CYBERSTORAGE

Continuously keeping all your unstructured data available and safe from attacks.

Jonathan Halstuch, CTO
jhalstuch@racktopsystems.com

RACKTOP

Up Front Cost vs Long Term Costs

$180 Thousand

Cost of storage software per PB per year

277 Days

Average time to identify and contain a data breach

$9.44 Million

Average cost of a breach in the United States, the highest of any country

$1.12 Million

Average savings from detecting a breach within 200 days or less

$4.54 Million

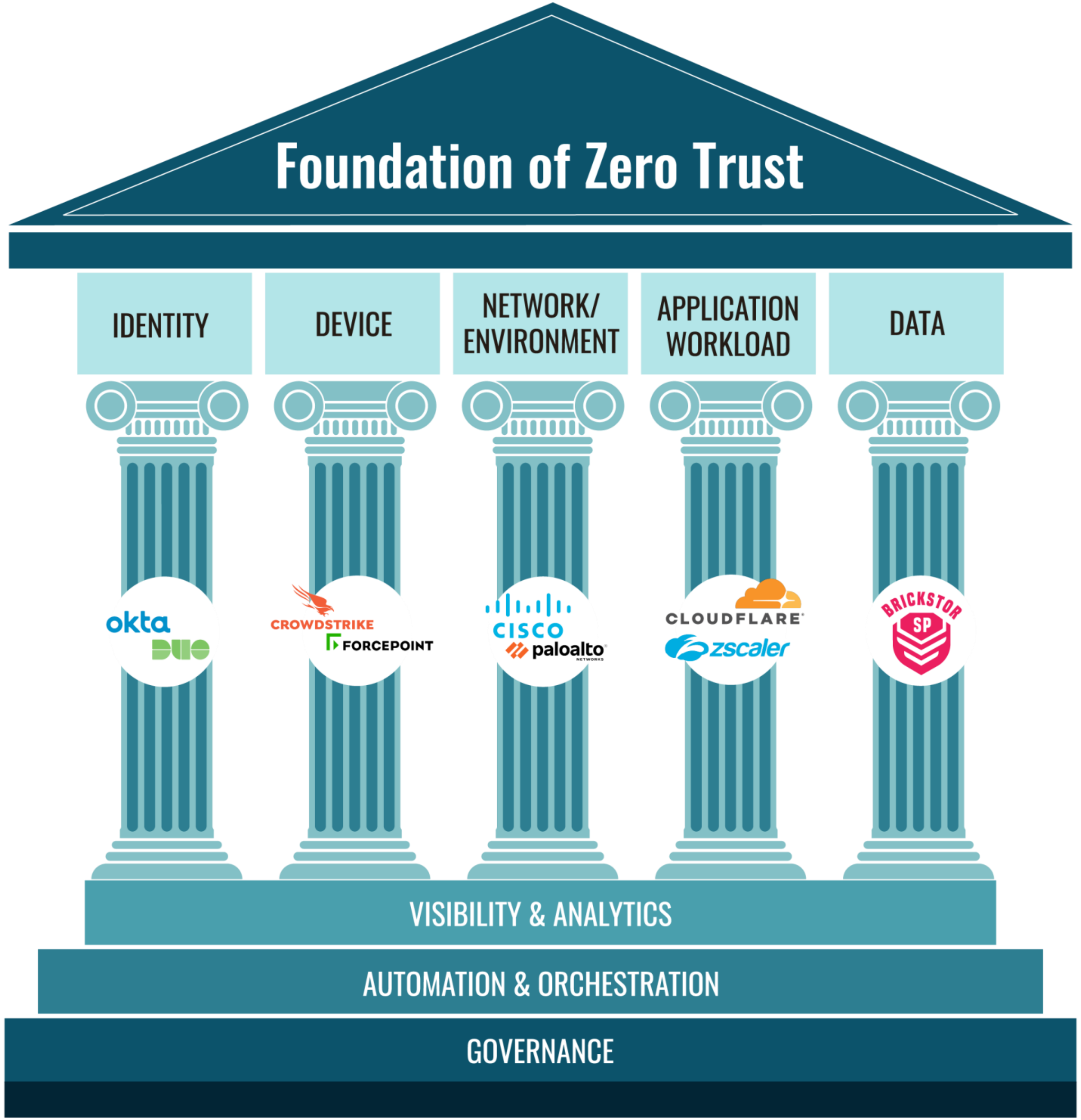
Average cost of a ransomware attack, not including the cost of the ransom itself

