Kiteworks

Tackling Risk Gaps in the Compliance Era

Tim Freestone, CMO

The confluence we are now in…

I.T.

Mainframe Era

Personal Computing Era

Client/Server Era

Enterprise Computing Era

Cloud Era

Cybersecurity

Mainframe Protection Era

ARPANET Era

Internet Protocols Era

Viruses Era

Hacker Era

APT Era

COMPLIANCE ERA

Data Protection and Privacy Legislation Worldwide

71%

COUNTRIES WITH
LEGISLATION

9%

COUNTRIES WITH
DRAFT LEGISLATION

15%

COUNTRIES WITH
NO LEGISLATION

5%

COUNTRIES WITH
NO DATA

** According to the United Nations Conference on Trade and Development*

OCTOBER 26, 2001

The USA PATRIOT Act of 2001

JULY 30, 2002

The Sarbanes-Oxley Act of 2002

NOVEMBER 13, 2002

The Federal Trade Commission's Safeguards Rule for Financial Institutions

MAY 23, 2002

The Gramm-Leach-Bliley Act (GLBA) Safeguards Rule

DECEMBER 4, 2003

The Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act of 2003

FEBRUARY 12, 2004

The Federal Information Processing Standard (FIPS) Publication 199: Standards for Security Categorization of Federal Information and Information Systems

MARCH 2006

The Federal Information Processing Standard (FIPS) Publication 200: Minimum Security Requirements for Federal Information and Information Systems

FEBRUARY 17, 2009

The Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009

DECEMBER 31, 2012

The Family Educational Rights and Privacy Act of 1974 (FERPA), as amended by the Protecting Student Privacy Act of 2012

JANUARY 25, 2013

The Health Insurance Portability and Accountability Act (HIPAA) Omnibus Rule

APRIL 15, 2013

The National Institute of Standards and Technology (NIST) Special Publication 800-53A Revision 4

JULY 1, 2013

The Children's Online Privacy Protection Act of 1998 (COPPA) Amendment to the FTC's Children's Online Privacy Protection Rule

DECEMBER 18, 2014

The Federal Information Security Modernization Act (FISMA) of 2014

AUGUST 15, 2015

The Department of Defense Directive 8500: Cybersecurity Requirements for DoD Contractors

The Department of Defense Directive 8570: Cybersecurity Requirements for DoD Contractors

Department of Defense Directive 8500: Cybersecurity Requirements for DoD Information Systems and Organizations

MAY 8, 2016

The European Union's Network and Information Security Directive 2016/1148/EU

JUNE 8, 2017

The National Institute of Standards and Technology (NIST) Special Publication 800-63B Digital Identity Guidelines Version 2.0

JUNE 28, 2017

The National Institute of Standards and Technology (NIST) Special Publication 800-171 Revision 1

APRIL 15, 2018

The Payment Card Industry Data Security Standard Version 3.2.1

APRIL 16, 2018

NIST Cybersecurity Framework Version 1.1

MAY 25, 2018

The General Data Protection Regulation (GDPR)

JUNE 28, 2018

The Federal Risk and Authorization Management Program (FedRAMP) Security Assessment Framework Version 3.0

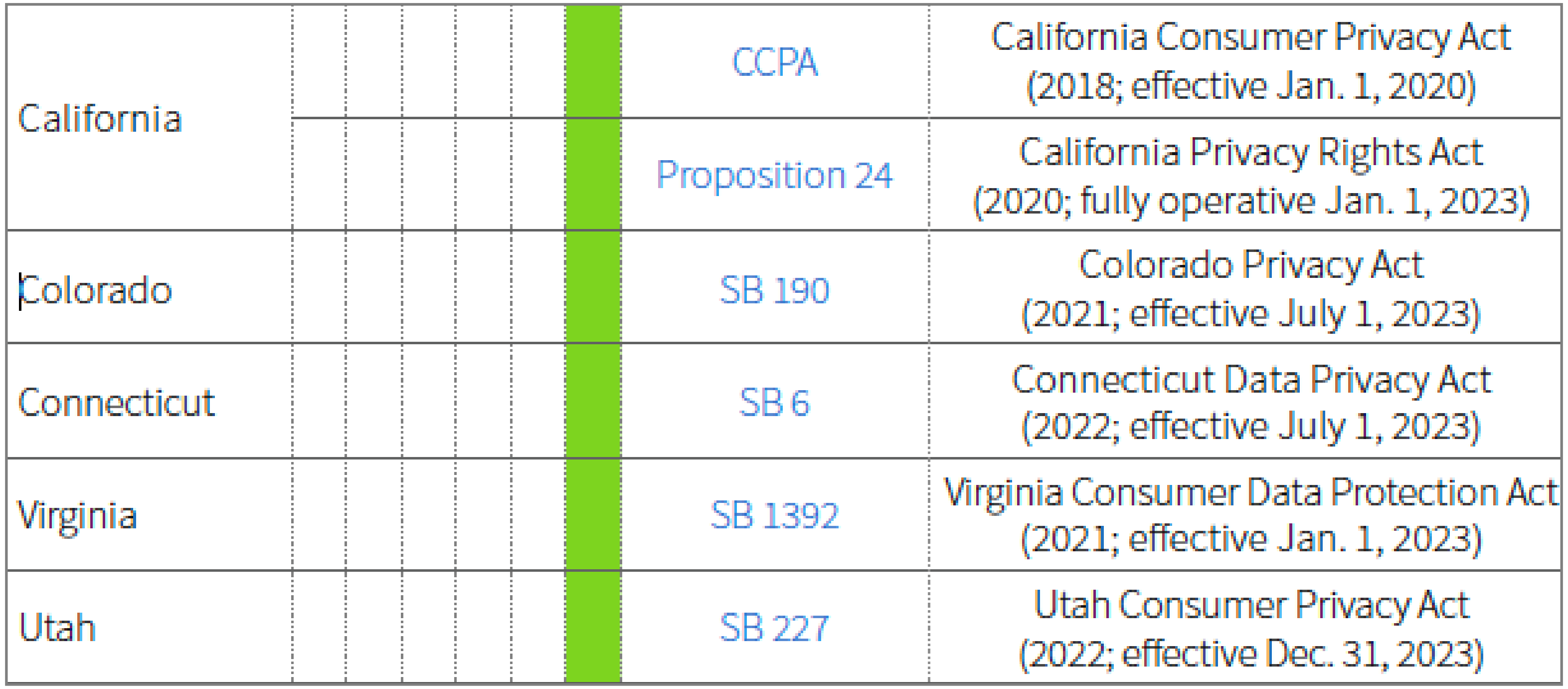
JANUARY 1, 2020

Cybersecurity Maturity Model Certification (CMMC)

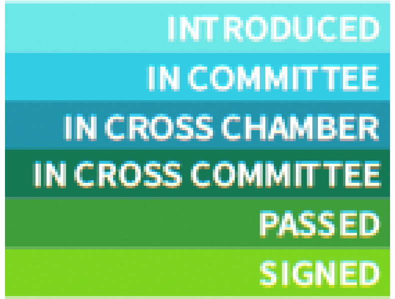
JANUARY 21, 2021

Cybersecurity Maturity Model Certification 2.0 (CMMC 2.0)

State Laws Signed To-Date



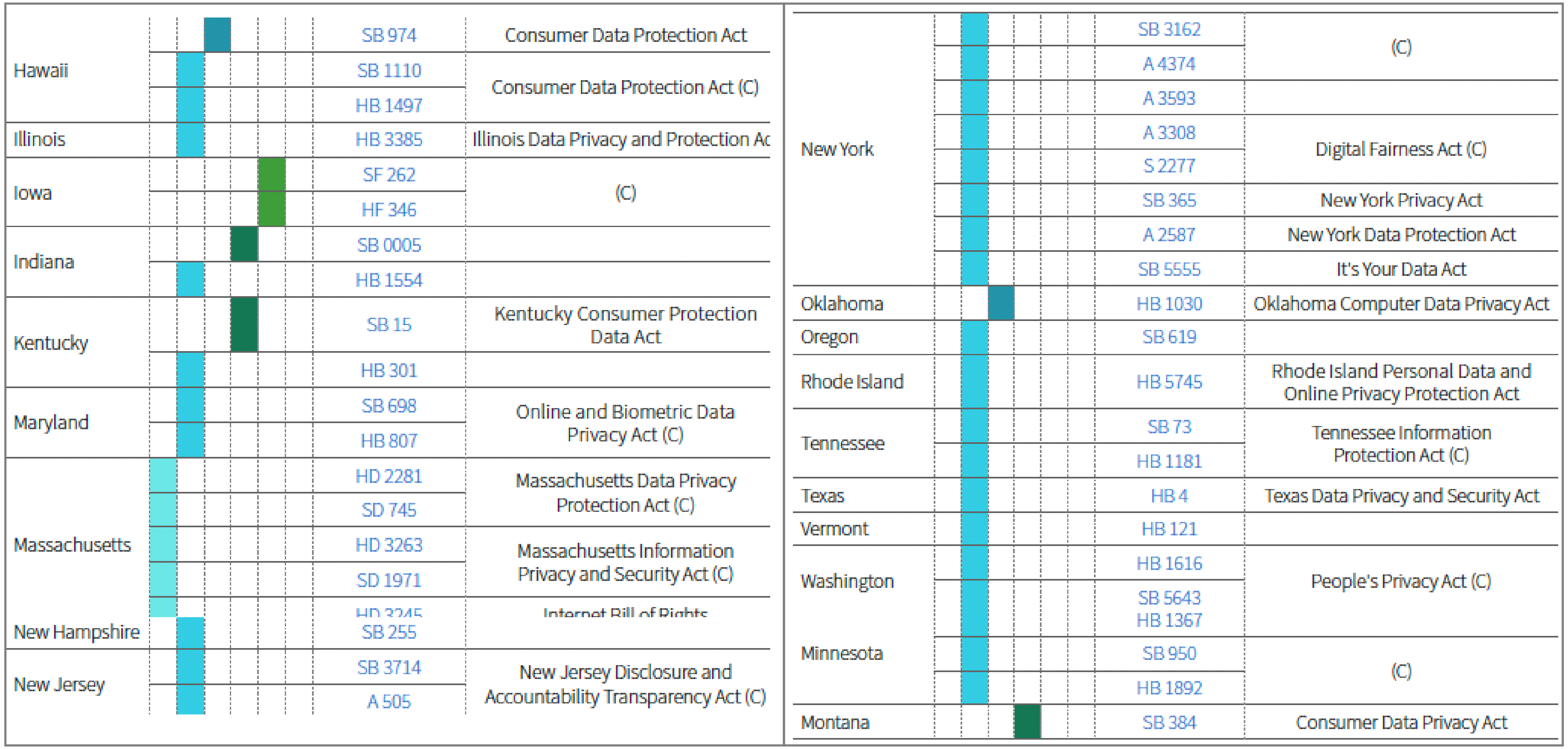
California						🟩	CCPA	California Consumer Privacy Act (2018; effective Jan. 1, 2020)
						🟩	Proposition 24	California Privacy Rights Act (2020; fully operative Jan. 1, 2023)
Colorado						🟩	SB 190	Colorado Privacy Act (2021; effective July 1, 2023)
Connecticut						🟩	SB 6	Connecticut Data Privacy Act (2022; effective July 1, 2023)
Virginia						🟩	SB 1392	Virginia Consumer Data Protection Act (2021; effective Jan. 1, 2023)
Utah						🟩	SB 227	Utah Consumer Privacy Act (2022; effective Dec. 31, 2023)



INTRODUCED
IN COMMITTEE
IN CROSS CHAMBER
IN CROSS COMMITTEE
PASSED
SIGNED

** According to the IAPP*

Active Bills



Hawaii			■				SB 974	Consumer Data Protection Act
		■					SB 1110	Consumer Data Protection Act (C)
		■					HB 1497	
Illinois		■					HB 3385	Illinois Data Privacy and Protection Ac
Iowa					■		SF 262	(C)
					■		HF 346	
Indiana				■			SB 0005	
		■					HB 1554	
Kentucky				■			SB 15	Kentucky Consumer Protection Data Act
		■					HB 301	
Maryland		■					SB 698	Online and Biometric Data Privacy Act (C)
		■					HB 807	
Massachusetts	■						HD 2281	Massachusetts Data Privacy Protection Act (C)
	■						SD 745	
	■						HD 3263	Massachusetts Information Privacy and Security Act (C)
	■						SD 1971	
	■						HD 3245	Internet Bill of Rights
New Hampshire		■					SB 255	
New Jersey		■					SB 3714	New Jersey Disclosure and Accountability Transparency Act (C)
		■					A 505	
New York		■					SB 3162	(C)
		■					A 4374	
		■					A 3593	
		■					A 3308	Digital Fairness Act (C)
		■					S 2277	
		■					SB 365	New York Privacy Act
		■					A 2587	New York Data Protection Act
		■					SB 5555	It's Your Data Act
Oklahoma			■				HB 1030	Oklahoma Computer Data Privacy Act
Oregon		■					SB 619	
Rhode Island		■					HB 5745	Rhode Island Personal Data and Online Privacy Protection Act
Tennessee		■					SB 73	Tennessee Information Protection Act (C)
		■					HB 1181	
Texas		■					HB 4	Texas Data Privacy and Security Act
Vermont		■					HB 121	
Washington		■					HB 1616	People's Privacy Act (C)
		■					SB 5643 HB 1367	
Minnesota		■					SB 950	(C)
		■					HB 1892	
Montana				■			SB 384	Consumer Data Privacy Act

