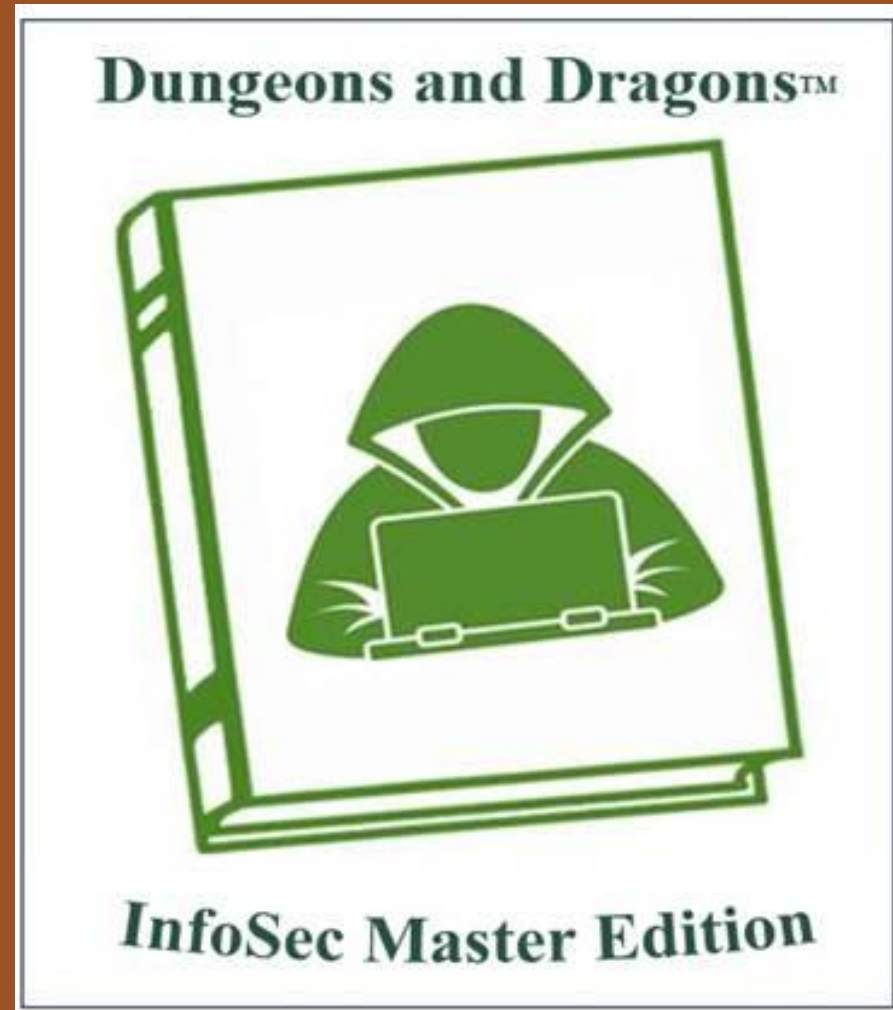


Welcome To The 10th Annual Hacking Conference



Welcome To The 10th Annual Hacking Conference

Remember to check-in to this session
on the app!





Kiteworks

Financial Services Hot Topic Protecting Content on the Cloud

Bob Ertl

Sr. Director, Product, Kiteworks



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**



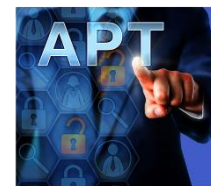
**Internet
Protocols
Era**



**Viruses
Era**



**Hacker
Era**



**APT
Era**



**COMPLIANCE
ERA**

Data Protection and Privacy Legislation Worldwide



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

1970



Bank Secrecy Act of 1970 (BSA)

1986



Money Laundering Control Act

1990



Annunzio-Wylie Anti-Money Laundering Act

2001



The USA PATRIOT Act of 2001

2002



The Sarbanes-Oxley Act of 2002 (SOX)

2002



The Federal Trade Commission's Safeguards Rule for Financial Institutions

2002



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

2003



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

2004



The Federal Information Security Modernization Act of 2002, 2014 (FISMA)

2005



Third EU Money Laundering Directive (3MLD)

2005



Information Security Management ISO 27001

2007



Financial Industry Regulatory Authority (FINRA)

2011



System and Organization Controls 2 (SOC 2)

2013



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

2015



Fourth EU Money Laundering Directive (4MLD)

2017



Title 23 of the New York Codes, Rules and Regulations Part 500 (23 NYCRR 500)

2018



The Payment Card Industry Data Security Standard Version 3.2.1 (PCI-DSS)

2018



NIST Cybersecurity Framework Version 1.1

2018



The General Data Protection Regulation (GDPR)

2025



Cybersecurity Maturity Model Certification (CMMC)

State Data Privacy Regulations 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

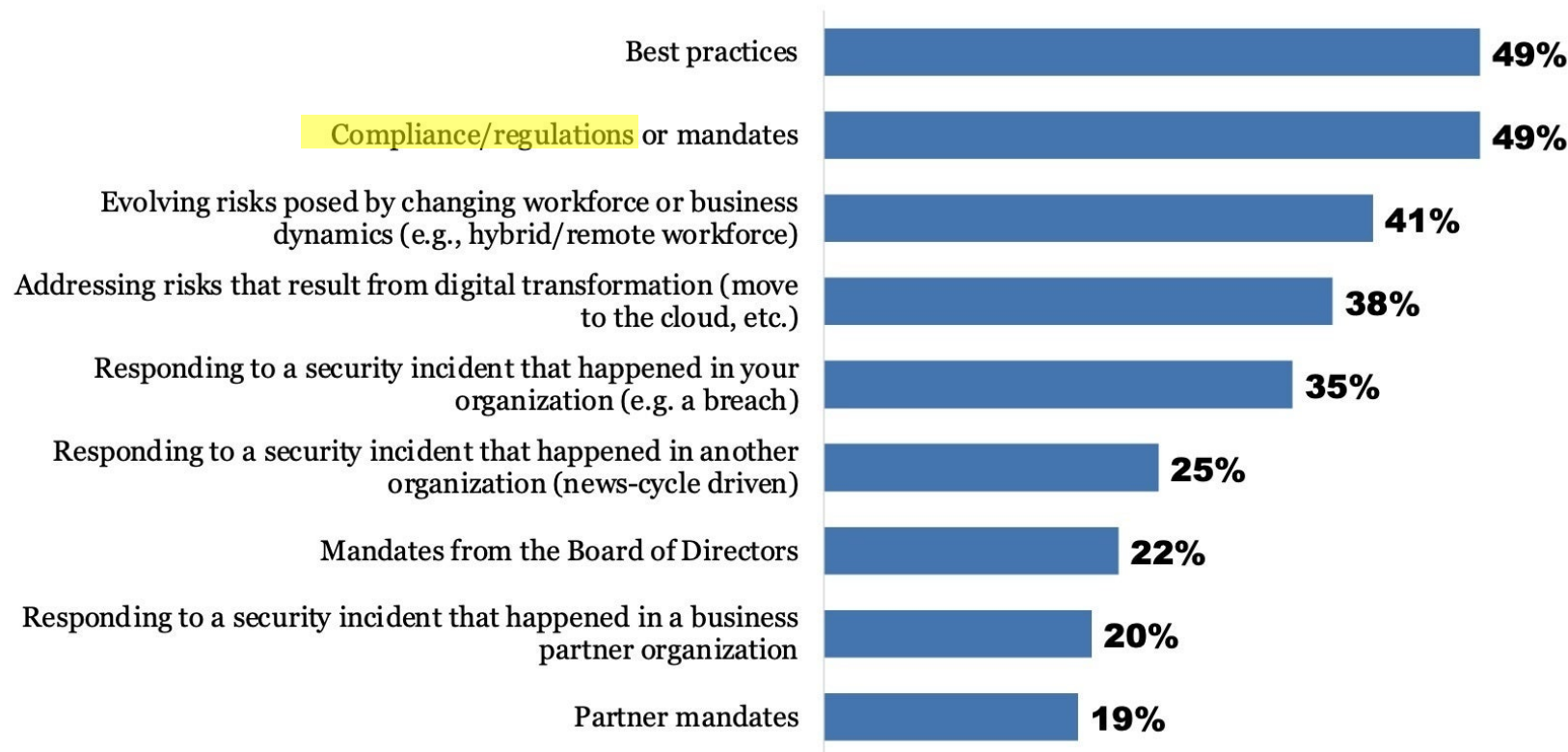
...And More are on Their Way

Hawaii					SB 974	Consumer Data Protection Act
					SB 1110	Consumer Data Protection Act (C)
					HB 1497	
Illinois					HB 3385	Illinois Data Privacy and Protection Act
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	
New Hampshire					LD 2745	Internet Bill of Rights
					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
Oklahoma					SB 5555	It's Your Data Act
Oregon					HB 1030	Oklahoma Computer Data Privacy Act
Rhode Island					SB 619	
Tennessee					HB 5745	Rhode Island Personal Data and Online Privacy Protection Act
					SB 73	Tennessee Information Protection Act (C)
Texas					HB 1181	
Vermont					HB 4	Texas Data Privacy and Security Act
Washington					HB 121	People's Privacy Act (C)
					HB 1616	
Minnesota					SB 5643	(C)
					HB 1367	
Montana					SB 950	
					HB 1892	
					SB 384	Consumer Data Privacy Act



* According to the IAPP

Factors Determining Security Spending



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



Agenda

- ~~1. The Compliance Era~~
2. Cloud Content Communication Risks
3. Impact of Cloud Cybersecurity and Privacy Risks
4. Risk Mitigation
5. Passing Audits With Reporting and Logging
6. How CMMC Affects Financial Services
7. Bonus: Protecting Sensitive Content From AI



Security & Compliance Risks of Sharing Content

Data is at the center of Compliance...



