SNIA CSTI | CLOUD STORAGE TECHNOLOGIES

Cyberstorage and XDR: Threat Detection through a Storage Lens

Live Webcast

April 4, 2023

10:00 am PT / 1:00 pm ET

Today's Presenters

Michael Hoard
Chair SNIA Cloud Storage Technologies Initiative
Intel

Erin Farr
Storage CTO Office, IBM
Vice Chair SNIA Cloud Storage Technologies Initiative

SNIA - By the Numbers

Industry Leading Organizations

180

Active Contributing Members

2,500

IT End Users & Storage Pros Worldwide

50,000

SNIA CSTI | CLOUD STORAGE TECHNOLOGIES

What We Do

Educate vendors and users on cloud storage, data services and orchestration

Support & promote business models and architectures: OpenStack, Software Defined Storage, Kubernetes, Object Storage

Understand Hyperscaler requirements Incorporate them into standards and programs

Collaborate with other industry associations

SNIA Legal Notice

The material contained in this presentation is copyrighted by SNIA unless otherwise noted.

Member companies and individual members may use this material in presentations and literature under the following conditions:

- Any slide or slides used must be reproduced in their entirety without modification
- SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.

This presentation is a project of SNIA.

Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.

The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

Agenda

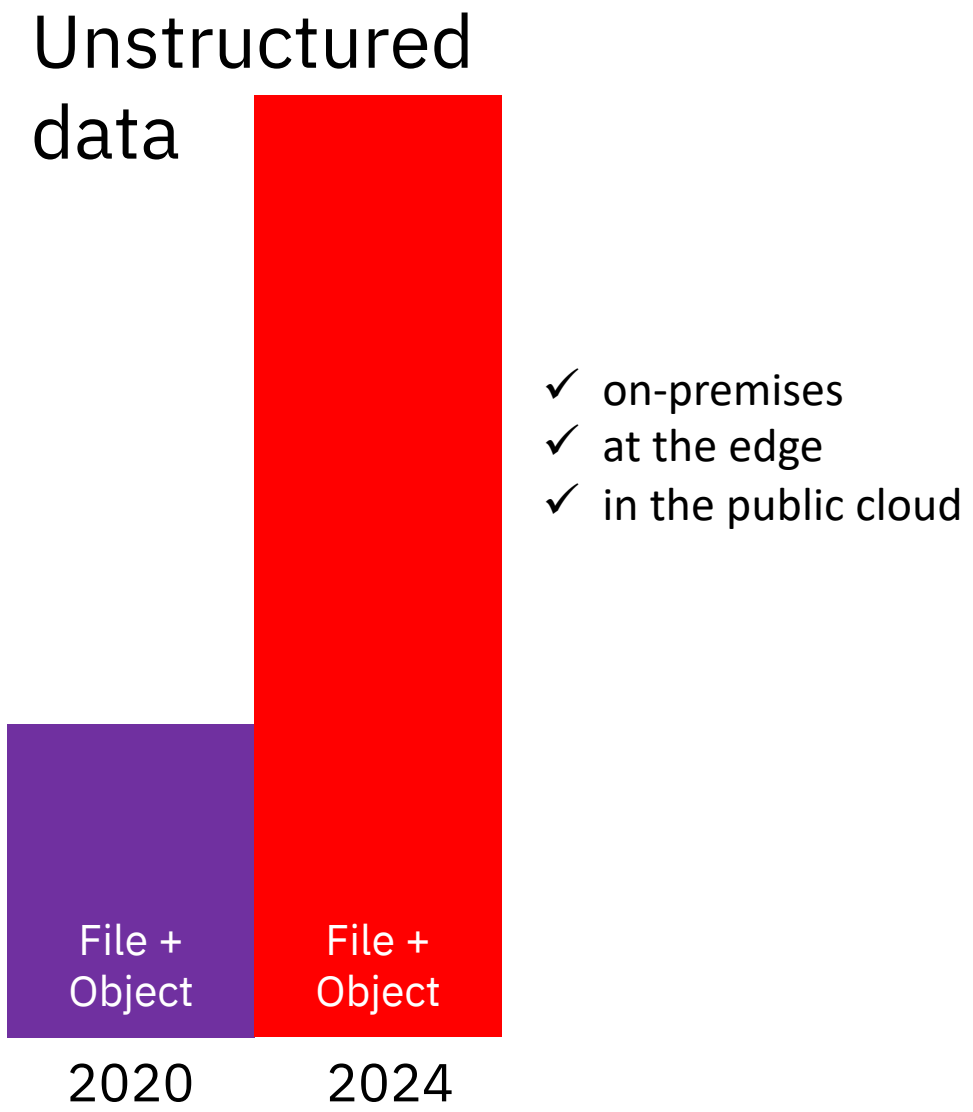
- Industry trends driving threat detection in Storage
- Challenges faced by Security and Infrastructure teams
- Detection and Response methods and alternatives
- Key characteristics needed