INTRODUCED

IN COMMITTEE

IN CROSS CHAMBER

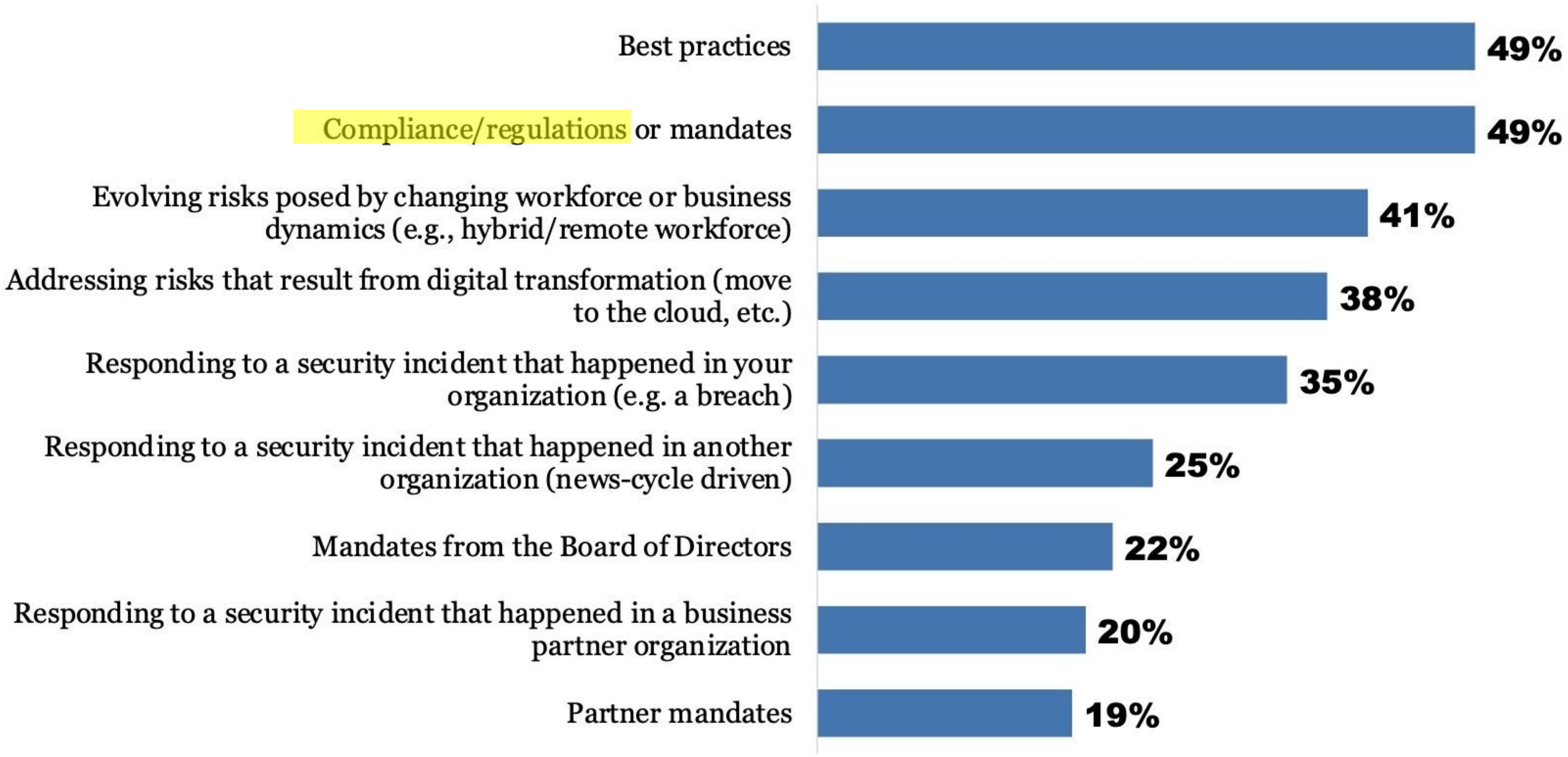
IN CROSS COMMITTEE

PASSED

SIGNED

** According to the IAPP*

Factors Determining Security Spending



Q: Which of the following factors help determine the priority of your security spending?

Data is at the center of Compliance…

Structured Data
(Databases)

PII

Semi-structured Data
(Logs and Emails)

PHI

Unstructured Data
(Files and Email Data)

IP

Compliance Requirements

Structured Data
(Databases)

Semi-structured Data
(Logs and Emails)

Unstructured Data
(Files and Email Data)

PII

PHI

IP

PROTECT

TRACK

CONTROL

The Growing Challenge – Data on the Move

Structured Data
(Databases)

PII

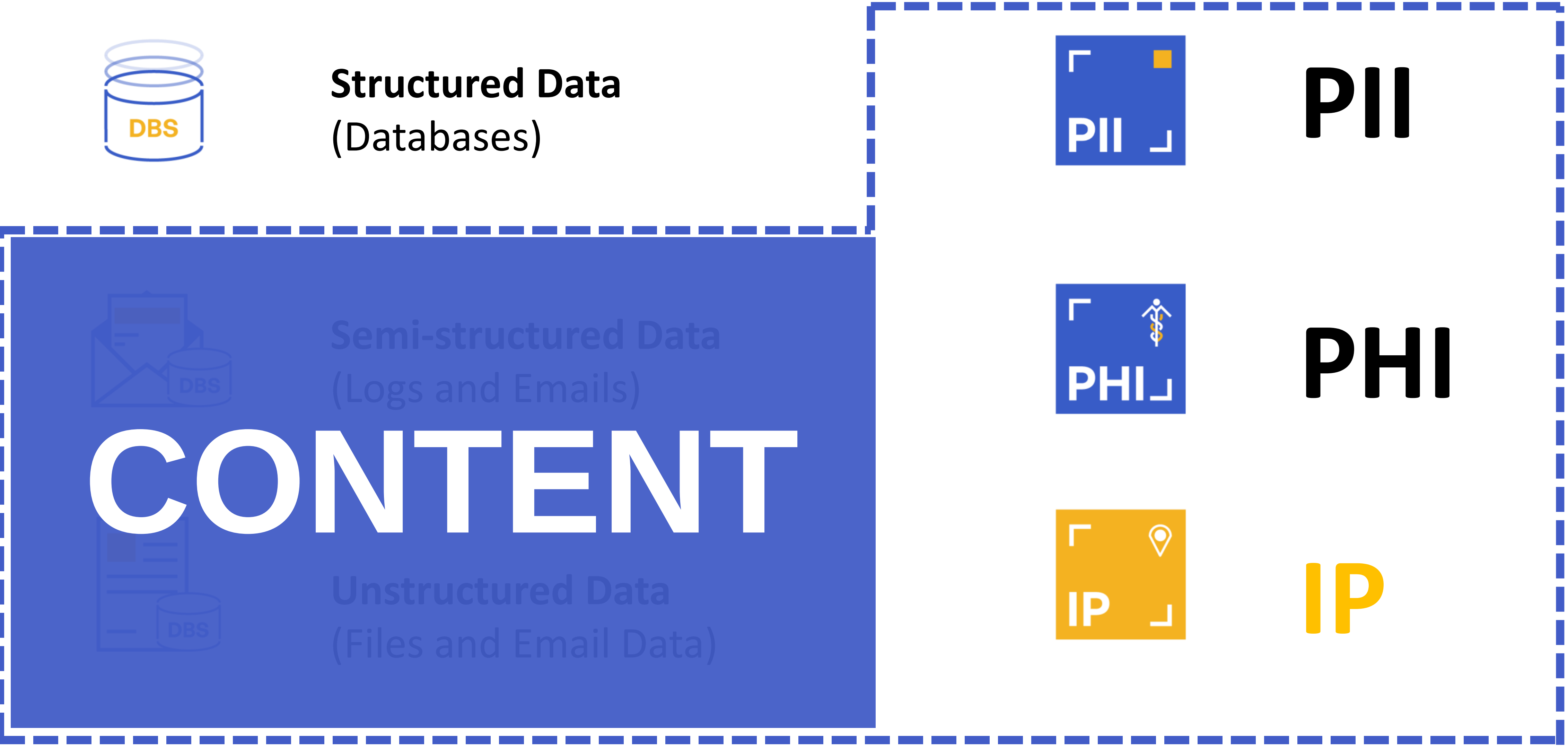
Semi-structured Data
(Logs and Emails)

PHI

Unstructured Data
(Files and Email Data)

IP

The Growing Challenge – Data on the Move



Structured Data
(Databases)

Semi-structured Data
(Logs and Emails)

CONTENT

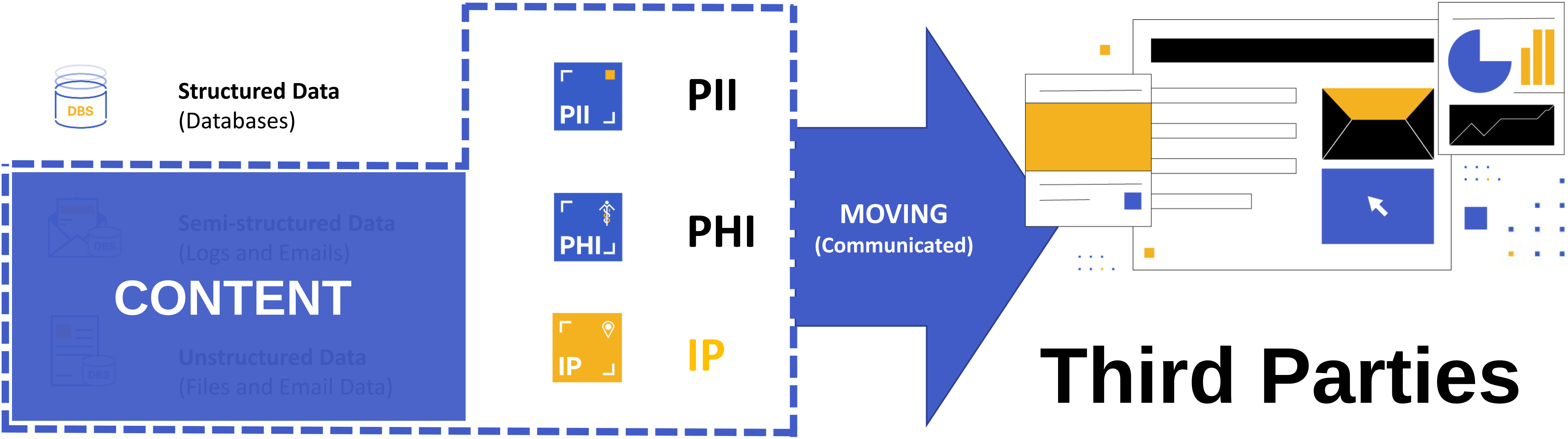
Unstructured Data
(Files and Email Data)

PII

PHI

IP

Data Protection and Compliance Nightmare



Structured Data
(Databases)

Semi-structured Data
(Logs and Emails)

CONTENT

Unstructured Data
(Files and Email Data)

PII

PHI

IP

MOVING
(Communicated)

Third Parties

2023 Sensitive Content Communications Privacy and Compliance Report

- Objective: Assess organizational maturity related to digital communications of confidential data
- Surveyed over 780 IT, security, risk, and compliance professionals in 15 different countries
- Targeted private sector enterprises in different industries such as manufacturing, finance, pharmaceuticals, healthcare, government, legal, and more
- Asked them 45 questions about sensitive content communications privacy and compliance

Kiteworks

2023

Kiteworks Sensitive Content Communications Privacy and Compliance Report

Growing Tool Soup, Malicious Cyberattacks, and Lack of Governance Tracking and Controls Demand DRM

Top Report Takeaways

PROBLEM: Organizations struggle to protect and control sensitive, unstructured data using traditional edge computing security and compliance protocols.

Nearly

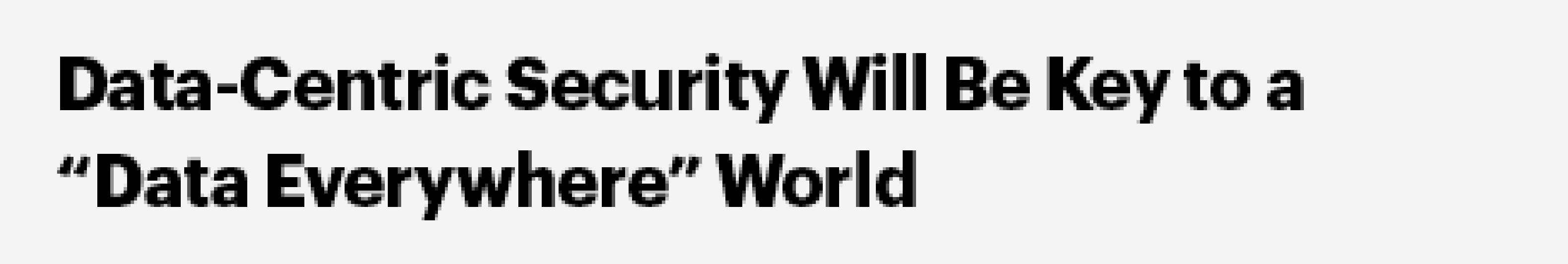
75%

of organizations indicate their measurement and management of sensitive content communications needs improvement.

62%

of organizations experienced financial damage as a result of an attack on sensitive content communications.