Structured Data
(Databases)



**Personally
Identifiable
Information**



Semi-structured Data
(Logs and Emails)



**Financial
Information**

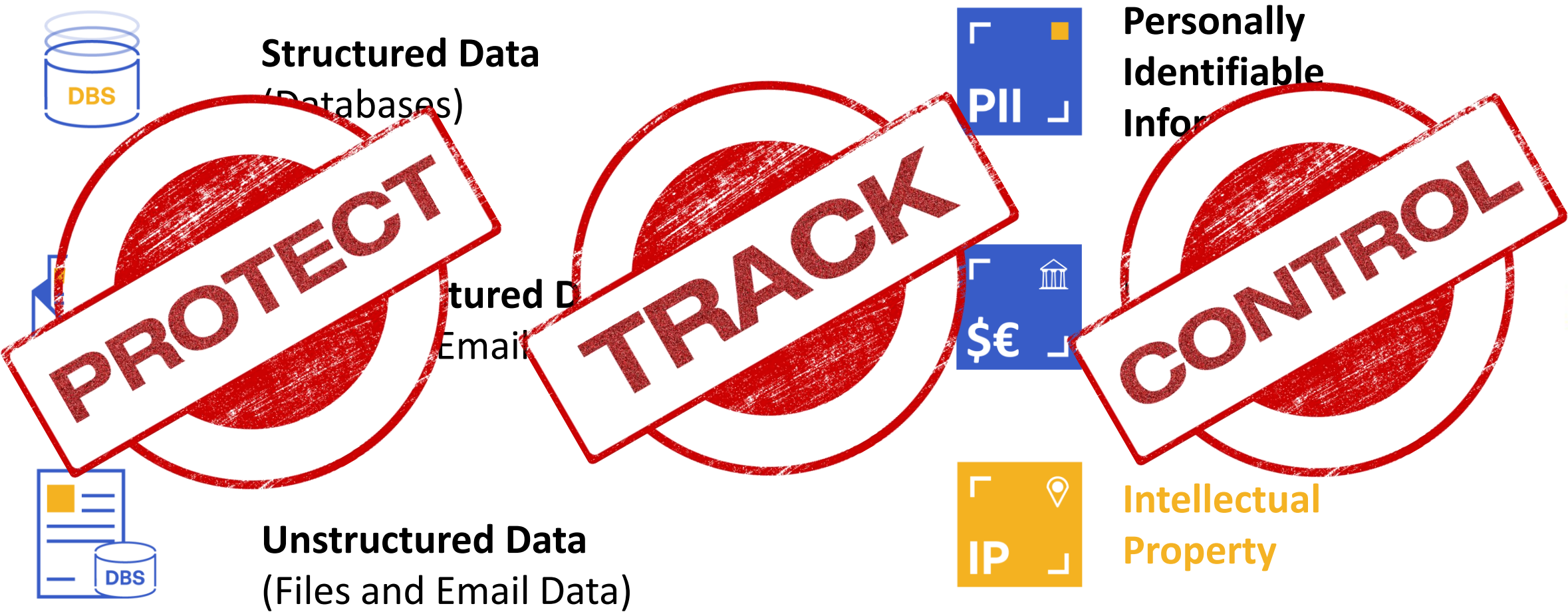


Unstructured Data
(Files and Email Data)



**Intellectual
Property**

Compliance Requirements



The Growing Challenge – Data on the Move



Structured Data
(Databases)



**Personally
Identifiable
Information**



Semi-structured Data
(Logs and Emails)



**Financial
Information**



Unstructured Data
(Files and Email Data)



**Intellectual
Property**

The Growing Challenge – Data on the Move



Structured Data
(Databases)



**Personally
Identifiable
Information**



**Financial
Information**



**Intellectual
Property**



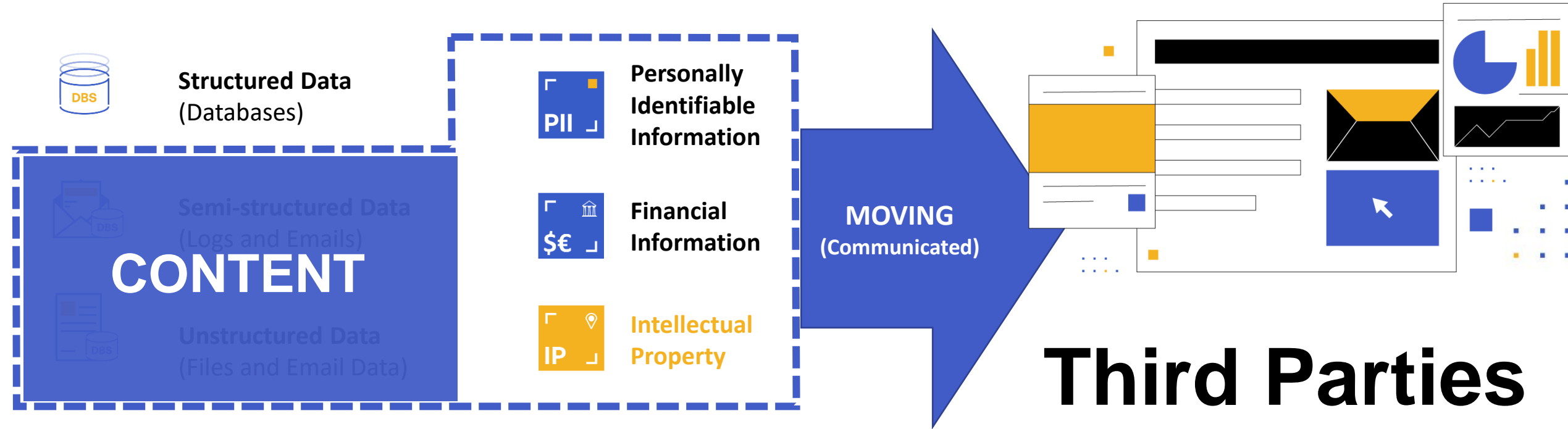
Semi-structured Data
(Logs and Emails)

CONTENT



Unstructured Data
(Files and Email Data)

Data Protection and Compliance Nightmare



According to Gartner

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

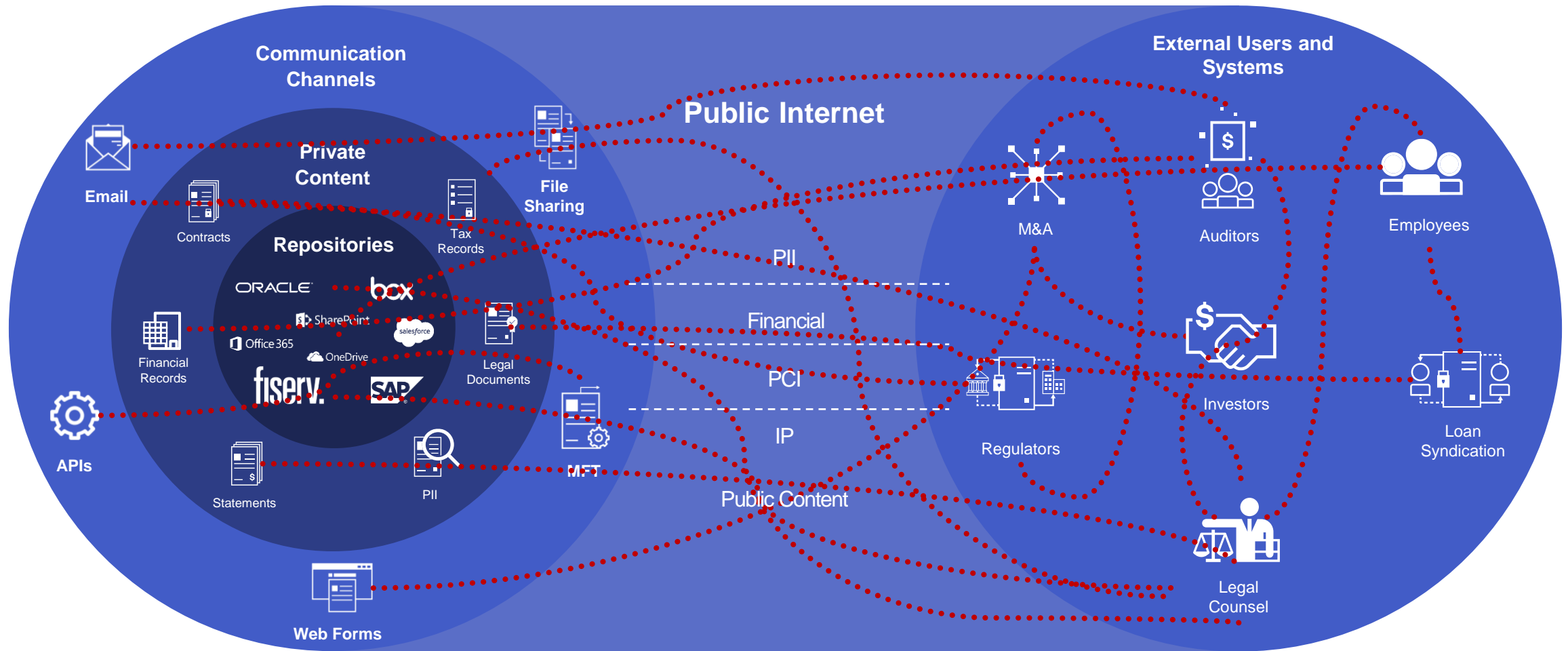


But in the Compliance Era...

Compliance

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





DISPARATE SYSTEMS

POOR TRACKING

NO CONTROL

WEAK SECURITY

Verizon DBIR 2023 Report

Intentional and Inadvertent Sharing of Confidential Data



Misdelivery

43% of Incidents Are Misdelivery

- Unintended recipients
- Unknown recipients
- Shared without controls



Publishing Errors

23% of Incidents Are Publishing Errors

- Wrong recipients

REASONS FOR INTENTIONAL SHARING

89%	Financial	5%	Espionage
13%	Grudge	3%	Convenience

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 financial services, manufacturing, legal, pharmaceuticals, healthcare, government, and more
- Asked them 45 questions about sensitive content communications privacy and compliance



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%

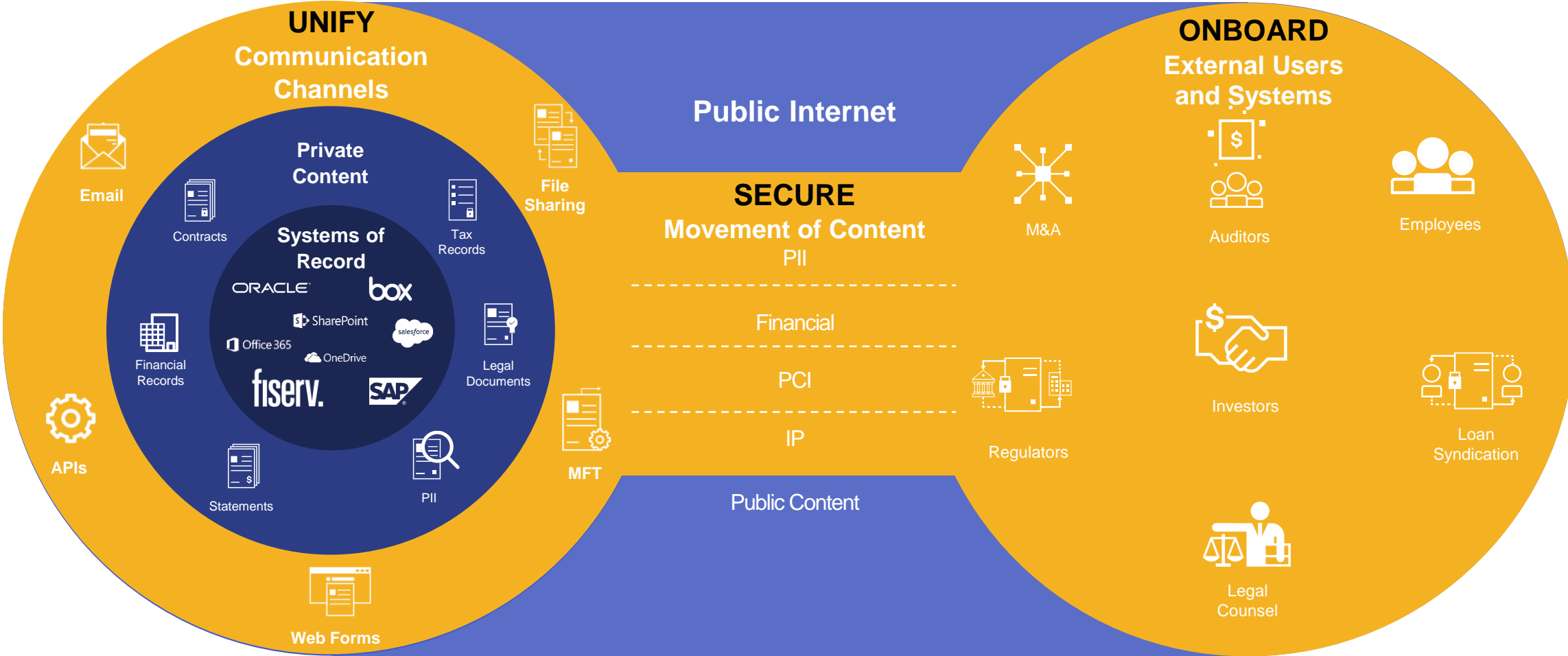
of organizations experienced financial damage as a result of an attack on sensitive content communications.

