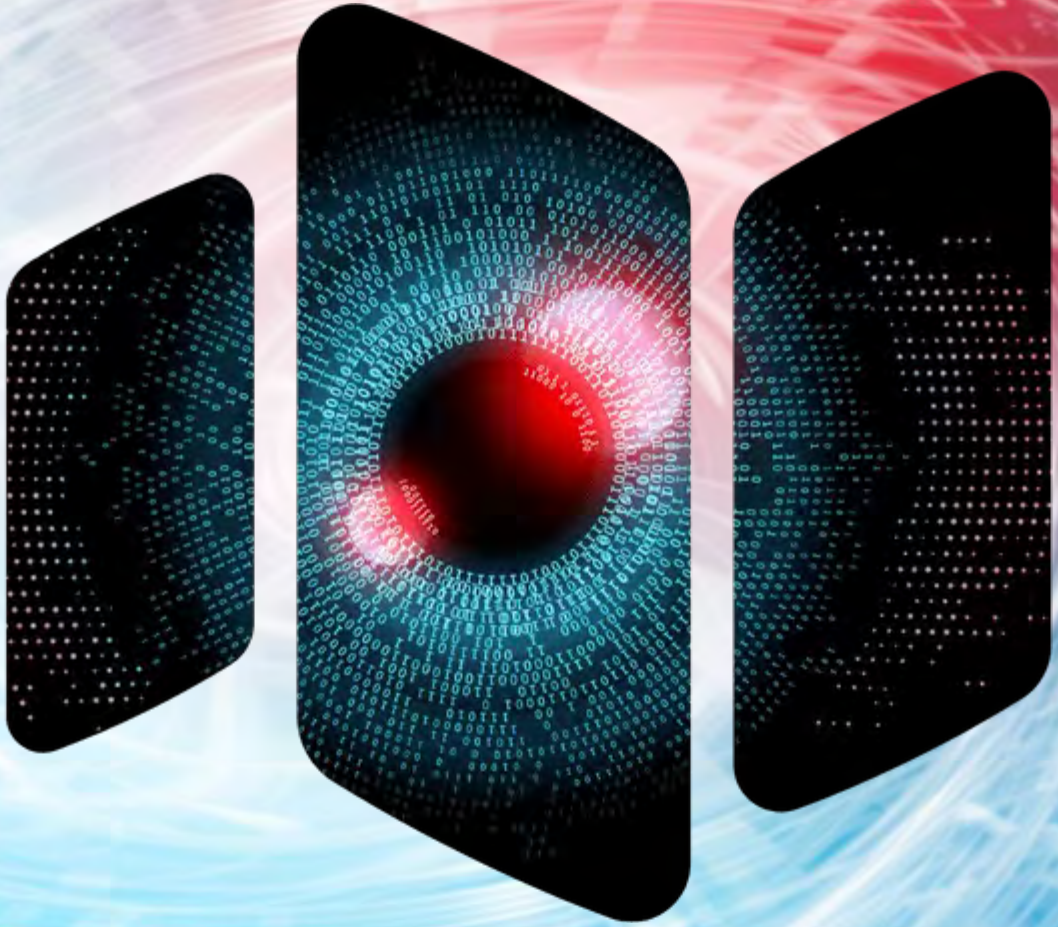
Cloud Security 2024: Managing Complexity

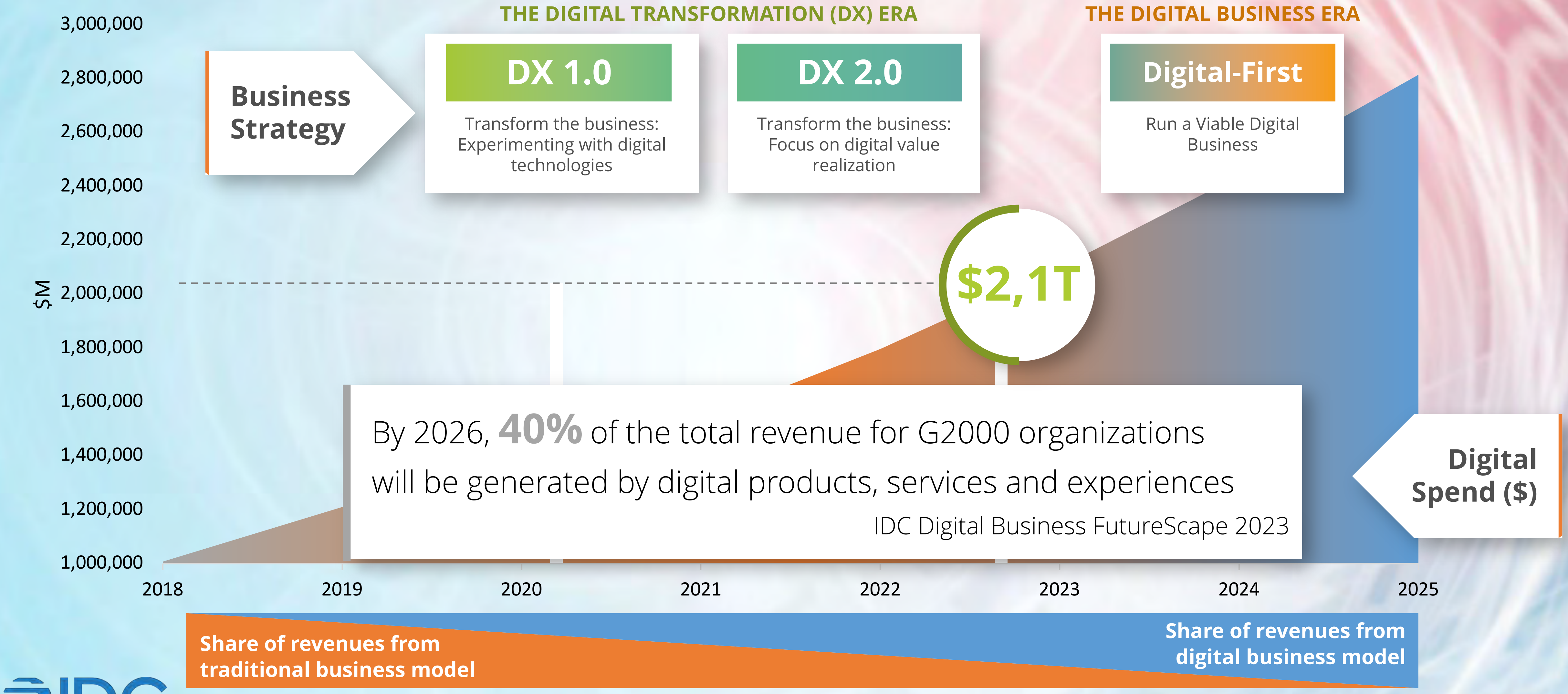


Frank Dickson
Group Vice President, Security & Trust

Cybersecurity Challenges in 2024

Digital First & Layer 0

The Shift to the Digital Business Era



Business Strategy

THE DIGITAL TRANSFORMATION (DX) ERA

DX 1.0

Transform the business: Experimenting with digital technologies

DX 2.0

Transform the business: Focus on digital value realization

THE DIGITAL BUSINESS ERA

Digital-First

Run a Viable Digital Business

By 2026, **40%** of the total revenue for G2000 organizations will be generated by digital products, services and experiences

IDC Digital Business FutureScape 2023

Digital Spend ($)

Share of revenues from traditional business model

Share of revenues from digital business model

Source: IDC Worldwide Digital Transformation Spending Guide, 2021 V2

Froto [illegible]

[illegible]GEMENT

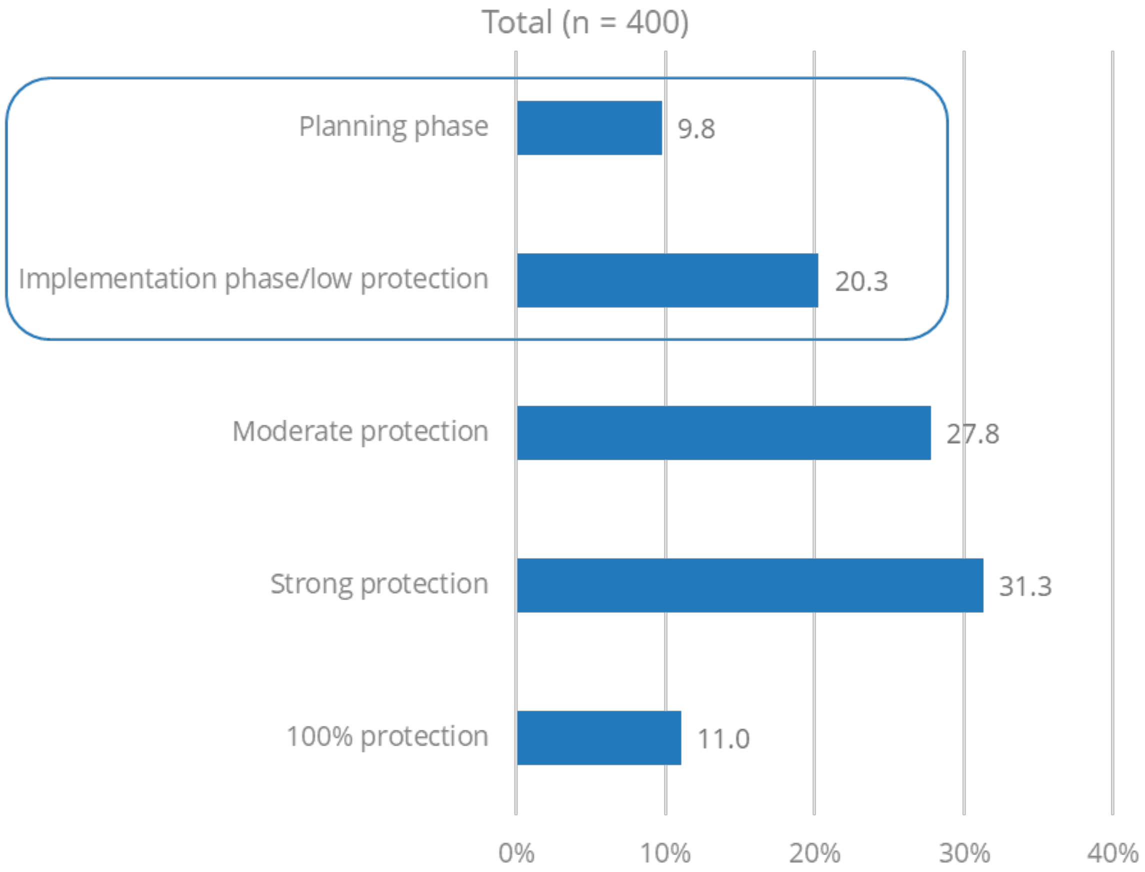
SCALE

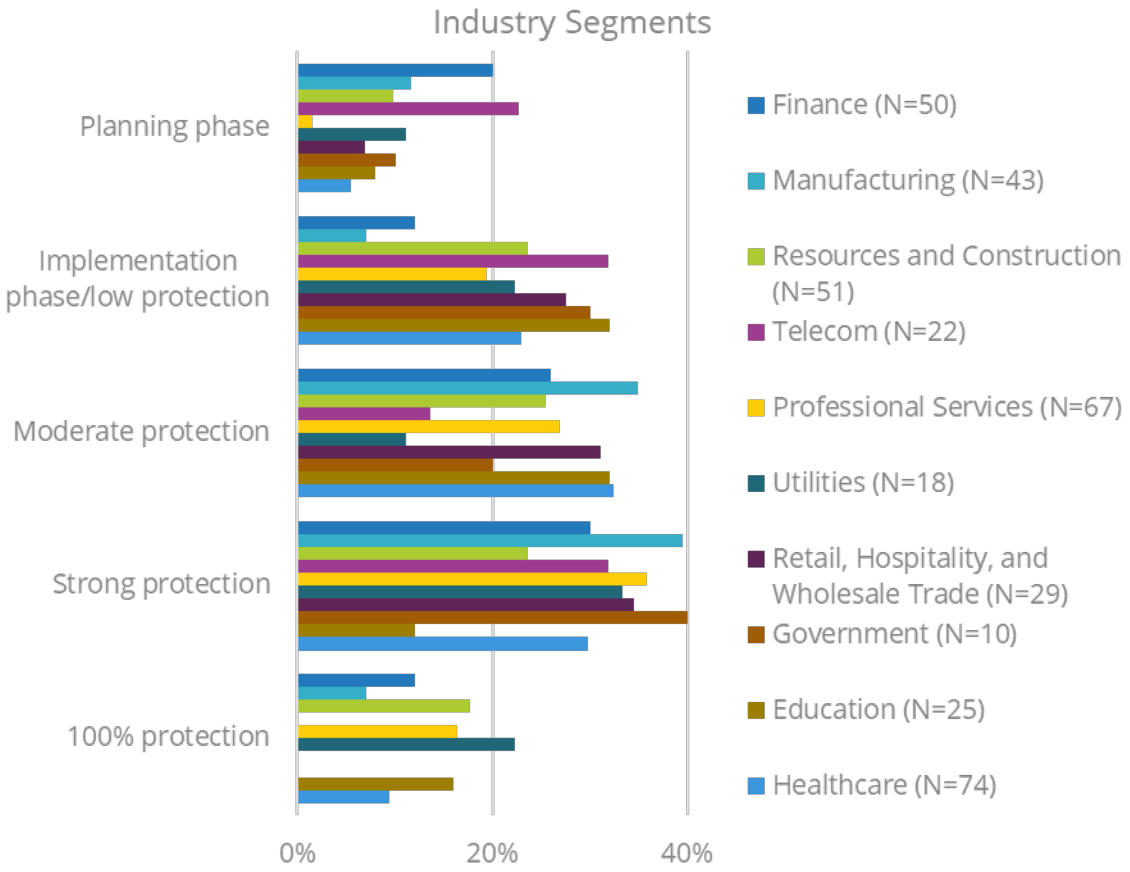
My bias

Complexity is the Enemy of Security.

30% of Organizations Identified Suboptimal Security Postures

Bad actors, some led by nation states, are now targeting organizations with mature cloud security programs. In light of this, how would you rate your organization's security posture readiness?