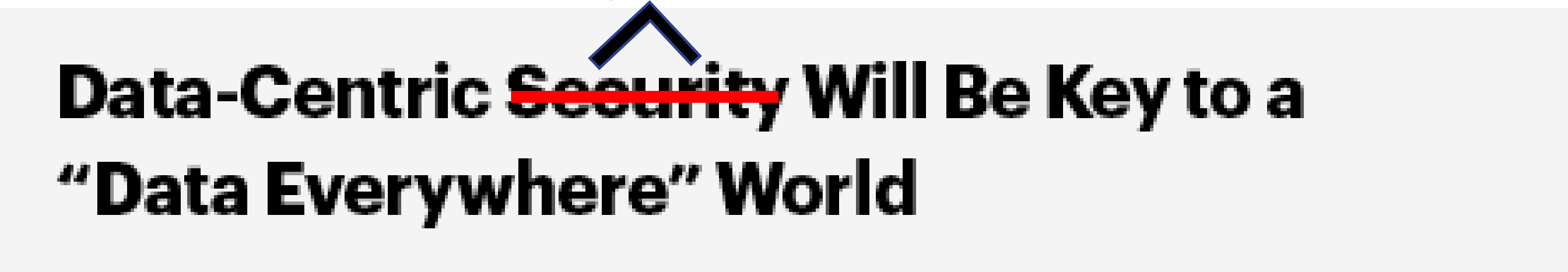
According to Gartner



Data-Centric Security Will Be Key to a "Data Everywhere" World

According to Kiteworks

Compliance

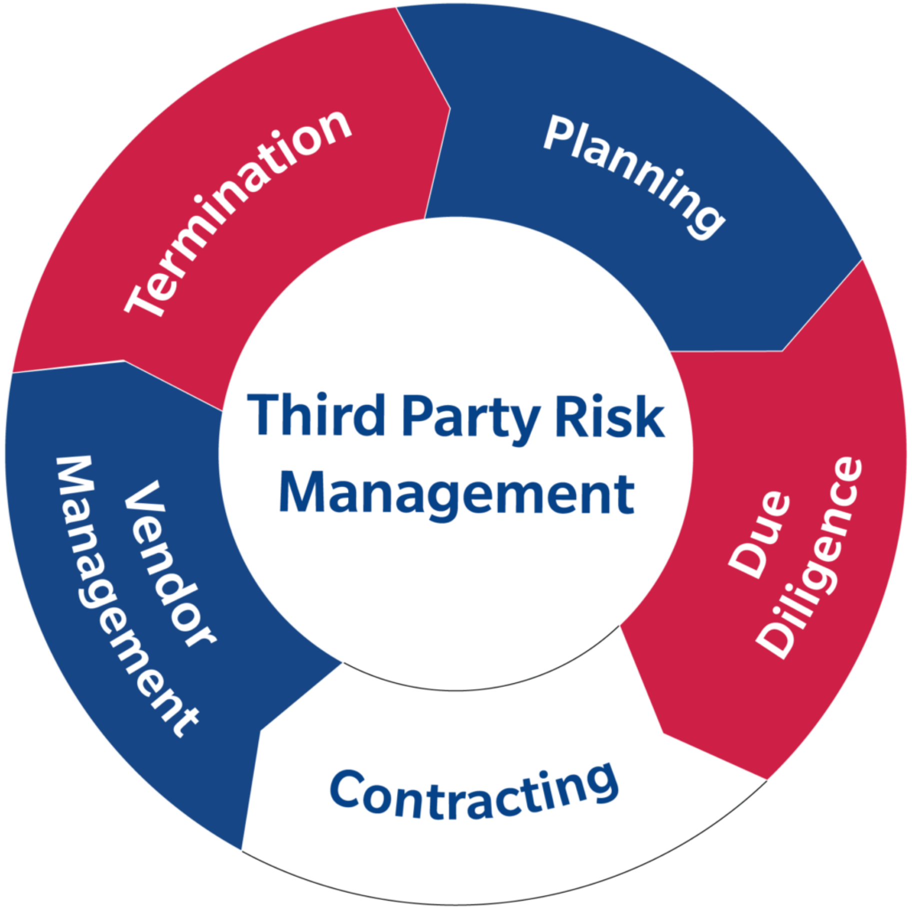


Data-Centric ~~Security~~ Will Be Key to a “Data Everywhere” World

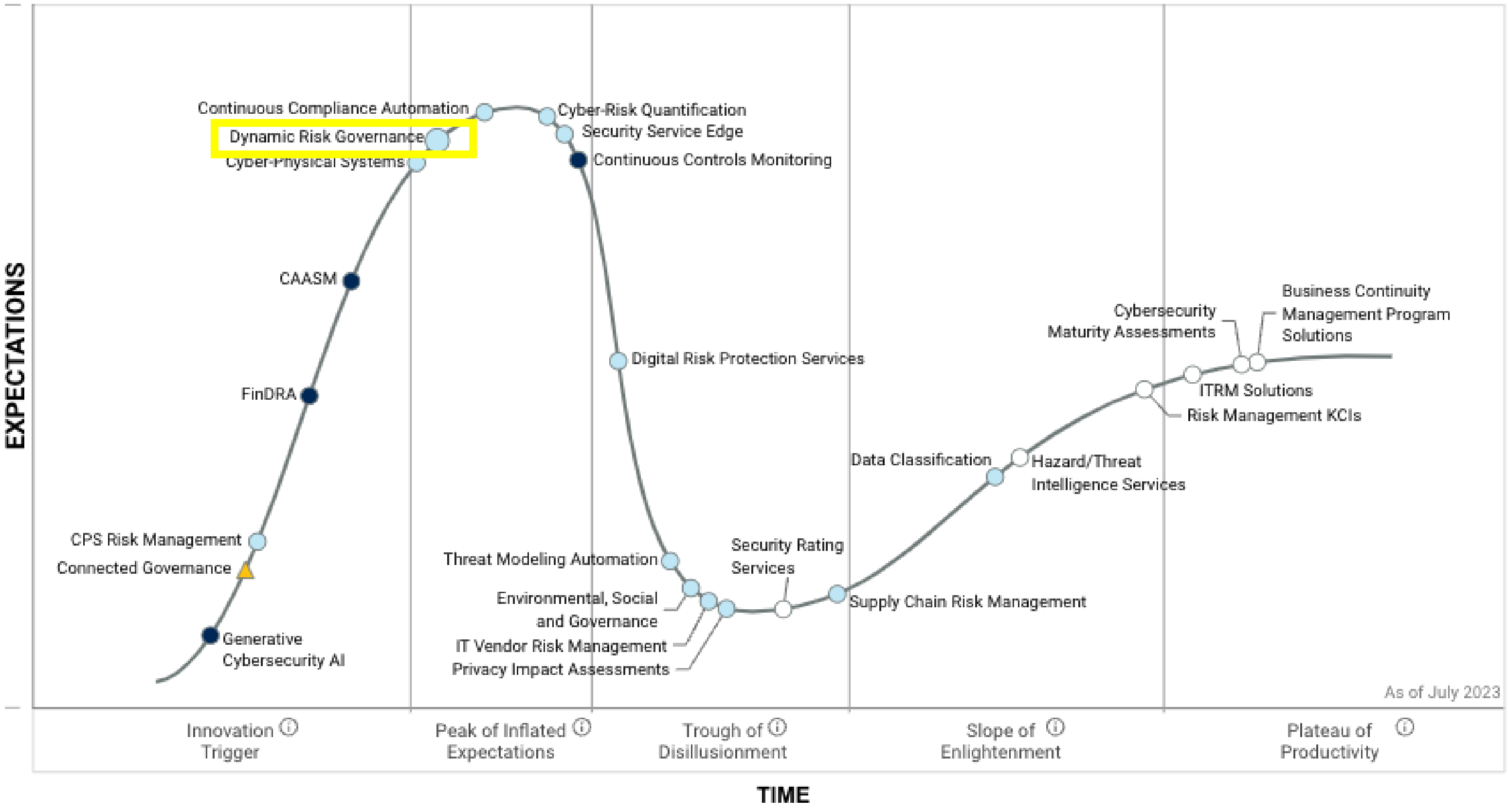
Gap #1

Third Party Risk Management

Tackling the Issue: TPRM



Hype Cycle for Cyber Risk Management, 2023



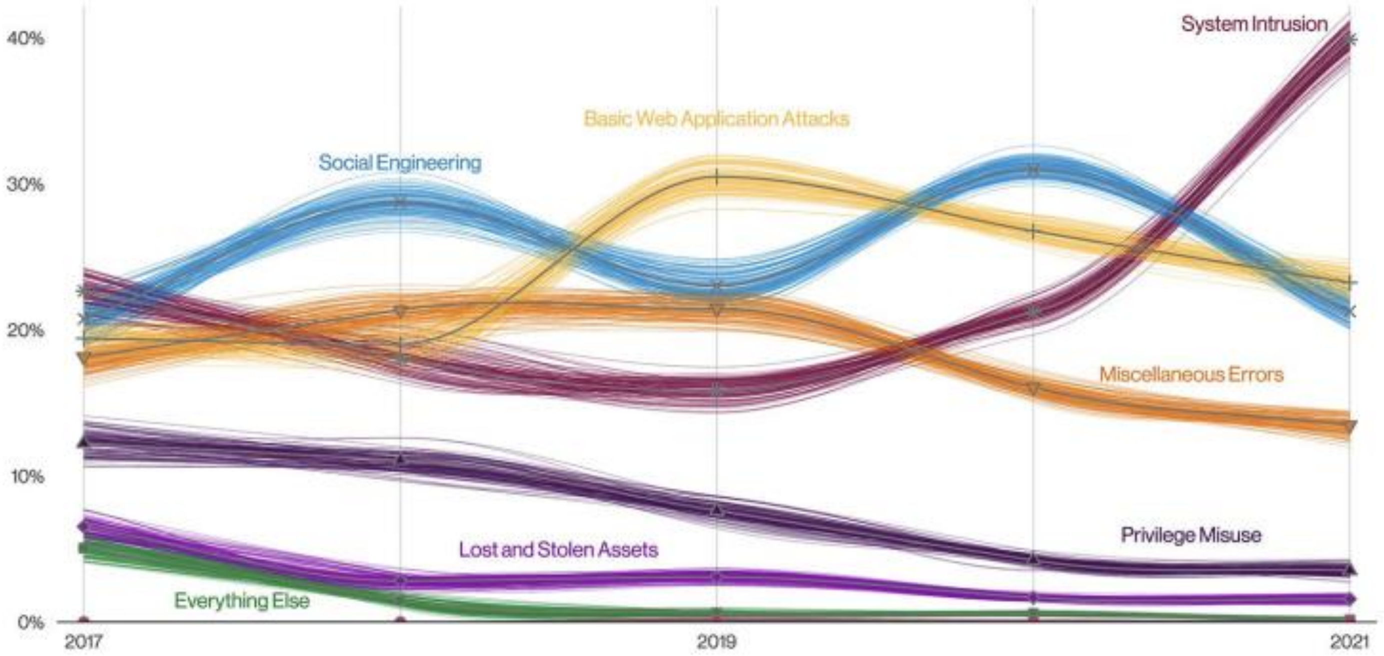
Dynamic Risk Governance
The risk landscape has been changed by several important drivers, among them are:

•The increased interconnectivity of risks. As organizations have become more complex, risks have become more interconnected. Today's top organizational risks, such as supply chain, cybersecurity and third-party risk, all cut across large parts of the organization.

•The increased digitalization of organizations. This has meant the creation of new, fully digital risks, such as ransomware, as well as an increase in the speed and volatility of other risks such as third-party risk. Risks now change in their nature more often and quickly.

2022 Data Breach Investigations Report

Gain vital cybersecurity insights from our analysis of over 23,000 incidents and 5,200 confirmed breaches from around the world—to help minimize risk and keep your business safe.



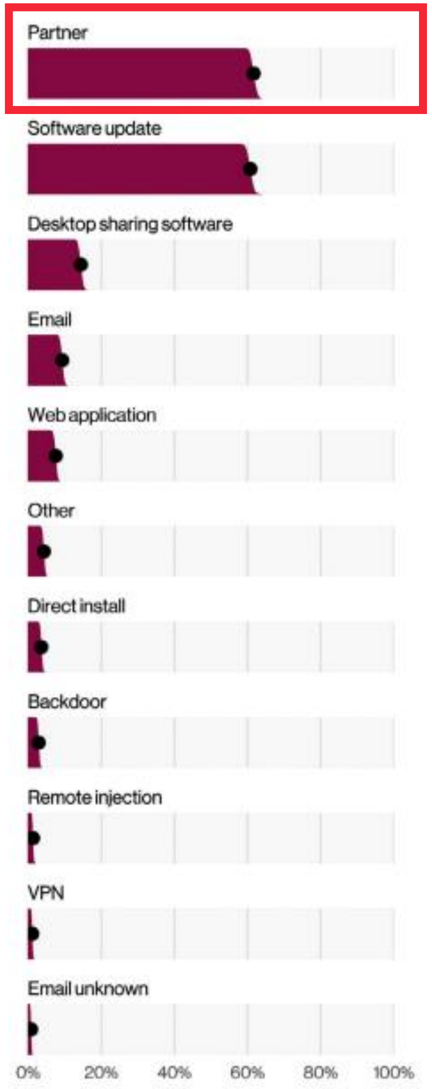
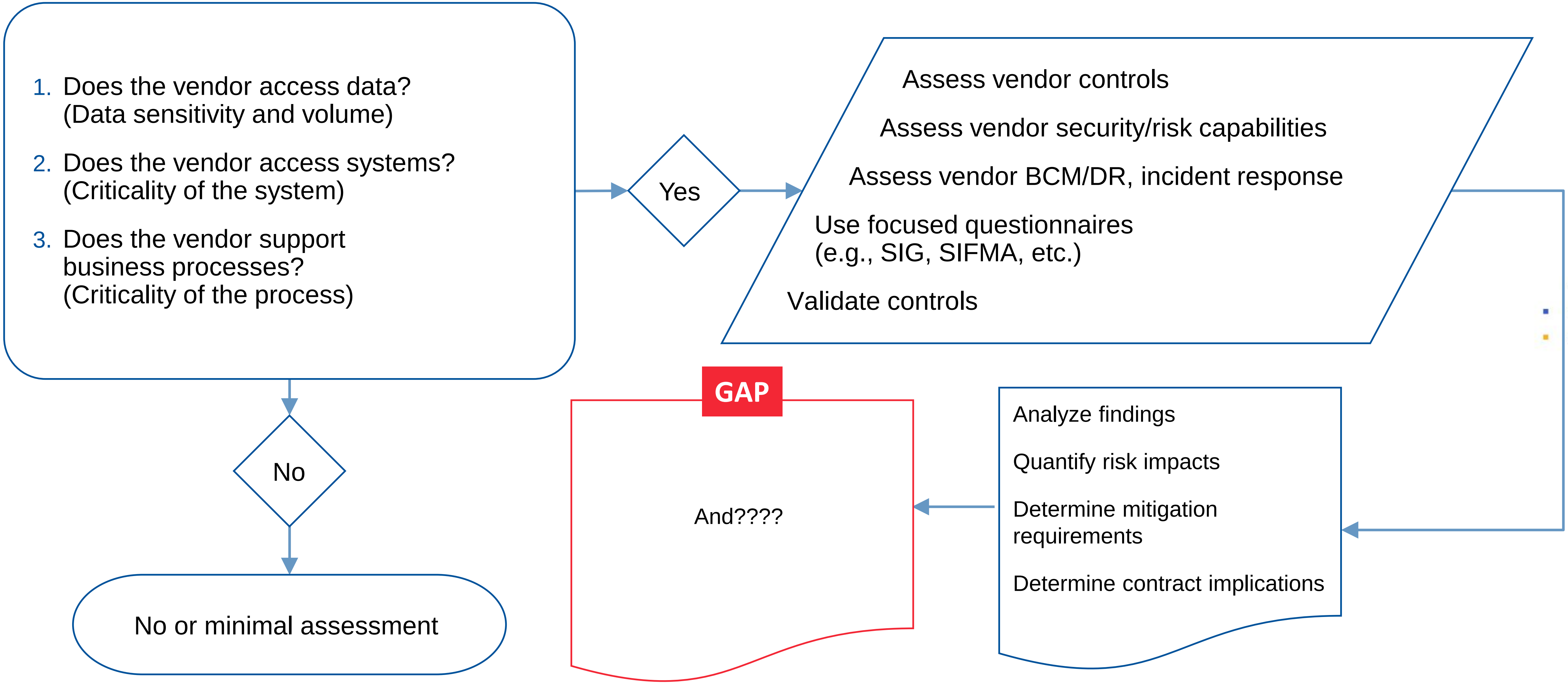


Figure 36. Top Action vectors in System Intrusion incidents (n=3,403)

Triage Approach to Assessing Risks According to Gartner



1. Does the vendor access data? (Data sensitivity and volume)
2. Does the vendor access systems? (Criticality of the system)
3. Does the vendor support business processes? (Criticality of the process)

Assess vendor controls

Assess vendor security/risk capabilities

Assess vendor BCM/DR, incident response

Use focused questionnaires (e.g., SIG, SIFMA, etc.)