**Statistics from the 2022 IBM Cost of a Data Breach Report*

CISA Zero Trust Maturity Model

Data is the 5th Pillar

- Enable zero trust principles around file access
- Evaluate each request to read, modify or write a file
- Stop suspicious or malicious behavior and enforce policy in real time



Foundation of Zero Trust

IDENTITY

DEVICE

NETWORK/ ENVIRONMENT

APPLICATION WORKLOAD

DATA

VISIBILITY & ANALYTICS

AUTOMATION & ORCHESTRATION

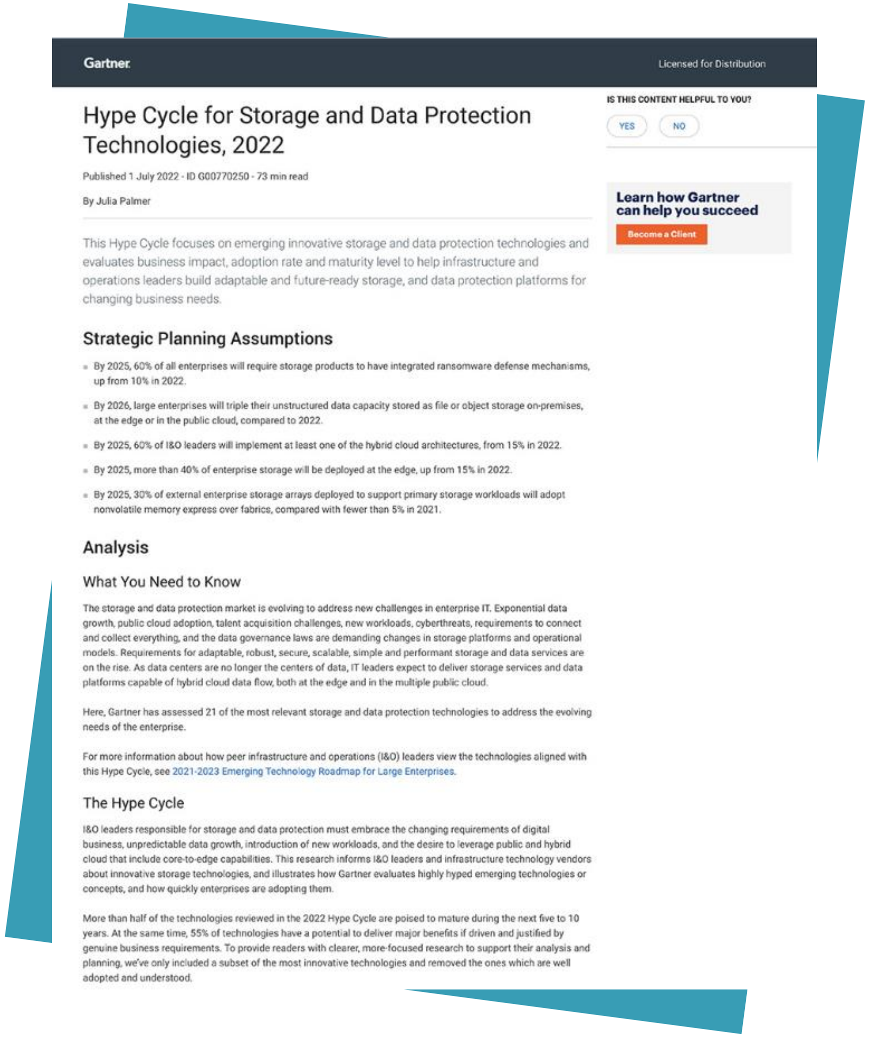
GOVERNANCE

According to Gartner, “By 2025, 60% of all enterprises will require storage products to have integrated ransomware and defense mechanisms, up from 10% in 2022.”

Storage Needs Active Defense

View complimentary Gartner research and learn more about RackTop Systems’ unique features, among other provider offerings, at https://resources.racktopsystems.com/gartner-research.

Gartner disclaimer
Gartner, Hype Cycle for Storage and Data Protection Technologies, 2022, Julia Palmer, 1 July 2022
Gartner does not endorse any vendor, product or service depicted in our research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.
Gartner and Magic Quadrant are registered trademarks of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.



Gartner
Licensed for Distribution
IS THIS CONTENT HELPFUL TO YOU?
YES
NO
Learn how Gartner can help you succeed
Become a Client

Hype Cycle for Storage and Data Protection Technologies, 2022

Published 1 July 2022 · ID G00770250 · 73 min read

By Julia Palmer

This Hype Cycle focuses on emerging innovative storage and data protection technologies and evaluates business impact, adoption rate and maturity level to help infrastructure and operations leaders build adaptable and future-ready storage, and data protection platforms for changing business needs.