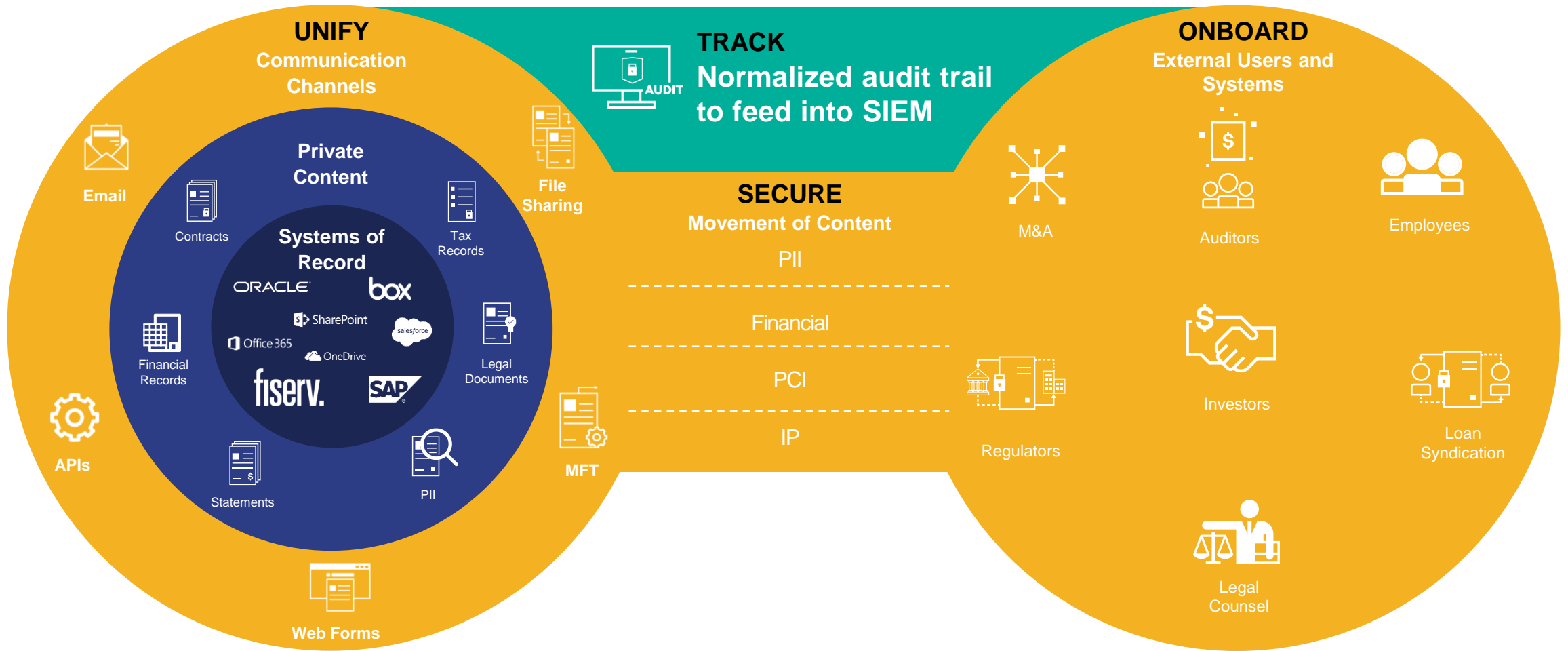




Risk Mitigation

Unify, Track, Control, and Secure Third-party Communication







TRACK

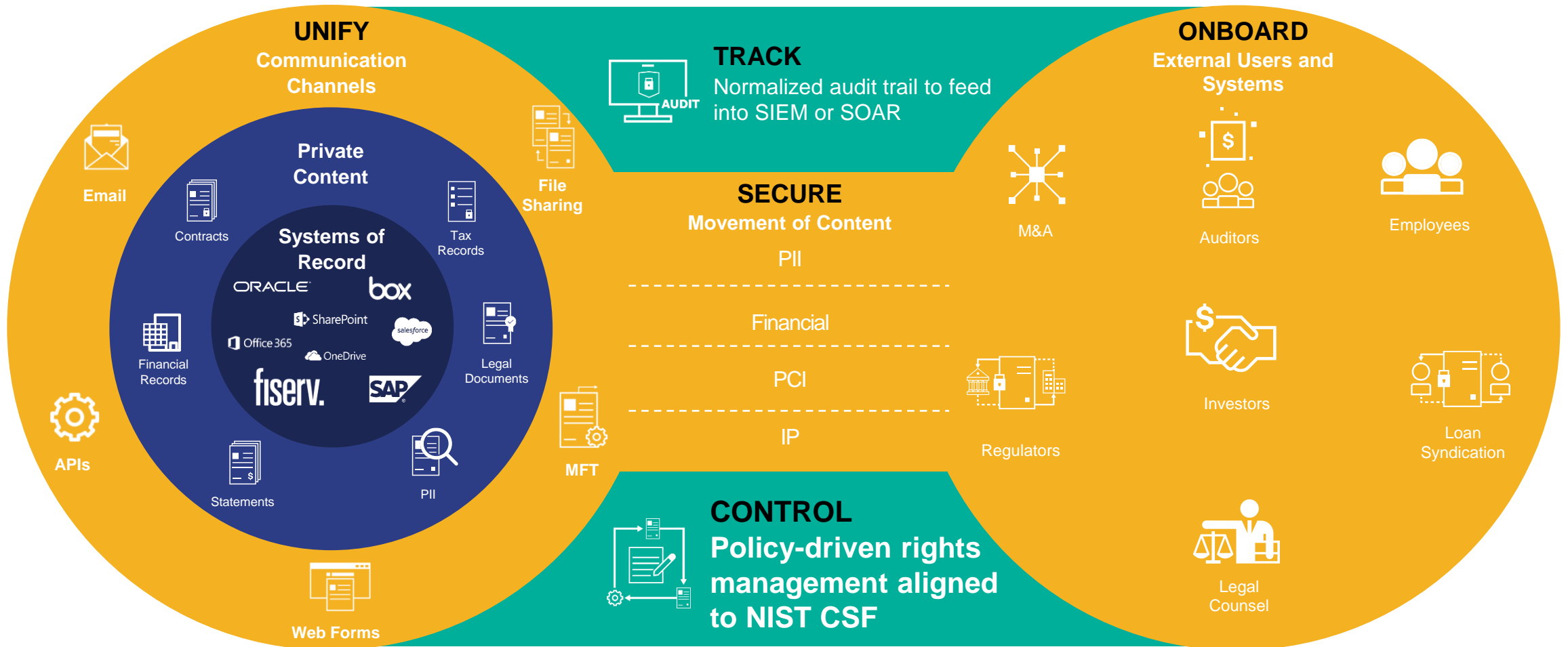
Pass Audits and Support SecOps

Tracking Enables Compliance Audits & SOC

- Comprehensive audit log
- Centralized, normalized, real time
- User, admin, system activities
- Custom and ad hoc reporting
- Canned reports for regulations

Security Information and Event Management (SIEM)

- Aggregates logs from across the infrastructure and apps
- Correlates events
- Monitors for incidents
- Built-in analytics
- Major vendors: Splunk, IBM QRadar, LogRhythm, etc.





CONTROL

Policy-driven rights management aligned to NIST CSF



DRM Policies Prevent Unintended Access

- Least-privilege defaults
- Granular access controls
- DLP with blocking & audit
- View-only with watermark
- Copy and forward controls
- File/folder expiration
- AIP sensitivity label content policies



Admin Policies Minimize Insider Risk

- Admin cannot access content
- Separation of duties
- Folder ownership management
- Data sovereignty
- Legal hold for eDiscovery



Authentication Validates Identity

- LDAP / MSAD / SCIM / native
- Credentials, certificate, SMS OTP
- MFA (RADIUS, native), OAuth
- SAML 2.0, Kerberos, PIV/CAC



Mitigation #1

Third Party Risk Management

Tackling the Issue: TPRM



Managing risks of sharing sensitive content:

- Regular risk assessments
- Contractual obligations
- Continuous monitoring
- Incident management
- Education and awareness
- TPRM in your data-centric security and compliance strategy

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.

