Unfortunately, you lost your data.

Who will knock on your door & Why?

Gopi Ramamoorthy

CISSP, CISA, CIPP/US, CISM

Head of Security & GRC Engineering

gopi@symmetry-systems.com

SYMMETRY

ISC2 East Bay Chapter

Agenda

Why this topic is important

Knowing key regulations and liabilities

Learning from the past

Summary and Takeaways

Why is this topic, about losing your data, important?

Why is this topic important?

Increased breach rate

Data breaches are on the rise despite increased security measures. Organizations must adopt a data-centric security approach to protect sensitive information and establish a robust incident response plan.

Tactical Approach

To combat the growing threat of data breaches, organizations need to shift their focus to data-centric security. This includes implementing strong access controls, encryption, and comprehensive data loss prevention strategies.

Risk Management

Failing to prioritize data-centric security can have severe consequences, including financial loss, reputational damage, and regulatory penalties. Organizations must take proactive steps to protect their sensitive data.

Know your data assets

TYPE OF DATA

- Customer data
- PII
- PHI
- PCI
- Finance
- CUI (CMMC)
- Classified / Top Secret
- IP
- Training Data for AI Systems
- Synthetic Data
- More

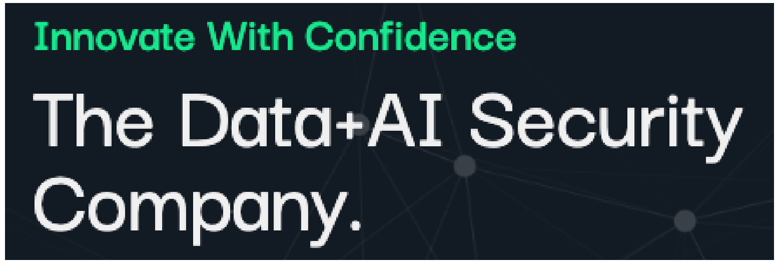
DATA SYSTEMS

- Databases
- File Systems
- Cloud data stores S3, RDS, Aurora
- Data lakes
- Data store vendors
- Online data storage
- More

DATA RESIDENCY

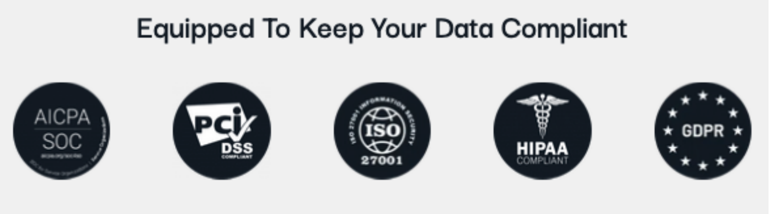
- Source country or region
- Storage country/region
- Vendors residency

A little bit about Symmetry



Innovate With Confidence

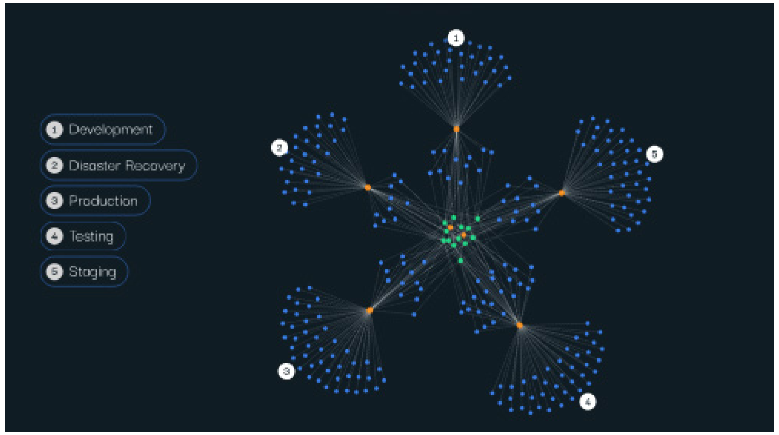
The Data+AI Security Company.