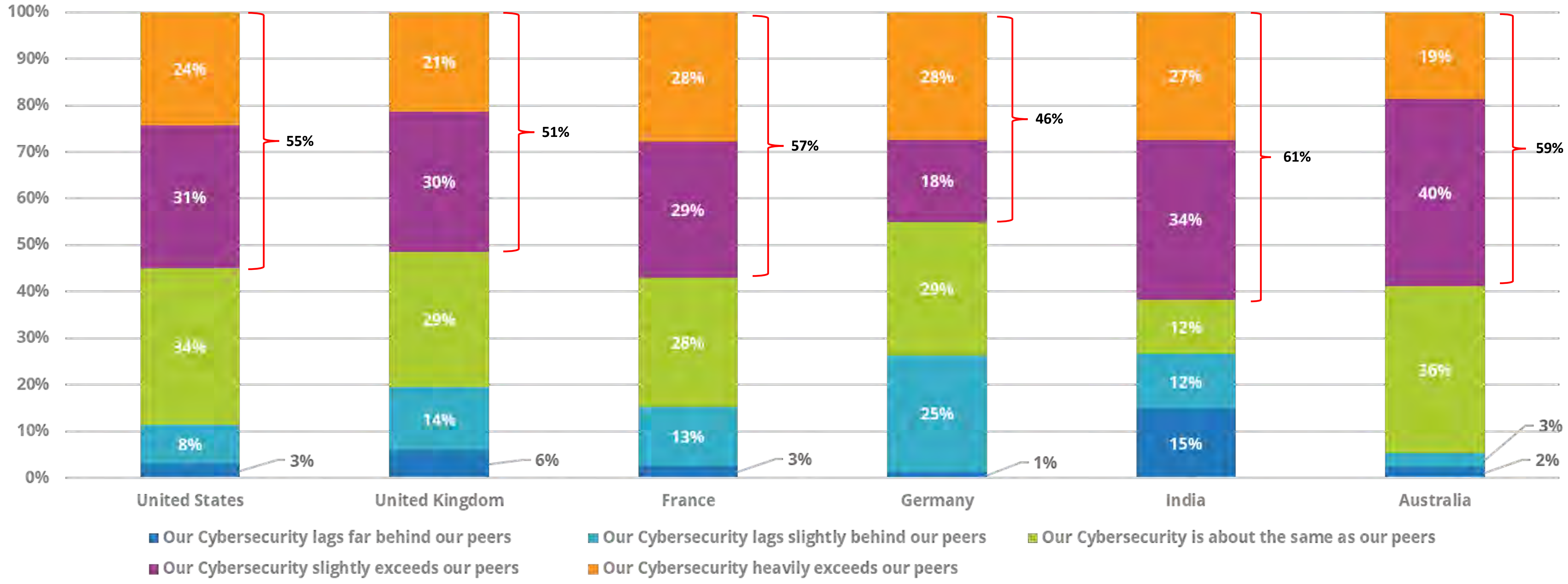




Base=All Respondents; Notes: Managed by IDC's Global Primary Research Group.; Data Not Weighted; Use caution when interpreting small sample sizes.
Source: US Cloud Security Survey, IDC, December, 2022

Most organizations around the world are optimistic that their cybersecurity programs exceed their peers.

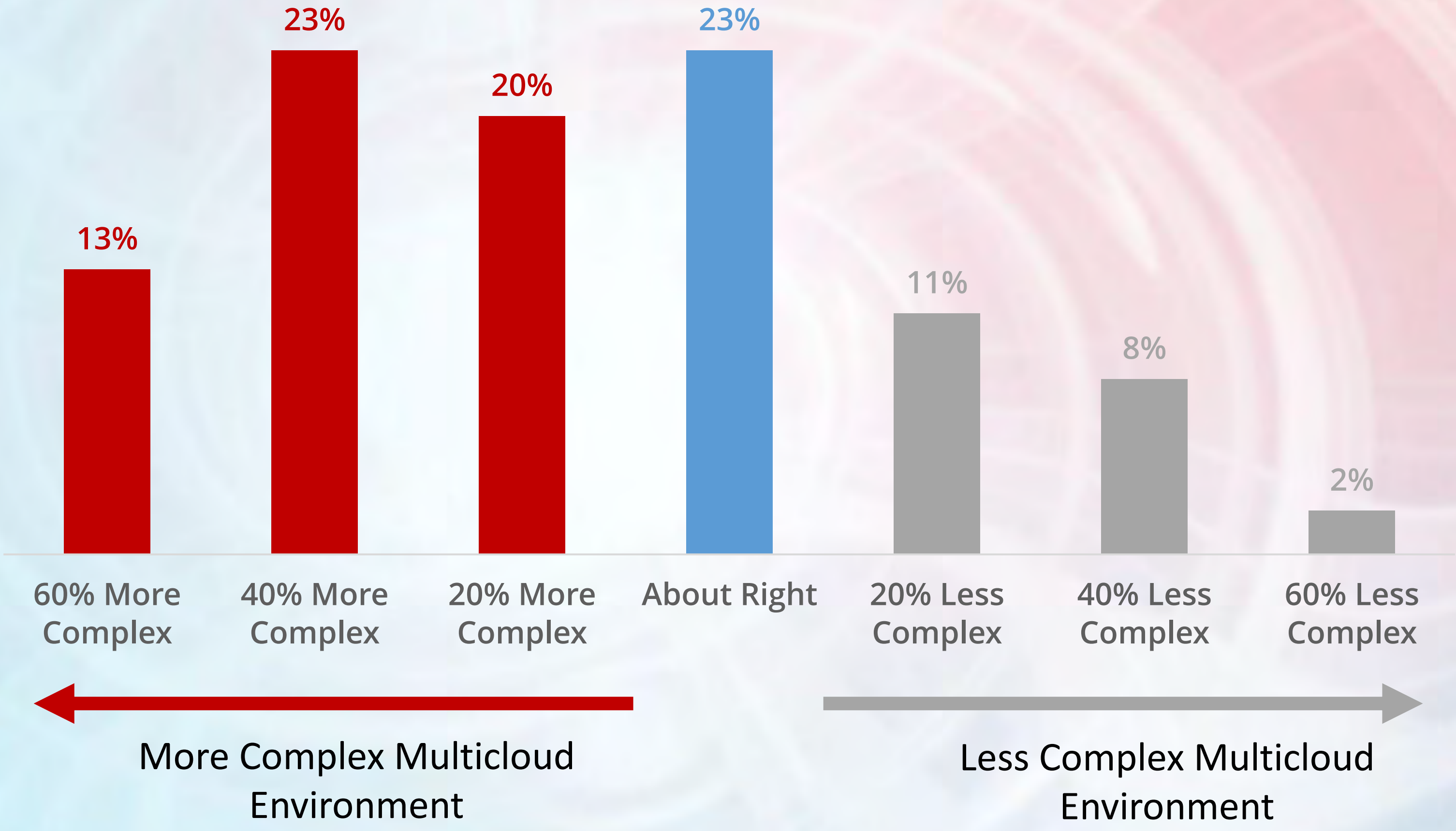
Q: How do you think your company's Cybersecurity compares with peers?



n = 819

Source: Cyber Risk Management Survey, IDC, July, 2022

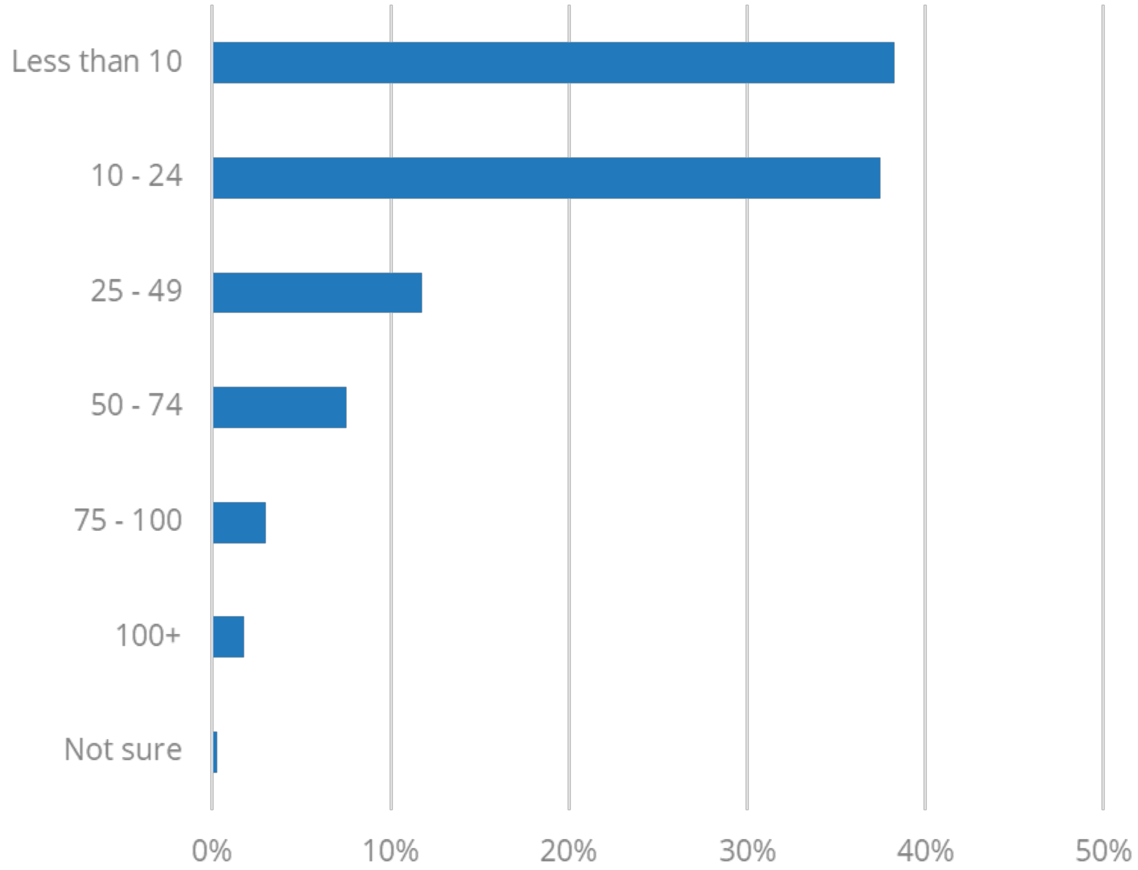
56% of organizations have a more complex multicloud environment than expected



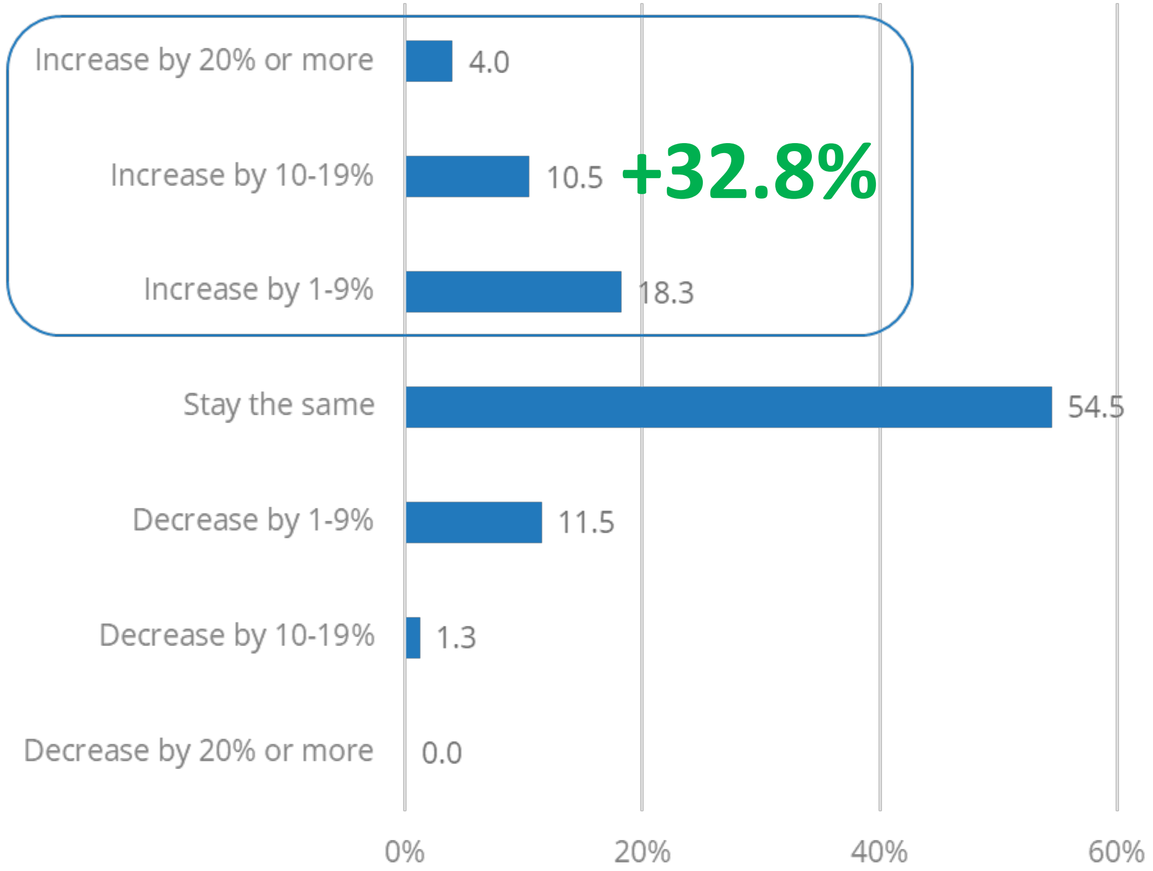
Source: Security ServicesView, February 2022 , IDC

Yet, as Cloud Complexity Grows, so do the Platform Tools

How many cloud security tools does your organization currently use?



How do you expect the number of security tools used by your organization to change in 2023?



n = 400; Base=All Respondents; Notes: Managed by IDC's Global Primary Research Group.; Data Not Weighted; Use caution when interpreting small sample sizes.
Source: US Cloud Security Survey, IDC, December, 2022

Layer 0 creates nontechnical issues to manage.

We are dealing with new tech buyers

LOB Buyer

50%

of tech spending
comes from outside IT Dept.

IDC Worldwide IT Spending Guide
Line of Business

Millennial Buyer

35%

of the global workforce

Digital CIO Buyer

Almost

1/3rd

of CIO see their role as driving innovation within the business.

IDC 2019 CIO Sentiment Study

Layer 0 creates nontechnical issues to manage.

