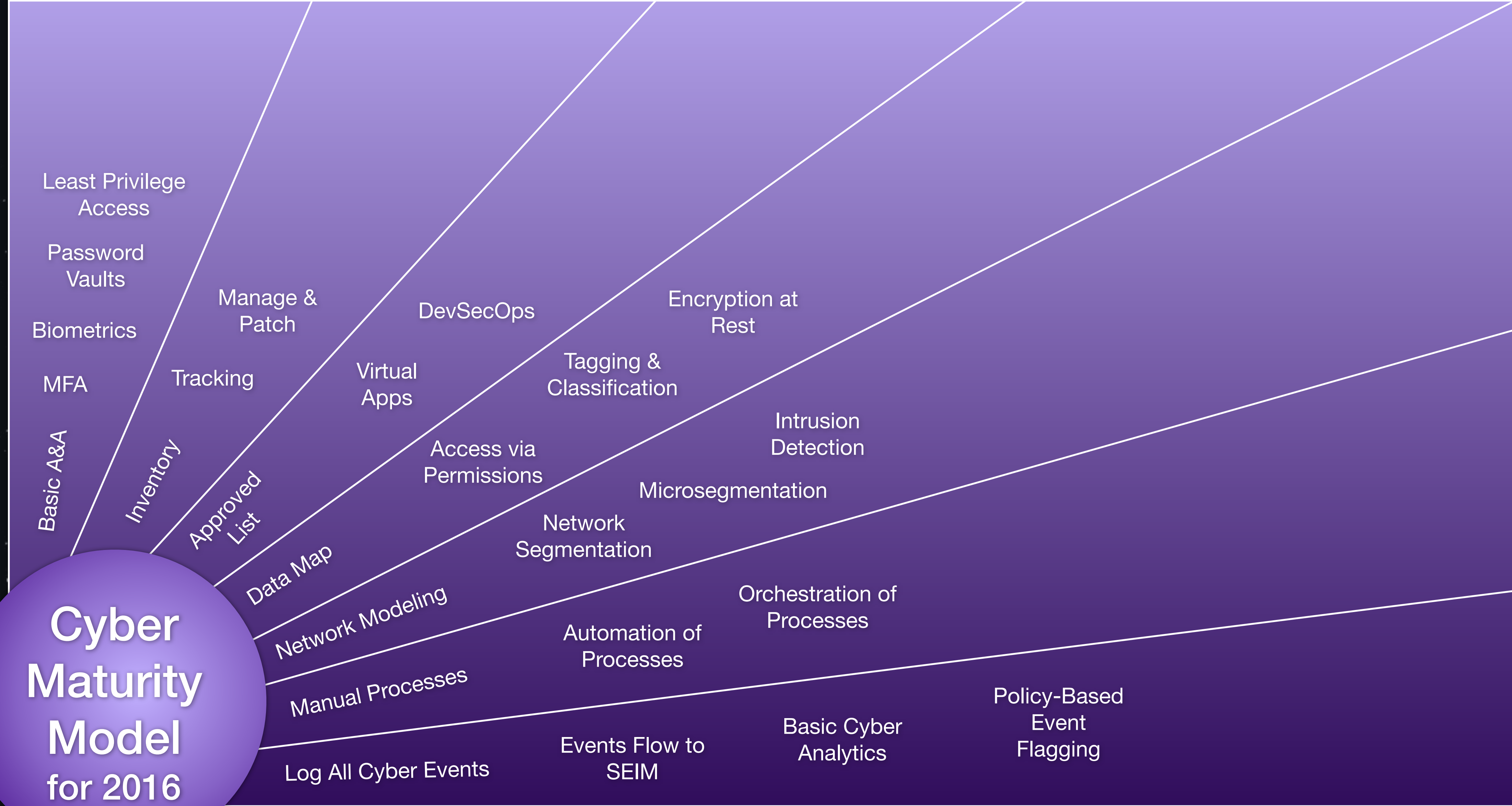


Apps & Workloads



Data and Payloads

Cyber Maturity Model for 2016



Network



Automation & Orchestration



Analytics

1 Initial

2 Basic

3 Intermediate

4 Advanced



Users



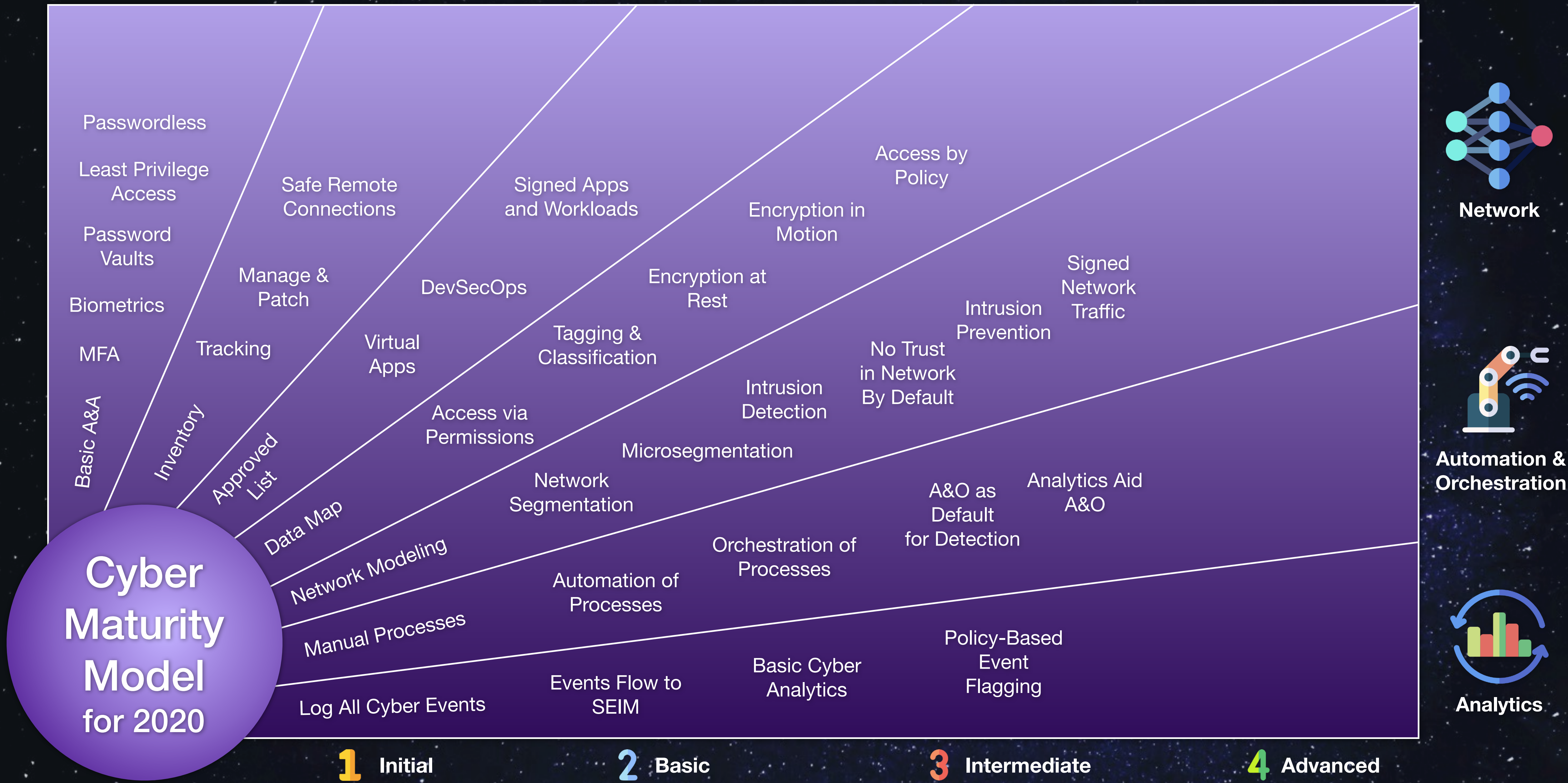
Devices



Apps & Workloads



Data and Payloads