Industry Trends Driving Threat Detection in Storage

Industry Challenges

For large enterprises, the amount of unstructured data stored as file or object storage will triple between 2020 and 2024

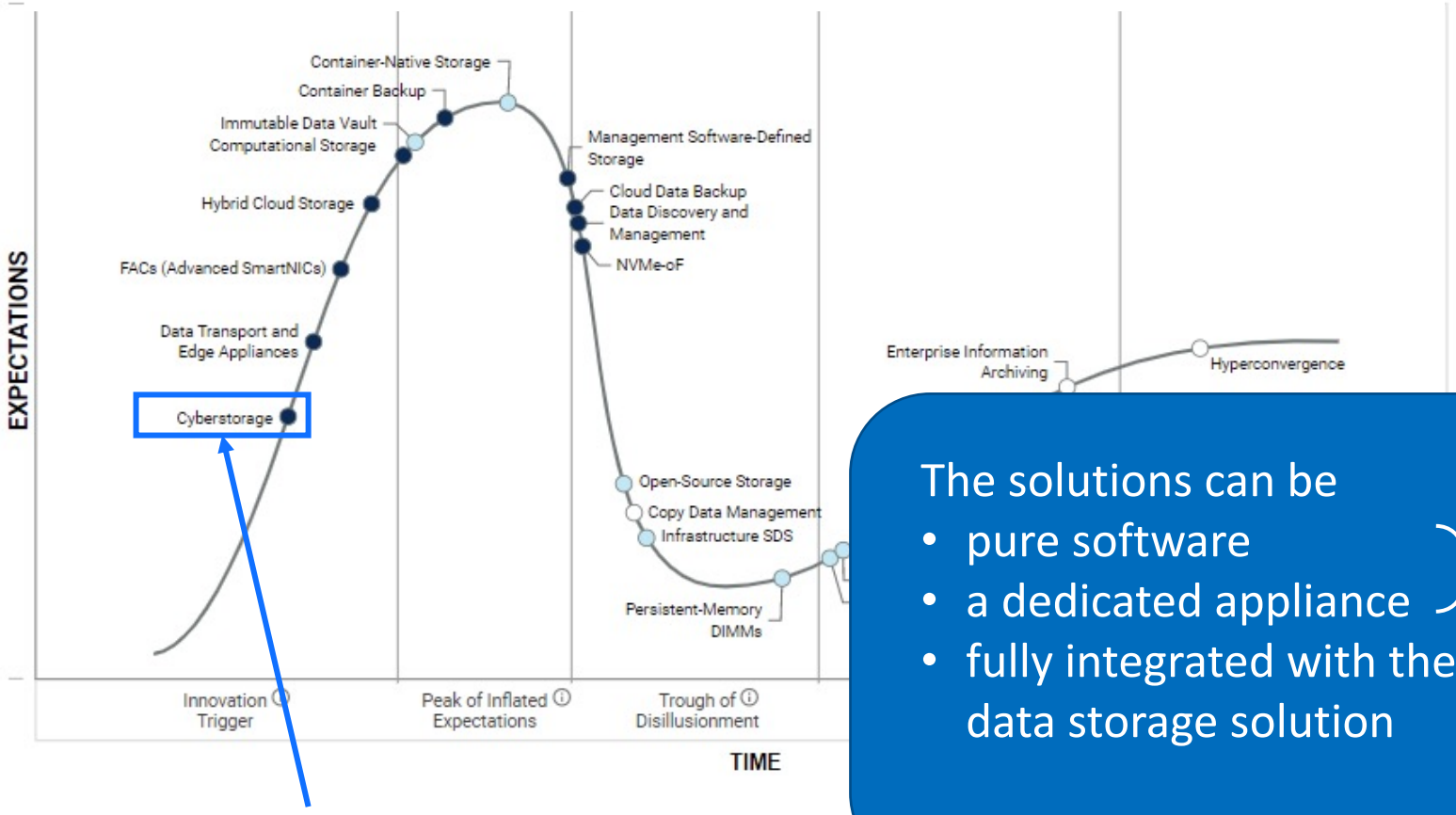
- Gartner, Hype Cycle for Storage and Data Protection Technologies, 2022