Validate controls

No or minimal assessment

Analyze findings

Quantify risk impacts

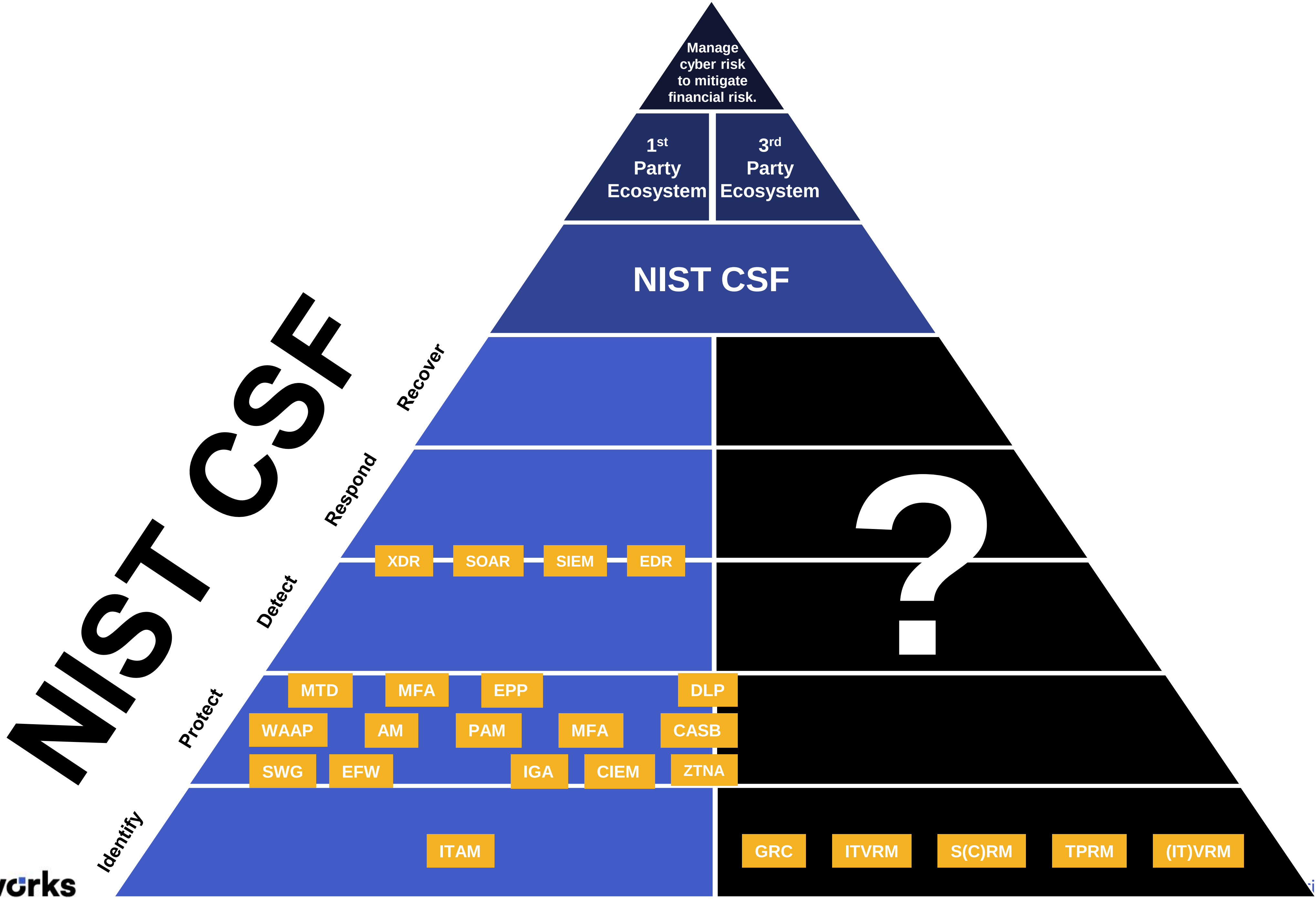
Determine mitigation requirements

Determine contract implications

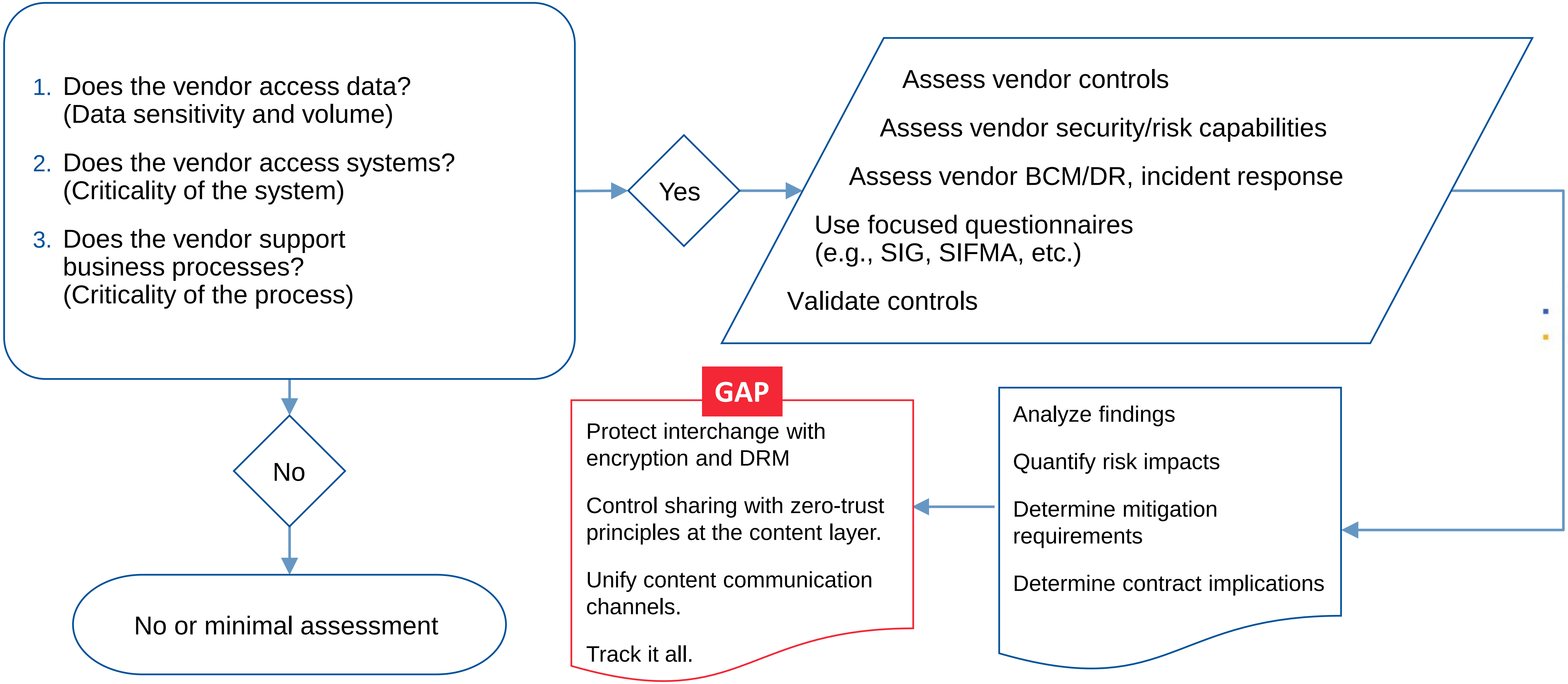
GAP

And????

Kiteworks


Manage cyber risk to mitigate financial risk.
1st Party Ecosystem
3rd Party Ecosystem
NIST CSF
NIST CSF
Recover
Respond
Detect
Protect
Identify
XDR
SOAR
SIEM
EDR
MTD
MFA
EPP
DLP
WAAP
AM
PAM
MFA
CASB
SWG
EFW
IGA
CIEM
ZTNA
ITAM
GRC
ITVRM
S(C)RM
TPRM
(IT)VRM
?

Close The Gap



1. Does the vendor access data? (Data sensitivity and volume)
2. Does the vendor access systems? (Criticality of the system)
3. Does the vendor support business processes? (Criticality of the process)

Yes

Assess vendor controls

Assess vendor security/risk capabilities

Assess vendor BCM/DR, incident response

Use focused questionnaires (e.g., SIG, SIFMA, etc.)

Validate controls

Analyze findings

Quantify risk impacts

Determine mitigation requirements

Determine contract implications

GAP

Protect interchange with encryption and DRM

Control sharing with zero-trust principles at the content layer.

Unify content communication channels.

Track it all.

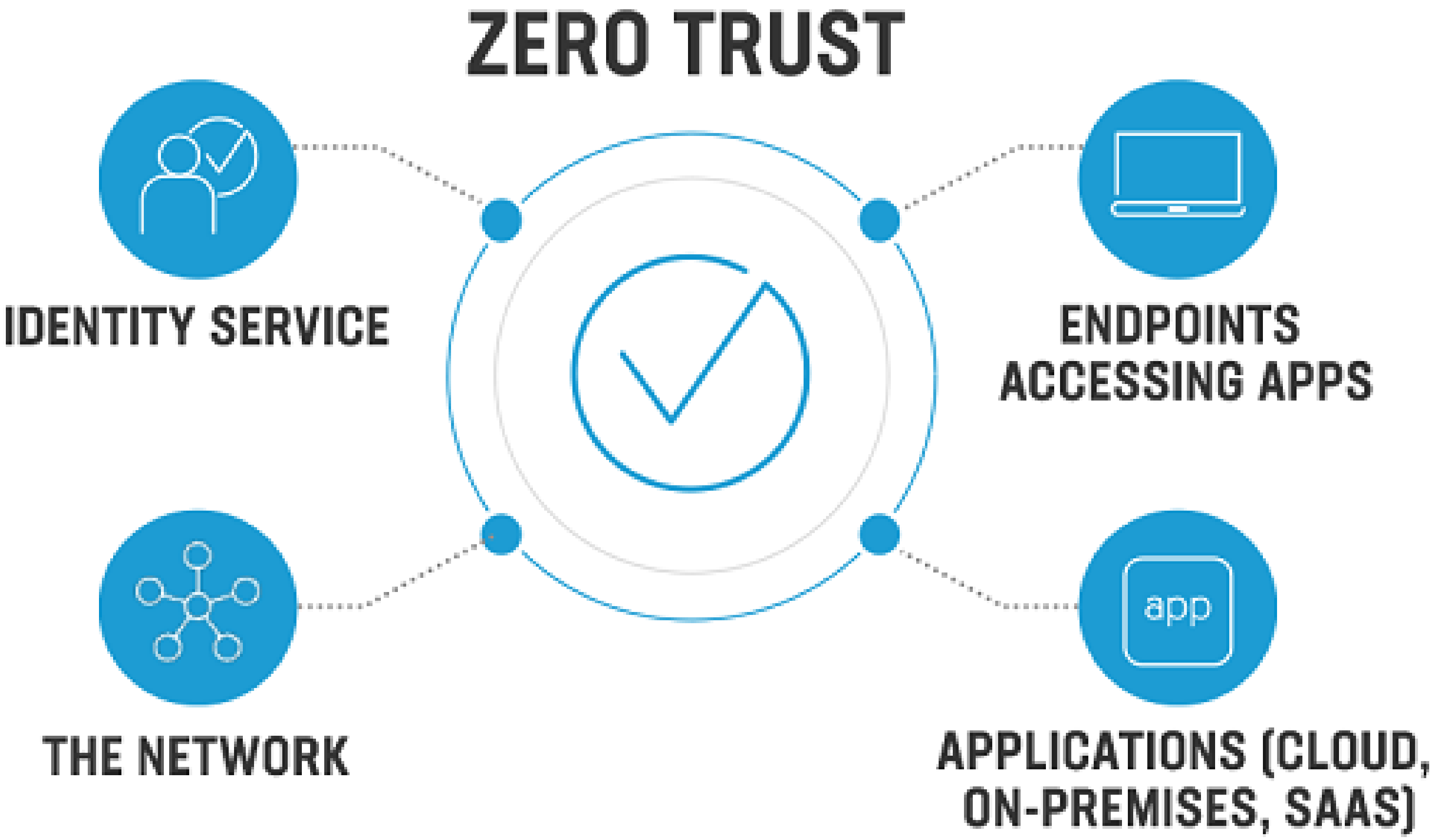
No

No or minimal assessment

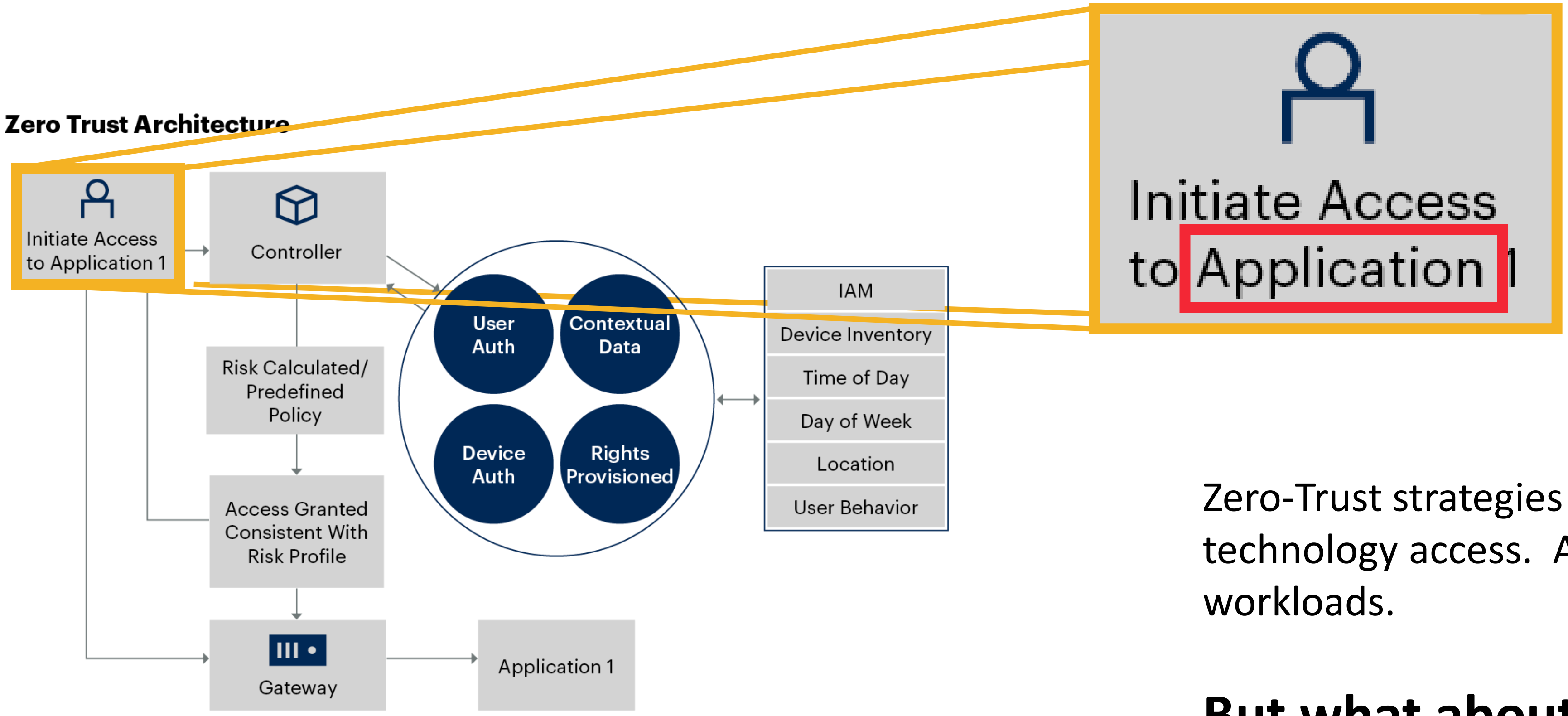
Gap #2

Zero Trust

Zero Trust


ZERO TRUST
IDENTITY SERVICE
ENDPOINTS ACCESSING APPS
THE NETWORK
app
APPLICATIONS (CLOUD, ON-PREMISES, SAAS)

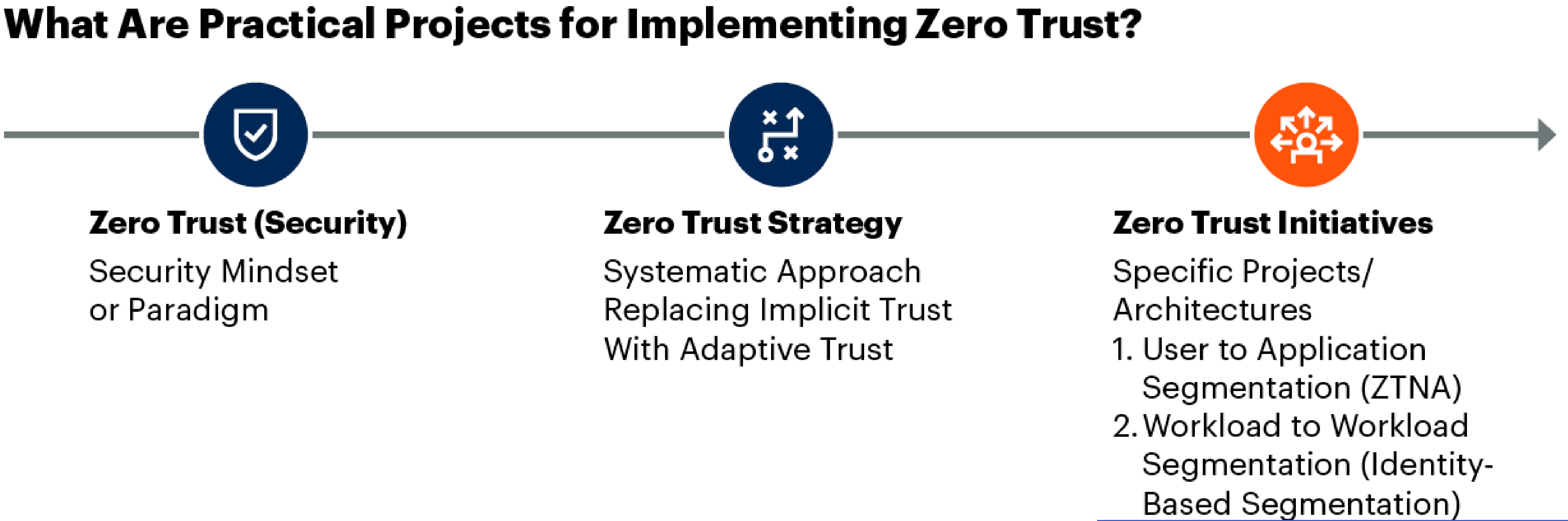
Extending Zero Trust for Compliance



Zero-Trust strategies tend to focus on technology access. Applications and workloads.