Network



Automation & Orchestration



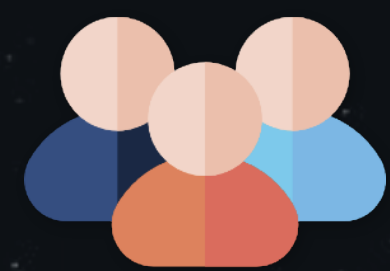
Analytics

1 Initial

2 Basic

3 Intermediate

4 Advanced



Users



Devices



Apps & Workloads



Data and Payloads



Cyber Maturity Model for 2023



Network



Automation & Orchestration



Analytics

1 Initial

2 Basic

3 Intermediate

4 Advanced

On a Timeless Way of Building Software

“This hinges on a form of representation which reveals all possible design processes, as versions of one most fundamental set of patterns.”

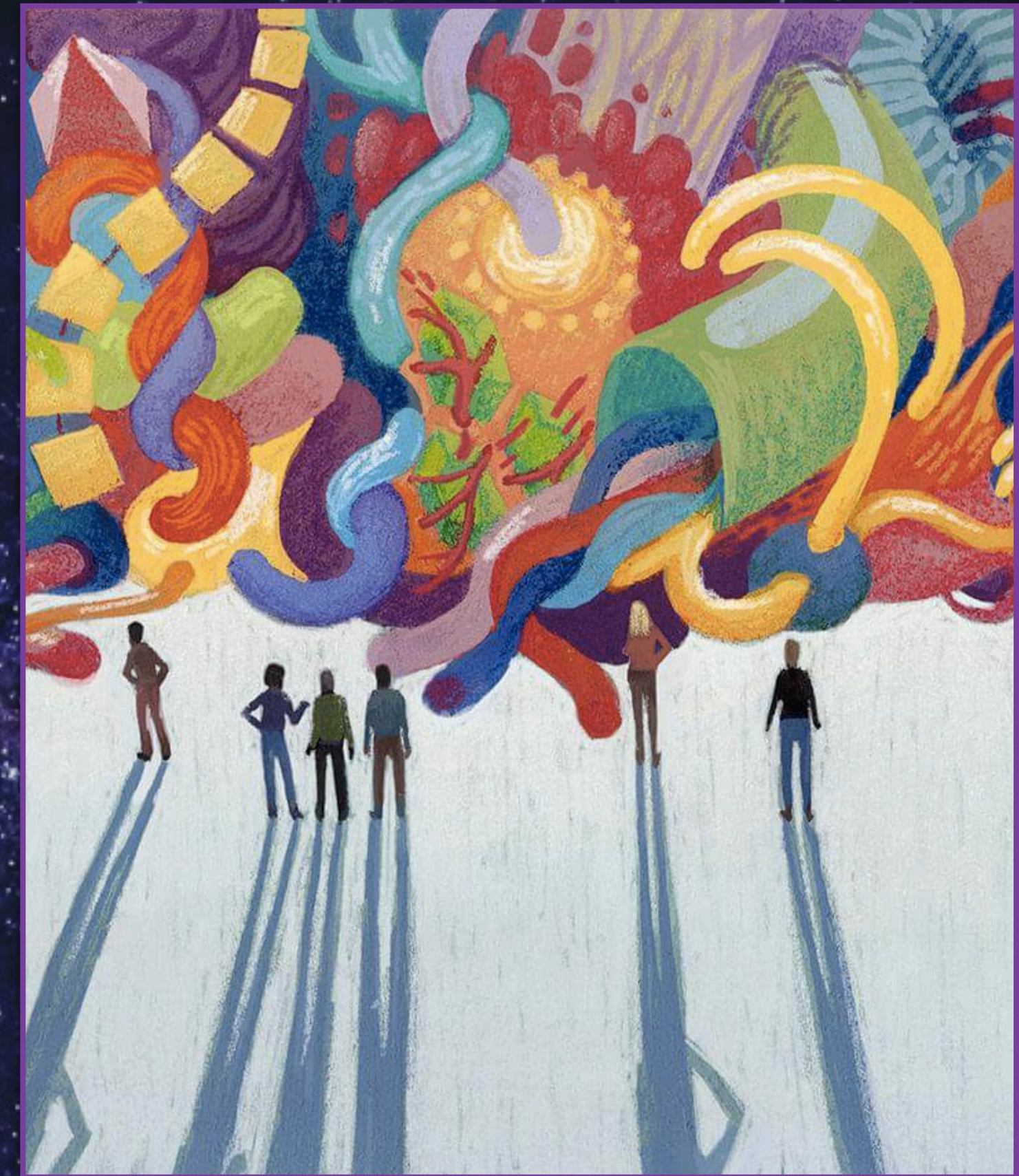
<https://dionhinchcliffe.com/2006/01/10/a-timeless-way-of-building-software/>