https://www.msp360.com/resources/blog/securing-your-digital-data-achieving-cyberstorage-today/

Industry Trend - Cyberstorage

Hype Cycle for Storage and Data Protection Technologies, 2022



Emerging Cyberstorage technology trend

Gartner defines as:

"Cyberstorage protects storage system data against ransomware attacks through **early detection and blocking of attacks** and **aids in recovery through analytics to pinpoint when an attack started**."

The solutions can be

- pure software
- a dedicated appliance

} Easier to add-on but offers less protection

- fully integrated with the data storage solution

} Gartner considers ideal, but acknowledges not everyone can switch storage vendors for the support

https://www.msp360.com/resources/blog/securing-your-digital-data-achieving-cyberstorage-today/

Cyberstorage in the Context of End-to-End Cybersecurity

NIST Cybersecurity Framework (NIST CSF)


Identify


Protect


Detect


Respond


Recover

Focus for today

Cyberstorage (as defined by Gartner) plays here.

Intent is to reduce the blast radius as much as possible.

Detect quickly
Detect accurately
Respond faster

NIST Cybersecurity Framework: https://www.nist.gov/cyberframework

Evolution to SIEM *and XDR*

Security Information and Event Management (SIEM)

Uses data that's
High volume

Low accuracy

Use cases

- Compliance
- Visibility
- Log management
- Operational Risk
- Security

Collects log and event data from across the Enterprise

A LOT of data (wide) with low fidelity (shallow)

eXtended Detection and Response (XDR)

Use cases

Threat Detection and Response

Uses data that's
Low volume

High accuracy

Enables ***automated*** and ***decentralized response***

At the point of interaction...
Endpoints (EDR)
Network (NDR)
Users (UBA)
OT/IOT
Apps and Data
Cloud
Threat Intelligence

Creates intelligent alerts from each domain (e.g. endpoint, network)

Scoped data (narrow) with high fidelity (deep)

Evolution to XDR – Where Can Storage Help?

Organizations recognize their risk surface keeps expanding beyond the traditional endpoint

eXtended Detection and Response (XDR)

Endpoints
Network
Users
OT/IOT
Apps and Data
Cloud
Threat Intelligence
+ Storage

Endpoint Detection and Response (EDR)

Network Detection and Response (NDR)

tells you…

What is the bad actor *doing*?

Storage Detection and Response

could tell you…

What ***data*** is the bad actor touching?