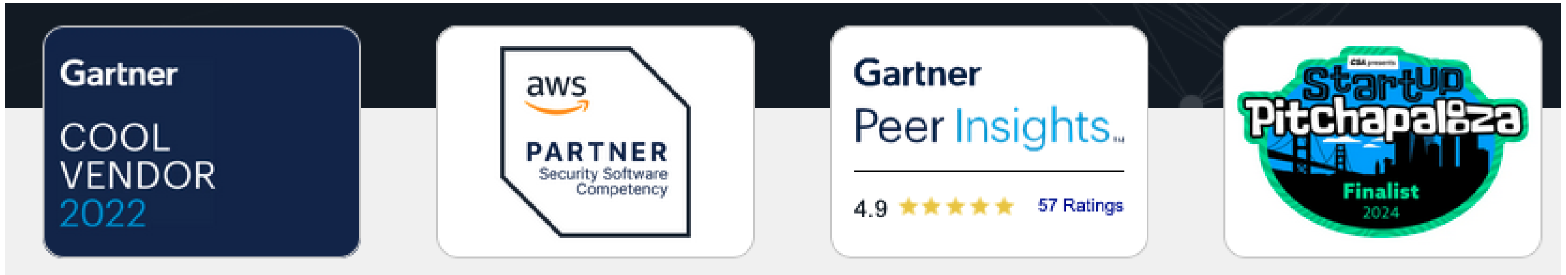


Equipped To Keep Your Data Compliant

Symmetry DataGuard is the leading DSPM Platform that helps companies to secure the data, crown jewel

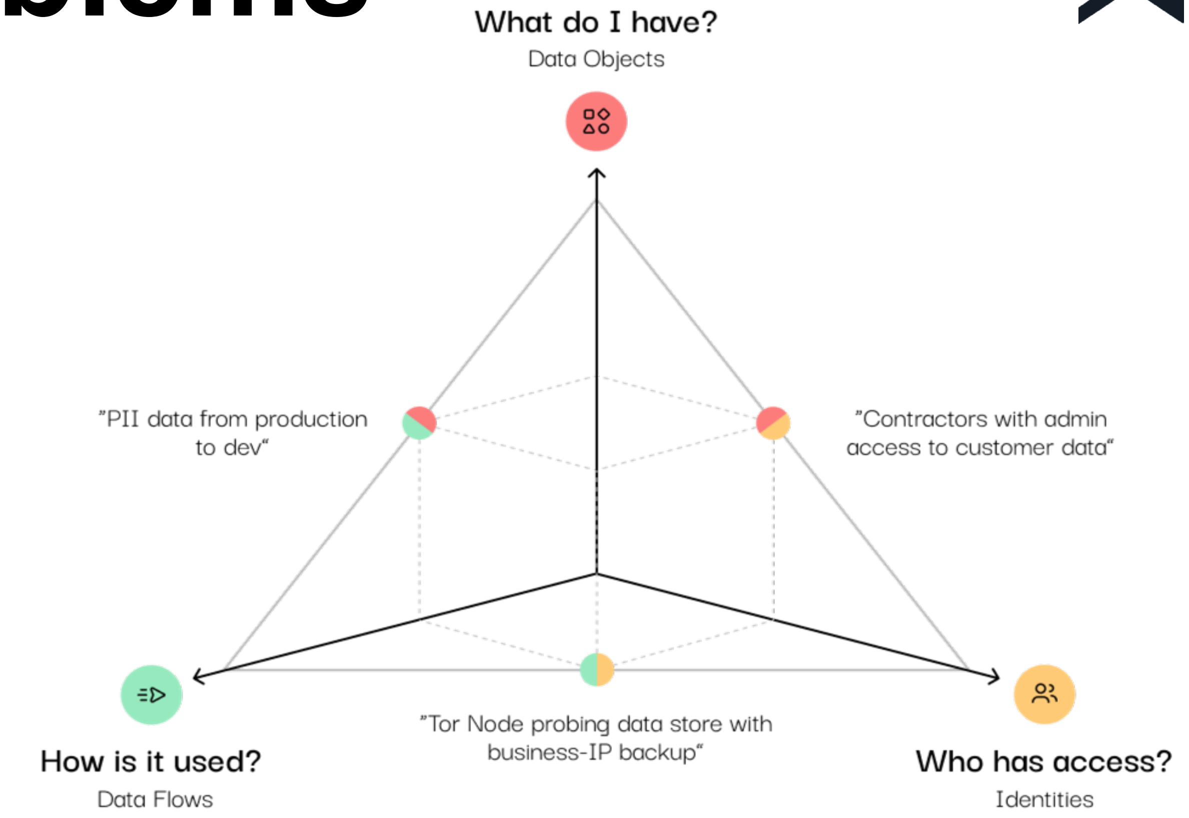
- Discover, classify, and safeguard data across multiple clouds and on-premise.
- Detect and respond to data-focused security & compliance concerns before they impact business.
- Deploy on cloud, on-prem, or in federated air-gapped environments.