But what about the content that moves *through* and *beyond* applications and workloads?

To Put It Another Way



What Are Practical Projects for Implementing Zero Trust?

Zero Trust (Security)

Security Mindset
or Paradigm

Zero Trust Strategy

Systematic Approach
Replacing Implicit Trust
With Adaptive Trust

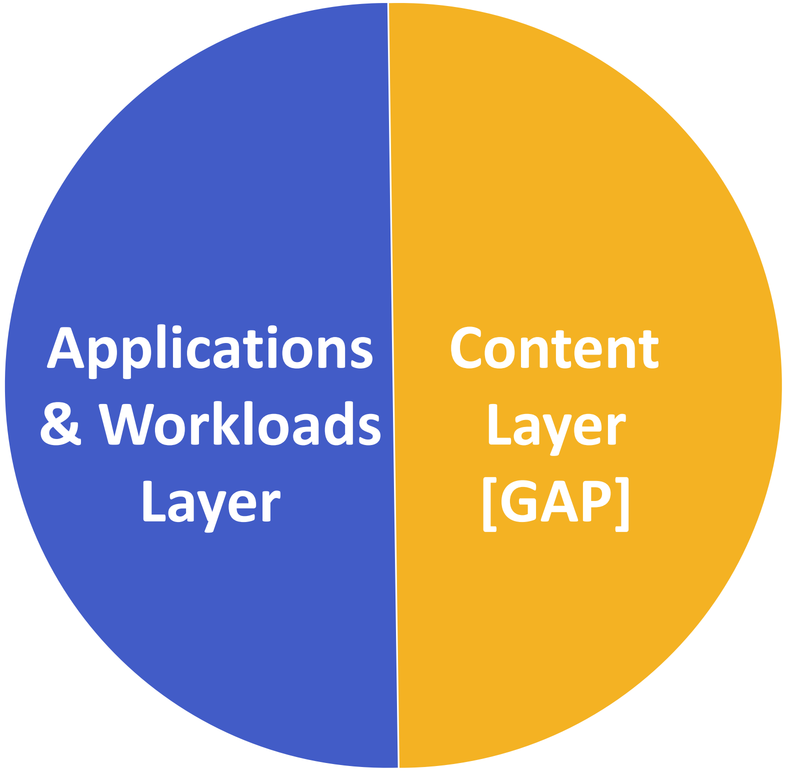
Zero Trust Initiatives

Specific Projects/
Architectures

1. User to Application Segmentation (ZTNA)
2. Workload to Workload Segmentation (Identity-Based Segmentation)

3.User-to-content segmentation

Data-centric Compliance Via Zero Trust Has Two Critical Layers



Content doesn’t *stay* in the managed applications and workloads.

Gap #3

Digital Rights Management

Digital Rights Management

?

What is it?

What It’s Not

Digital Rights Management

According to Gartner….

Enterprise digital rights management offers persistent data-centric defense, solving security and compliance challenges with clear goals and governance. Security and risk management technical professionals should follow this EDRM framework when building use cases to design, implement and operate.

Digital Rights Management

A cryptographic element: Information is encrypted so that protection travels with data no matter where it moves or rests.

An identity element: Users must be authenticated and match policies related to specific user roles and groups before accessing rights-protected data on any system.

A granular usage control element: Users are granted specific rights within applications (such as the ability to only view, edit, print, copy/paste, or screen capture sensitive information).

Digital Rights Management

Administrator-defined protection of intellectual property (IP):

User-initiated protection of arbitrary files

Compliance-driven protection of regulated information

Today’s Approach to DRM is Legacy

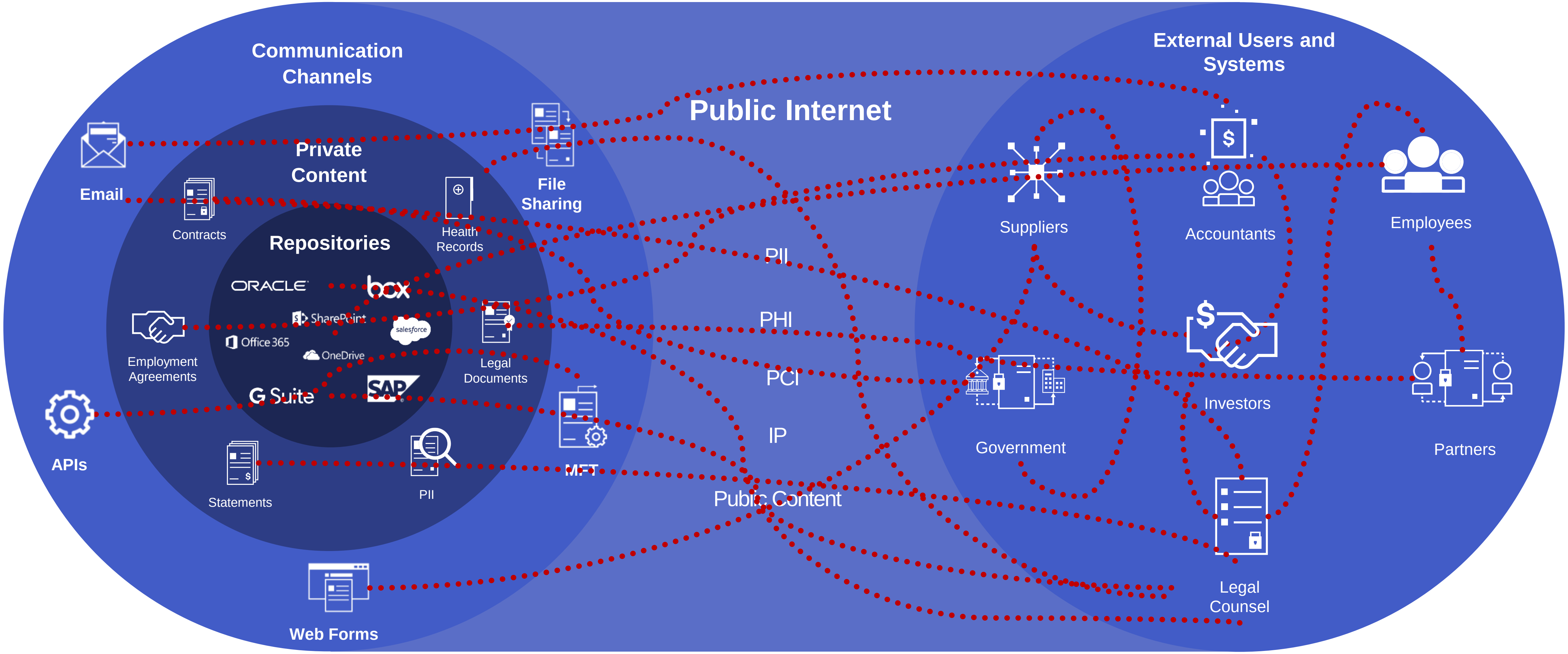
“A cryptographic element: Information is encrypted so that protection travels with data no matter where it moves or rests”

!

Accomplished primarily as agent-based digital

- Issues in scale and functionality – low adoption
- File leaves the/a network – increased risk

Solutioning the Gaps



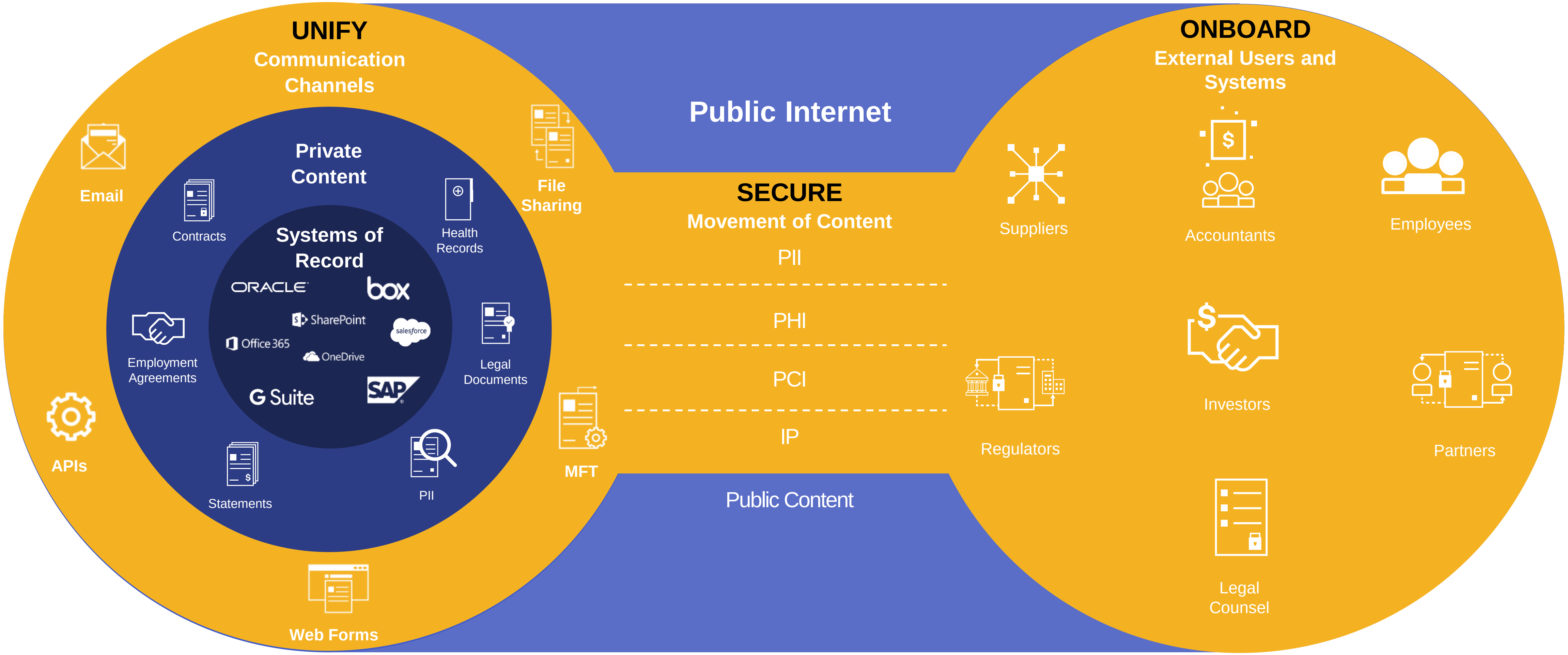
DISPARATE SYSTEMS POOR TRACKING NO CONTROL WEAK SECURITY

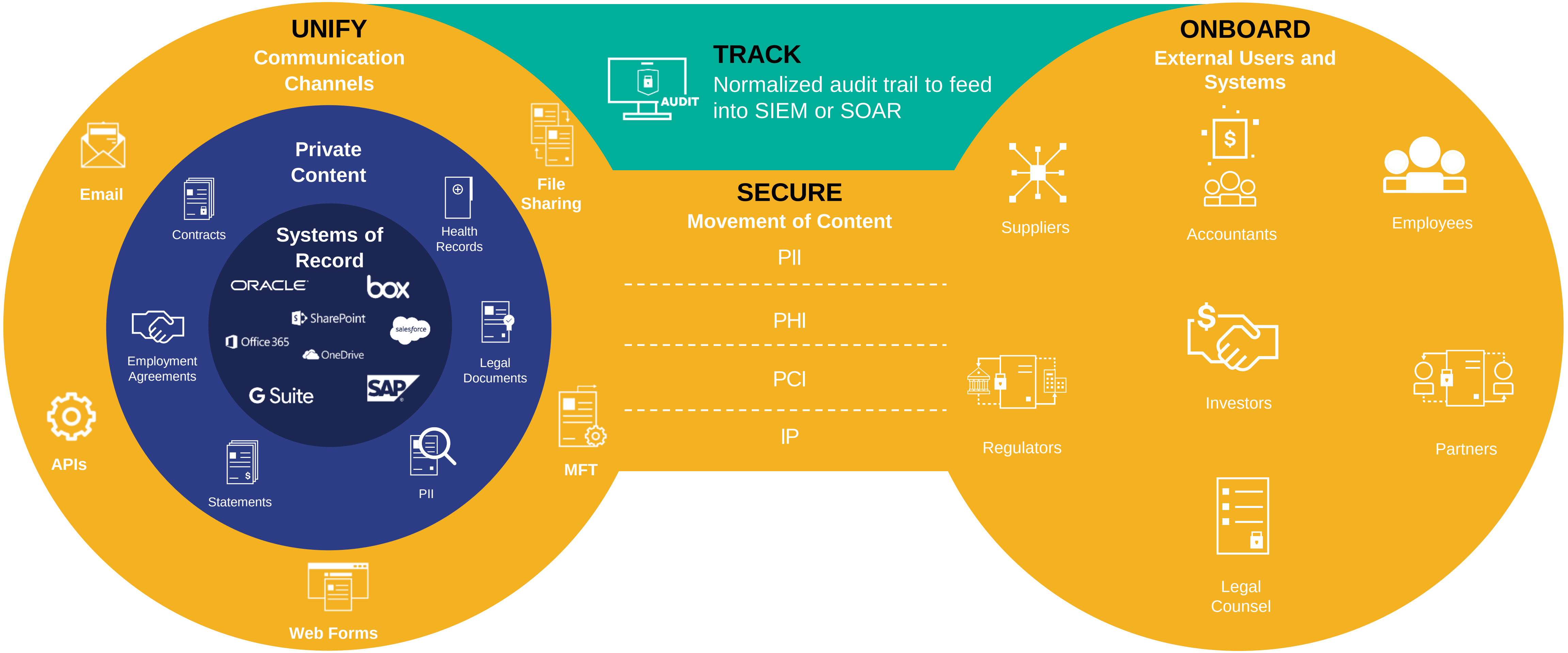
Kiteworks

A Private Content Network

A Kiteworks-enabled Private Content Network (PCN) unifies, tracks, controls, and secures the communication of private information.