A Security Product may serve multiple users
Example: Cloud Security Posture Management Personas

Application Developer

Requirements

Validate open-source dependencies & code

Seamlessly integrate security & security tools into the IDE and CI/CD pipeline without impacting velocity

Automated checks for vulnerabilities at dev, deploy & production (and maybe runtime)

Implement and bridge security requirements

Cloud-Native AppSec Practitioner

Requirements

Validation of vulnerability exposure at deployment and production

Verification of baseline integrity

Creation of asset taxonomy/tagging

Leadership of compliance initiatives

Prioritize and alert based on severity

Cloud Operations

Requirements

Validation of runtime vulnerability exposure

Control Configurations, set cloud policies

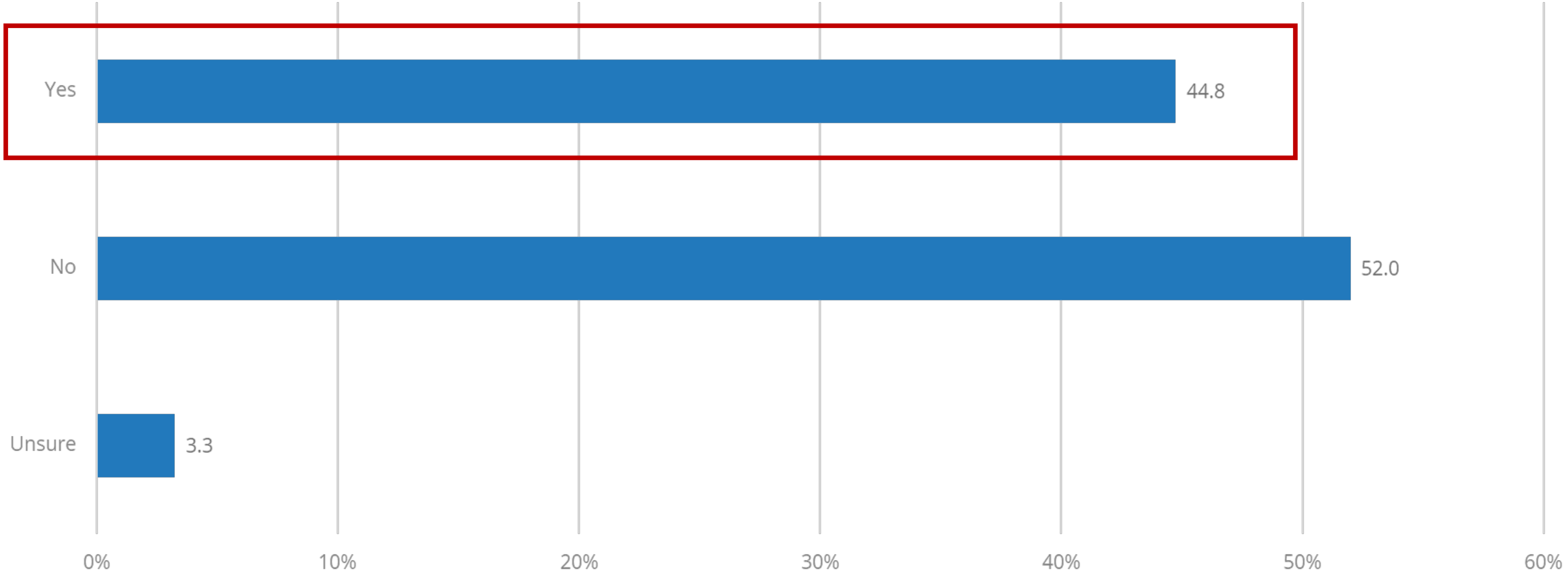
Ensure ability to collect compliance data

Observe and alert but don’t break

Shift Left

Layer 0 creates nontechnical issues to manage.
Resource Consumption, Siloed Teams/Organizational Friction or Something Else?

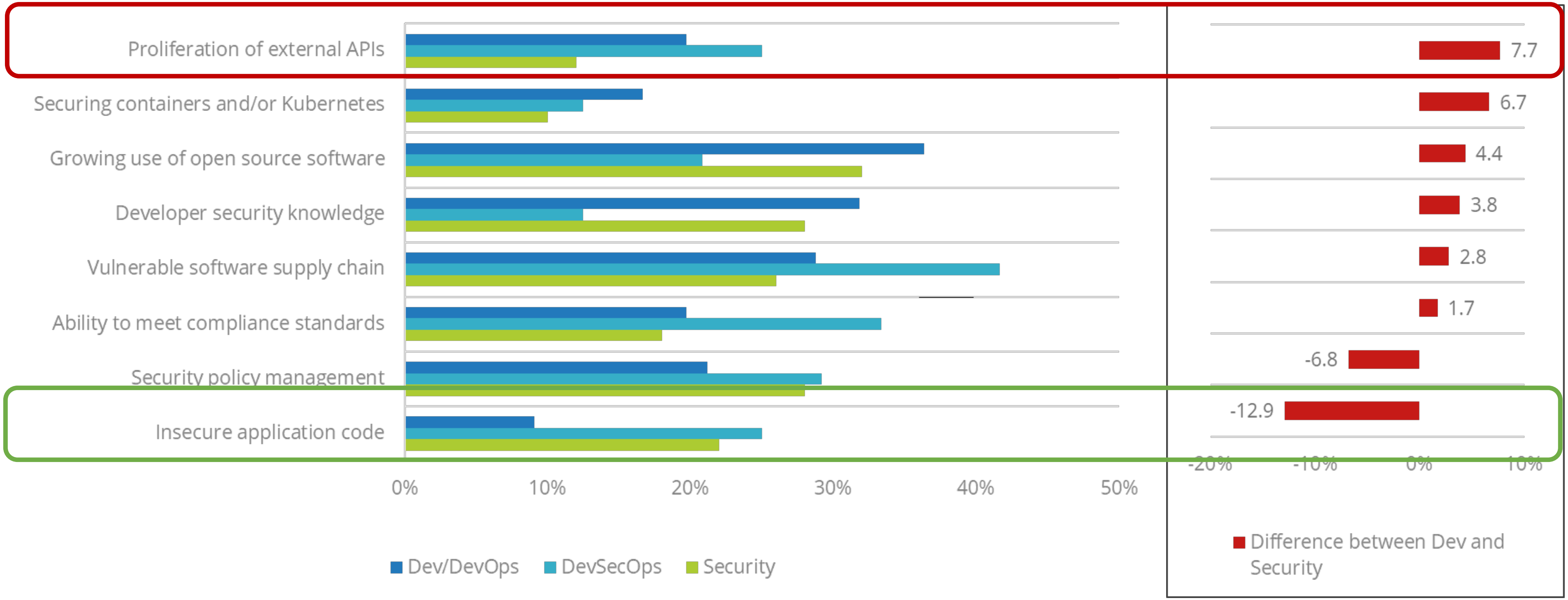
Do your app dev teams forbid the use of an agent to implement Cloud Workload Security?



n = 400; Base=Respondents indicated cloud/cloud workload security providers; Notes: Managed by IDC's Global Primary Research Group.; Data Not Weighted; Use caution when interpreting small sample sizes. Source: US Cloud Security Survey, IDC, December, 2022

Security is significantly more concerned with insecurity of application code. The proliferation of external APIs is a larger worry for Dev/DevOps. They both feel more susceptible by the growing use of open source software.

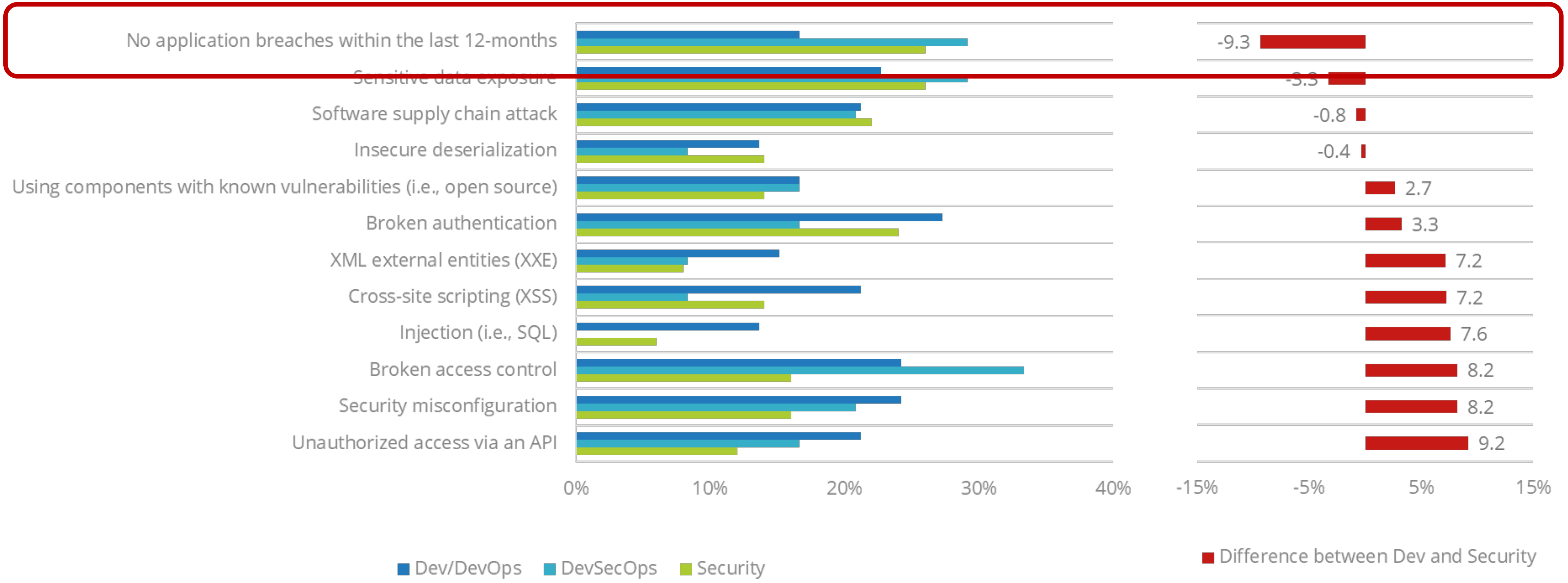
What do you currently consider to be your two biggest application security gaps or exposures?



Dev/DevOps n = 66, DevSecOps n = 24, Security n = 50 QA10 Table 18
Source: U.S. DevSecOps Adoption Survey, IDC, January 2023

Overall, Dev/DevOps acknowledge many more application breaches than Security, making it appear that they may remediate application breaches without sharing information with Security.

What types of application security breaches have you experienced within the last 12-months?



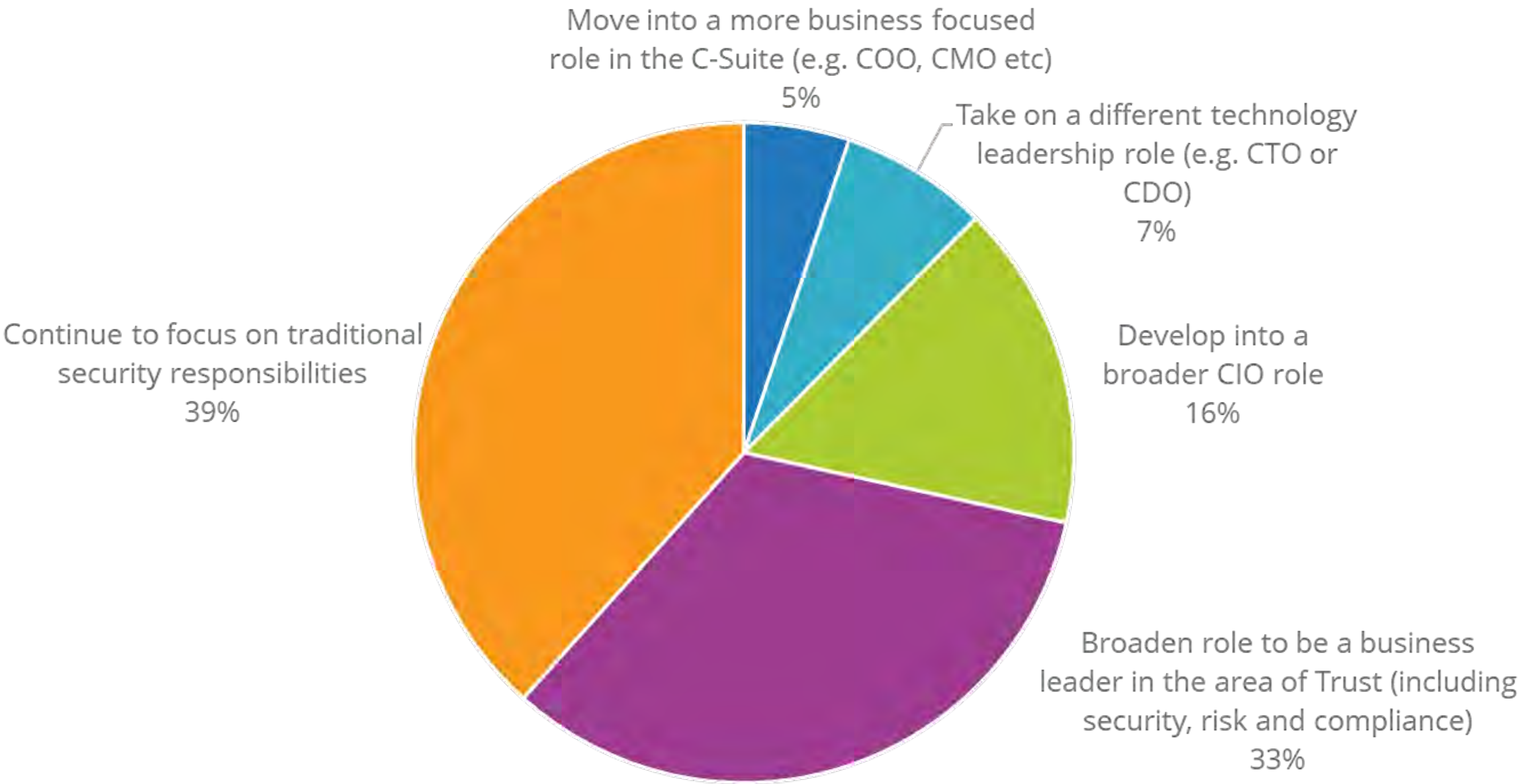
Dev/DevOps n = 66, DevSecOps n = 24, Security n = 50 QB3 Table 30
Source: U.S. DevSecOps Adoption Survey, IDC, January 2023

IDC Survey Spotlight

Does a CISO need to worry about the goals of the business or just focus on security?