Strategic Planning Assumptions

- By 2025, 60% of all enterprises will require storage products to have integrated ransomware defense mechanisms, up from 10% in 2022.
- By 2026, large enterprises will triple their unstructured data capacity stored as file or object storage on-premises, at the edge or in the public cloud, compared to 2022.
- By 2025, 60% of I&O leaders will implement at least one of the hybrid cloud architectures, from 15% in 2022.
- By 2025, more than 40% of enterprise storage will be deployed at the edge, up from 15% in 2022.
- By 2025, 30% of external enterprise storage arrays deployed to support primary storage workloads will adopt nonvolatile memory express over fabrics, compared with fewer than 5% in 2021.

Analysis

What You Need to Know

The storage and data protection market is evolving to address new challenges in enterprise IT. Exponential data growth, public cloud adoption, talent acquisition challenges, new workloads, cyberthreats, requirements to connect and collect everything, and the data governance laws are demanding changes in storage platforms and operational models. Requirements for adaptable, robust, secure, scalable, simple and performant storage and data services are on the rise. As data centers are no longer the centers of data, IT leaders expect to deliver storage services and data platforms capable of hybrid cloud data flow, both at the edge and in the multiple public cloud.

Here, Gartner has assessed 21 of the most relevant storage and data protection technologies to address the evolving needs of the enterprise.

For more information about how peer infrastructure and operations (I&O) leaders view the technologies aligned with this Hype Cycle, see 2021-2023 Emerging Technology Roadmap for Large Enterprises.