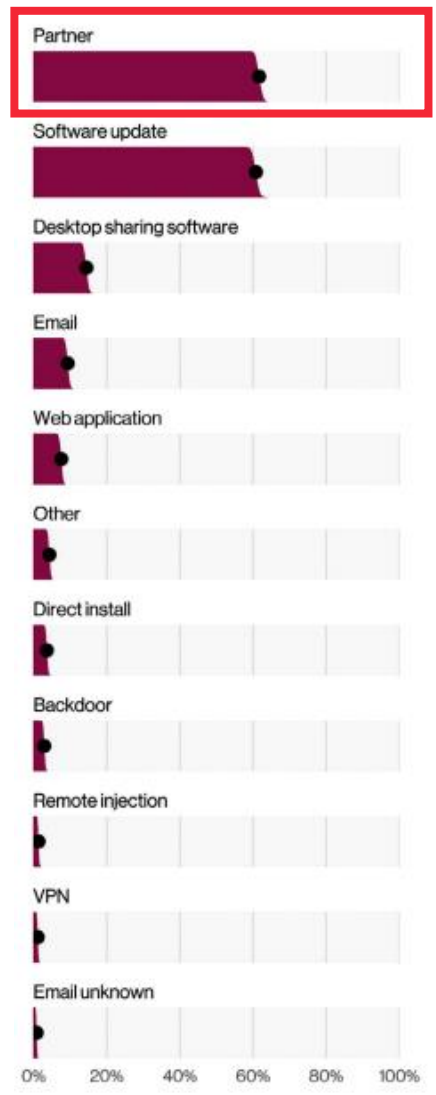
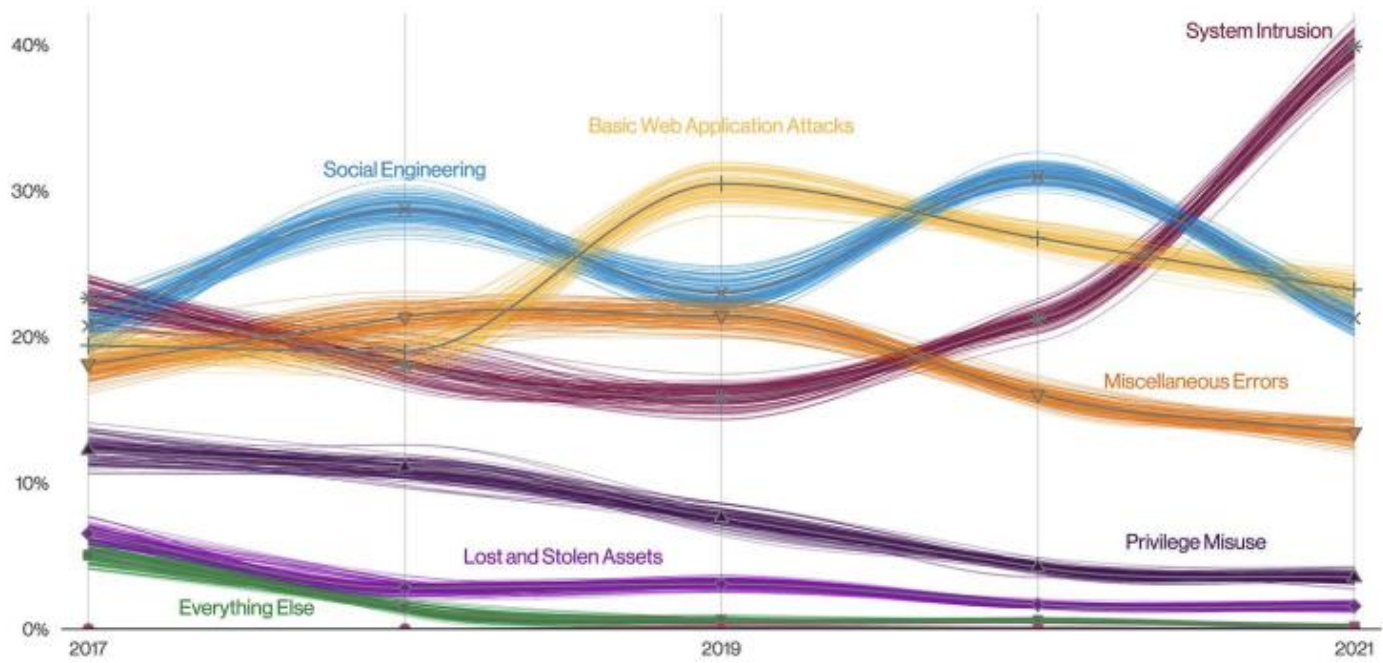


Figure 36. Top Action vectors in System Intrusion incidents (n=3,403)

Triage Approach to Assessing Risks According to Gartner

1. IDENTIFY RISKS

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

2. ASSESS VENDOR

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

No or minimal assessment

GAP

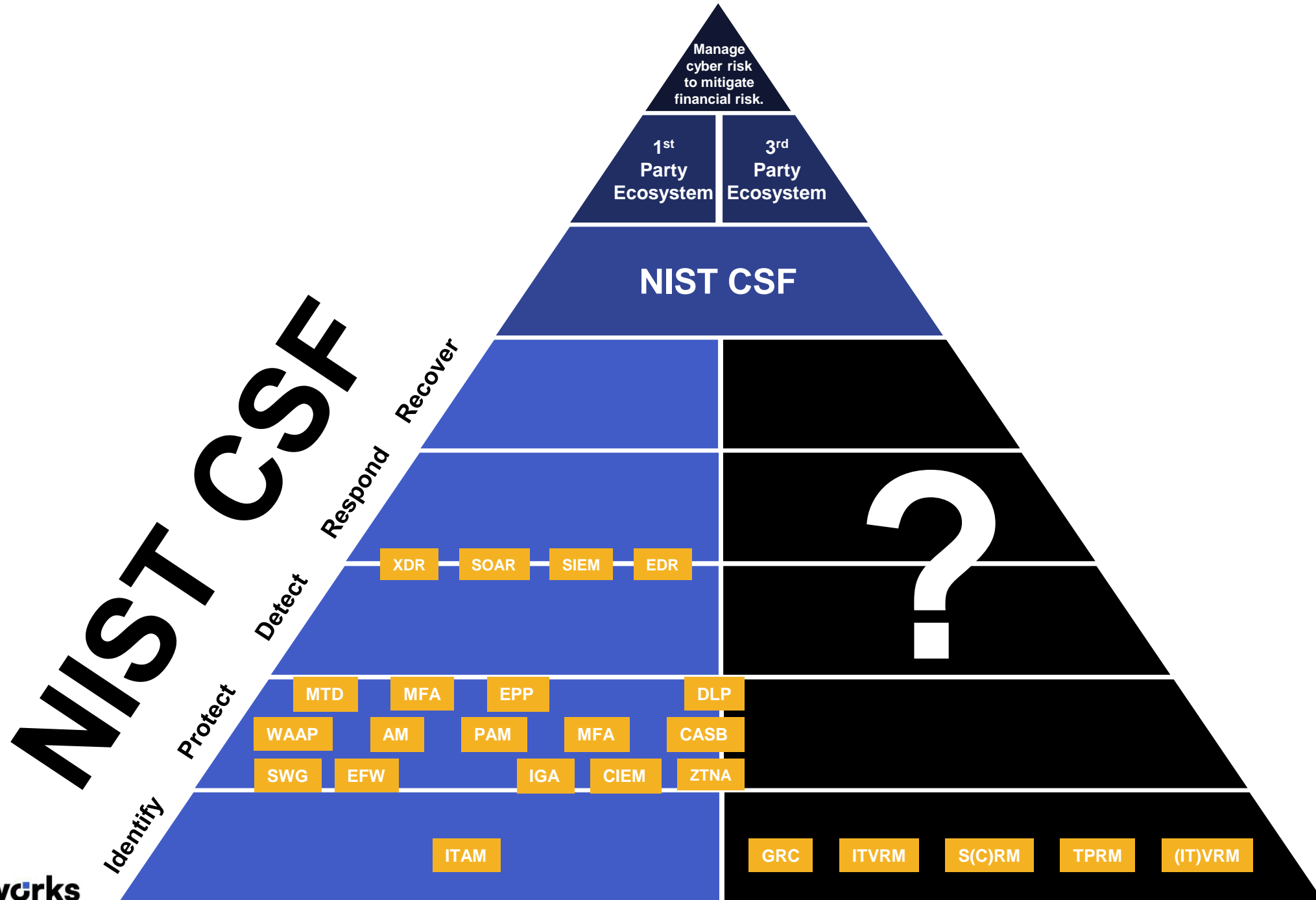
**How to
manage data
after vendor
approval?**

3. ANALYZE

Quantify risk impacts

Determine mitigation
requirements

Determine contract implications



Close The Gap

1. IDENTIFY RISKS

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

2. ASSESS VENDOR

Assess vendor controls
Assess vendor security/risk capabilities
Assess vendor BCM/DR, incident response
Use focused questionnaires
(e.g., SIG, SIFMA, etc.)
Validate controls

GAP

- **Control: zero-trust principles at the content layer.**
- **Protect: encryption and DRM**
- **Unify content communication channels.**
- **Track it all.**

3. ANALYZE FINDINGS

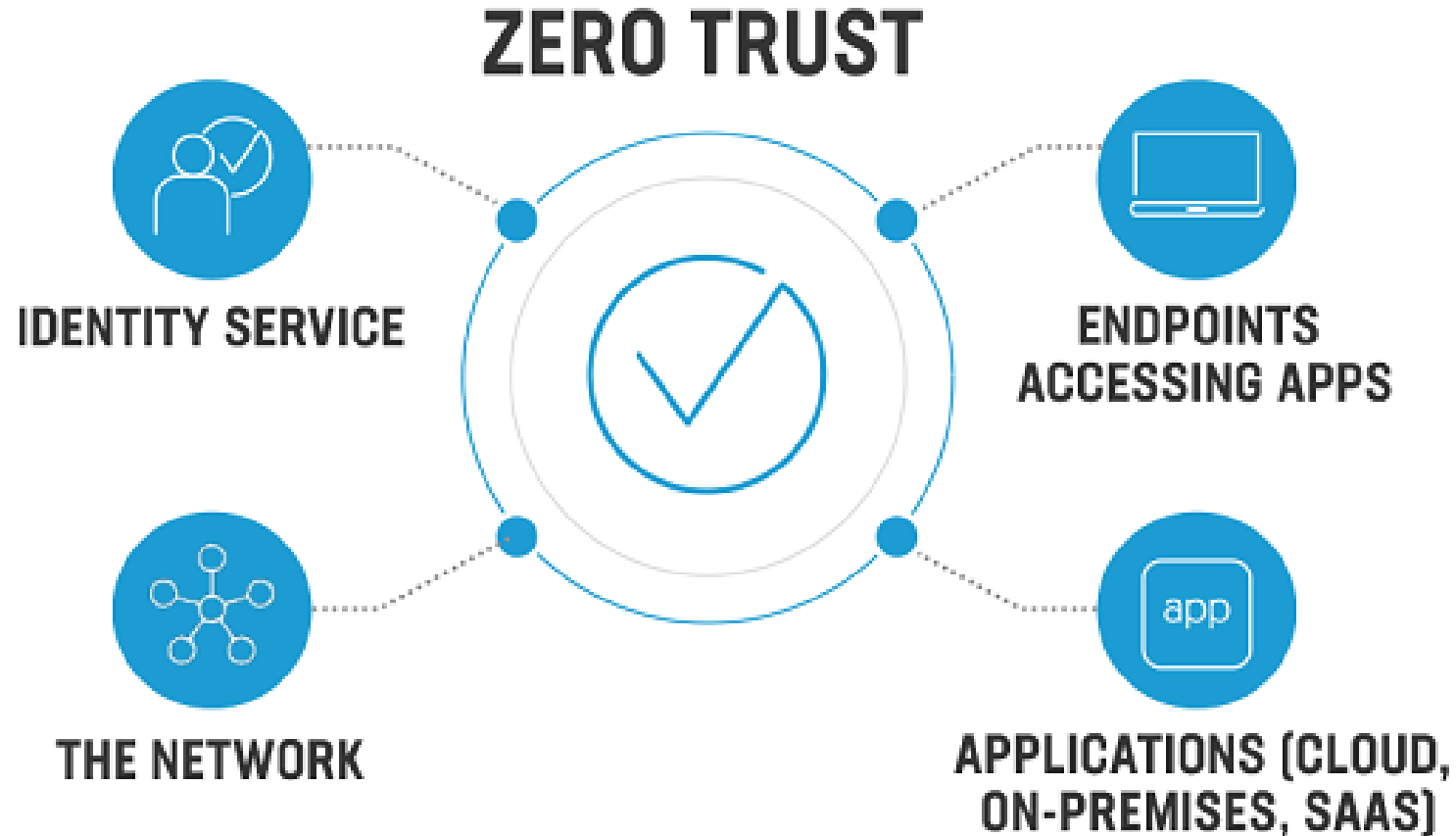
Quantify risk impacts
Determine mitigation
requirements
Determine contract implications