TODAY → TOMORROW

DEFENSE IN DEPTH

Challenges Faced by Security and Infrastructure Teams

Where Storage is Involved Today

Cybersecurity	Cyber Resilience

Ideally, an organization should be both cyber secure and cyber resilient

Cybersecurity is about prevention; it's about trying to keep the bad actors out of your environment

It's also about detecting and responding to an incident to reduce the impact

Cyber Resilience is about an organization's ability to continue operations despite a cyber-incident

CISO's responsibility

Infrastructure's responsibility

Ownership has silos across the NIST Cybersecurity Framework

Holistic Data Security requires seamless operation and coordination across both

https://www.nist.gov/cyberframework

The Data Protection Lenses – Current Landscape

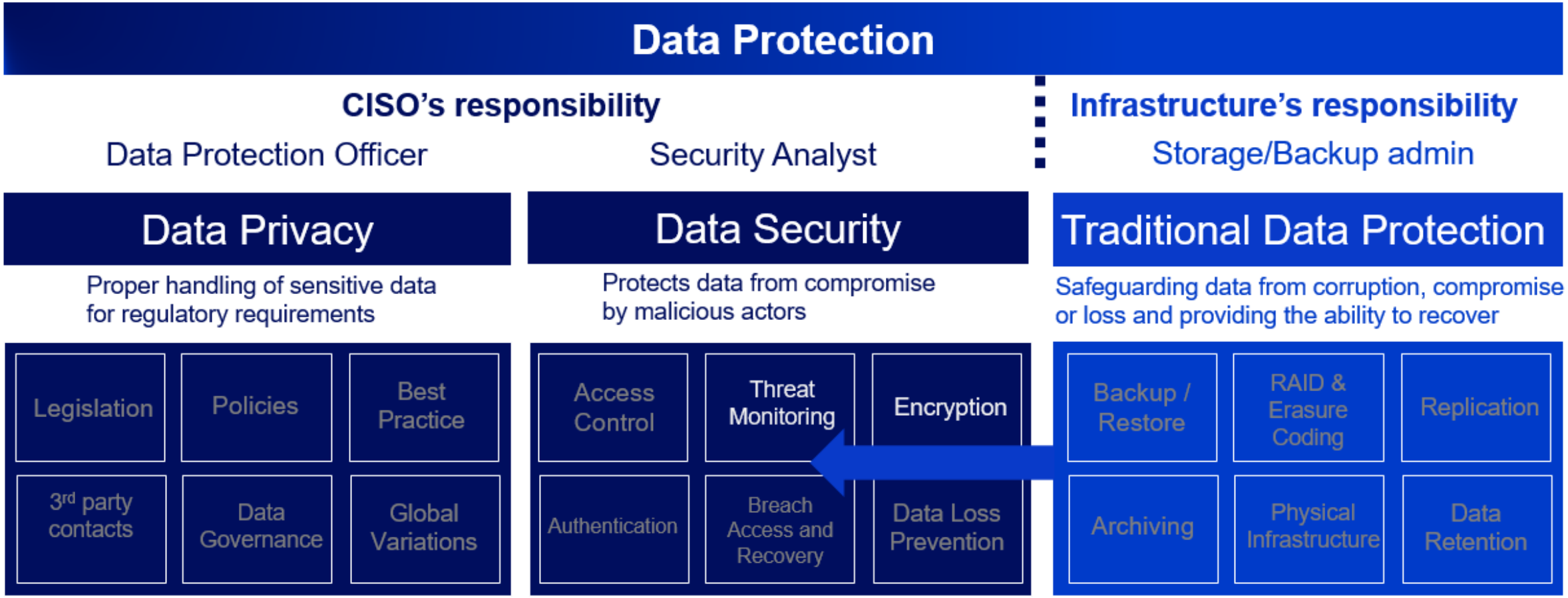


Figure: The Three Categories of Data Protection from: https://www.snia.org/education/what-is-data-protection