The End Game: Complexity Management

What Is True About IT Today, Is Just as True About Cybersecurity

Due to the critical needed removal of barriers to exponential IT growth and change, the future of IT is now about **complexity management**.

Corollary: This must now apply equally to the domain of cybersecurity as IT.





**Takeaway: Collectively, The Cyber Domain
As Defined Today Exceeds the
Grasp of Our Organizations**



**The End Game in Cybersecurity:
What Is the Simplest, Most
Holistic Route?**

Seeking Cyber Synthesis of a New Approach

What Holistic Approach That Results in Highest Cybermaturity

Insight: Piecemeal techniques are increasingly ineffective in a rapidly changing operating environment that sees new cyber channels, threats, and innovations emerging daily.

Applied Threat Intelligence

Managing the Most Significant Aspects of Scale in Cyber, As One

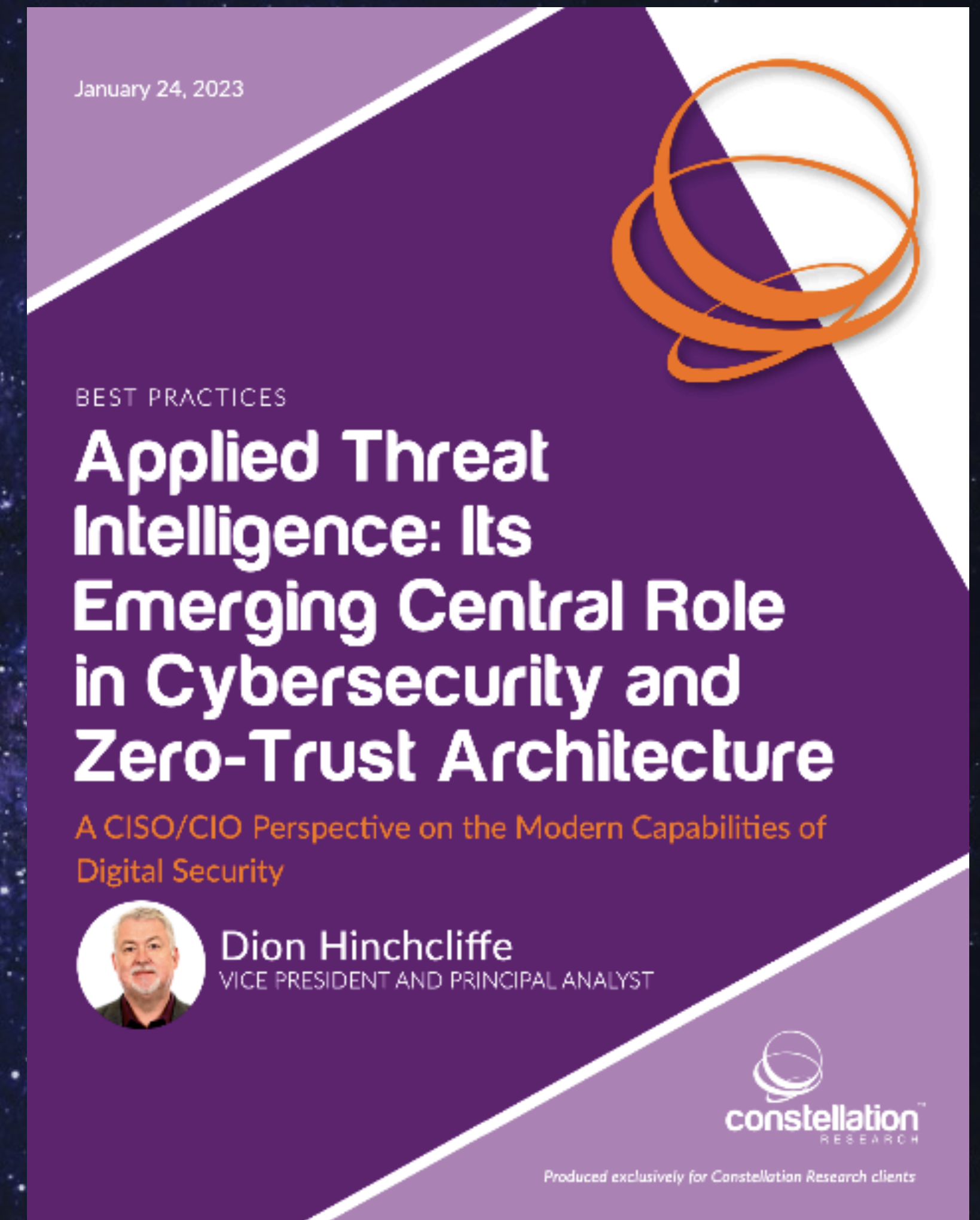
ATI consists of the following core elements in real-time:

- **An account of the network.** This includes all local networks as well as the broader internet. An effective ATI approach must have a database of network nodes that is as thorough as possible. ATI thrives best with rich network databases.
- **A reputation record.** An automatic record of all prior misbehavior by agents on all relevant networks is made and kept for later reference. This is a large, systematically built database as well and is typically augmented by expert analysis of new malicious behaviors and anomalies as they are discovered by the industry and/or the organization.
- **An assessment of behavior.** This critical examination and evaluation of suspicious patterns of misbehavior on the network must be continuous and include every network connection within the organization as well as any external connected entities that must be protected. It is the operational component of ATI.

Full View of Network

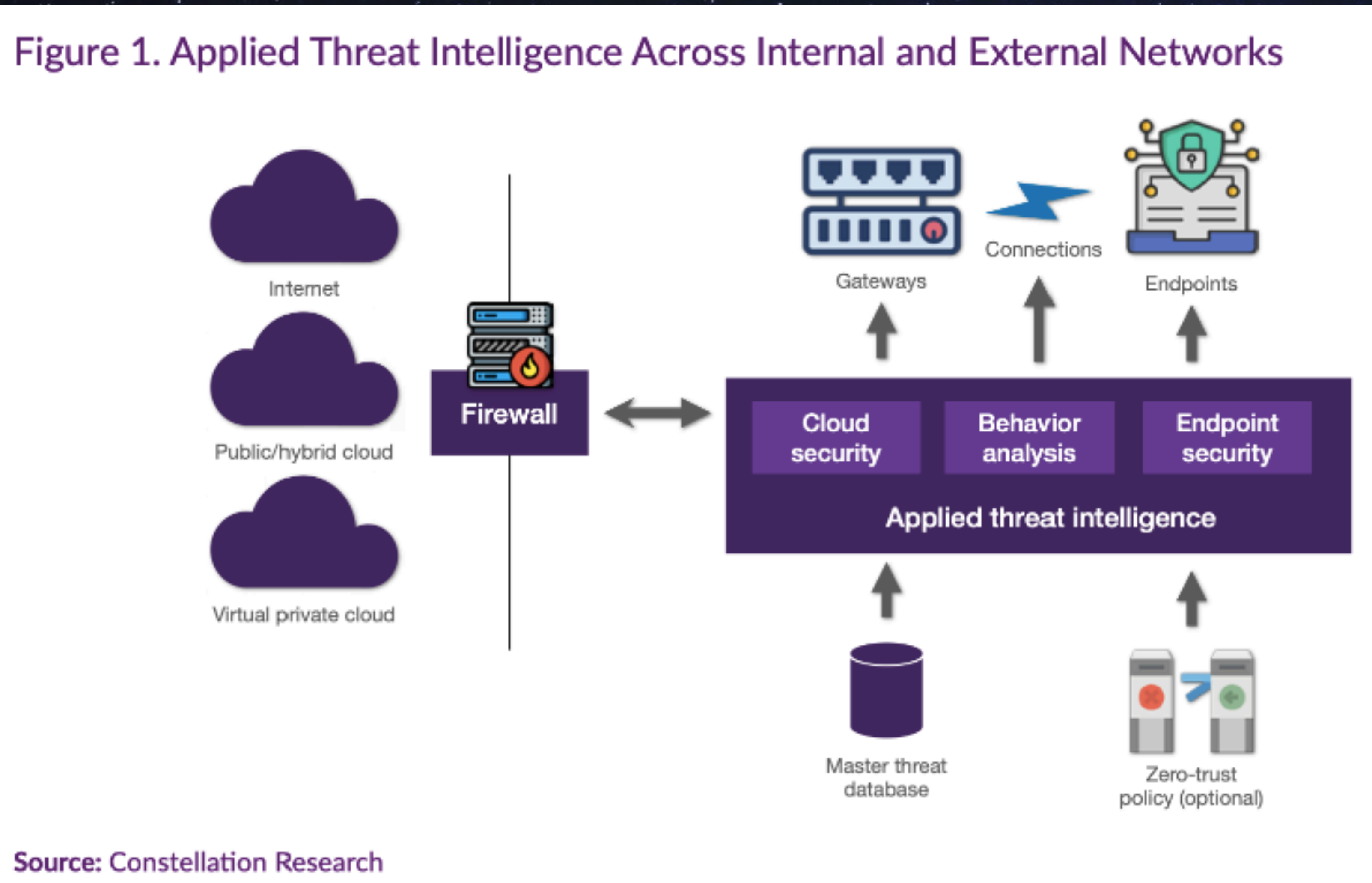
Reputation Data

Continuous Behavioral
Analysis



A View of Applied Threat Intelligence

Zero Trust + Behavior + Endpoint Security



A Sustainable End State for Cyber?

The Ability To Comprehensively Eliminate Threats - Excluding Insider Threats

Benefits of ATI

- **Least complexity.** Organizations can reduce their overall cybermanagement burden for threat detection while gaining a more integrated picture of the threat landscape.
- **Fewest required solutions.** The cybersecurity threat product portfolio can be trimmed and duplication eliminated.