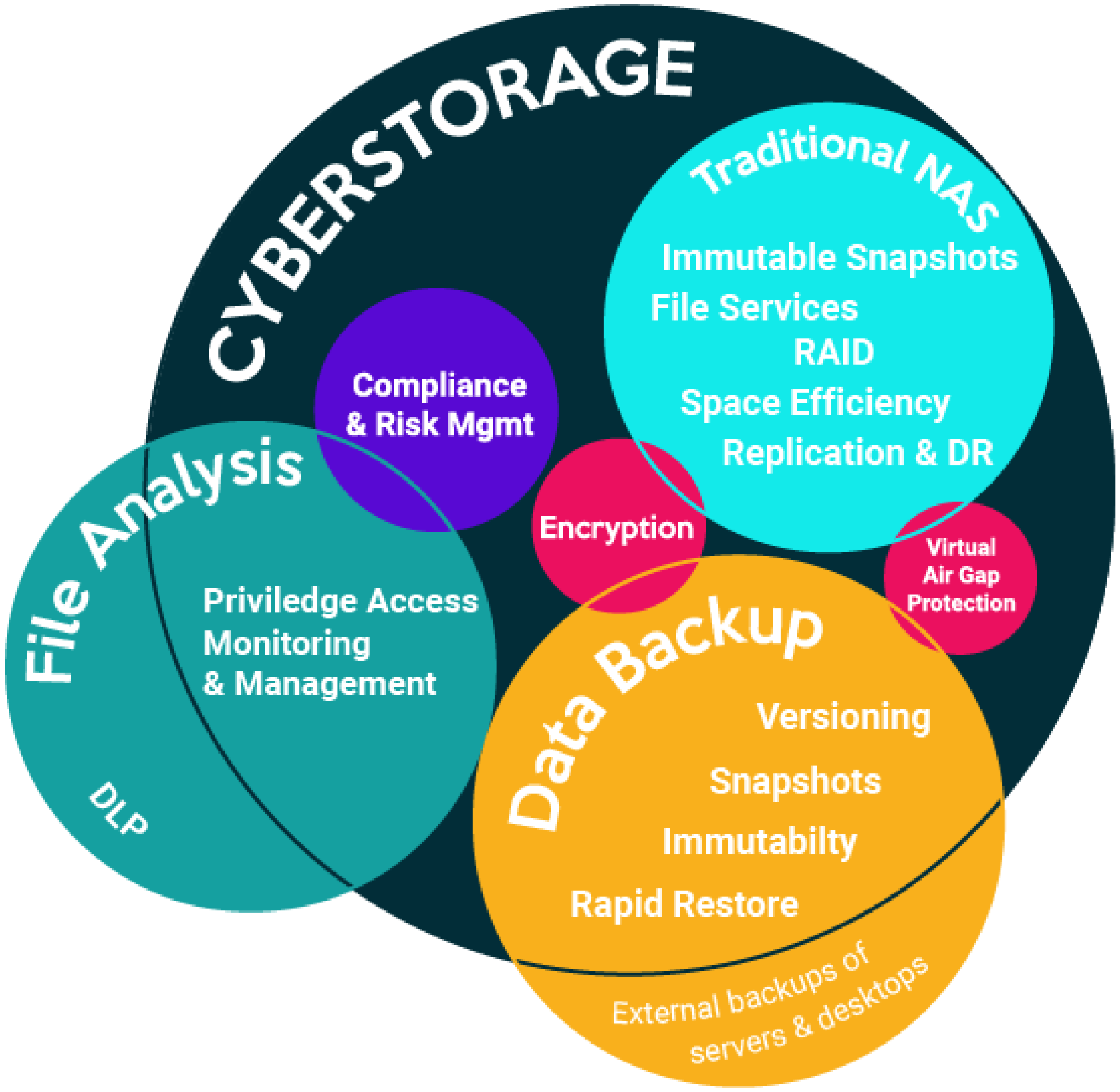
The Hype Cycle

I&O leaders responsible for storage and data protection must embrace the changing requirements of digital business, unpredictable data growth, introduction of new workloads, and the desire to leverage public and hybrid cloud that include core-to-edge capabilities. This research informs I&O leaders and infrastructure technology vendors about innovative storage technologies, and illustrates how Gartner evaluates highly hyped emerging technologies or concepts, and how quickly enterprises are adopting them.

More than half of the technologies reviewed in the 2022 Hype Cycle are poised to mature during the next five to 10 years. At the same time, 55% of technologies have a potential to deliver major benefits if driven and justified by genuine business requirements. To provide readers with clearer, more-focused research to support their analysis and planning, we’ve only included a subset of the most innovative technologies and removed the ones which are well adopted and understood.