As storage capabilities advance, the lines are becoming blurred

https://www.snia.org/education/what-is-data-privacy

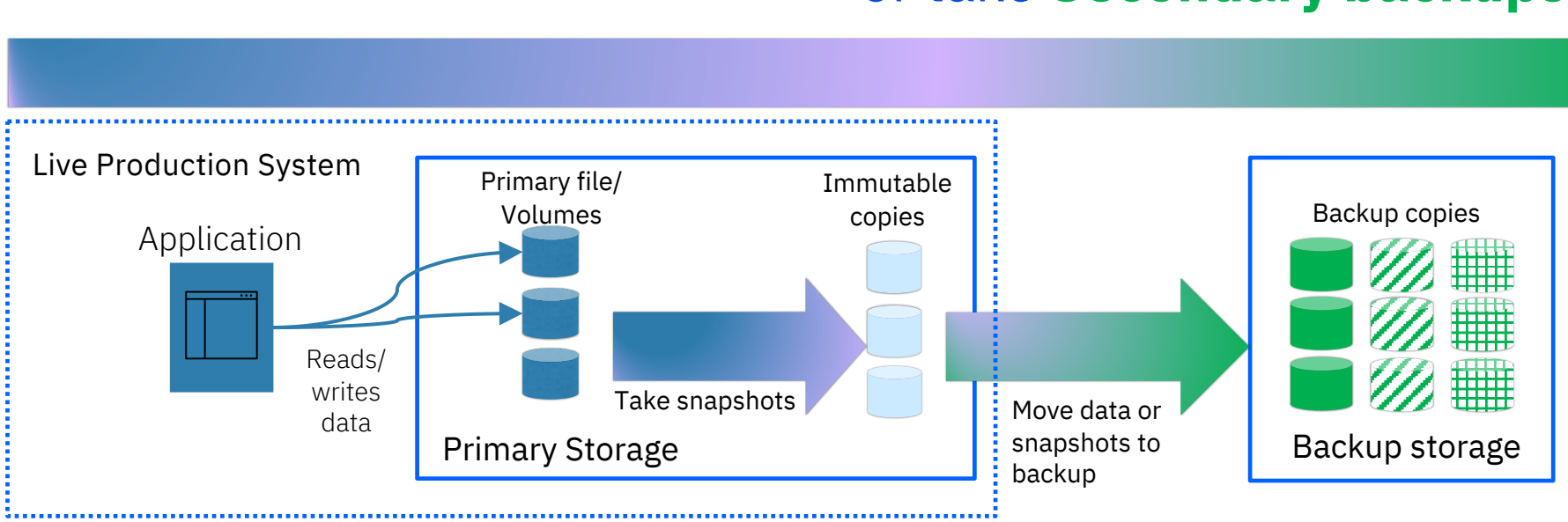
Poll Question #1

Who should be responsible for detecting threats surfaced by storage?

The Traditional Data Protection Landscape Today

Businesses take **Primary snapshots + Secondary backups** with **different admins** and **different software**