Mitigation #2

Zero Trust

Assume Attackers Have Infiltrated Your Organization

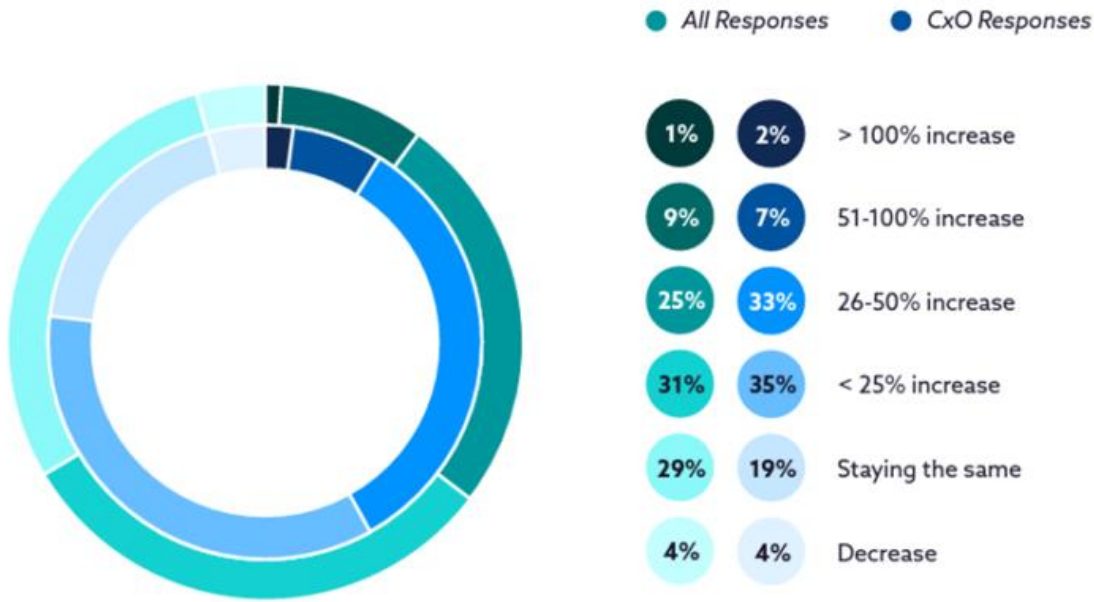


Principles

1. Always authenticate
2. Least privilege access
3. Micro-segment networks
4. Continuously monitor and analyze

Organizations Are Adopting Quickly Now

Describe your organization's investment in Zero Trust over the next 12 months.



The Cloud Security Alliance (CSA) recently published its latest report, CISO Perspective and Progress in Deploying Zero Trust. The study is based on interviews with security and risk management professionals and C-level executives who provided insights into current and future zero trust deployment plans. It found that

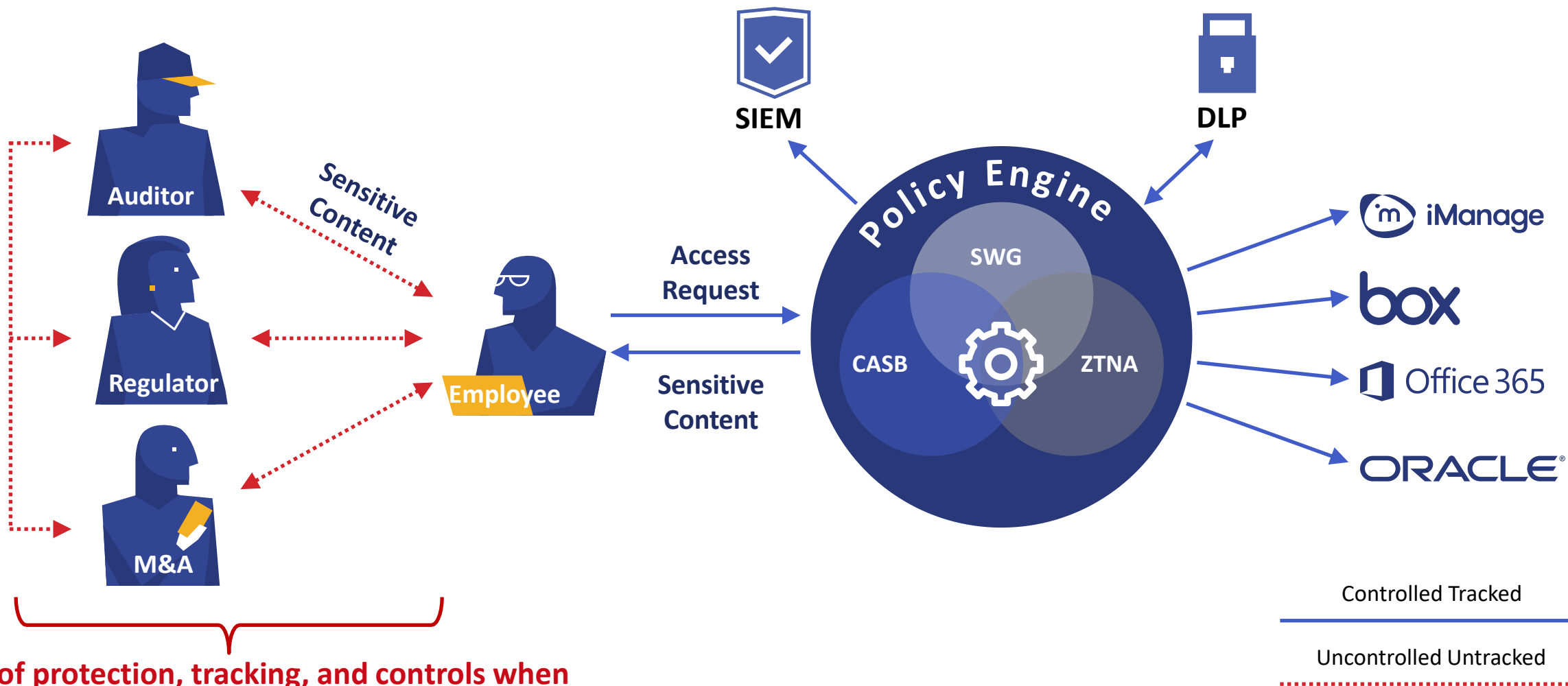
- 80% of C-level executives cite zero trust as a priority for their organizations, and
- 94% are implementing zero-trust strategies.

Ericom's Zero Trust Market Dynamics Survey found that

- 80% of organizations plan to implement zero-trust security in less than 12 months, and
- 83% agree that zero trust is strategically necessary for their ongoing business.

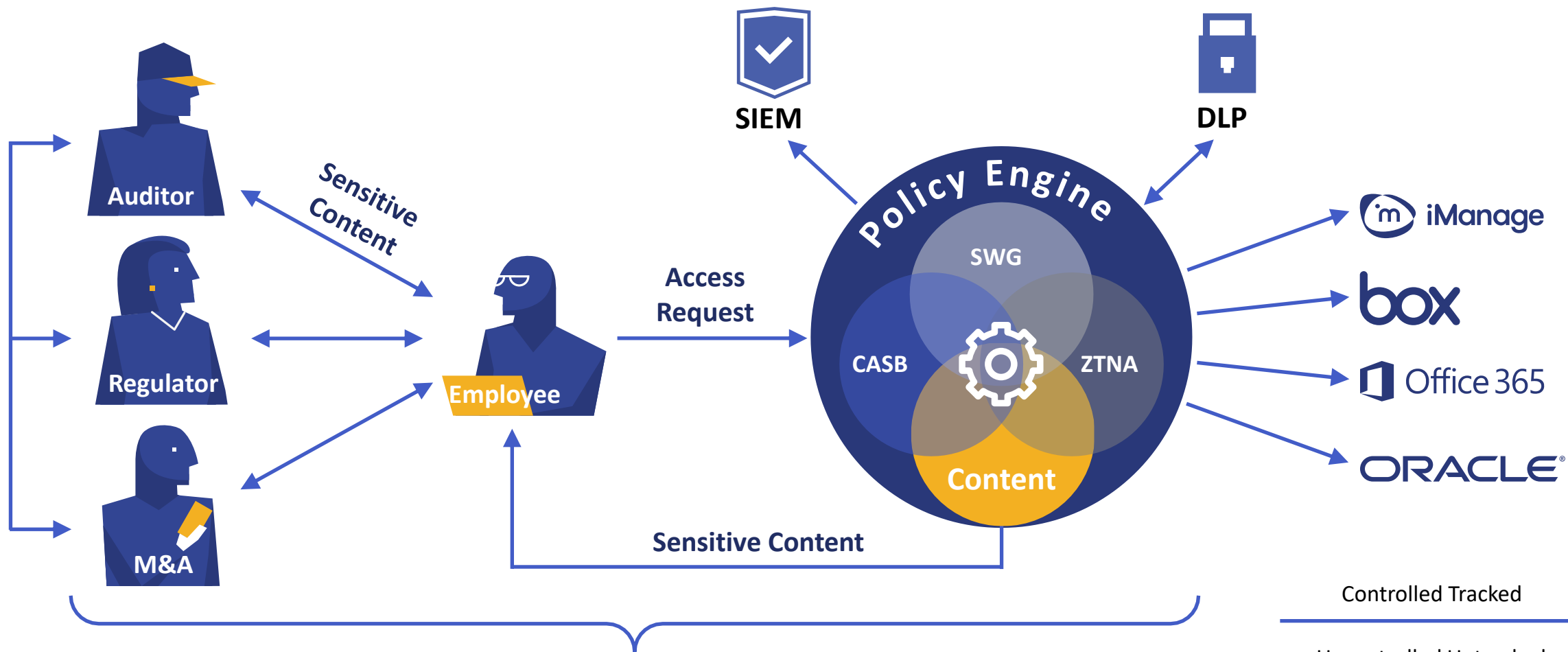
CISOs must remove trust from tech stacks and define their unique strategy to adopt the framework.

Managed Risk in Network and Application Access



Loss of protection, tracking, and controls when sensitive content moves to third-parties.

Adding Content-defined Zero Trust



Sensitive content is now fully tracked and controlled with zero-trust principles applied.



Mitigation #3

Digital Rights Management (DRM)

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.



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).