Addressing the problems

- Exploding volume of data stores and **data sprawl** across dispersed networks with **limited visibility of the sensitivity and type of data.**
- Existing methods can't scale cost effectively or keep up with the yottabyte scale of data to be classified. Inventories are out of date before they can be leveraged.
- Security blind spots in the sensitivity and location of data restrict the effectiveness of data governance.


What do I have?
Data Objects
"PII data from production to dev"
"Contractors with admin access to customer data"
"Tor Node probing data store with business-IP backup"
How is it used?
Data Flows
Who has access?
Identities

Our Data Security Posture Management (DSPM) solution delivers unparalleled insight into the data you have, who has access to it, and how those identities are using it,

Know the stakeholders & Regulations

Who could sue?

Which organizations have suffered data breaches?

CUSTOMERS AND INDIVIDUALS

- Direct Customers
- Indirect Customers (data subjects)
- Employees
- Private law firms representing the public (victims, data subjects) through class action

PRIVATE INSTITUTIONS

- Card acquiring banks
- Payment processors
- Card payment brands
- Financial institutions in the chain
- Partners in the supply chain
- Insurance companies

GOVT INSTITUTIONS

- Multiple federal institutions
- FTC, CFPB, SEC, FCC
- HHS
- States and State institutions
- Supervisory authority(s) / EU countries
- Other International
- E.g. Office of Australian Info. Com.
- more

Disclaimer: I am not a lawyer

Who could be sued?

Apart from the organization that suffered data breach?

SERVICE PROVIDERS

- Cybersecurity service providers *
- Contractors
- Suppliers *
- IT service providers *

SUPPLY CHAIN

- Payment processors
- Card payment brands
- Financial institutions in the chain
- Partners in the supply chain
- Insurance companies

NOT IN SCOPE FOR THIS SESSION

- Government agencies
- Private companies providing free services
- Organizations to which data subjects voluntarily upload the data

Reference

- 2013 Target PCI auditor Trustwave sued by banks; more details on Target in coming slides
- 2020 In the Marriott data breach, Accenture was included in the lawsuit as well

What are the repeated causes cited in lawsuits?

VIOLATION CATEGORY

- Violation of its own policy(s) and promise
- Lack of fundamental cybersecurity hygiene
- Lack of reasonable & adequate security (based on risk)
- UDAP (misuse, deceptive…)
- Negligence
- Negligent misrepresentation
- Unjust enrichment
- Breach of express contract
- Breach of implied contract
- Breach of implied covenant of good faith
- Fraudulent inducement
- Constructive or equitable fraud

CASES BROUGHT BY FI

- Negligence
- Negligence per se
- Negligence misrepresentation by omission
- Violation of state consumer protection laws
- Violation of state credit card disposal laws

UDAP: Unfair or deceptive acts or practices

Under what laws are organizations sued?

VIOLATION OF LAWS

- Data breach notification laws (50 plus DC)
- Cybersecurity laws
- Data protection laws
- Unfair Competition Laws
- False Claim Acts
- Privacy laws (comprehensive and sectoral)
- Biometric data protection laws (4+)
- State privacy laws (6)
- Fed (Sectoral) Privacy laws (40+)
- Consumer Protection laws
- UDAP Acts
- Credit card data disposal laws

RELATED

- FTC Act
- Security Exchange Act Sec 10(b) 20(a)
- GLBA Safeguards Rule
- Executive Orders (EO)
- IoT Cybersecurity Improvement Act (2020)

Let’s learn from the past

Company 1 data breach

SUMMARY

- 390+ civil lawsuits
- Spent approximately $ 700 million in settlements
- 2 plus years of distraction

Consolidated class action

- 575 pages, 99 claims
- Court sorts through each of these claims
- Even if only one survives, the case goes forward

Source: ftc.gov

OUTCOMES

- Implement comprehensive infosec program
- Consider principles of zero-trust and implement where feasible
- Designate CISO, reporting to CEO and BoD
- Maintain incident response plan
- Conduct biennial exercises to test security incident response
- Minimize data collection (not sure how credit agencies will follow this)
- Encrypt PII
- Segment networks, disable unnecessary ports
- Conduct risk-based pentest
- Reorganize patch management team, more ….