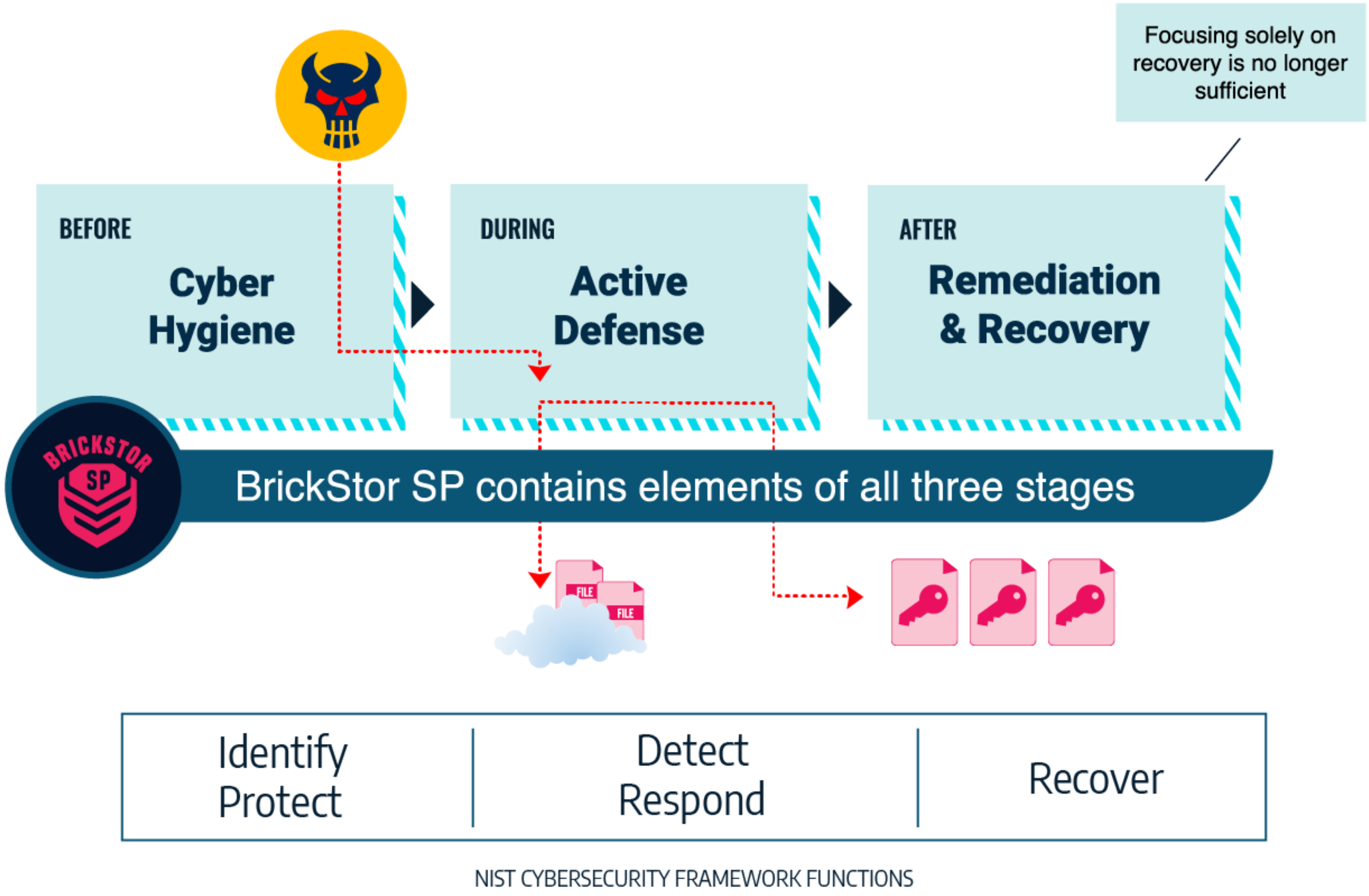
RackTop’s unique Cyberstorage features

- Active defense against data theft and ransomware
- Real-time user behavior analytics
- Incident management
- SIEM integration
- Zero Trust policy enforcement



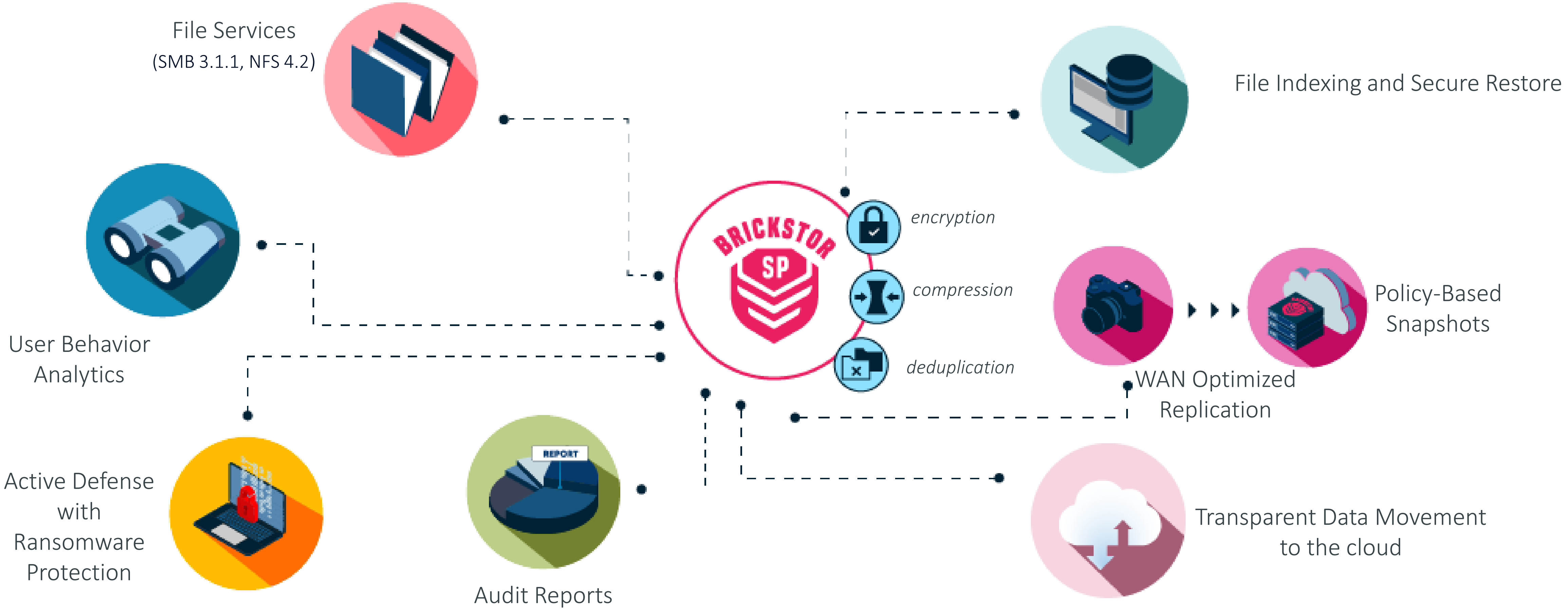
BrickStor SP: the only Cyberstorage solution to address all 5 functional areas of the Cybersecurity Framework

- ✓ 100% Agentless
- ✓ Standards based – drop into any organization on-prem, edge or the cloud
- ✓ Installs in 15 minutes and stops Ransomware in 1 second