Today's Approach to DRM is Legacy



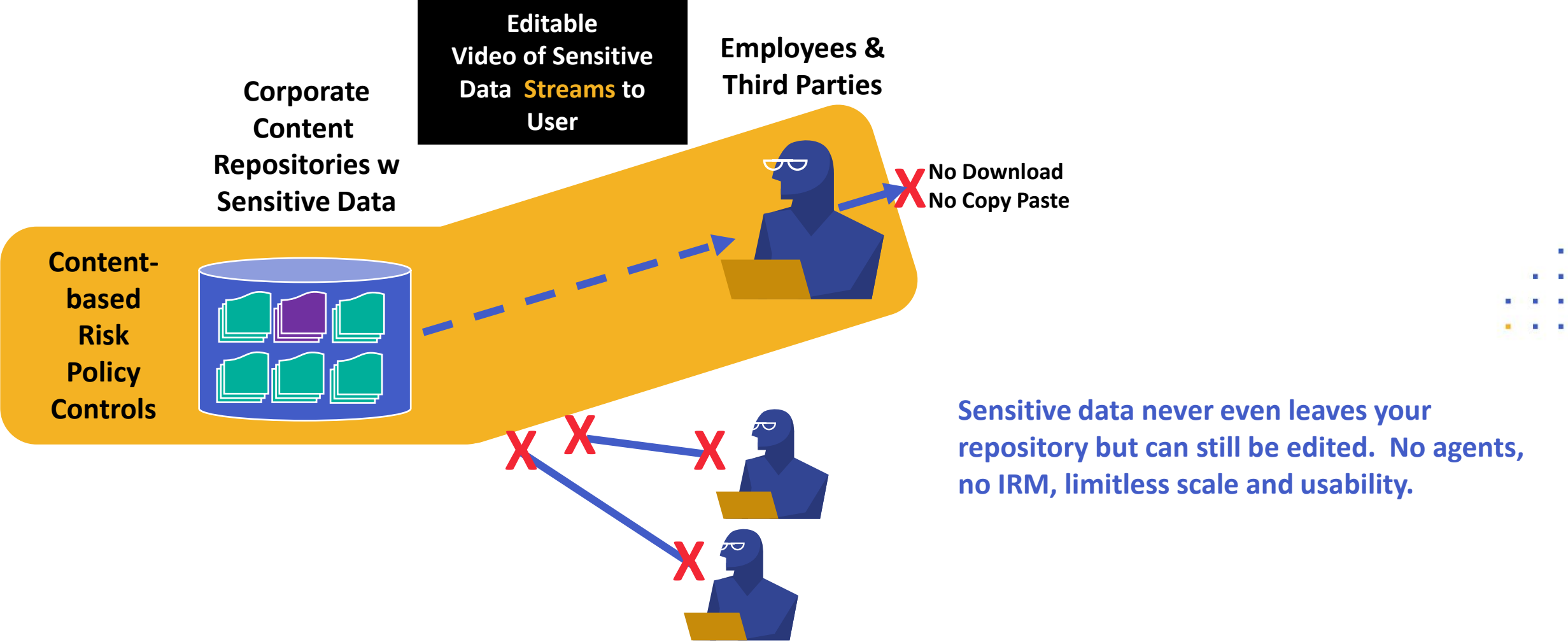
“A cryptographic element: Information
is encrypted so that protection
travels with data no matter where it
moves or rests”



Accomplished primarily as agent-based digital

- Issues in scale and functionality – low adoption
- File leaves your environment – increased risk

Enter Next-Gen DRM





Mitigation #5

Privacy Protection from AI

The Exploding Problem



Generative AI a Top Emerging Risk for Organizations: Gartner Survey

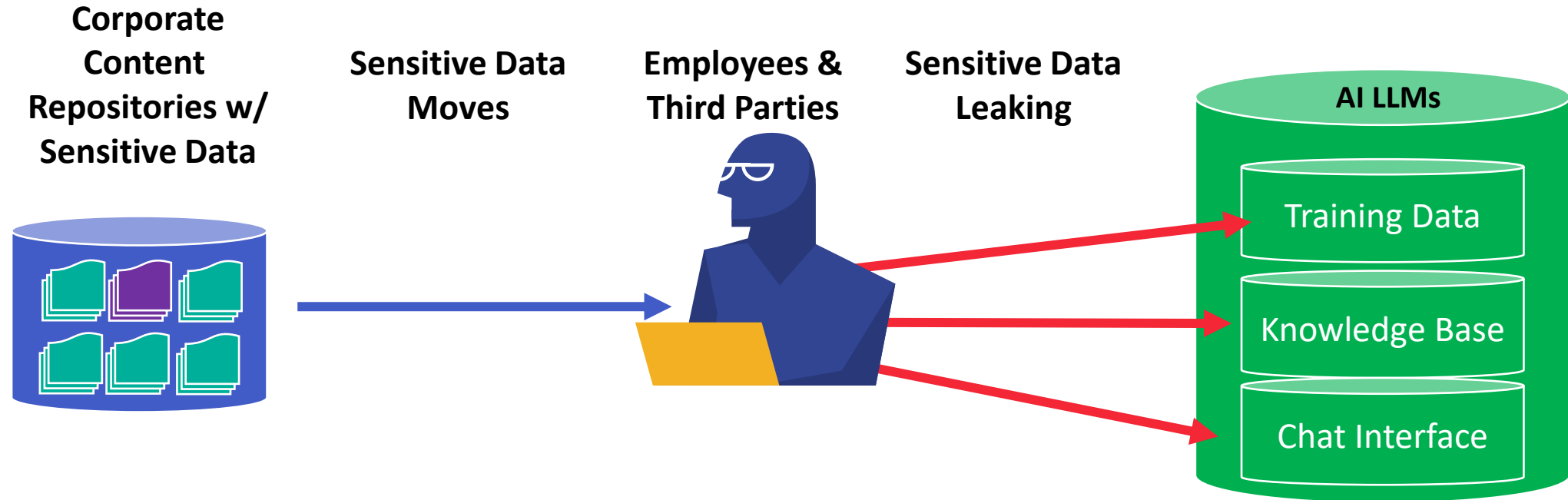
Intellectual property, data privacy and cybersecurity are three areas that need to be addressed quickly, according to Gartner.

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

**Sensitive Biz Data
Security Fears**

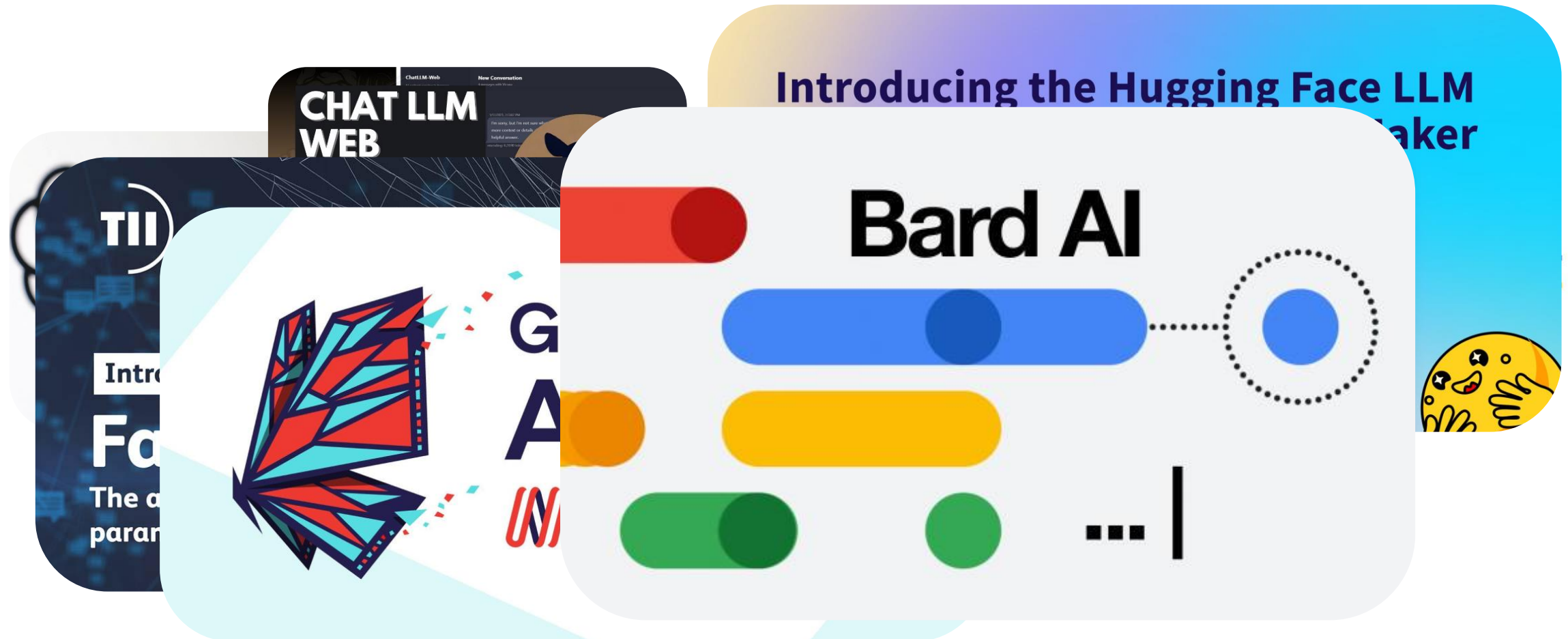
More than 4% of employees have put sensitive corporate data into the large language model, raising concerns that its popularity may result in massive leaks of proprietary information.

What Is Happening?



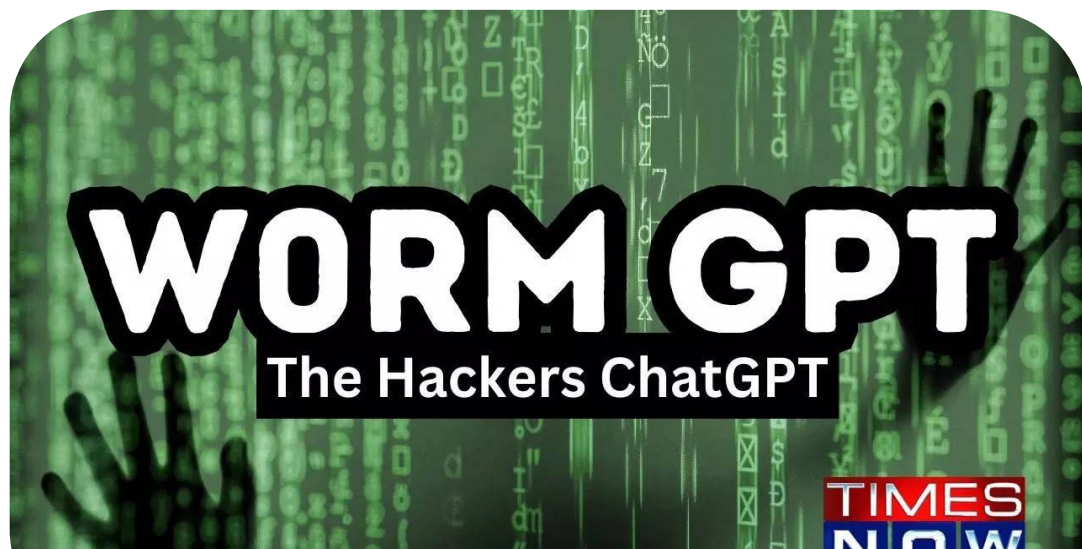
Why Is the Problem Growing Exponentially?

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?