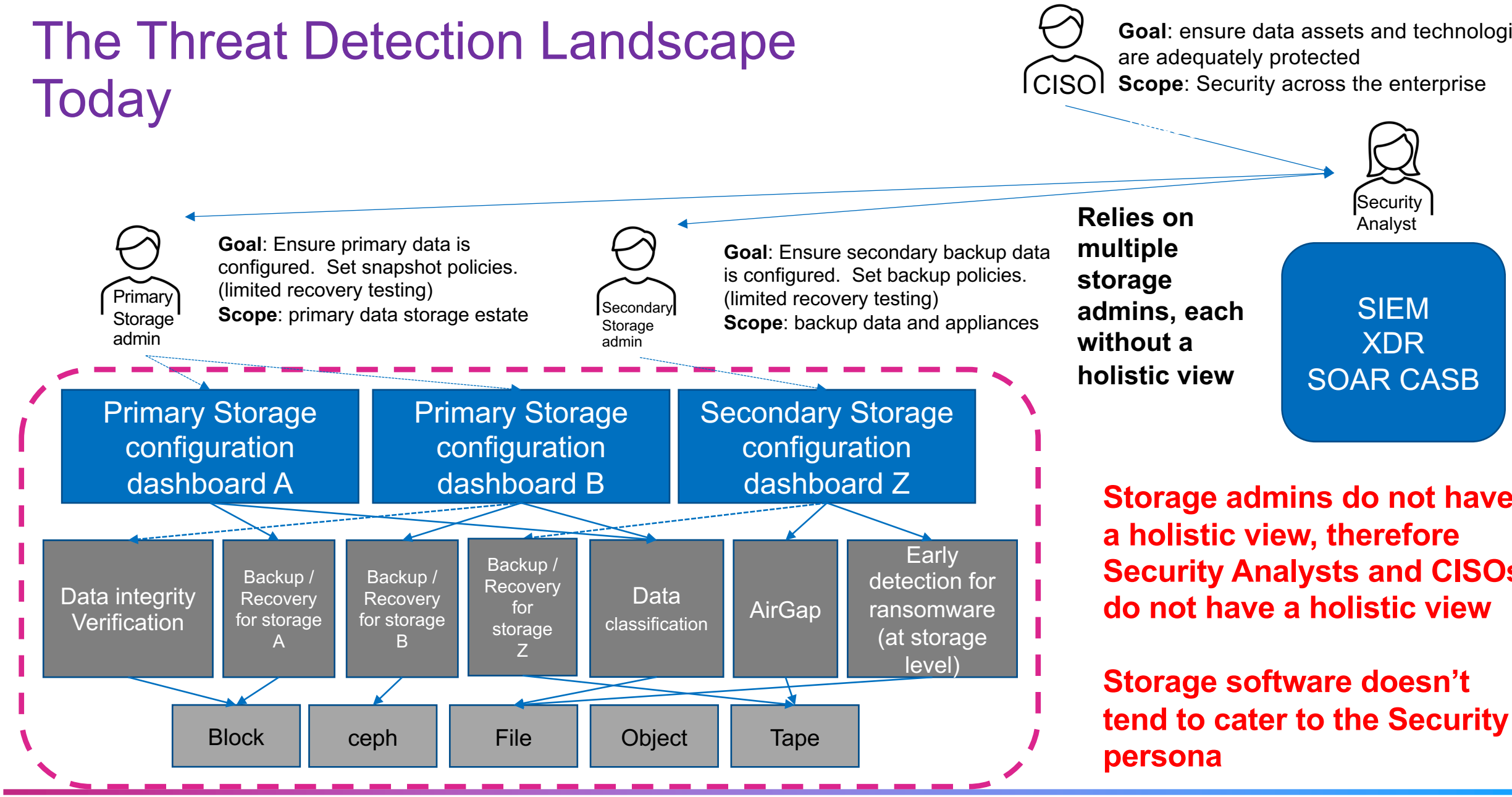
or take **Secondary backups only** which can **lengthen time to recovery**



and… keeping copies on primary storage alone is too expensive

Data Protection is either siloed or is not readily available, which slows recovery

The Threat Detection Landscape Today



Storage admins do not have a holistic view, therefore Security Analysts and CISOs do not have a holistic view

Storage software doesn't tend to cater to the Security persona

Poll Question #2

Are you concerned about silos across primary and secondary storage?

The Attack Landscape Today

How LONG does it take for a ransomware attack to encrypt your files?
LESS than 1 DAY, and often just hours or minutes

7 minutes to infect the global network of shipping company
-CISA

Don't Wake Up to a Ransomware Attack. Apr 2021
https://www.youtube.com/watch?v=GdXLp1bEnZE

Ransomware research from Splunk against **10 ransomware variants** showed it can take between 5 minutes to 2 hours to encrypt 100K files (~53GB of data), depending on the strain.