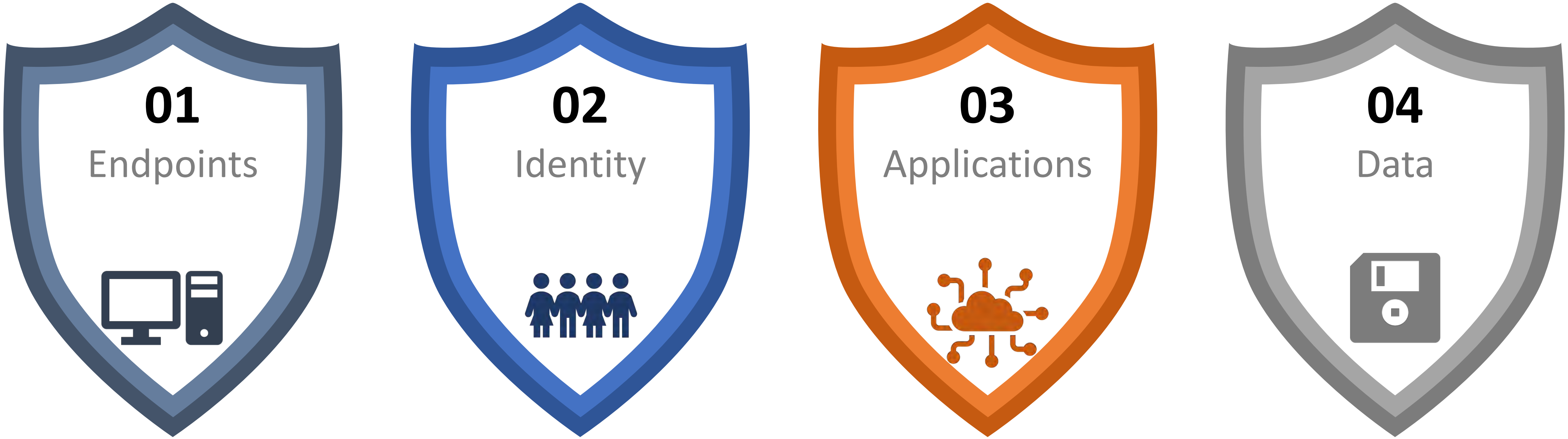
Frank Dickson

What is the most important way you see your role evolving over the next 12-24 months?



IDC #US51249523 (September 2023)
Source: WW C-Suite Tech Survey, IDC, August, 2023, n = 89

The new four central control points of Digital Transformation as network- and perimeter-centric security measures become more permeable.



01 Endpoints

02 Identity

03 Applications

04 Data

Endpoints

A dark internet will require a security presence at key termination points. In addition, endpoints are the source of most productive activity and also the most common first stop in an attack. Endpoints provide key telemetry data for analysis and detection.

Identity

Digital transformation means a higher level of connectivity between applications and business processes with the aim of increasing business agility. Things that were once not connected are now connected. The goal is to integrate trust into the "machine." In such a context, ***identity becomes the new perimeter.***

Applications

As applications are increasingly disassociated from specifically defined servers, networks, and infrastructure, network-centric security measures are increasingly ineffective; the only way to compensate is to apply security at the application. For security applications, ***Layer 7 is the new Layer 3.***

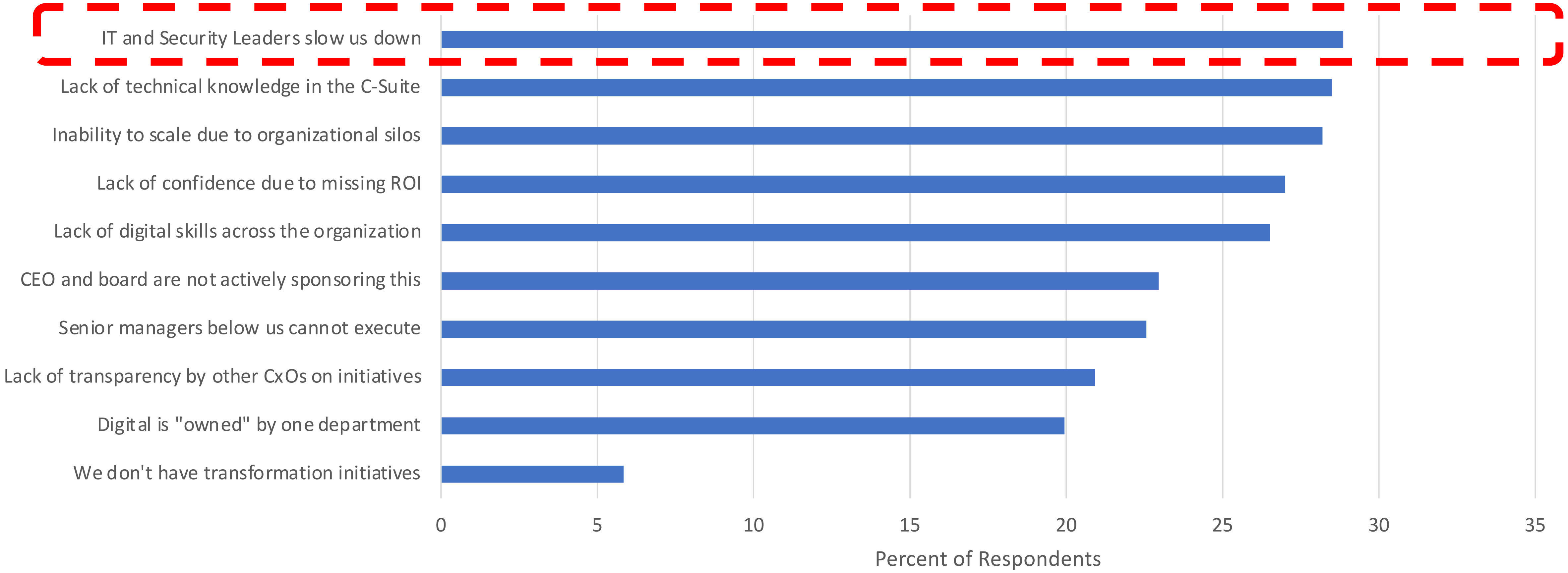
Data

Data is the fuel of the DX machine; data is also the hacker's bounty of choice. Security measures that travel with the data can dramatically improve the integrity of the DX activity. ***Prioritizing protection while retaining sufficient usability is the new paradigm of enterprise defense.***

Source: March 2019, IDC #US44938819

Worldwide Top 5 C-Suite hurdles to digital initiatives

What are the most serious hurdles to completing digital initiatives in your organization?



n = 858

Source: WW C-Suite Tech Survey, IDC, August 2022

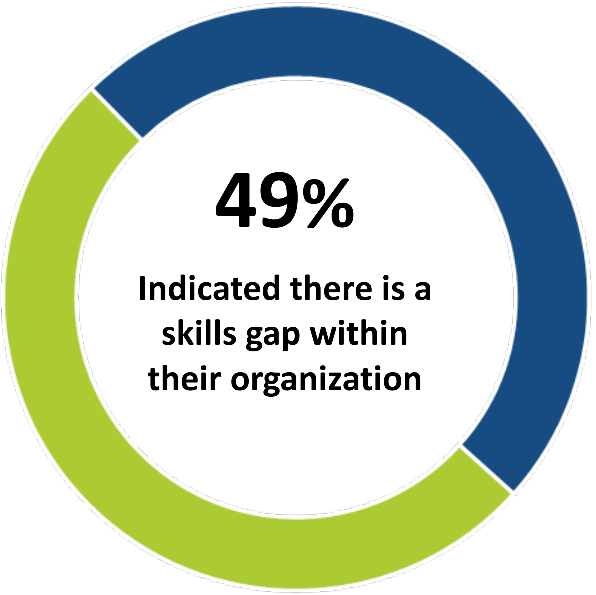
Cybersecurity Challenges in 2024

Digital First & Layer 0

Staff Shortage

Talent Shortage is a Global Phenomenon

Q. Is there a security skills gap within your organization?

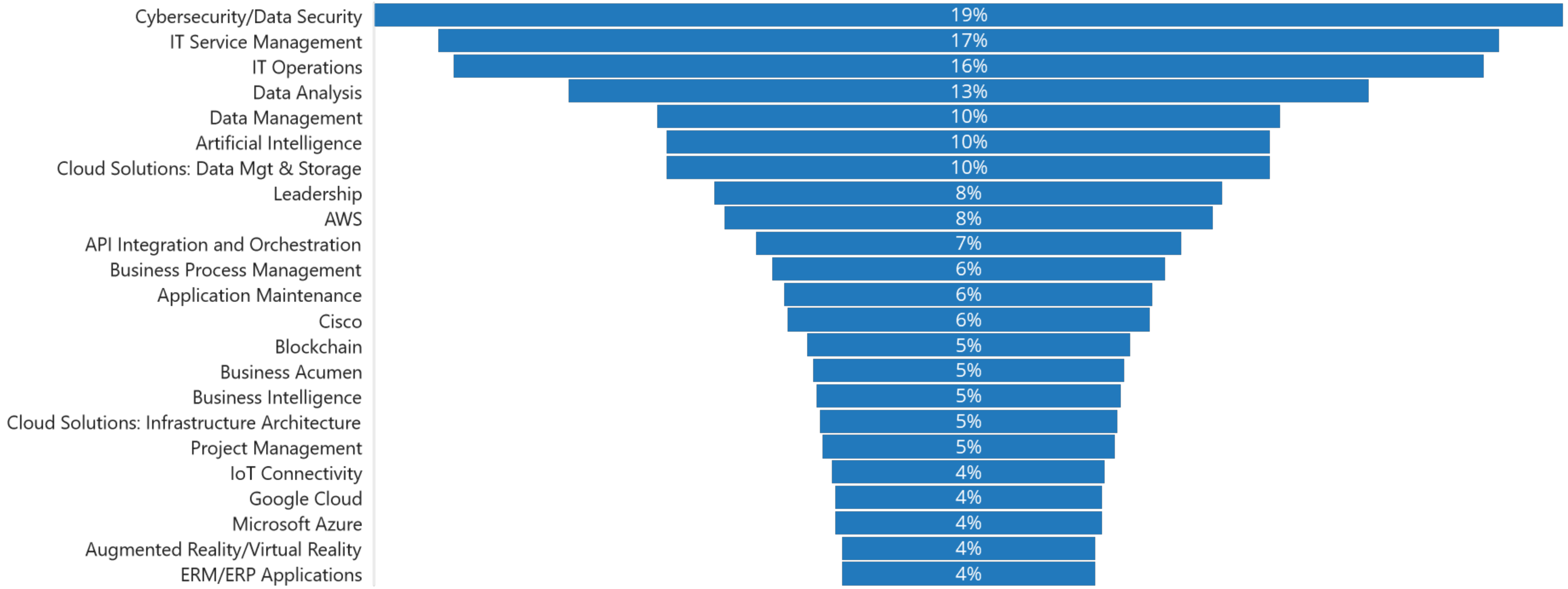


Skill shortage drives the need for managed services/ as-a-service where security services vendors have the right skills, expertise, and experiences.

n=1,500
Source: IDC's Security ServicesView, February 2022

Consider Future Skills – Peer Data

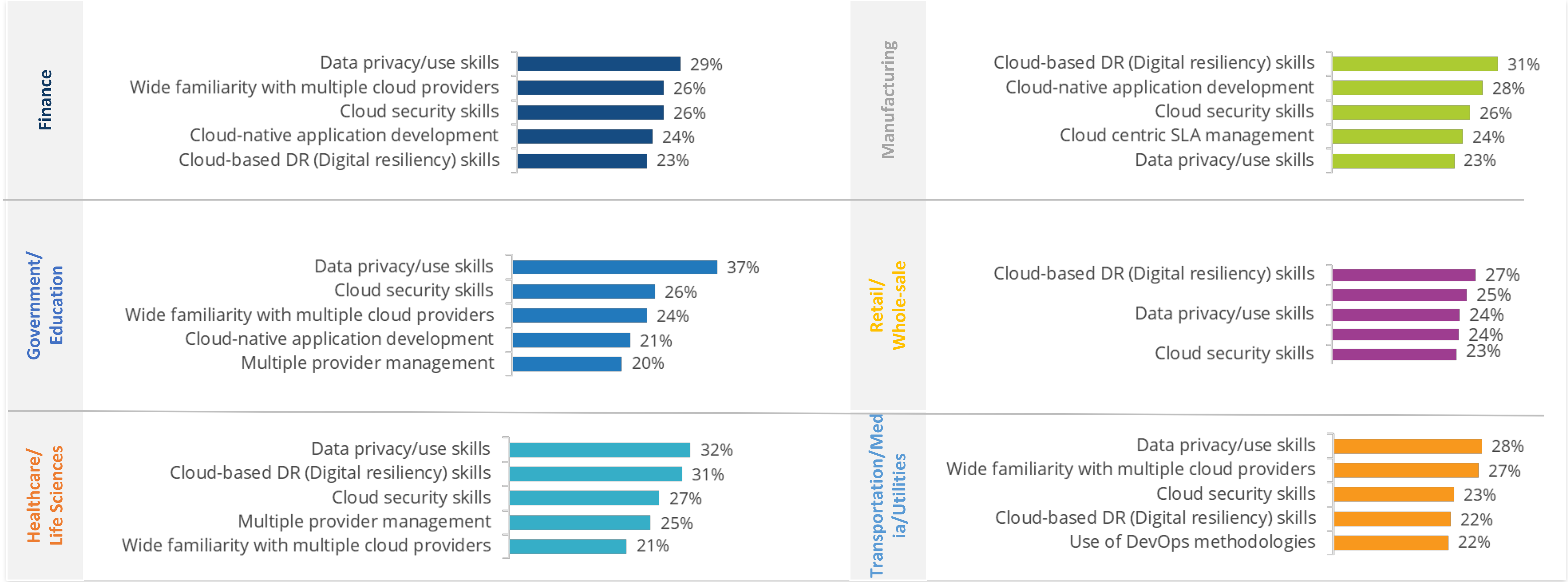
Q. Of those IT skills you said were most important, which skill do you consider to be the most important?



IDC Survey Spotlight: *What IT Skills Are Most Important to Enterprise Leaders Worldwide?* Doc #US48510622
Source: IDC 2022 IT Skills Survey, July 2022, n = 1,820

Skills Gaps by Sector: Data Privacy Is Most Important for Government Companies, While Cloud Security Is Critical for Professional Services

What are the operational skills your organization will most need to develop in its own IT and development teams in the next two years to take full advantage of your cloud platform approach?