Kiteworks-enabled PCN





UNIFY

Communication Channels

Email

File Sharing

APIs

MFT

Web Forms

Private Content

Contracts

Health Records

Employment Agreements

Legal Documents

Statements

PII

Systems of Record

TRACK

Normalized audit trail to feed into SIEM or SOAR

SECURE

Movement of Content

PII

PHI

PCI

IP

ONBOARD

External Users and Systems

Suppliers

Accountants

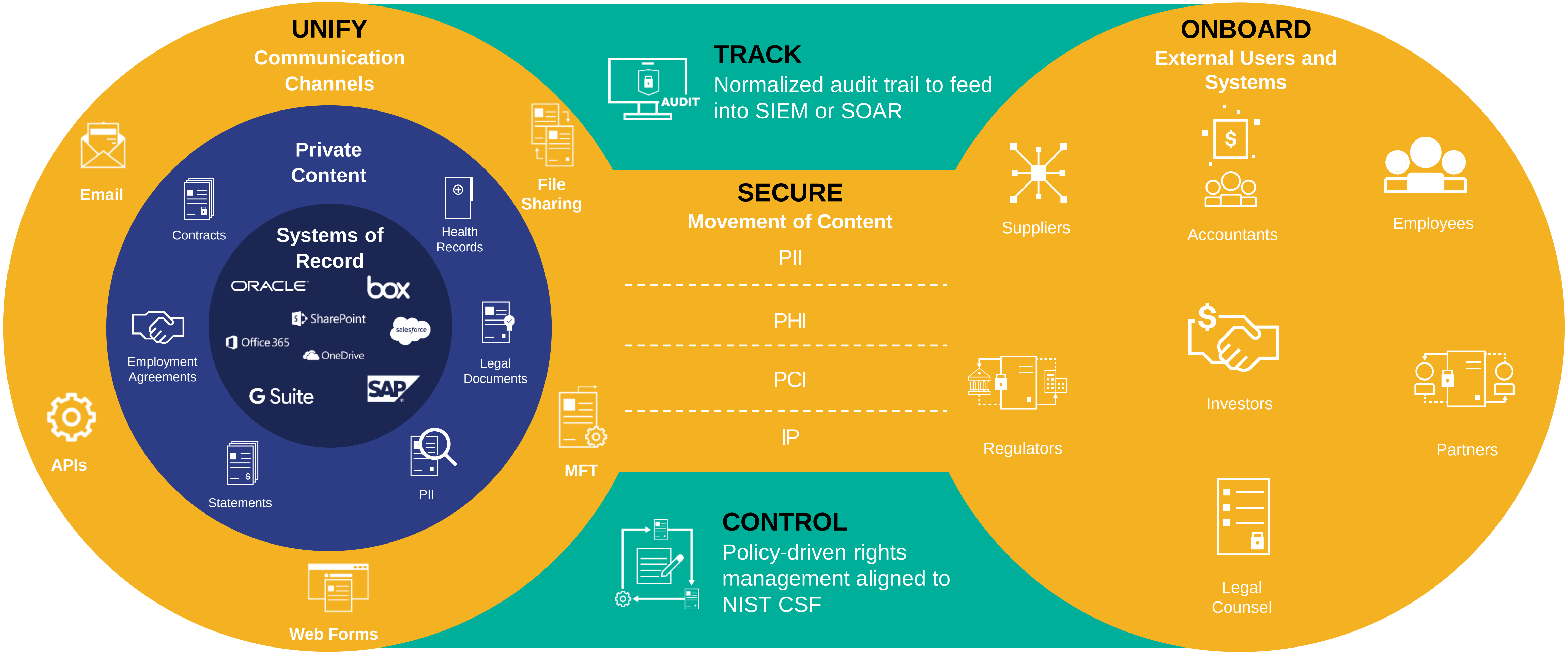
Employees

Regulators

Investors

Partners

Legal Counsel



UNIFY

Communication Channels

Email

File Sharing

MFT

APIs

Web Forms

Private Content

Contracts

Health Records

Employment Agreements

Legal Documents

Statements

PII

Systems of Record

ORACLE

box

SharePoint

salesforce

Office 365

OneDrive

G Suite

SAP

TRACK

AUDIT

Normalized audit trail to feed into SIEM or SOAR

SECURE

Movement of Content

PII

PHI

PCI

IP

CONTROL

Policy-driven rights management aligned to NIST CSF

ONBOARD

External Users and Systems

Suppliers

Accountants

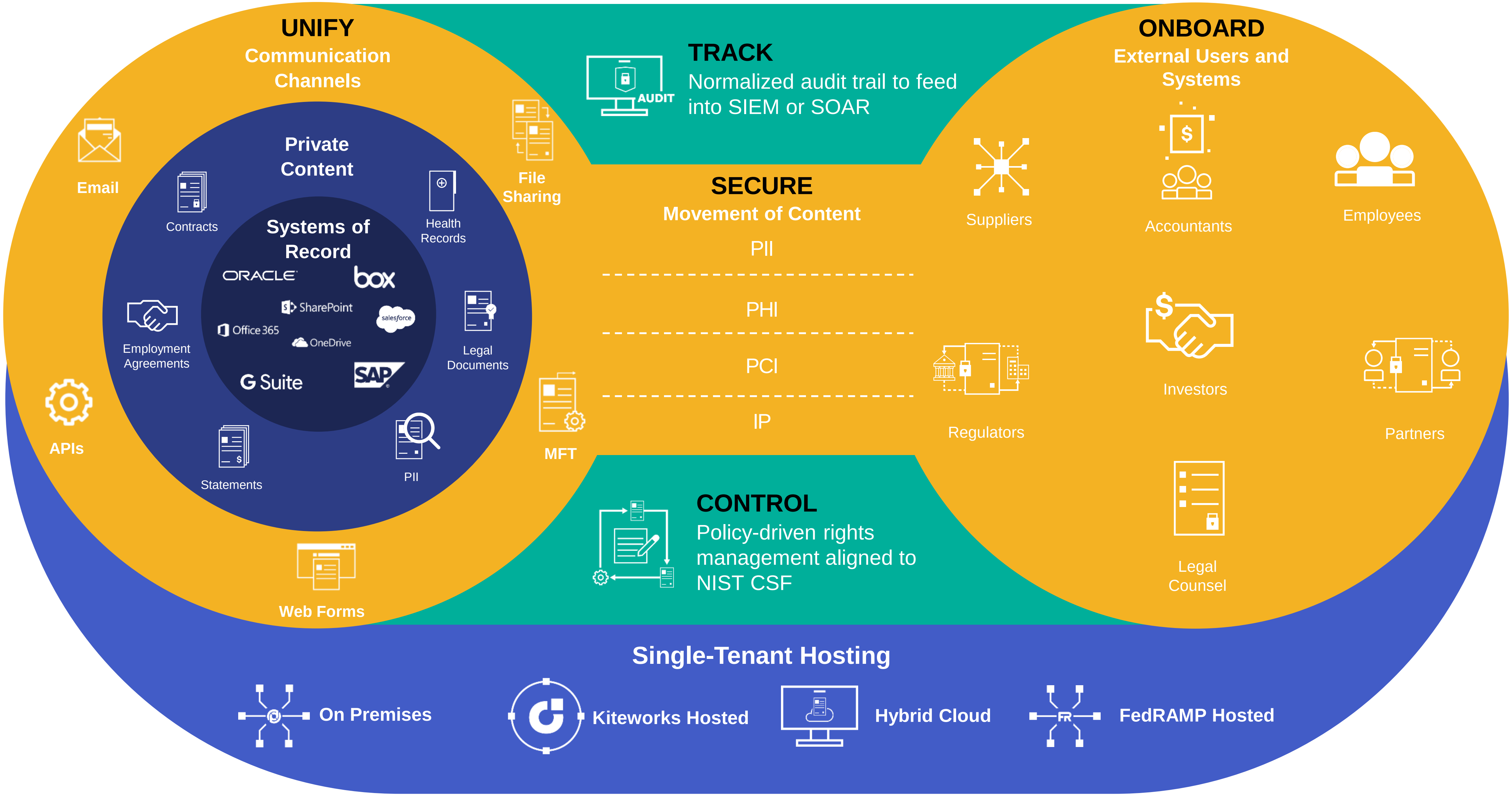
Employees

Regulators

Investors

Partners

Legal Counsel



UNIFY
Communication Channels

Email

File Sharing

APIs

MFT

Web Forms

Private Content

Contracts

Health Records

Employment Agreements

Legal Documents

Statements

PII

Systems of Record

TRACK
Normalized audit trail to feed into SIEM or SOAR

SECURE
Movement of Content

PII

PHI

PCI

IP

CONTROL
Policy-driven rights management aligned to NIST CSF

ONBOARD
External Users and Systems

Suppliers

Accountants

Employees

Regulators

Investors

Partners

Legal Counsel

Single-Tenant Hosting

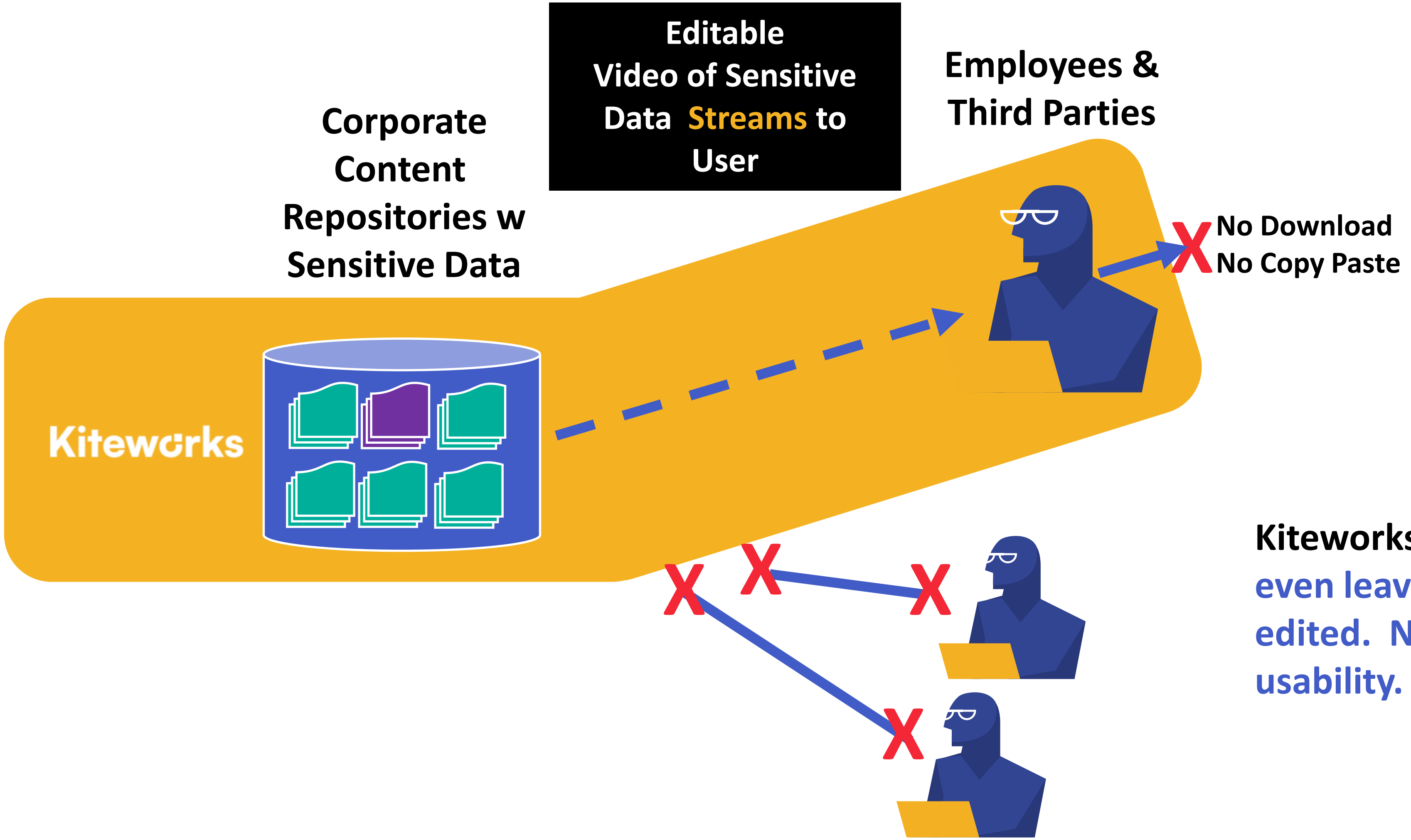
On Premises

Kiteworks Hosted

Hybrid Cloud

FedRAMP Hosted

Enter Next-Gen DRM

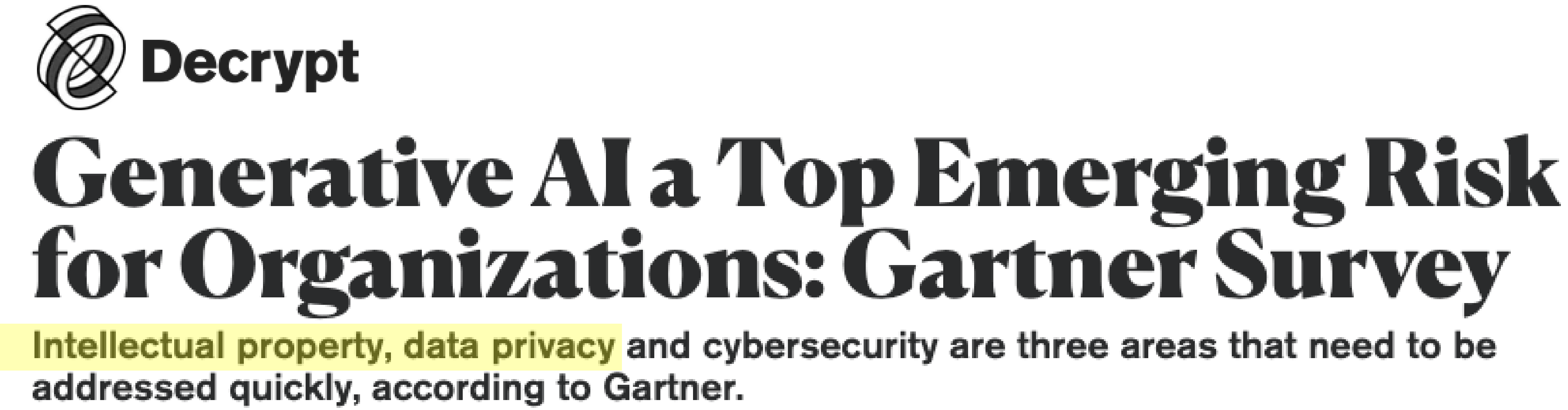

Corporate Content Repositories w Sensitive Data
Editable Video of Sensitive Data Streams to User
Employees & Third Parties
Kiteworks
X
No Download
No Copy Paste
X
X
X
X

Kiteworks SafeEDIT - sensitive data never even leaves your repository but can still be edited. No agents, no IRM, limitless scale and usability.