Focusing solely on recovery is no longer sufficient
BEFORE
Cyber Hygiene
DURING
Active Defense
AFTER
Remediation & Recovery
BRICKSTOR SP
BrickStor SP contains elements of all three stages
FILE
FILE
Identify
Protect
Detect
Respond
Recover
NIST CYBERSECURITY FRAMEWORK FUNCTIONS

RACKTOP

Key Features of BrickStor SP



File Services
(SMB 3.1.1, NFS 4.2)

User Behavior Analytics

Active Defense with Ransomware Protection

Audit Reports

encryption

compression

deduplication

File Indexing and Secure Restore

Policy-Based Snapshots

WAN Optimized Replication

Transparent Data Movement to the cloud

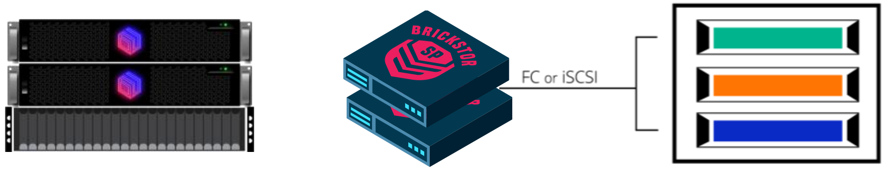
Scale-*Right* Deployment Model

Store and Protect Enterprise Data ANYWHERE – at the Edge, Core, or Cloud

Cloud/Hyperscalers

aws

Data Center and Edge



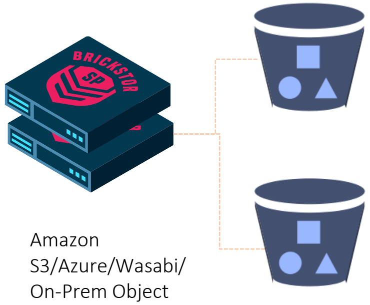
AHV

KVM

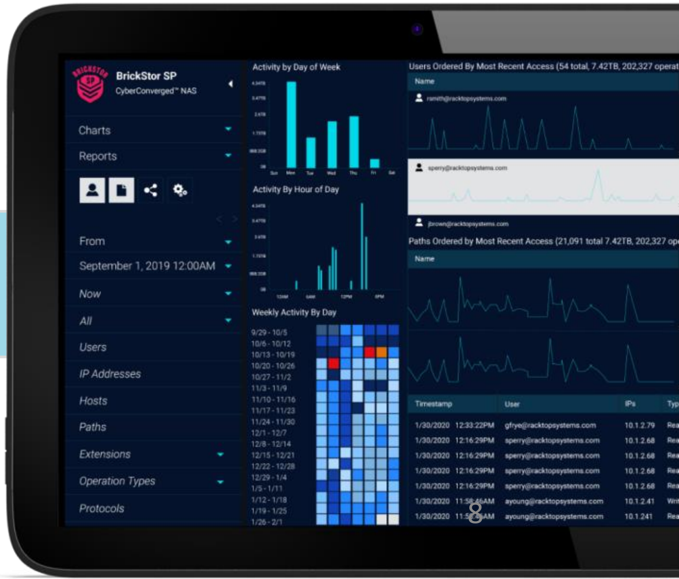
Microsoft Hyper-V

vmware

Hybrid (S3 Object)



Multi-System Management Through Single Interface



BrickStor SP
CyberConverged™ NAS

- Charts
- Reports
- From
- September 1, 2019 12:00AM
- Now
- All
- Users
- IP Addresses
- Hosts
- Paths
- Extensions
- Operation Types
- Protocols

Activity by Day of Week

Activity By Hour of Day

Weekly Activity By Day

9/29 - 10/5
10/6 - 10/12
10/13 - 10/19
10/20 - 10/26
10/27 - 11/2
11/3 - 11/9
11/10 - 11/16
11/17 - 11/23
11/24 - 11/30
12/1 - 12/7
12/8 - 12/14
12/15 - 12/21
12/22 - 12/28
12/29 - 1/4
1/5 - 1/11
1/12 - 1/18
1/19 - 1/25
1/26 - 2/1

Users Ordered By Most Recent Access (54 total, 7.42TB, 202,327 operat

Name
rsmith@racktopsystems.com
sperry@racktopsystems.com
jbrown@racktopsystems.com