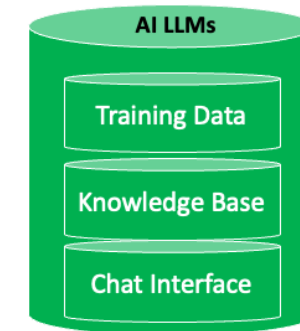
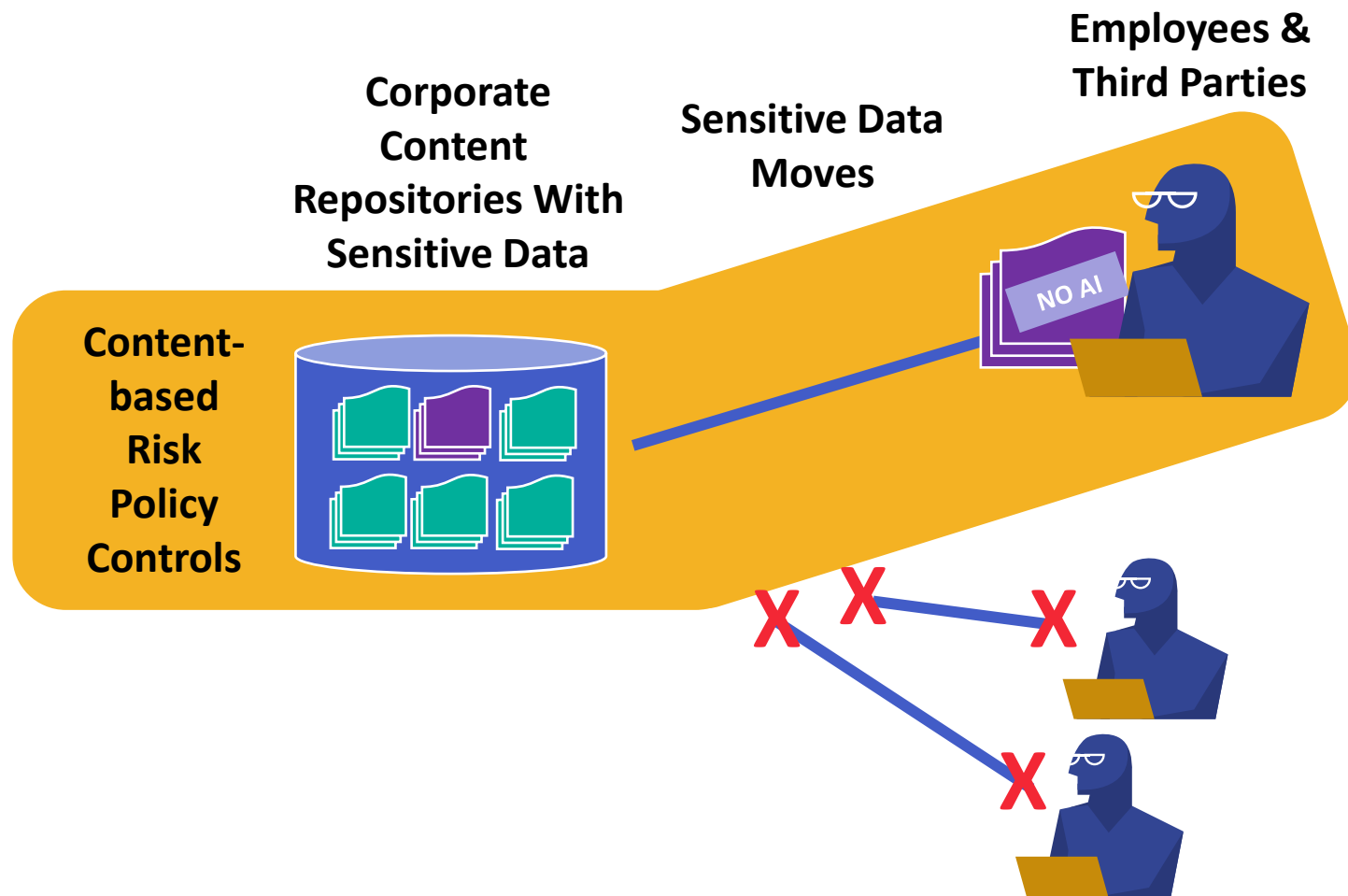
SIMPLE:



Lack of data encryption
and content-based risk
policies to prevent AI
ingestion.



Solutioning: Content-defined Zero-trust Controls

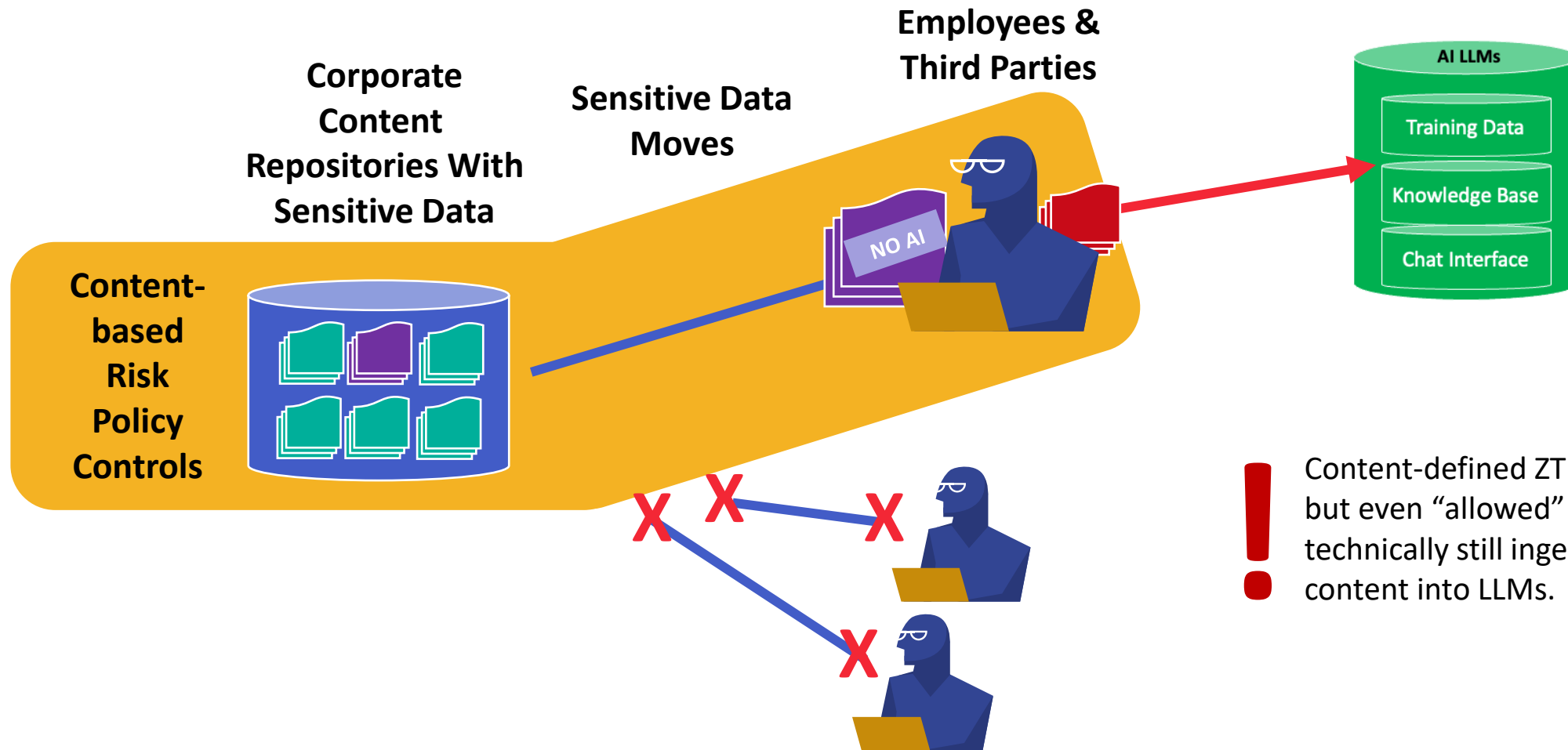


Least privilege access policies defined at the content layer for Risk Reduction.

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

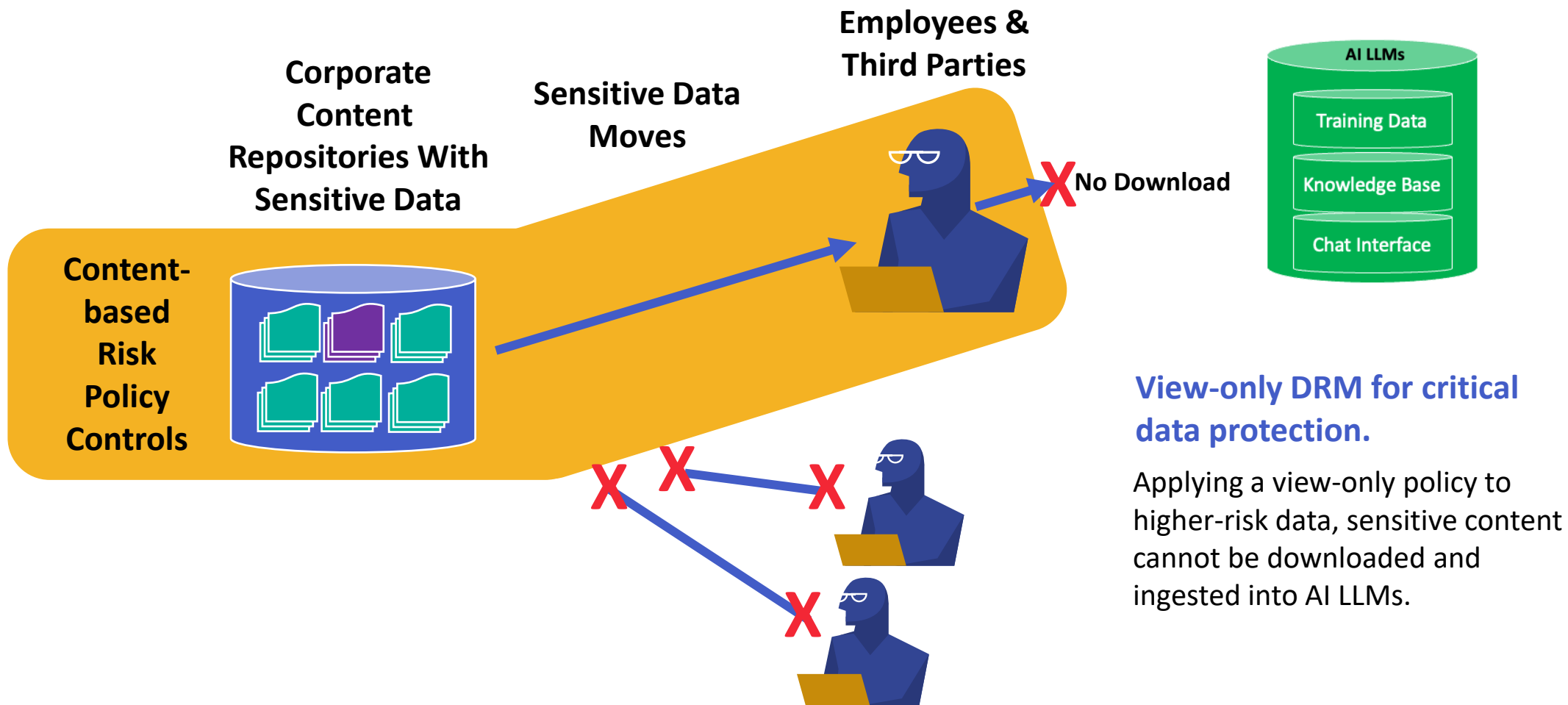
Watermarking can be applied to alert users that specific content should not be used in AI LLMs.