Top 5 Boxes

Source: Future Enterprise Resiliency & Spending Survey - Wave 6, IDC, July 2022, n = 816 and Wave 5, June 2022, n = 832
IDC Tech Buyer Presentation: IDC State of Global Skills, Doc #US49747822

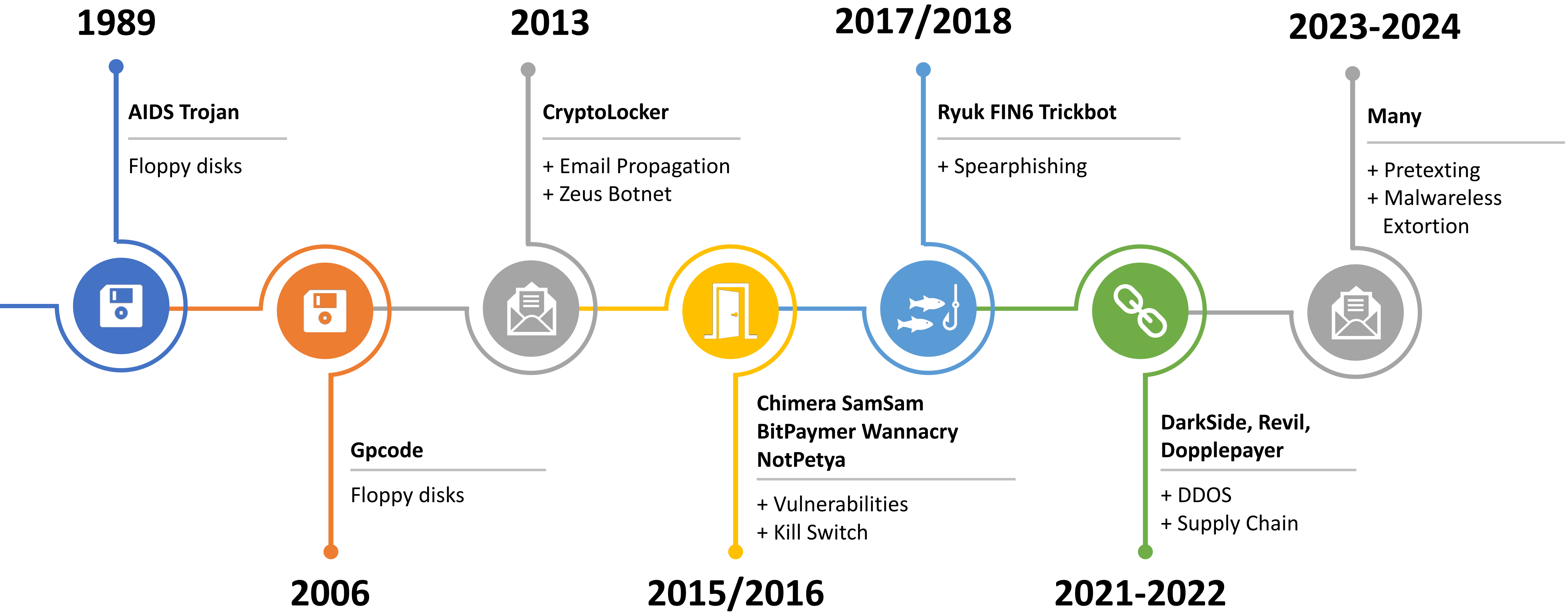
Cybersecurity Challenges in 2024

Digital First & Layer 0

Staff Shortage

Threat Landscape

History of Things Getting Progressively More Targeted



1989

AIDS Trojan

Floppy disks

2006

Gpcode

Floppy disks

2013

CryptoLocker

+ Email Propagation
+ Zeus Botnet

2015/2016

Chimera SamSam BitPaymer Wannacry NotPetya

+ Vulnerabilities
+ Kill Switch

2017/2018

Ryuk FIN6 Trickbot

+ Spearphishing

2021-2022

DarkSide, Revil, Dopplepayer

+ DDOS
+ Supply Chain

2023-2024

Many

+ Pretexting
+ Malwareless Extortion

Why is Ransomware Such an Issue? Isn't Ransomware Straightforward?

What is Ransomware?

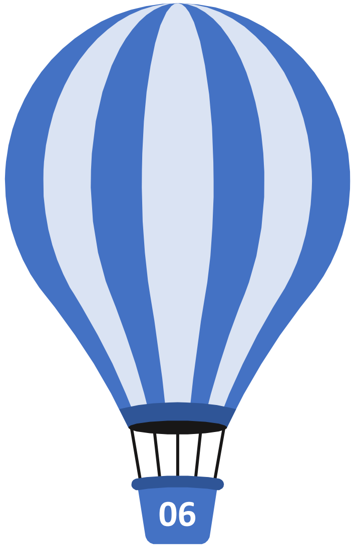
1 is a type of malware

2 from crypto virology that encrypts the victim's files

3 making files inaccessible

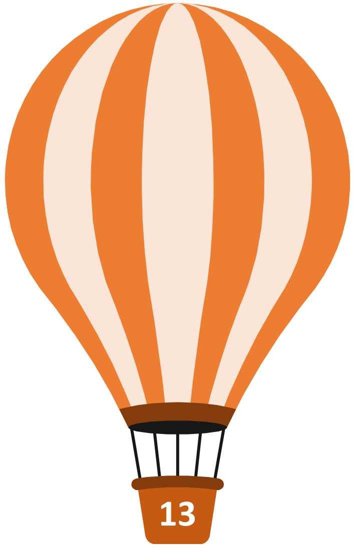
4 and demands a ransom payment to decrypt them

Growing Sophistication Driven Higher by Profit Motive
Don’t Fear Ransomware: Fear the Attacker!



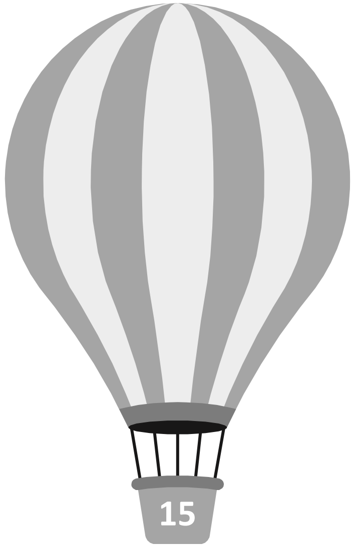
$100–$200

660-bit RSA public key



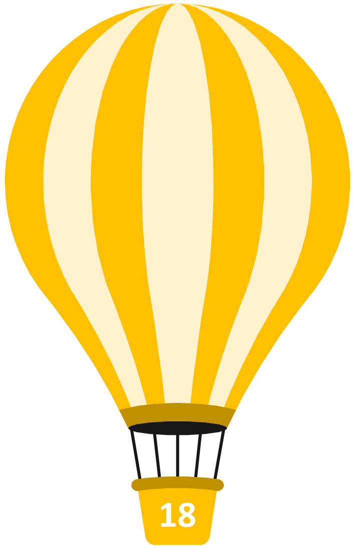
< 1000 USD

- C&C
- Encryption
- Cryptocurrency



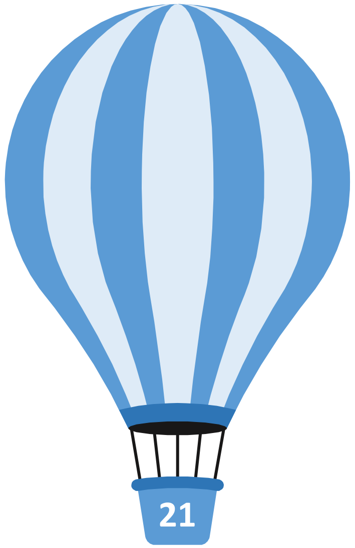
$40K–$60K

- Lateral movement
- Privilege escalation
- Deep lock MBR Update



$100K ‘s

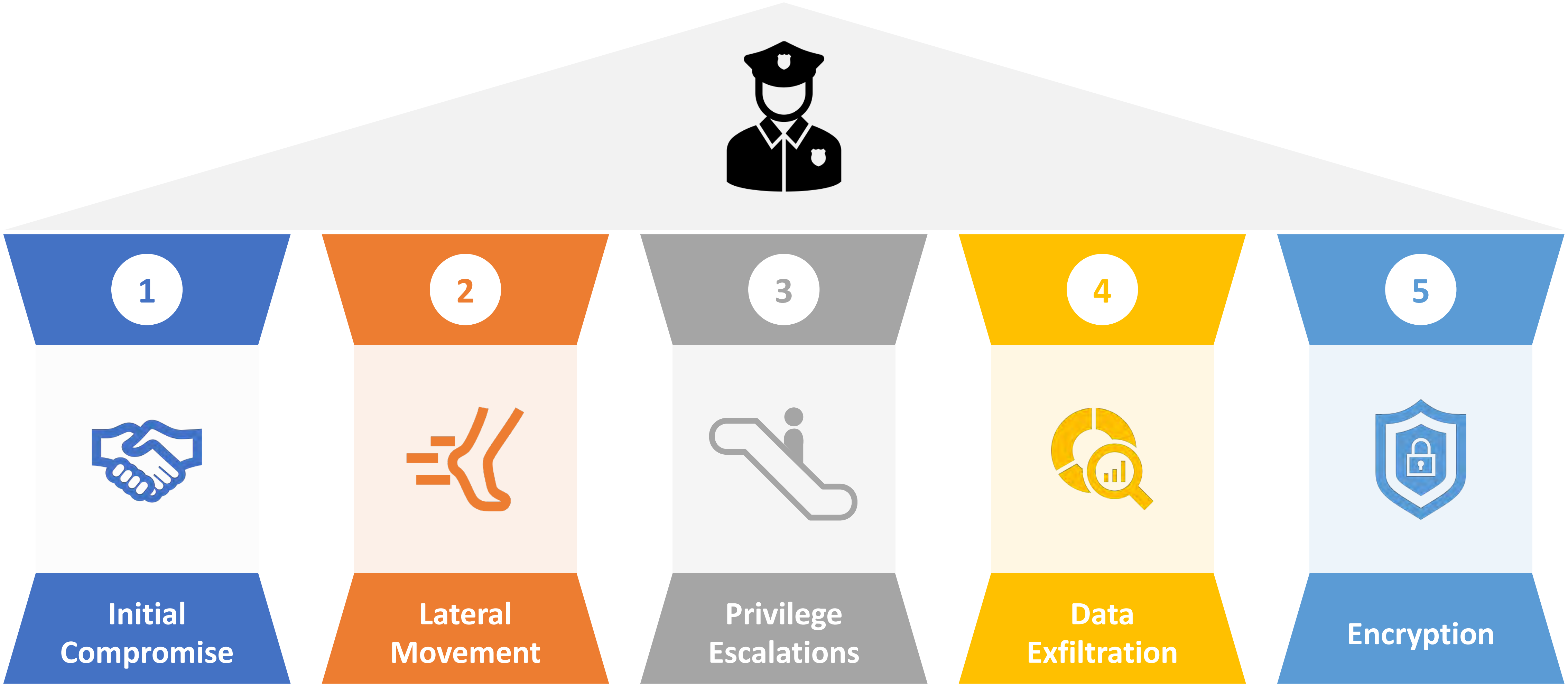
- Ransomware as a service
- Evasion
- Modify Services
- Backdoor
- Identity theft
- Encryption



$Millions

- Multi Faceted Extortion
- Calling Media
- Data theft
- Shaming
- Vertical targeting

5 Opportunities to Defend Against the Ransomware Attacker



1 Initial Compromise

2 Lateral Movement

3 Privilege Escalations

4 Data Exfiltration

5 Encryption

Cybersecurity Challenges in 2024

Digital First & Layer 0

Staff Shortage

Threat Landscape

Compliance

Cyber Threats and Keeping Up With the Regulations That Are Supposed to Help to Keep Us Safer, Are Top of Mind to CEOs

Q4. Of the following political, social, and economic risks, which 3 do you expect will have the greatest impact on your business?

Top 3 Risks Impacting Business

2022	2023	2024
1. Cyber Threats and Regulations	1. Economic Pressures	1. Cyber Threats and Regulations
2. Ensuring Health/Safety of Employees and Customers	2. Changing ESG targets and regulations	2. Addressing new data sharing
3. Operations Resiliency (e.g., supply chain risk)	3. Cyber Threats and Regulations	3. Operations Resiliency

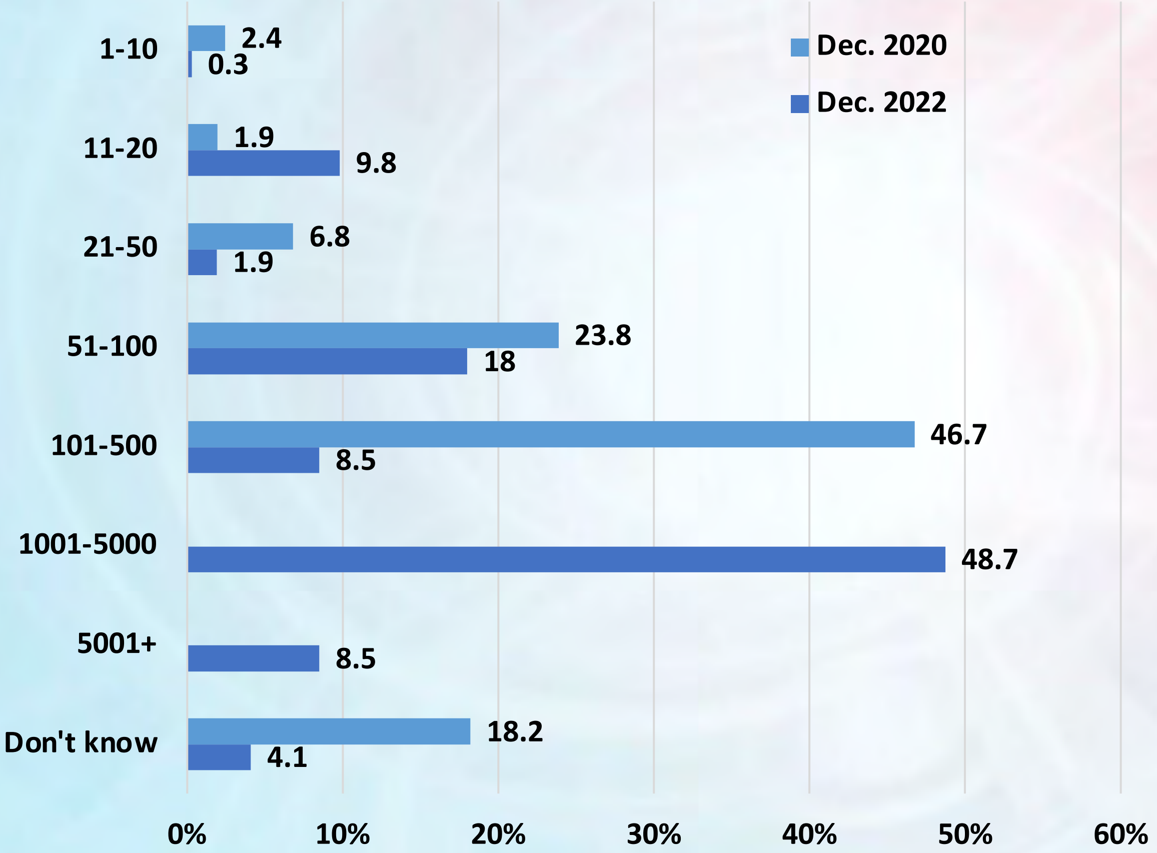
n = 389 (2022) & 395 (2023)
Source: IDC Worldwide CEO Sentiment Survey, January 2022 and IDC’s CEO Survey, February 2023

IDC Survey Spotlight

How much have Data Subject Access Requests Increased Over the Past Two Years?