- **Greatest threat coverage.** With the fullest knowledge of malicious network actors and cross-network behavior analysis at the firewall, gateway, and endpoint level, organizations can detect and stop more threats than with a system comprising a patchwork of different and disjointed threat intelligence sources at fewer network interfaces.
- **Lowest cost.** Fewer threat detection solutions are required, and the loss from cybersecurity incidents, which are less likely, is thus lower as well. There also is less overhead in managing fewer solutions, resulting in multiple sources of savings.
- **Sustainable integration,** management, and governance. With a smaller footprint, albeit a deeper presence on the network, ATI provides a more centralized point of threat intelligence and resolution, with fewer moving parts, fewer connections to third-party systems that weren't designed to work together, and therefore less management and oversight from the security team needed to keep it functioning well.
- **Zero Trust Everywhere.** By creating automatic compartmentalization at a network node level, ATI can be used as the basic mechanism to achieve end-to-end ZTA over time on a network.

The End of Cyber Evolution Is Not Here: But a Sustainable Future Is

The Best Cybersecurity Can Be Achieved Through A Far Smaller, But More Comprehensive Approach

- The cybersecurity industry cannot be overtaken by exponential factors
- Approaches in holistic complexity reduction is a key pathway
- ATI is just one example of a solution, there are others emerging
- The industry must find the simplest fitness landscape for cyber, or lose the battle
- Significant breakthrough that allow fighting exponential facts now exist
- But it requires system thinking and a move well beyond tactical response
- We are at a new dawn in cyber, if we are willing to change our thinking