Solutioning: Content-defined Zero-trust Controls

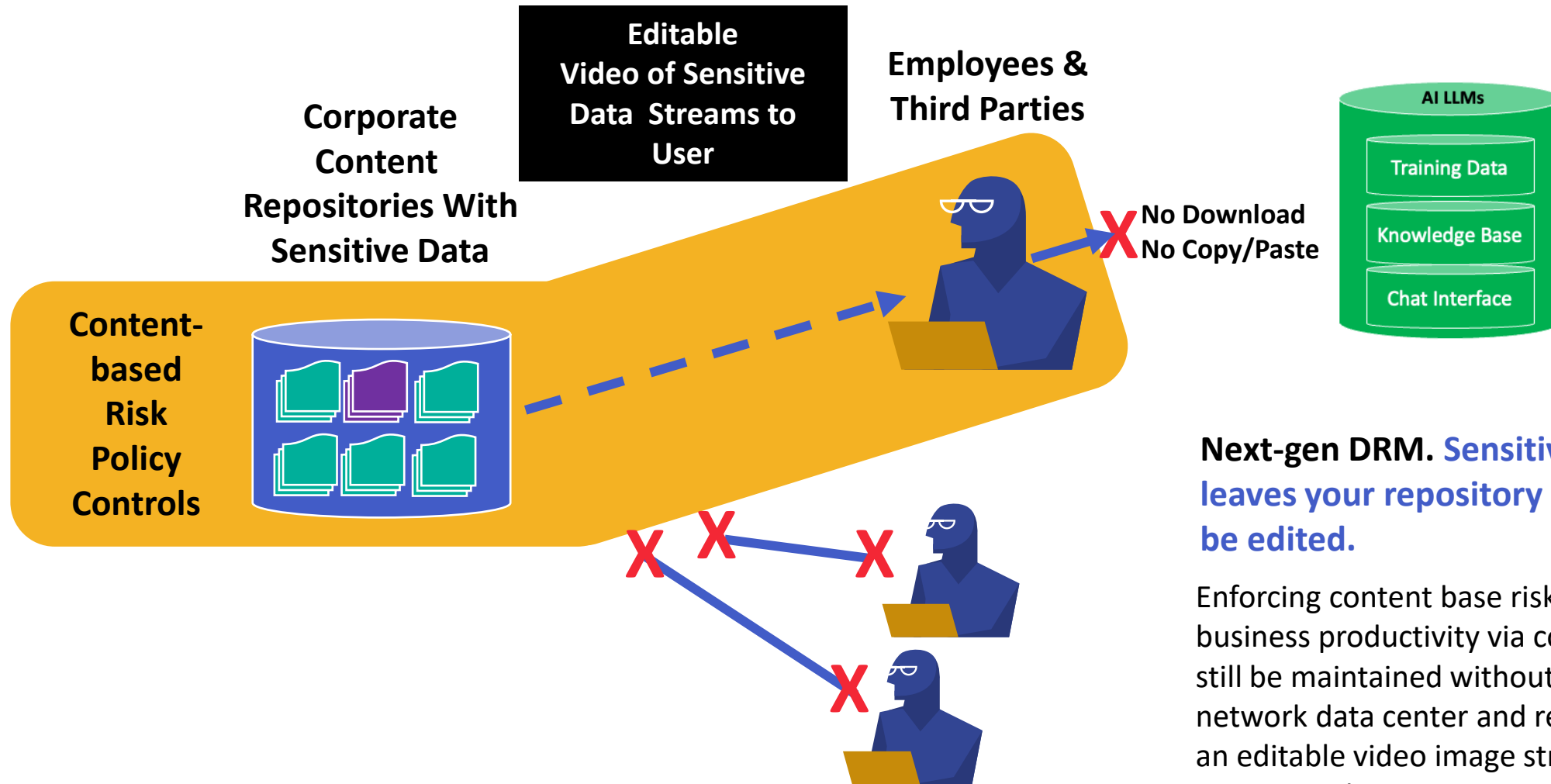


Content-defined ZT reduces risk, but even “allowed” users *could* technically still ingest sensitive content into LLMs.

Solutioning: View-only DRM Protection



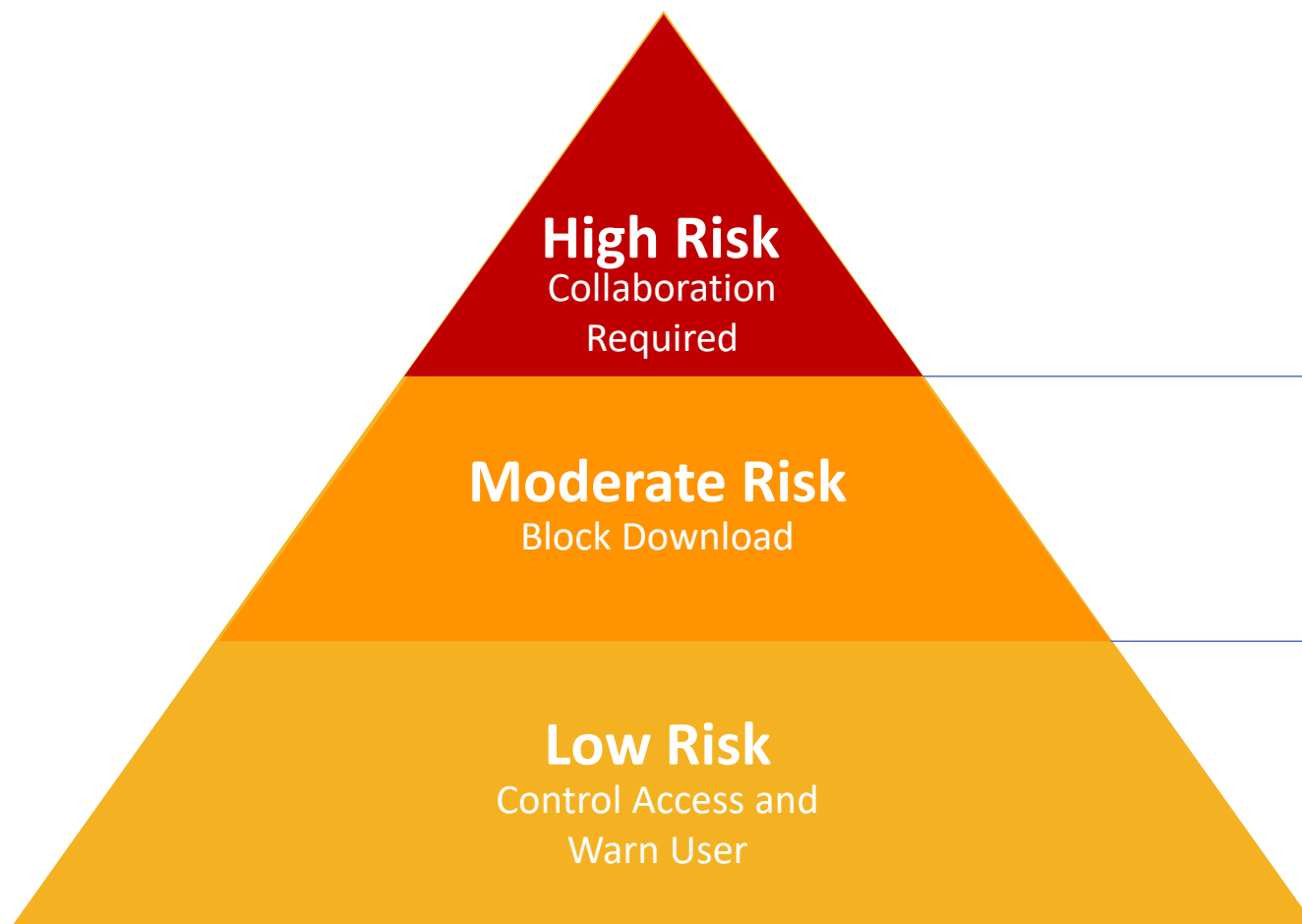
Solutioning: Next-gen DRM Protection



Next-gen DRM. Sensitive data never leaves your repository but can still be edited.

Enforcing content base risk 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.

Protect Your Sensitive Content From AI Leaks



Next-gen DRM – With safe video streamed editing that blocks downloads and copy/paste.

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

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



Mitigation #6

CMMC

Cybersecurity Maturity Model Certification

CMMC

Cybersecurity Maturity Model Certification



- **What:** Framework for cybersecurity practices across DoD supply chain
- **Standard for:** Cybersecurity practice implementation and compliance verification
- **Required for:** All DoD suppliers including subcontractors
- **Required before:** October 2025 it will be included in all DoD contracts



CMMC

Content Classes Protected

FCI – Federal Contract Information

Requires protection but is not critical to national security

Most common for financial services organizations



CUI – Controlled Unclassified Information

Requires safeguarding or dissemination controls per laws, regulations, and government policies



CMMC 2.0: 3 Levels



Level 1

Foundational

Applies to: Contractors working with FCI only

Regulation: 17 practices

Annual Self-Assessment: Attestation from senior company official

Level 2

Advanced

Applies to: Contractors working with CUI

Regulation: NIST 800-171 (110 practices)

Certification: Conducted and reported every three years year by accredited C3PAO



Level 3

Expert

Applies to: Contractors working with CUI on DoD's highest priority programs such as developing parts for a weapons system or C&C communications system

Regulation: NIST 800-172 (110+ practices)

Assessments: Triennial assessments by Defense Industrial Base Cybersecurity Assessment Center audit teams

To recap:

1. We're in the compliance era together
2. Data is everywhere – and compliance controls, tracking, and reporting should be everywhere too
3. Some issues need to be tackled:
 - a) Third Party Risk Management (TPRM) gap
 - b) Zero-trust gap
 - c) Antiquated approach to DRM
4. Data and privacy protection and compliance have two new vectors to be addressed: AI and CMMC



Kiteworks

THANK YOU



kiteworks.com/kiteworks-brief-sensitive-content-communications-privacy-and-compliance-in-financial-services/

kiteworks.com/sensitive-content-communications-report

Welcome To The 10th Annual Hacking Conference

Remember to check-in to this session
on the app!



Speaker: Bob Ertl, Sr. Director of Product Marketing, Kiteworks

Title: Financial Services Hot Topic - Protecting Content on the Cloud

Synopsis:

In a fast-paced digital world, businesses rely heavily on email and file sharing to communicate and collaborate internally and with external parties. However, with the rise of cyberattacks and data breaches, secure file sharing has become an increasingly critical issue for organizations.

Financial services organizations rely heavily on exchanging and storing vast quantities of sensitive documents, making secure file sharing a critical component of their cybersecurity strategy. By implementing certain file sharing practices, these institutions can mitigate risks associated with unauthorized access, content breaches, and potential disruptions to critical infrastructure. And by instituting comprehensive audit logging and reporting practices, they can reduce the risks of adversarial and potentially failed regulatory audits.

In this talk, Bob will explore how organizations, particularly the financial services industry, play an important role in protecting critical infrastructure, based on professional experience and lessons learned from how companies implement cybersecurity measures.

At the end of the campaign, you will learn (takeaways):

- **What good compliance and reporting means in the financial services space,**
- **How CMMC applies to financial services, and**
- **Why not having unresolved issues coming out of your financial risk management is important. .**

Date: November 6, 2023