Company 2 data breach

SUMMARY

- Data breach of 57 million customers & drivers
- Company 2 paid reporter/bad actor
- Disclosed a year after approximately
- Felony charge against CISO

LAWSUIT

- All 50 states + DC
- UDAP laws
- Data protection laws
- Data breach notification laws

OUTCOMES

- Third-party access controls, with better credentials management
- Strong password
- Encryption of PII
- Regularly identification of internal and external risks and implement appropriate safeguards
- A biennial periodic third-party assessment
- Maintain comprehensive incident response and data breach plan
- Develop a corporate integrity program
- Report to BoD
- Incorporate privacy-by-design
- More…

Company 3 data breach

SUMMARY

- 80+ civil lawsuits
- Spent approximately $ 300 million in settlements
- Received $ 90 million from insurance payment
- Cost the CEO his job
- 4 plus years of distraction
- 92 claims, consolidated
- Violation of consumer protection laws of 49 states (except Alaska), DC
- Violation of data breach statutes of 38 states
- Investigated by FTC
- Claims of negligence
- Breach of implied contract
- Bailment
- Unjust enrichment

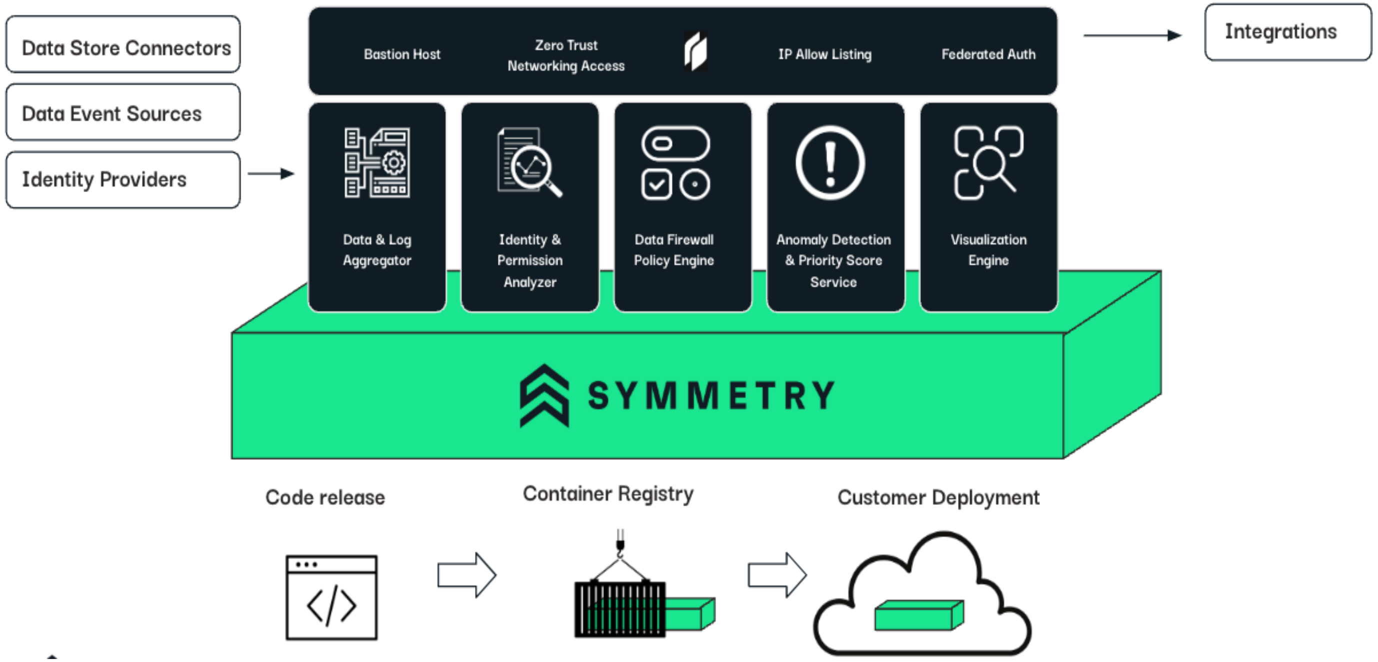
OUTCOMES

- Comprehensive and adequately resourced cybersecurity program
- Executive officer with appropriate background to manage cybersecurity and report to CEO
- Risk-based auditing of vendor compliance
- Ensure proper handling of security events involving PII
- Maintain encryption protocols
- Segment PCI data network, 2FA, FIM
- Monitor network activity, more….