Just When You Thought It Was Safe to Go Back in the Pool

Enter: Artificial Intelligence Risk

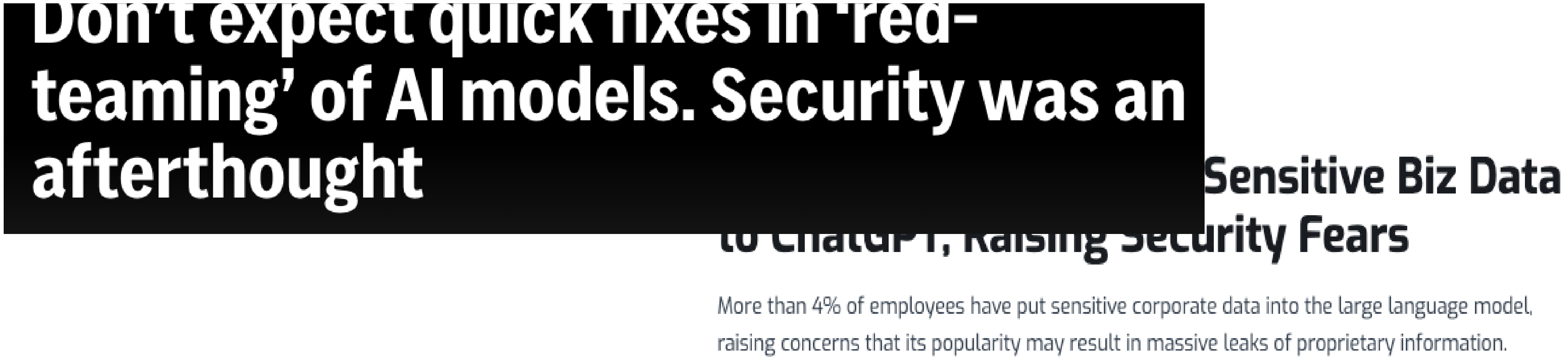
The Exploding Problem



Decrypt

Generative AI a Top Emerging Risk for Organizations: Gartner Survey

Intellectual property, data privacy and cybersecurity are three areas that need to be addressed quickly, according to Gartner.

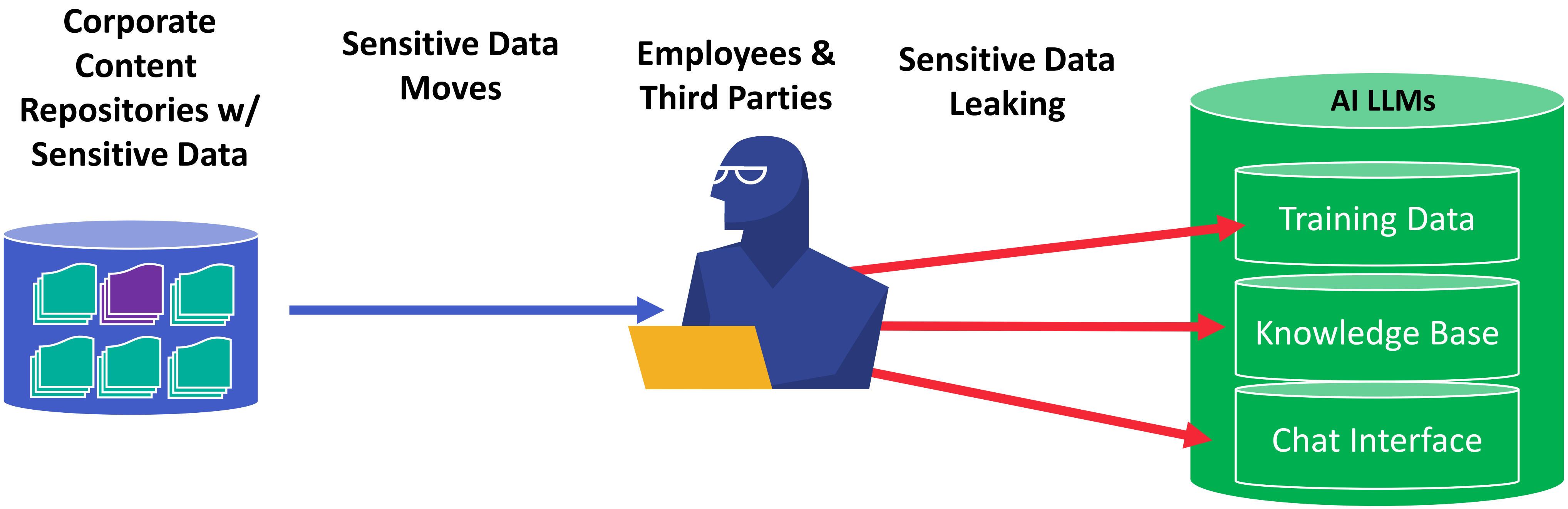


Don't expect quick fixes in 'red-teaming' of AI models. Security was an afterthought

Sensitive Biz Data to ChatGPT, Raising Security Fears

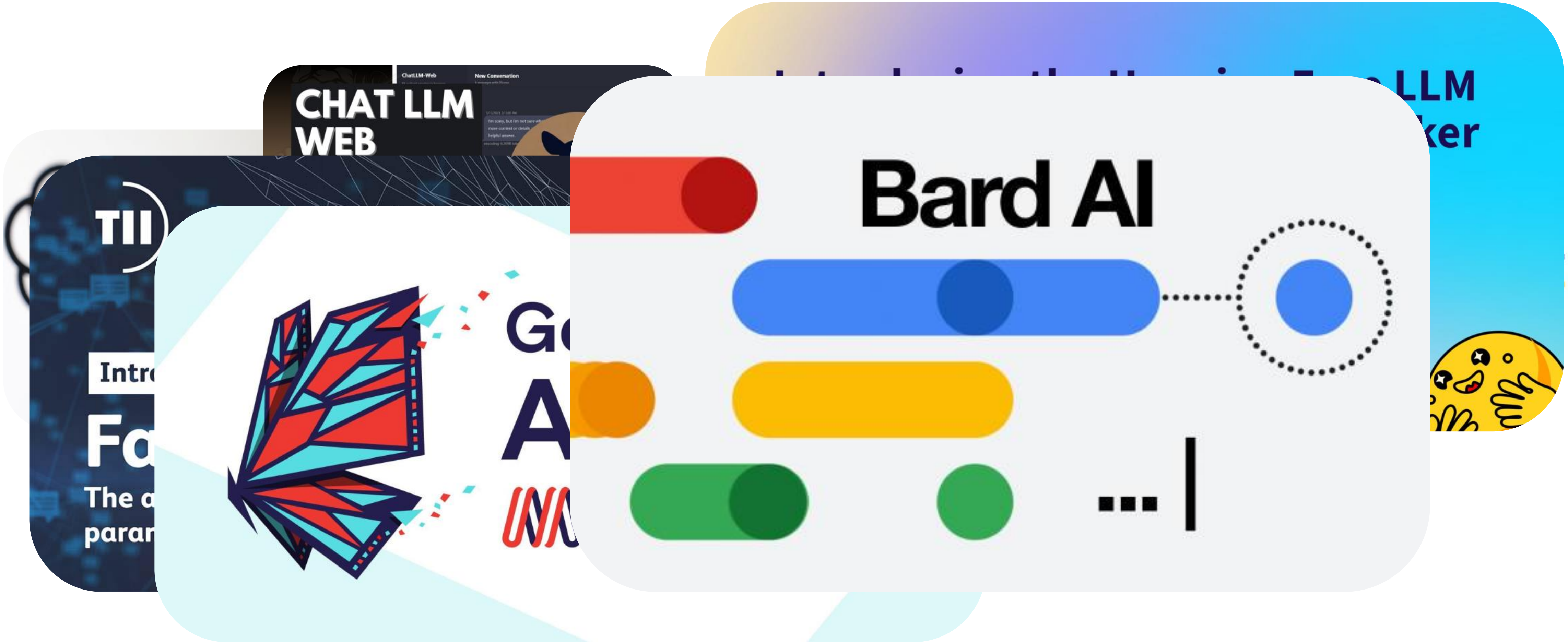
More than 4% of employees have put sensitive corporate data into the large language model, raising concerns that its popularity may result in massive leaks of proprietary information.

What is happening?



Why is the problem growing exponentially?

Because AI LLMs are exploding in offerings and use.



Further compounding the problem…

AI can be a BAD BAD Boy

Meet WormGPT, ChatGPT Alternative Without Boundaries, Ethics and Limits Used by Hackers

Meet PoisonGPT: An AI Method To Introduce A Malicious Model Into An Otherwise-Trusted LLM Supply Chain

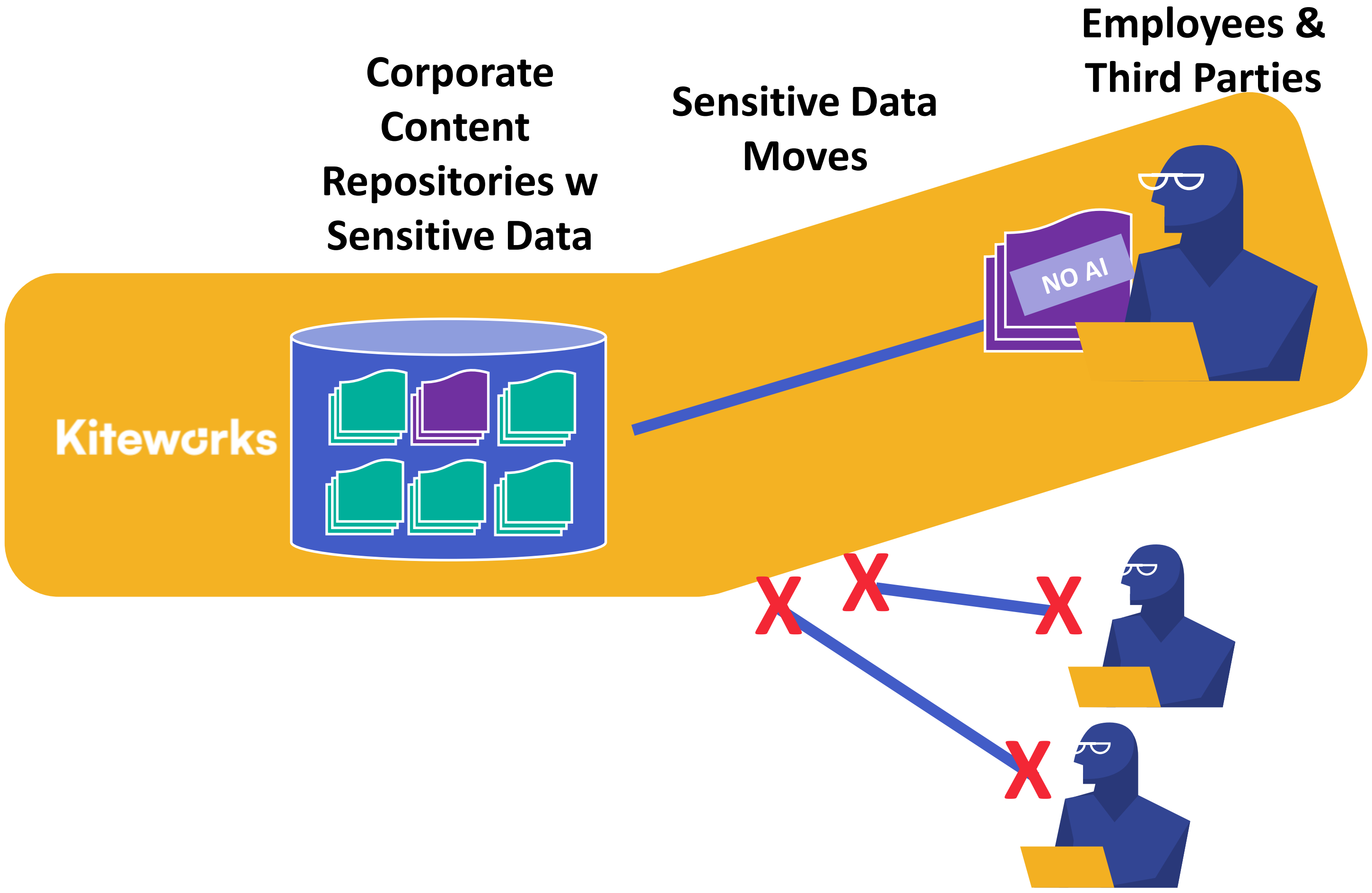
New AI Tool 'FraudGPT' Emerges, Tailored for Sophisticated Attacks

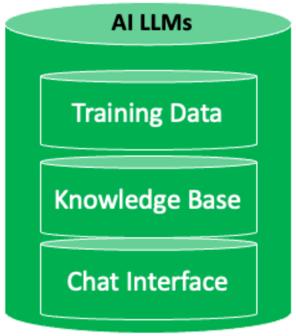
Why is this happening?

SIMPLE:

! Lack of content-based risk policies to prevent AI ingestion.