Paths Ordered by Most Recent Access (21,091 total 7.42TB, 202,327 ope

Name

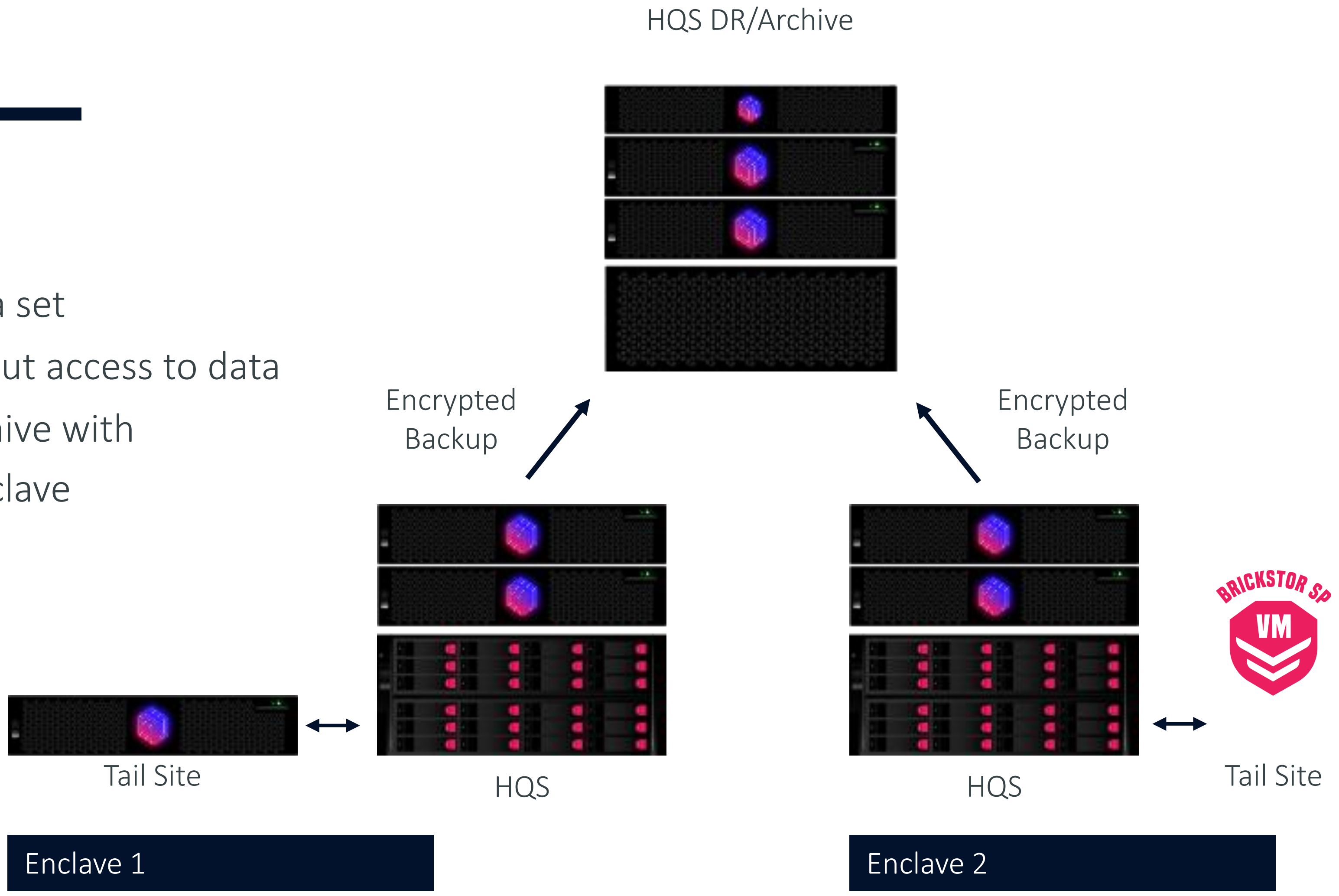
Timestamp	User	IPs	Typ
1/30/2020 12:33:22PM	gfrye@racktopsystems.com	10.1.2.79	Rea
1/30/2020 12:16:29PM	sperry@racktopsystems.com	10.1.2.68	Rea
1/30/2020 12:16:29PM	sperry@racktopsystems.com	10.1.2.68	Rea
1/30/2020 12:16:29PM	sperry@racktopsystems.com	10.1.2.68	Rea
1/30/2020 12:16:29PM	sperry@racktopsystems.com	10.1.2.68	Rea
1/30/2020 11:58:46AM	ayoung@racktopsystems.com	10.1.2.41	Wri
1/30/2020 11:58:46AM	ayoung@racktopsystems.com	10.1.241	Rea

RACKTOP

Secure Enclaves

Scalable Appliances

- Data is uniquely encrypted per data set
- Systems can be administered without access to data
- Replicate encrypted data to an archive with encryption keys held within the enclave