Overview Core Technology

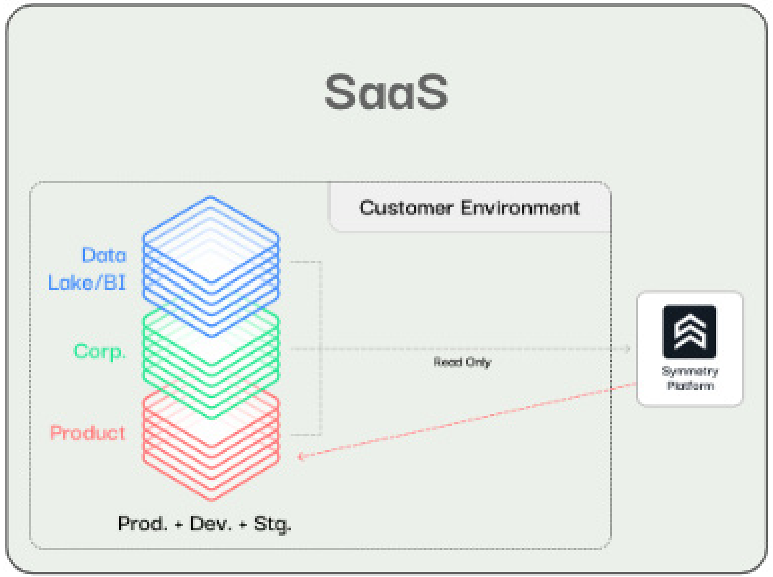
Symmetry Solution could have stopped the breach

Symmetry's Core technology has been built to meet the most stringent compliance requirements regarding data protection.

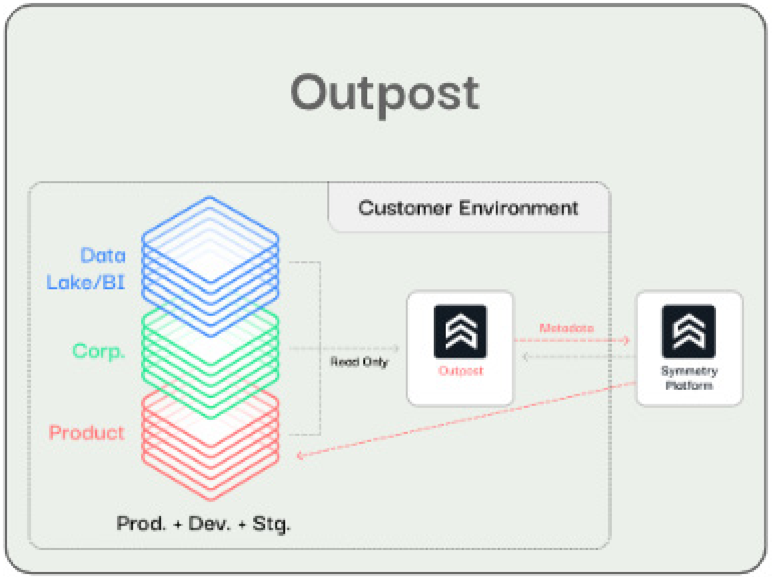


Symmetry Solution Deployment Options

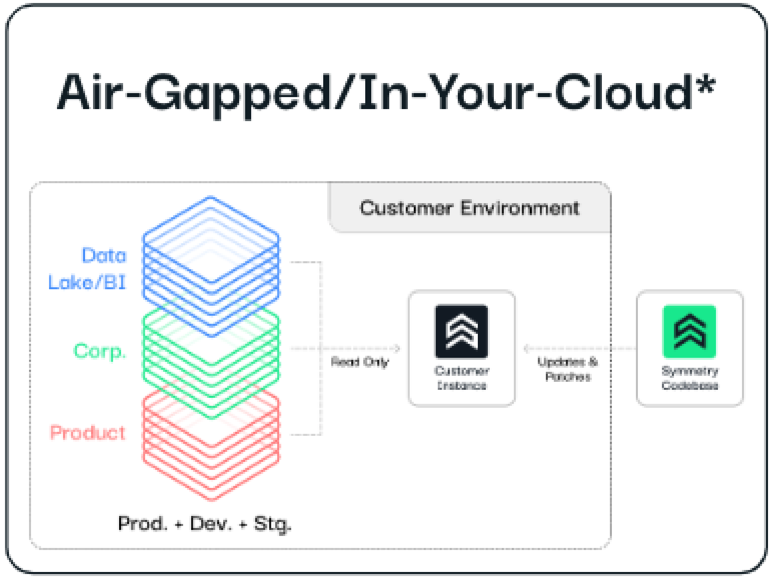
Symmetry supports SaaS, Outpost, and in-your-cloud deployments. We recommend in-Your-Cloud deployment to reduce access to your data and supply chain risk.