Solutioning: Content-defined Zero-Trust Controls w/ a PCN


Corporate Content Repositories w Sensitive Data
Sensitive Data Moves
Employees & Third Parties
Kiteworks
NO AI
X
X
X
X

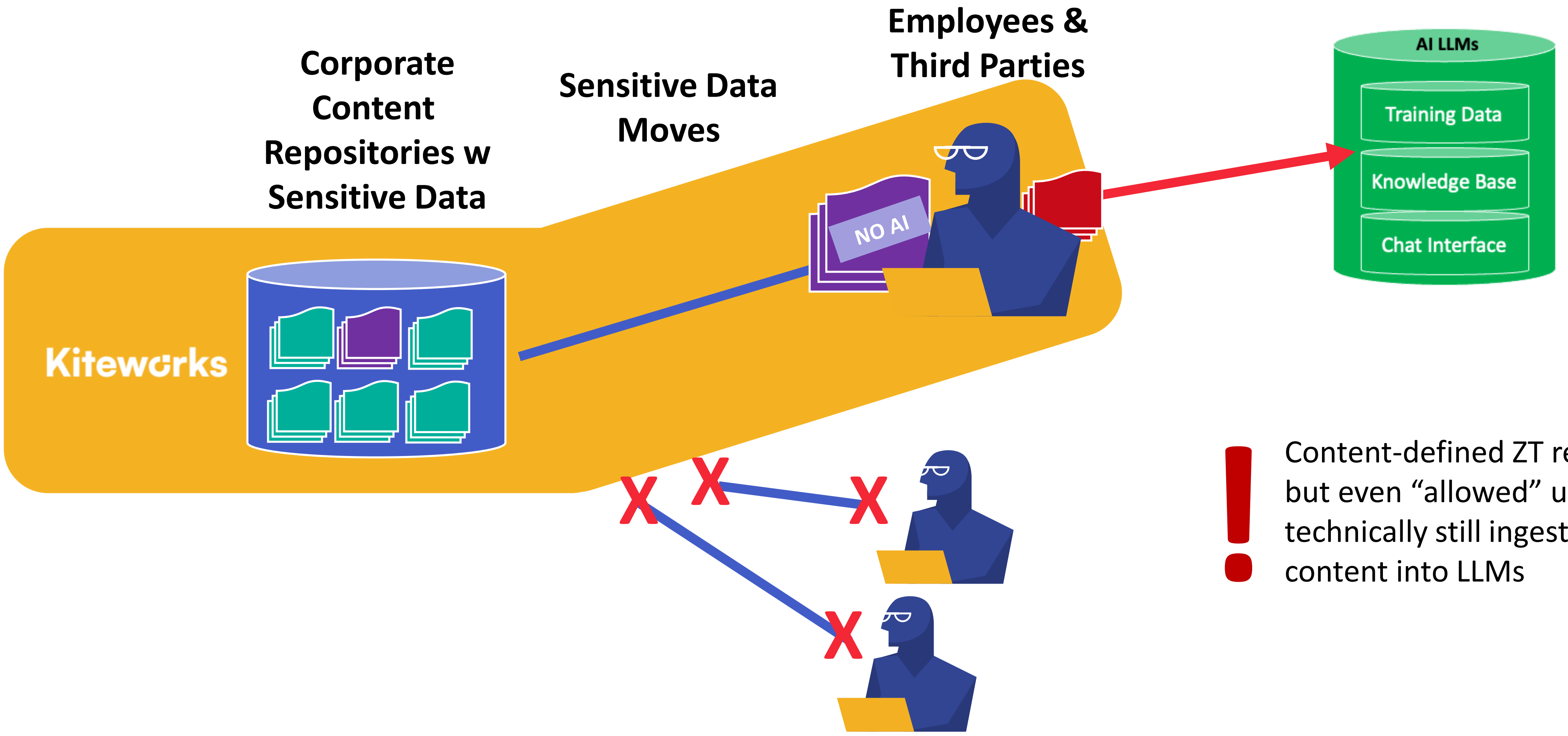


Least privilege access policies defined at the content layer for Risk Reduction

Apply access and use controls by employees and third parties for "least privilege" access to content assets, defined by sensitivity of content assets.

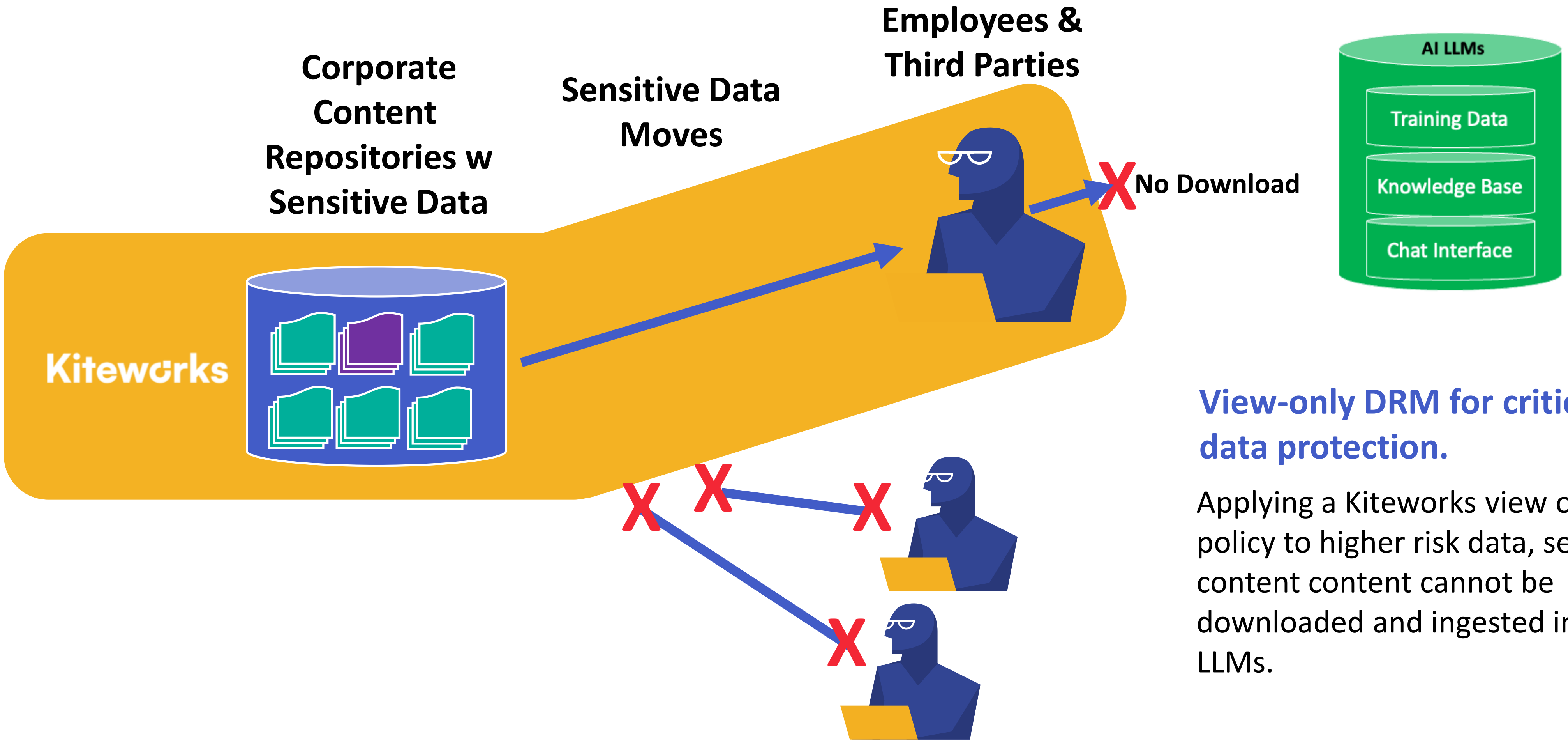
Watermarking can be applied to alert users that specific content should not be used in AI LLMs.

Solutioning: Content-defined Zero-Trust Controls w/ a PCN



! Content-defined ZT reduces risk, but even “allowed” users *could* technically still ingest sensitive content into LLMs

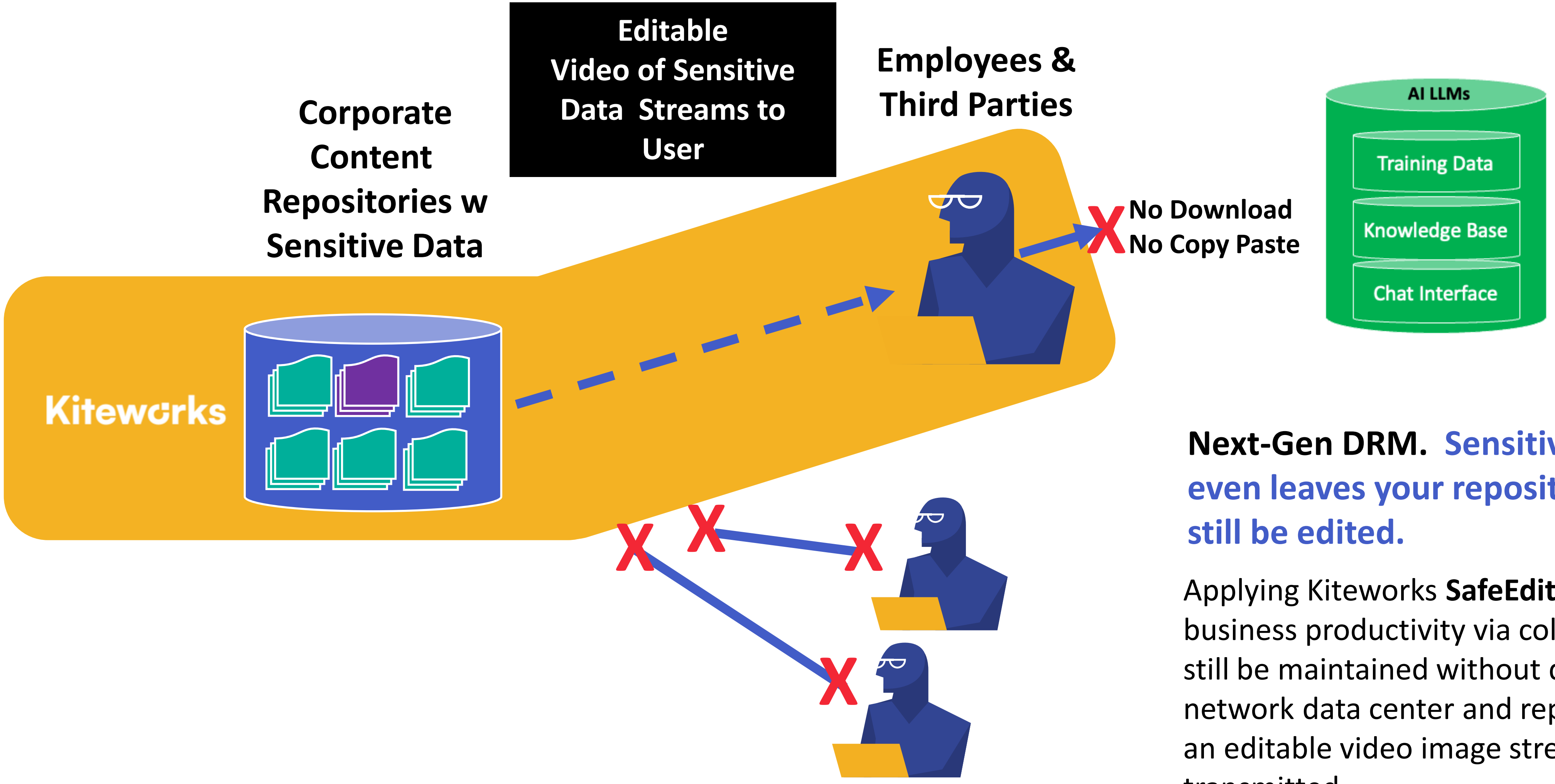
Solutioning: View-only DRM protection with a PCN



View-only DRM for critical data protection.

Applying a Kiteworks view only policy to higher risk data, sensitive content content cannot be downloaded and ingested into AI LLMs.

Solutioning: Next-gen DRM protection with a PCN

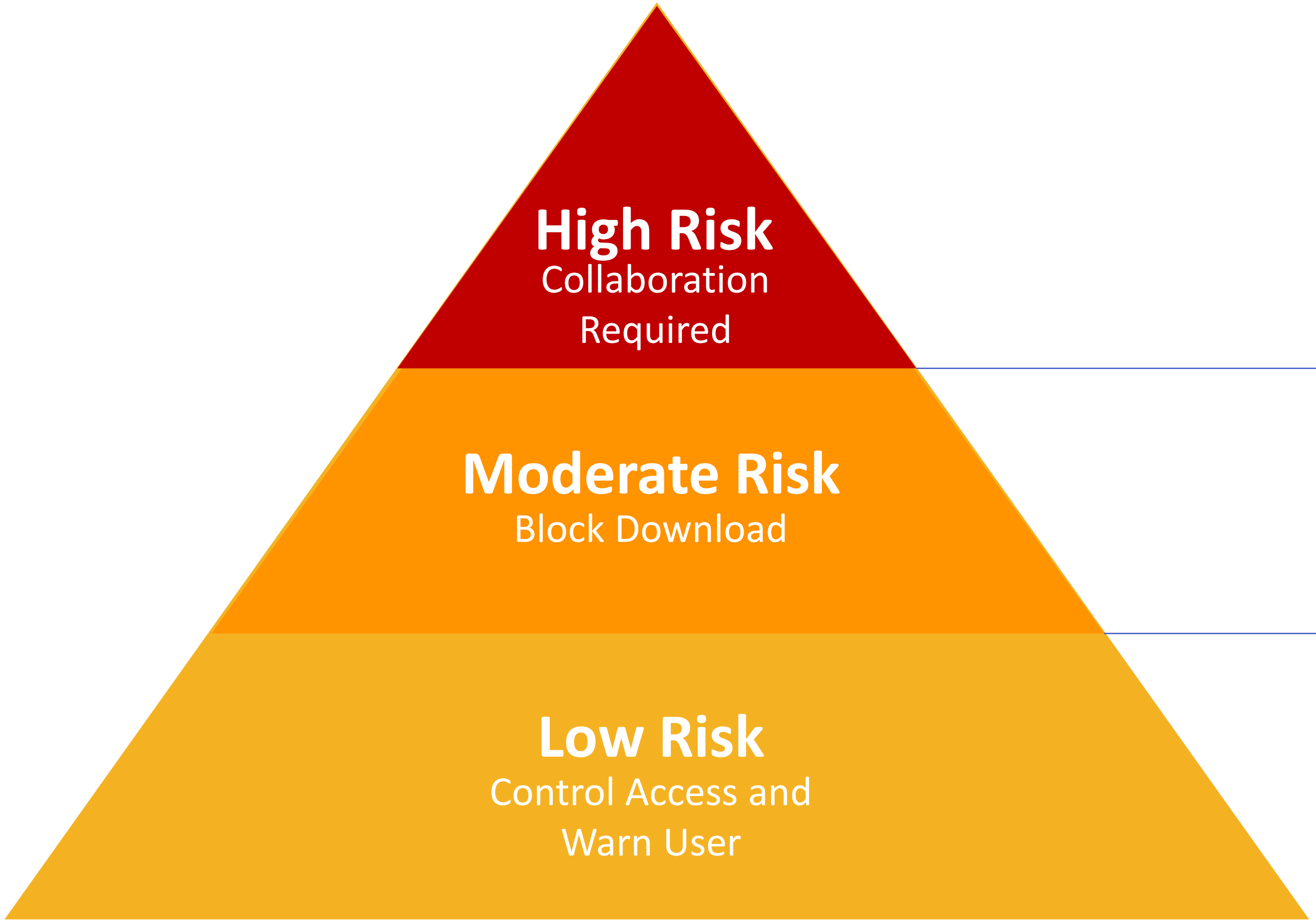


Next-Gen DRM. **Sensitive Data never even leaves your repository but can still be edited.**

Applying Kiteworks **SafeEdit*** policy ensures business productivity via collaboration can still be maintained without data leaving your network data center and repository, as only an editable video image streamed is transmitted.

**Available now in customers on KiteworksLABS axnd in first half 2024 for general access.*

Protect your sensitive content from AI Leaks



Next-Gen DRM – with SafeEDIT* video streamed editing to block downloads and copy paste.

View-only DRM – Block downloads while still transmitting information.

Content-defined Zero Trust Controls – Least-privilege access and applying watermarks.

**Available now in customers on KiteworksLABS axnd in first half 2024 for general access.*

To recap:

1) We’re in the compliance era together
2) Data is everywhere and so to should compliance controls, tracking and reporting
3) Some issues need to be tackled:

    Zero-trust gap
    TPRM gap
    Antiquated approach to DRM

4) Data and privacy protection and compliance has a new vector to be addressed: AI

Kiteworks

THANK YOU