Ryan O’Leary

How many Data Subject Access Requests (DSARs) does your organization receive in a month?



Source: Source: Data Protection and Privacy Survey December, 2020, N=336, Source: Data Privacy Survey, IDC, December, 2022, N=302

DSARs at a Glance

- 2020 the average organization saw 135.61 DSARs a month. In 2022 that number is now 2061.96.
- That is a 1420% increase in just 2 years.

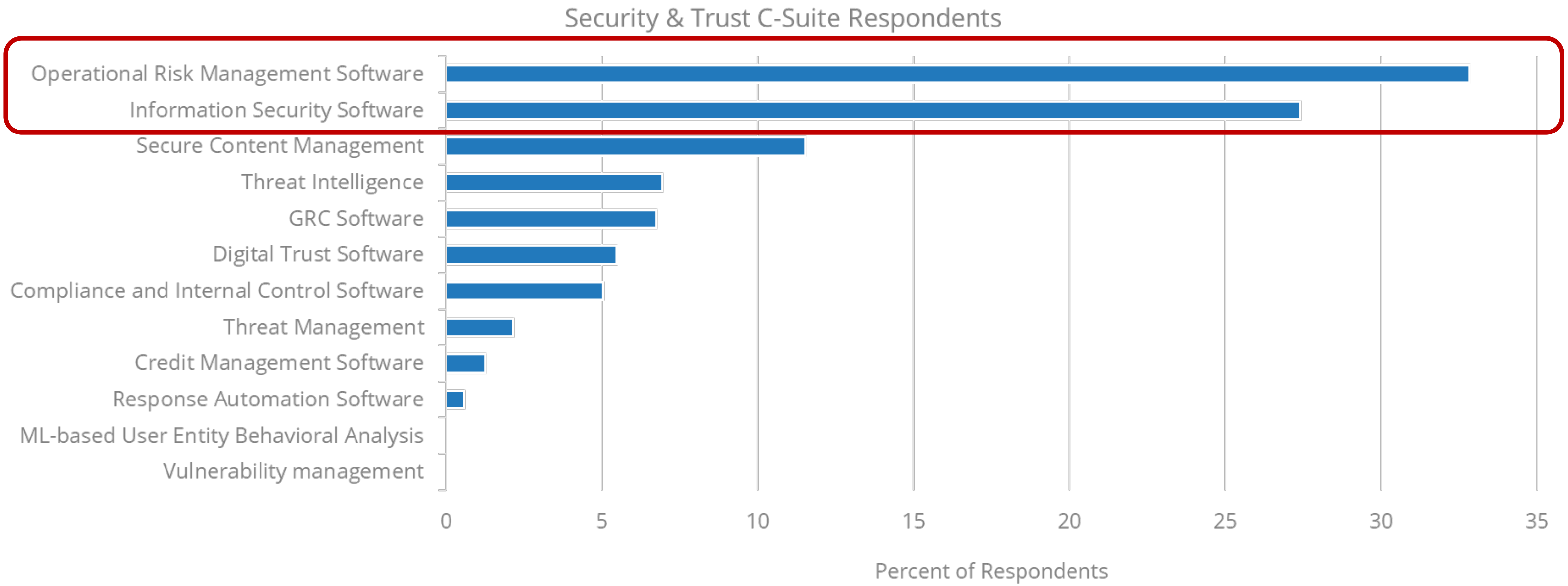
IDC Survey Spotlight

Where do the top priorities reside when planning for near-term security initiatives?

Pete Finalle

Frank Dickson

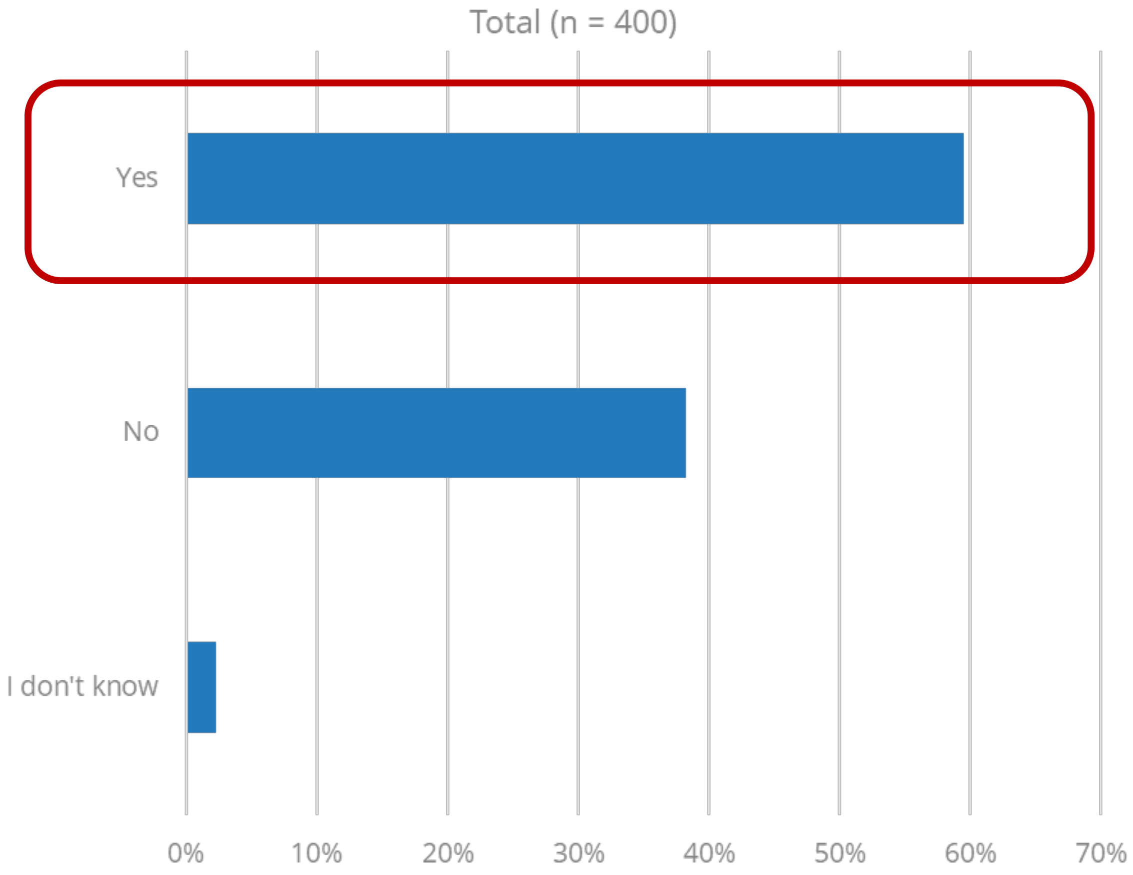
Thinking about Security (Risk / Compliance / IT Security)'s top priorities in the next 12 months, please rank the top technology initiatives in order of importance?

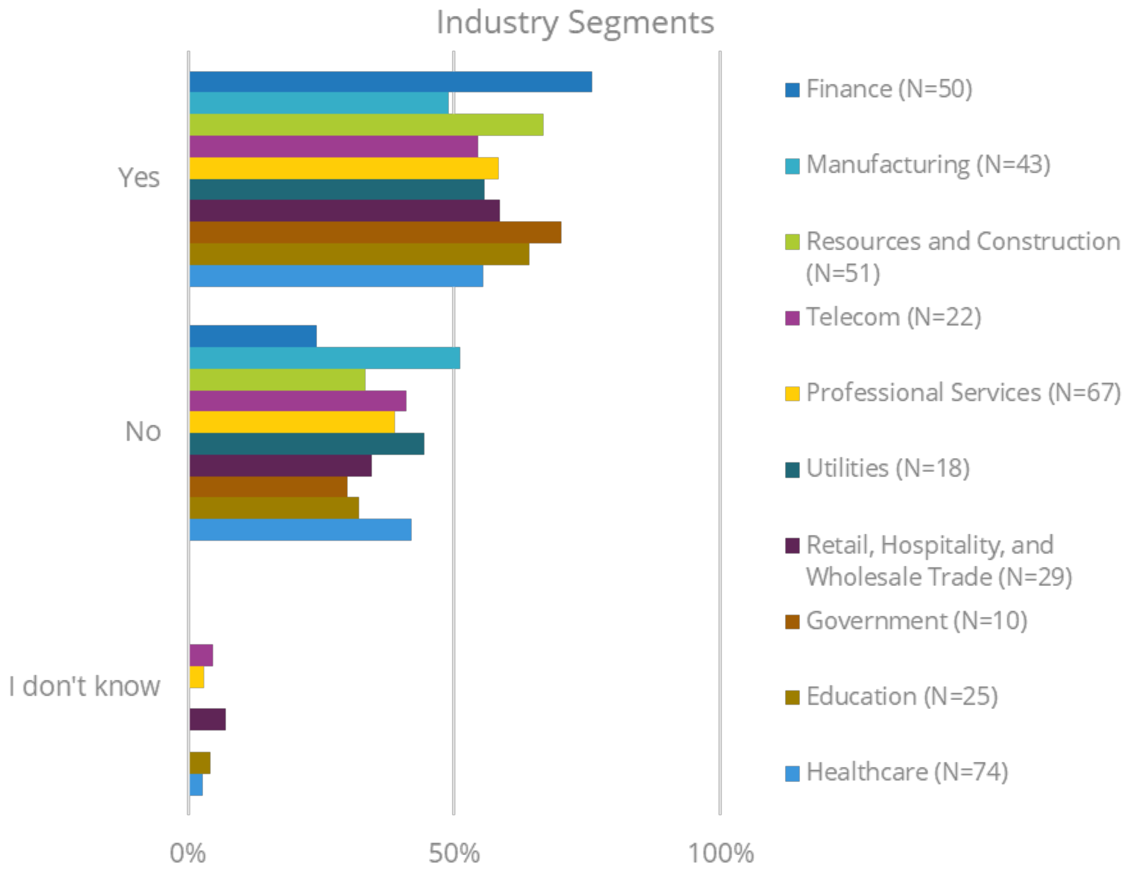


IDC #US51249423 (Sepetember 2023)
Source: WW C-Suite Tech Survey, IDC, August, 2023, n = 89

Finance, Government and Construction Industries most challenged by Data Residency/Sovereignty Requirements

Are data residency/sovereignty requirements ever a challenge for your organization?

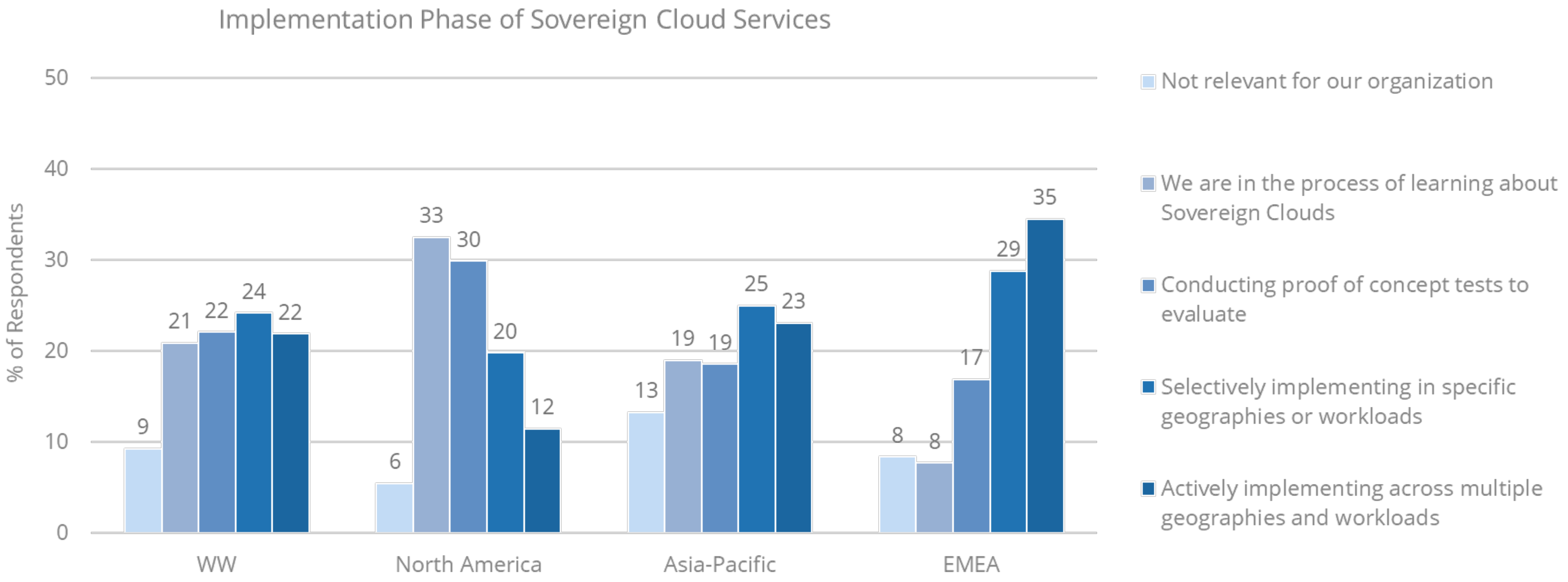




Base=All Respondents; Notes: Managed by IDC's Global Primary Research Group.; Data Not Weighted; Use caution when interpreting small sample sizes.
Source: US Cloud Security Survey, IDC, December, 2022

How prevalent are Sovereign Cloud services globally?