The median was ~43 minutes.

Splunk: https://www.splunk.com/en_us/blog/security/ransomware-encrypts-nearly-100-000-files-in-under-45-minutes.html

Ransomware recovery ***requires*** primary storage data protection for faster recovery

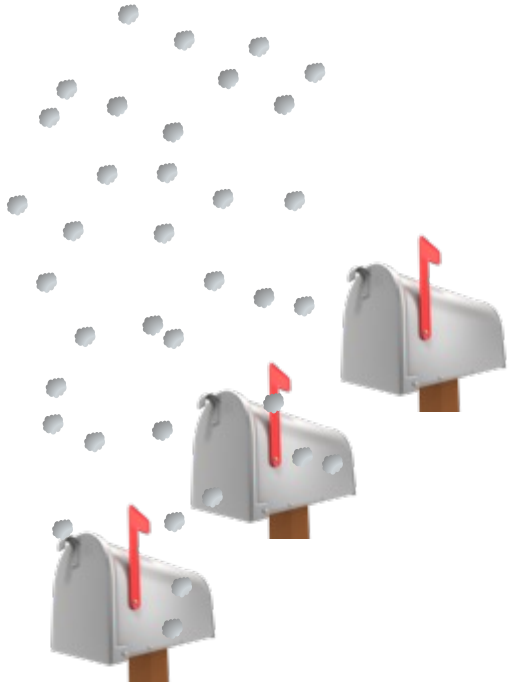
Cost requires that some data be kept on secondary storage

Detection and Response Methods and Alternatives

Detection Mechanisms Today

Signature-based scanning (Antivirus/malware scans)

User behavior-based detection (UBA/UEBA)



Anomaly detection (Machine Learning, stats-based, heuristics)

Detection of destruction (e.g. data integrity checks)