Data and metadata leave the customer environment.



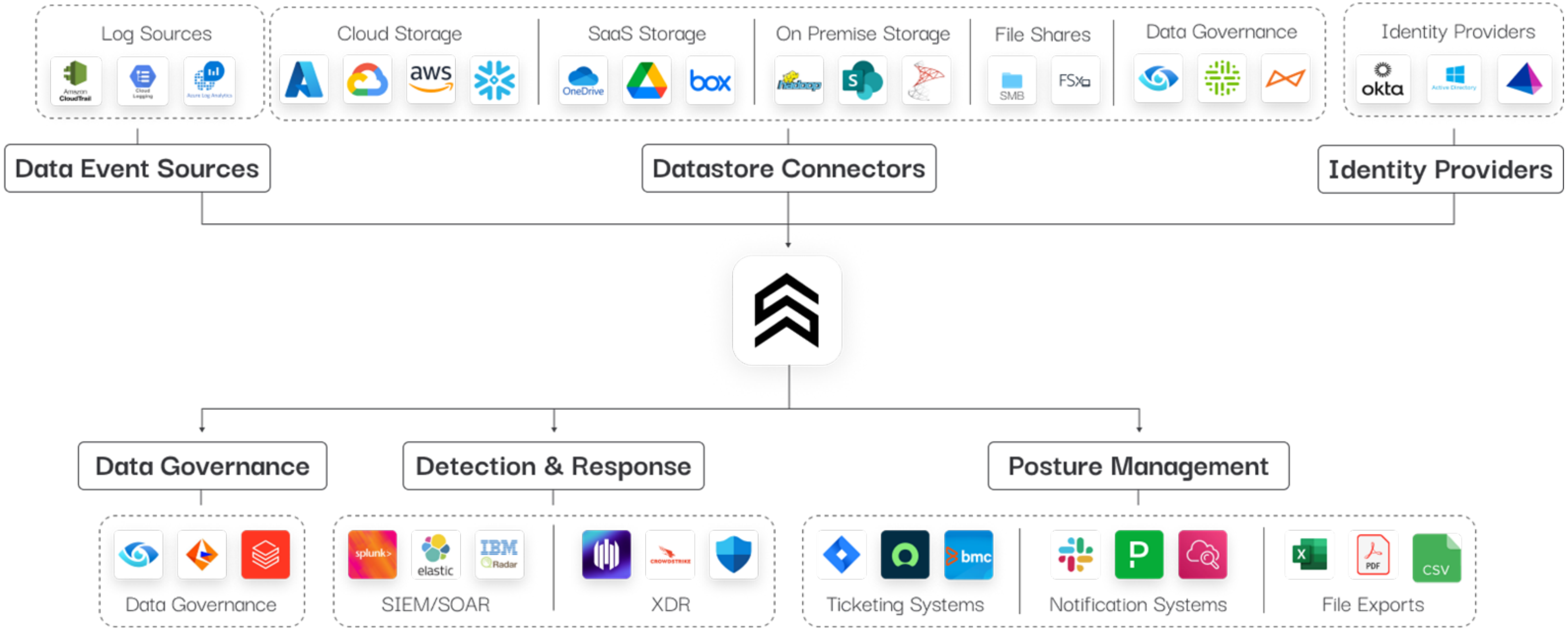
Only metadata i.e. file names, leave the environment.



No metadata or data leaves the environment.

Symmetry Solution - necessary coverage

Symmetry DataGuard was designed to cover Cloud, On-Premise and Hybrid environments while maintaining the same UI, workflows, rulesets and classification schema across environment types. Our Coverage and integrations are continually being updated.



Summary & Takeaways

Summary

- Create a comprehensive Cybersecurity program. Start with a reasonable one, and maintain at least at adequate level of maturity
- Know your data assets and update the data assets inventory at reasonable intervals
- **Build data-centric security, use the latest technologies such as DSPM**
- Know jurisdiction and applicable laws
- Keep a breach notification procedure and generic breach notification report template
- Regularly monitor, test, and tune

Thank You

Gopi Ramamoorthy

CISSP, CISA, CIPP/US, CISM

Head of Security & GRC Engineering

gopi@symmetry-systems.com