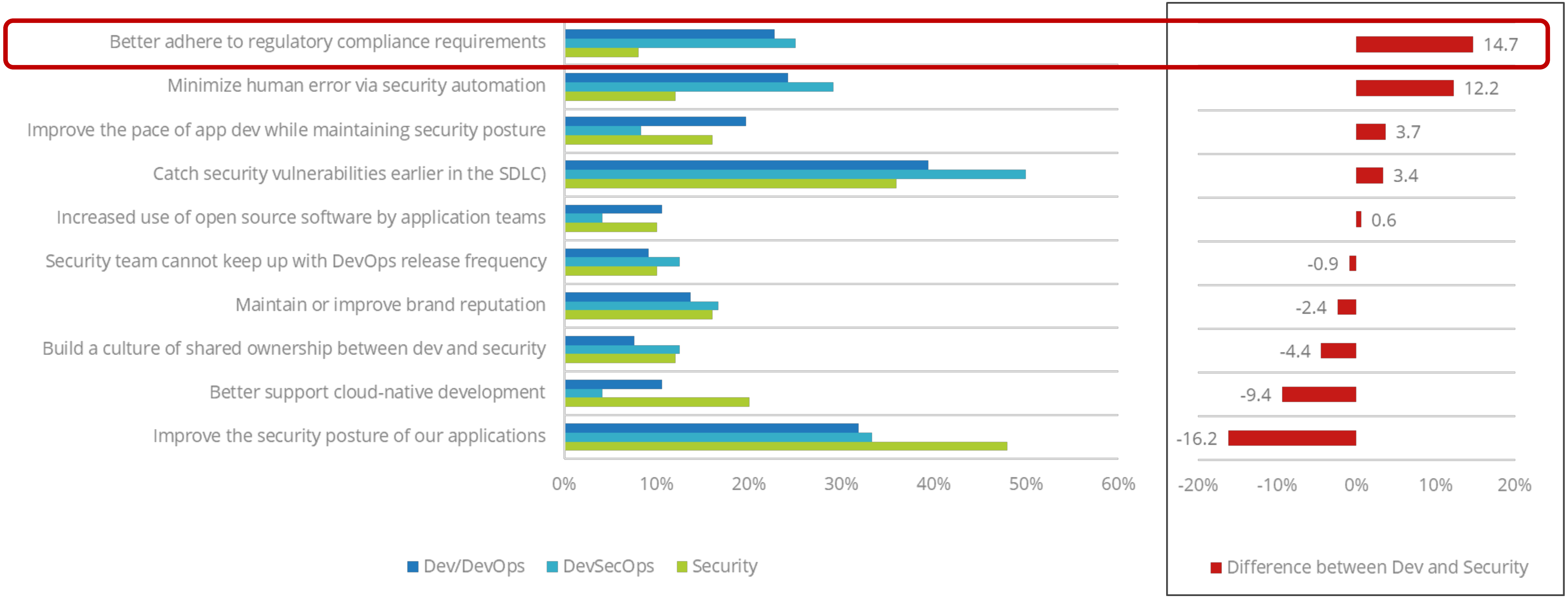
To what extent is your organization implementing Sovereign Cloud services?



Source: Future Enterprise Resiliency & Spending Survey - Wave 10, IDC, November 2022, N=824

Dev/DevOps and Security find identifying security vulnerabilities earlier in the SDLC as a driver for DevSecOps adoption. Security see improving the security posture of applications as a driver more often, and Dev/DevOps is more fixated on compliance.

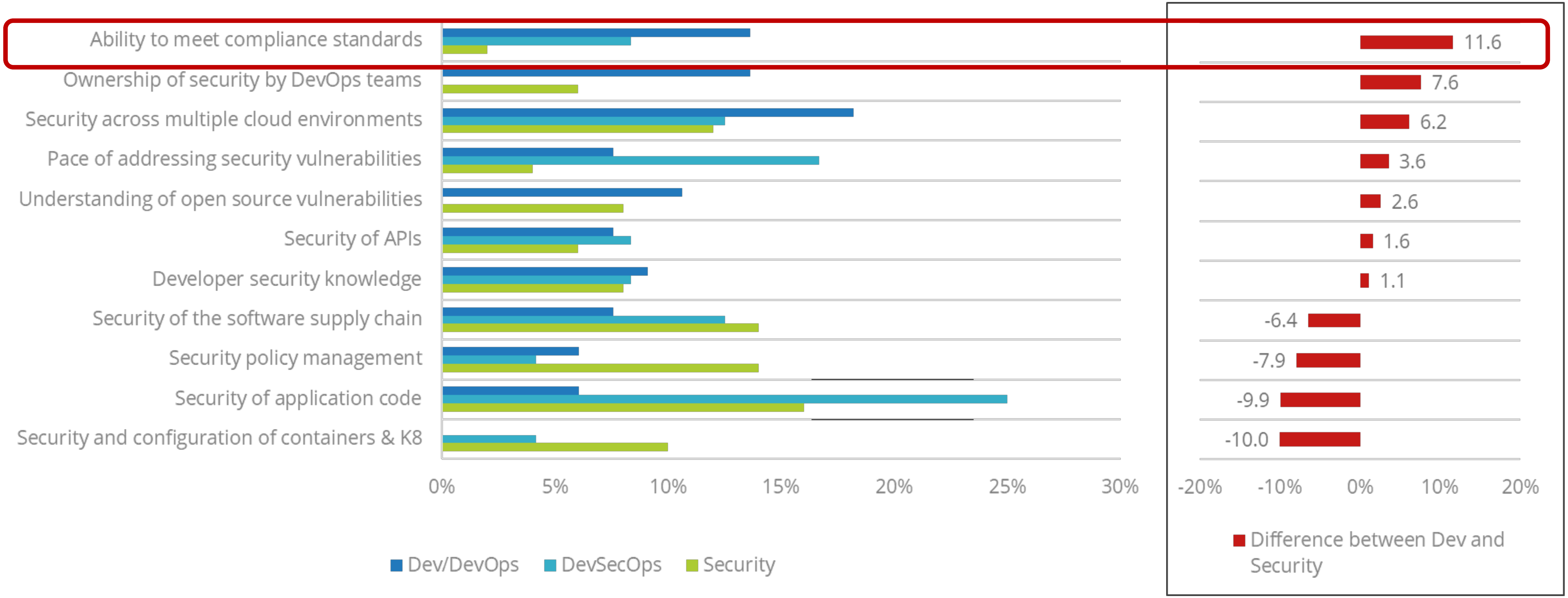
What are the top two drivers for adopting DevSecOps at your organization?



Dev/DevOps n = 66, DevSecOps n = 24, Security n = 50 QA5 Table 13
Source: U.S. DevSecOps Adoption Survey, IDC, January 2023

Dev/DevOps feels that DevSecOps addresses the risks of multicloud security, compliance, and security ownership, while Security sees it as addressing security policy management, and the security of application code and containers/K8s.

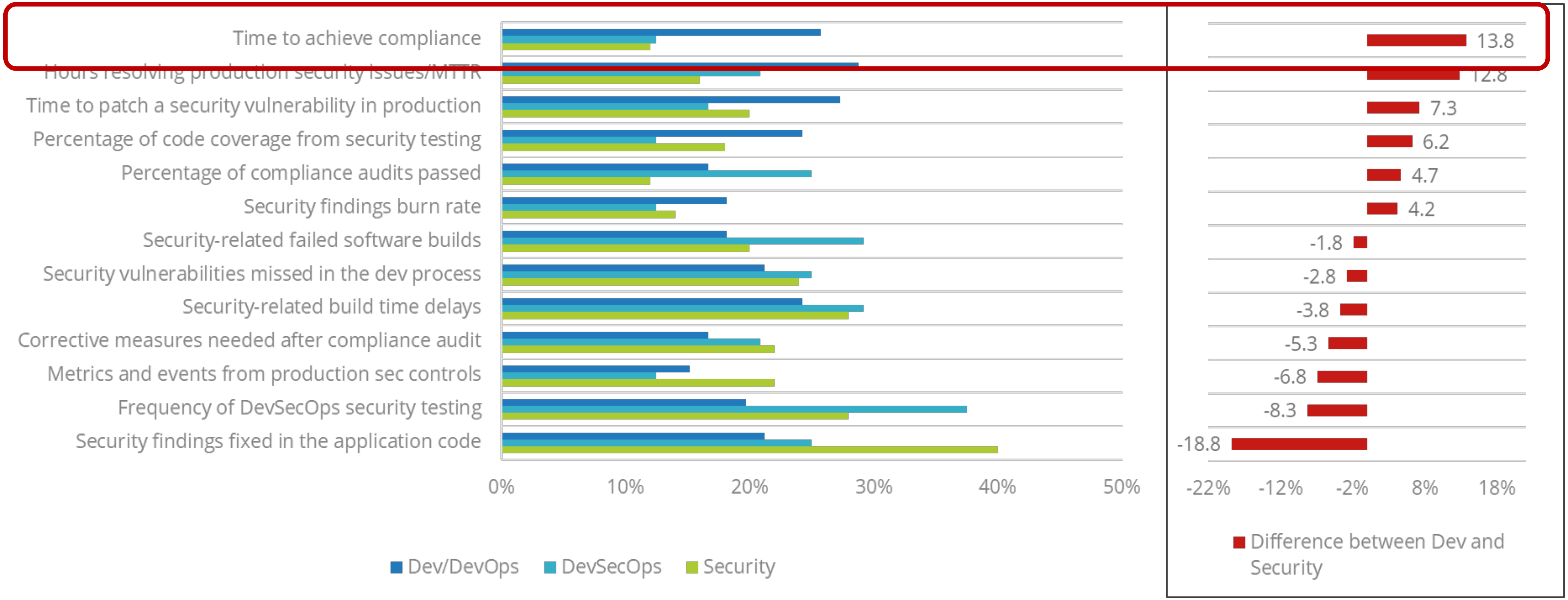
What do you consider your highest priority security risk being addressed by DevSecOps?



Dev/DevOps n = 66, DevSecOps n = 24, Security n = 50 QA6 Table 14
Source: U.S. DevSecOps Adoption Survey, IDC, January 2023

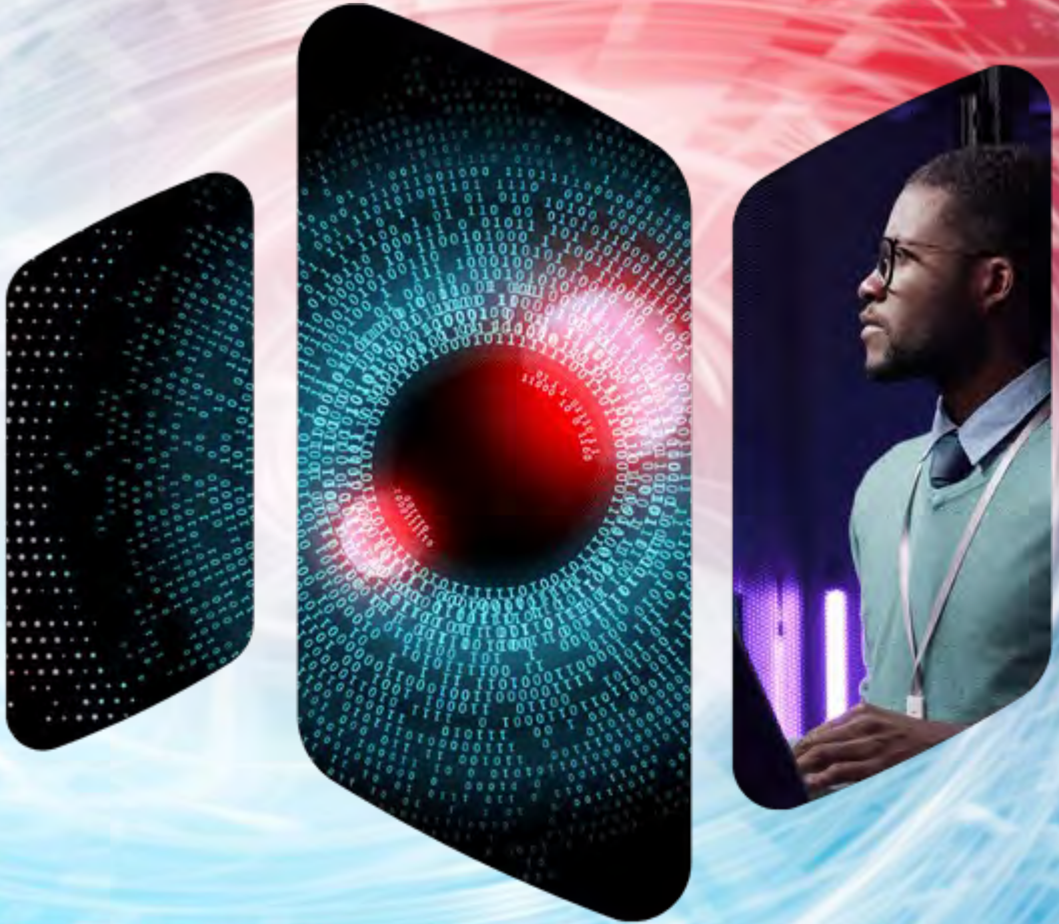
To measure the effectiveness of DevSecOps efforts, Security prioritizes measuring the number of findings fixed and the frequency of scans, whereas Dev/DevOps is more likely to look to speed of time to compliance and MTTR.

What are the top three metrics or KPIs you use to measure the effectiveness of your DevSecOps efforts?