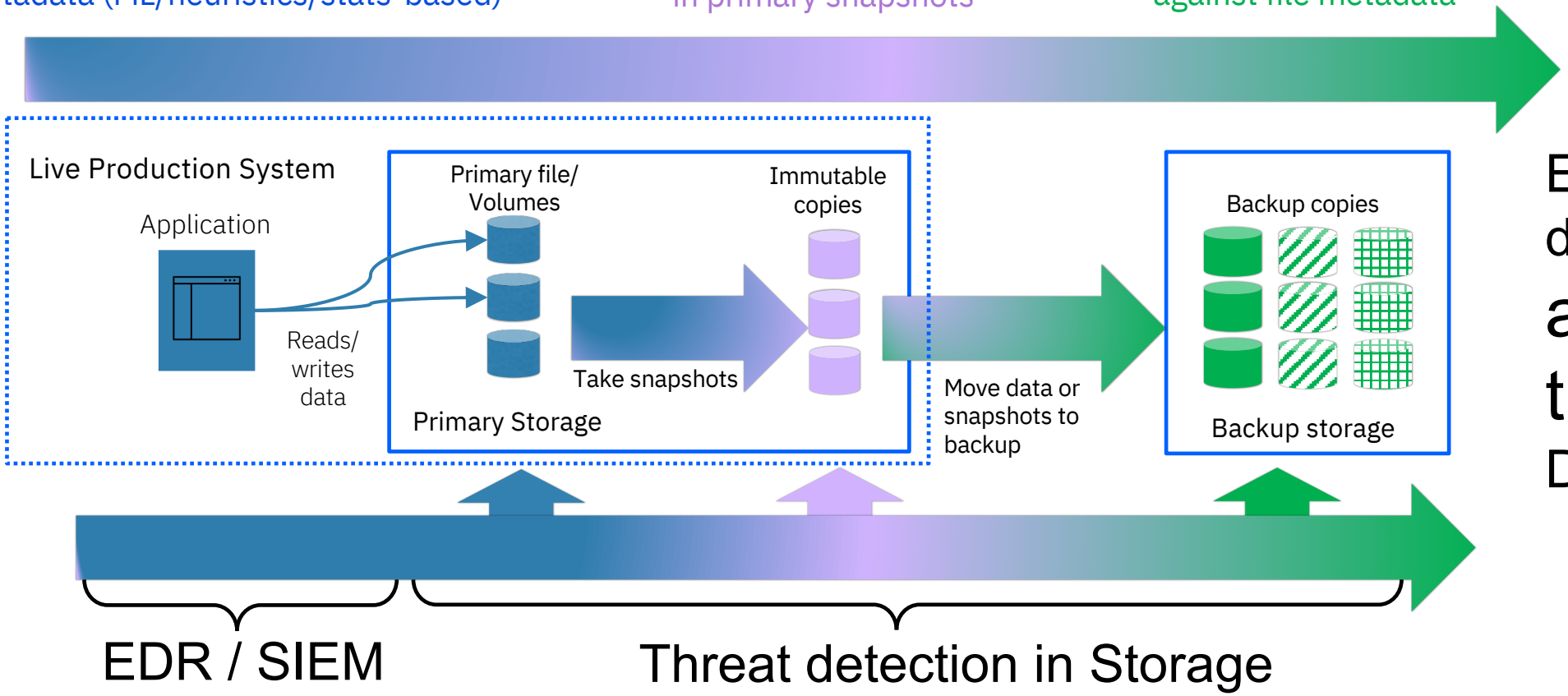
Detection in the Storage Layer

Across the entire data lifecycle

Analyze patterns on a live system
Detect anomalies on a live system by analyzing attack patterns against file metadata (ML/heuristics/stats-based)

Analyze snapshots
Detect data corruption (evidence of malware) in primary snapshots

Analyze backup metadata
Detect attacks against primary storage using Machine Learning against file metadata



Each focuses on a different **approach** and **timeline** for Defense in Depth

Key Characteristics Needed

Detection and Response

Common techniques and features *through a* ***storage lens***

Detect malware through **signature-based** scanning

Not relevant for *detection* at the storage layer since its **redundant** with endpoint-based (host) scanning, but it can **add value during recovery**.

Detect **data destruction** (evidence of malware)

Determine if time to detect is fast enough, given where the detection is occurring in the data lifecycle.
Its **highest value** is identifying unimpacted data for recovery.

Detect malware through **anomaly detection** (ML-based or heuristic)

Can provide value if the quantity and quality of storage telemetry is sufficient and the false positive rate is low.

Detect **data exfiltration**

If data exfiltration is detected at the storage layer, this can **reduce the amount of data that needs sent to SIEM.**
Storage can instead send a high-fidelity alert to XDR.

Highest Value for Detection and Response

Integrate with security tooling (XDR, SIEM, SOAR)

Table stakes because:

- Users need a holistic view
- Storage has only partial context needed for detection

Respond - halt malware or restrict activities

Industry trend with XDR is moving toward ***automated*** **response** in each domain (e.g. networking, storage) though one must prove they can detect accurately.

What to Look for in Storage Detection and Response

A solution…

- MUST be integrated with SEIM/XDR
  - Check if sufficient data is surfaced or if further drill down would be needed
- Doing detection in secondary storage *alone* may be too slow.
  - Check backup frequency (if every 24 hours, ransomware could be detected too late)
- Should provide ability to warn before automatically responding
- If providing automated response (e.g. it blocks writes to disk), check false positive rates for detection. Run in warning mode first.

Image by Peggy und Marco Lachmann-Anke from Pixabay

Thanks for Viewing this Webcast

- Please rate this presentation and provide us with feedback
- This webcast and a copy of the slides are available at the SNIA Educational Library https://www.snia.org/educational-library
- A Q&A from this webcast will be posted to the SNIA Cloud blog: www.sniacloud.com/
- Follow us on Twitter @SNIACloud

Thank You!