Dev/DevOps n = 66, DevSecOps n = 24, Security n = 50 QB9 Table 39
Source: U.S. DevSecOps Adoption Survey, IDC, January 2023

Recommendations



Planning

Best Defense to Address Layer 0 Issues

Plan up front

- *Virtualization and cloud mean "Freedom" for developers. Complexity builds insecurity*
- *Simplicity over Complexity*
  - *"Rule of one."*
  - *Law of Integration*
    - *Bundle = Discount*
    - *Integration = Premium*
- *Security is becoming a Layer 0 problem*

Collaborate

- *Developers, Security, and Cloud Ops all need access to security data.*
- *Multiple tool selection is often driven by individual department evaluation processes.*

The days of after-the-fact security are over

- *Modern application development requires the ability to build security into applications. Bolt-on, after-the-fact security solutions just will not work. Security should be viewed as a continuous process rather than products. It is a journey and not a destination.*

9 Concerns that You Better Understand

Benefit

Must explain EXACTLY what you do

- Reduces mean-time-to-detect?
- Satisfies NIST 800-53 requirements?

Scability

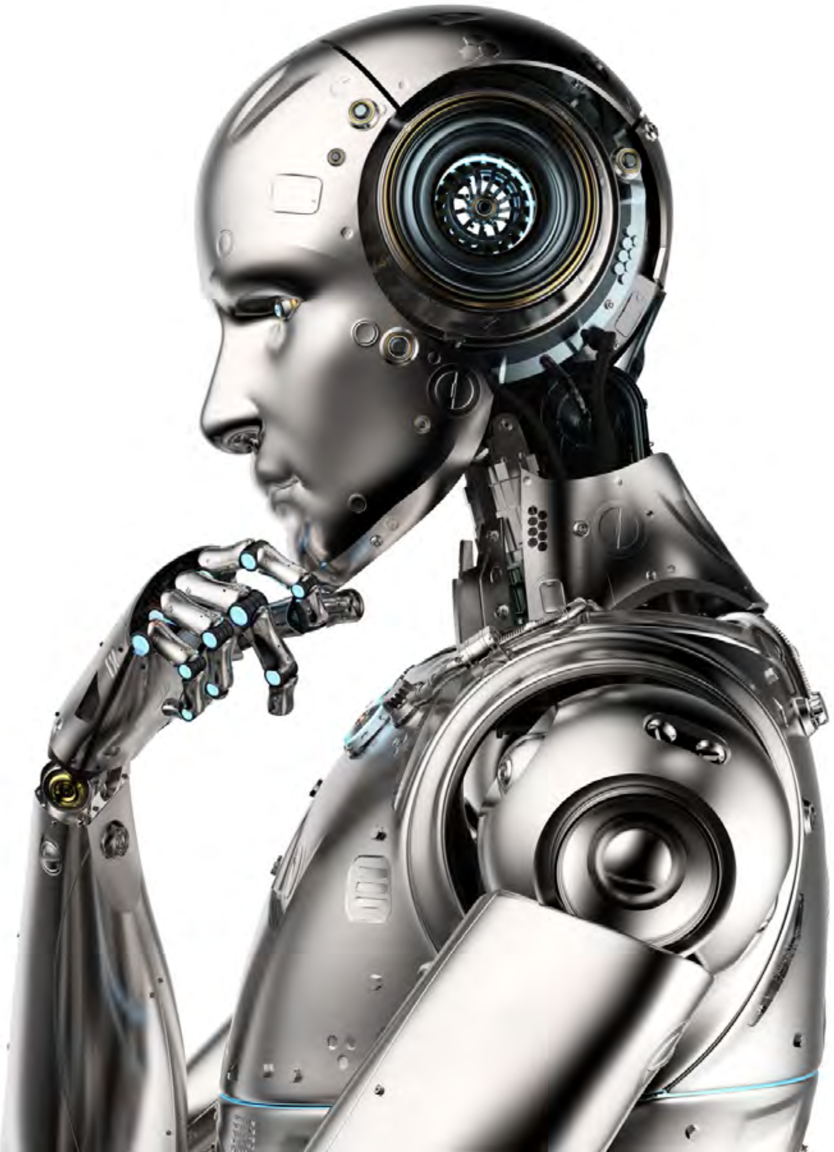
What happens at capacity?

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

Feature, Product or Platform

Integrations add unique value

Time to Value

Demonstrate ROI, defined by metrics!

- Time to detect under 1 hour?
- Payback in 4 months?

My other bias

Vendors use too many words and not enough numbers.

Qualys took my words to heart.

Business Value White Paper, sponsored by Qualys | November 2023

The Business Value of Qualys

Megan Szurley
Senior Research Analyst,
Business Value Strategy Practice, IDC

Philip D. Harris, CISSP, CCSK
Research Director,
Risk, Advisory, Management, and Privacy, IDC

How do you calculate the value customers realize?
You talk to them.

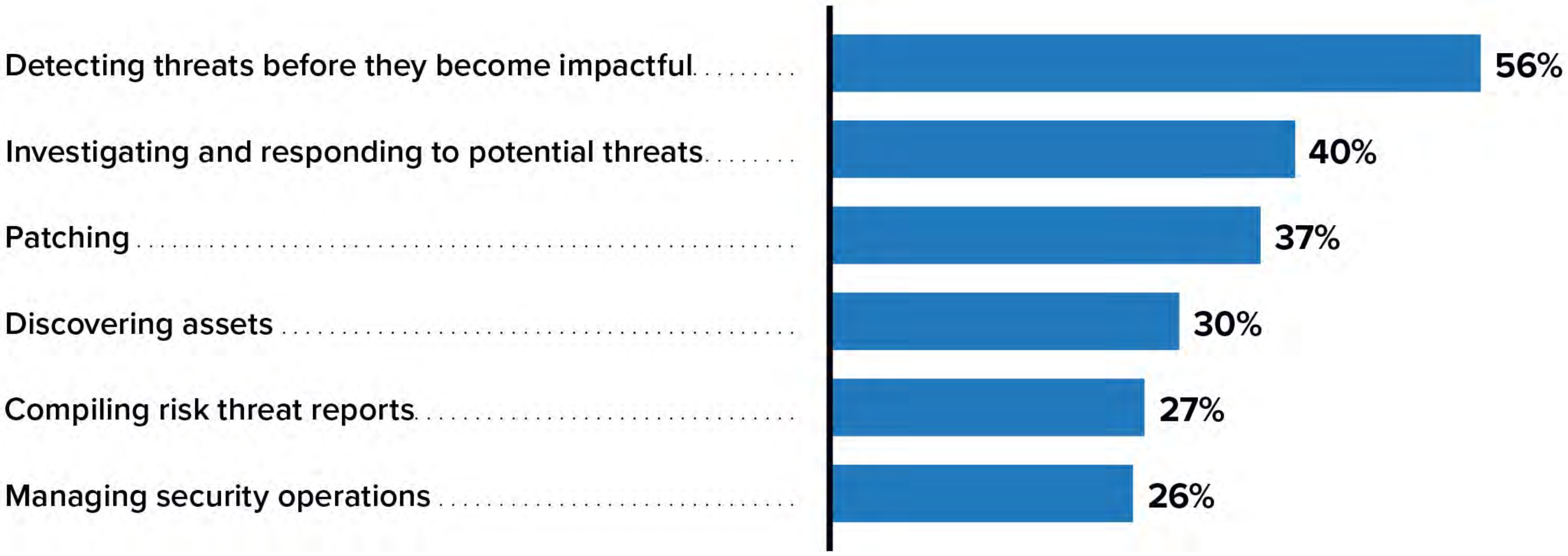
Firmographics	Average	Median	Range
Number of employees	63,319	3,550	750 to 400,000
Number of IT staff	1,047	550	38 to 4,000
Number of security staff	144	50	2 to 500
Number of total employees using information systems for job	50,481	3,050	750 to 300,000
Number of customers/external users	3.2M	17,500	25 to 34M
Number of business applications	1,230	213	15 to 5,000
Annual revenue	$31.1B	$4.6B	$136M to $156B
Countries	US (5), Australia (2), UK		
Industries	Healthcare (4), Education (2), Insurance, Financial Services		

How do customers describe the benefits realized?

FIGURE 2

Security Team KPIs

(% more effective)

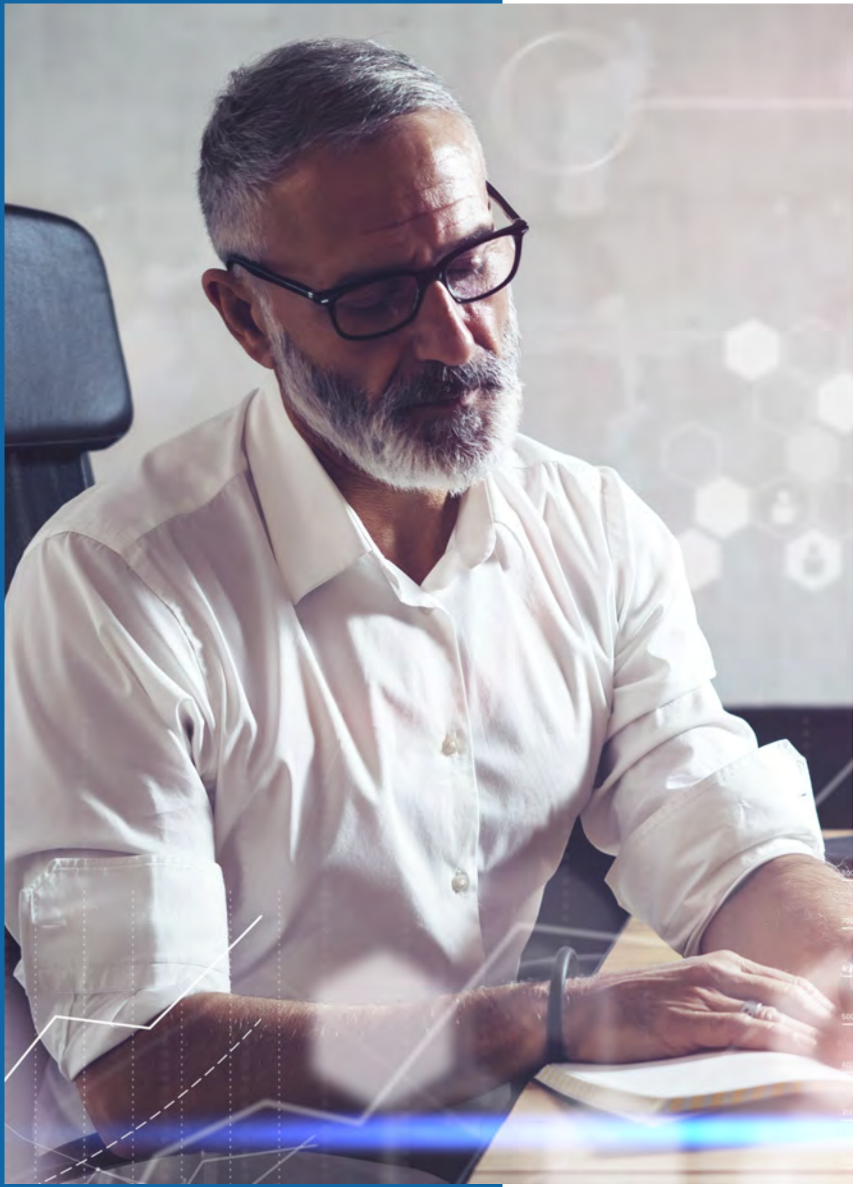


n = 9, Source: IDC Business Value In-Depth Interviews, August 2023

Security Staff Benefits

Education Organization

"By using the Qualys patch management module, we have been able to increase the bandwidth of our security operations team. Previously they were maxed out with other things, because during the global pandemic we have increased the number of devices while the number of staff has remained the same. We have been able to scale and maintain a good security posture by using the Qualys platform. We always have real-time visibility of assets; this is a huge impact."



Other Staff Benefits

Financial Organization

"Qualys has definitely reduced overhead for security and operations teams. The benefit is, we all look at the same data and use the same tool. That reduces the amount of debate we have. There are efficiencies in access and maintenance, we can grant access to individuals to various modules. It makes it easier to maintain."

Unplanned Downtime & Risk Reduction

Education Organization

“Qualys has reduced the risk and impact of a cyber incident. It has improved our security posture, given better confidence to our board, and protected the university brand.”

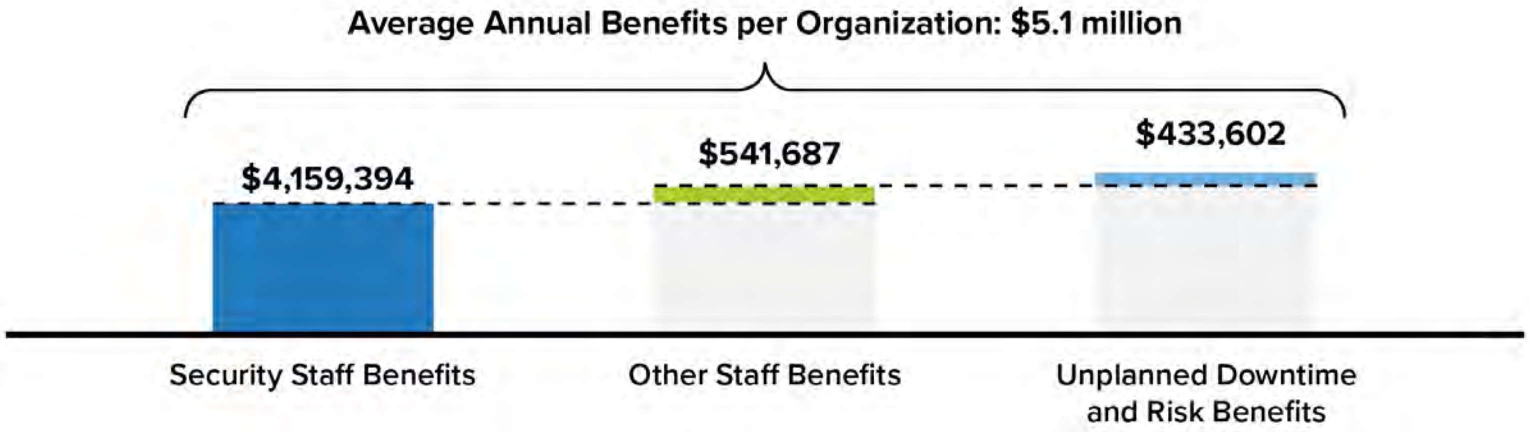
Doing the Math!

- 403% 3-year ROI
- $102,000 average annual benefits per 1,000 internal users
- 5 month payback period
- 24% more efficient security teams
- 65% less unplanned application downtime
- 66% quicker to resolve events
- 24% reduction in the risk of compliance-related fines

FIGURE 1

Average Annual Benefits per Organization

($ per organization)



n = 8, Source: IDC Business Value In-Depth Interviews, August 2023