HQS DR/Archive

Encrypted Backup

Encrypted Backup

Tail Site

HQS

HQS

BRICKSTOR SP

VM

Tail Site

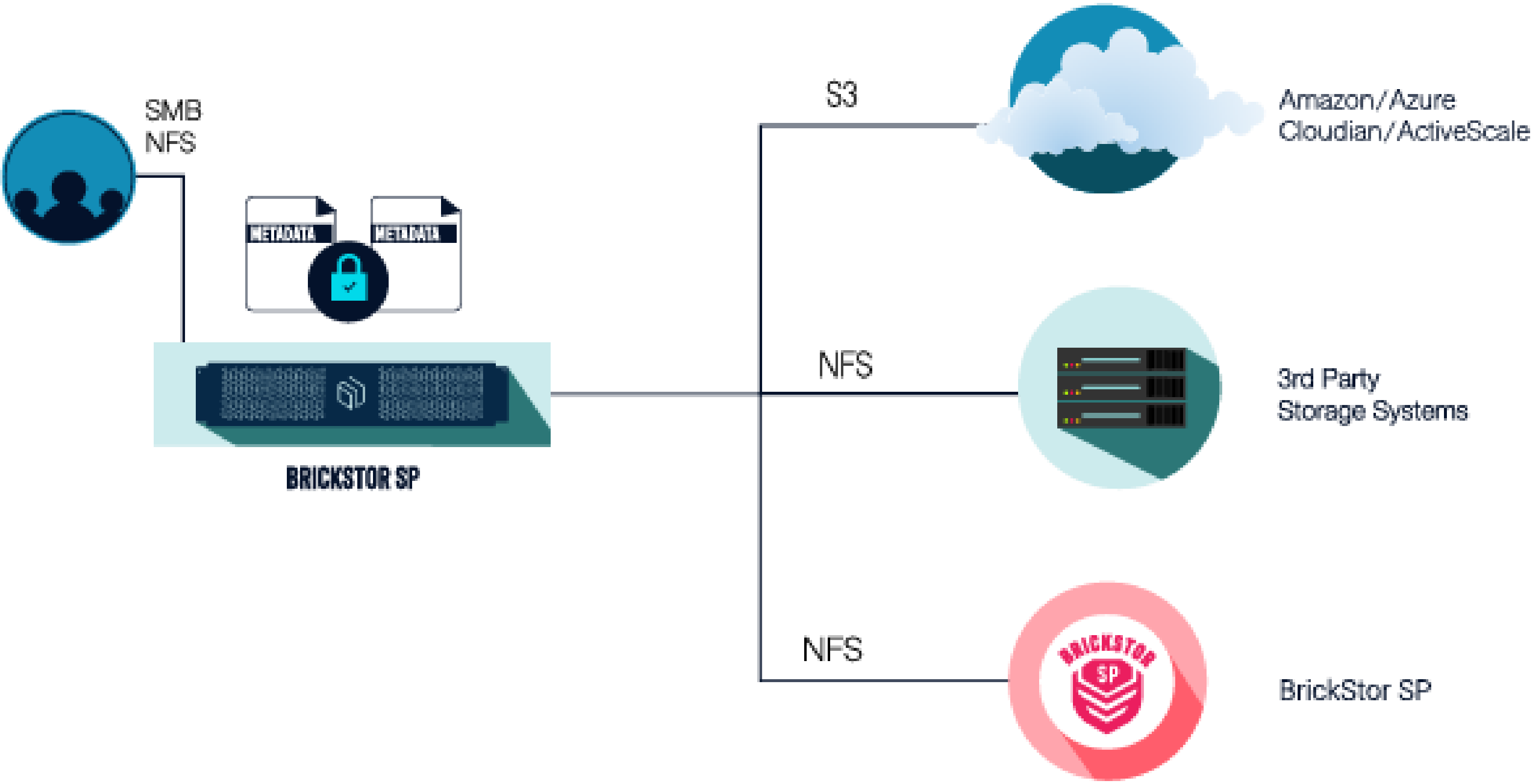
Enclave 1

Enclave 2

Transparent Data Movement (TDM)

Secure and Efficient Hierarchical Lifecycle Management

- Compress and encrypts before it leaves BrickStor SP
- Maintain control of keys
- Support multiple targets
- Workflow stays the same
- Reduce storage costs



Use Cases

Store and Protect Enterprise Data ANYWHERE – at the Edge, Core, or Cloud

Enterprise Applications & IoT

HPC

Secure Backup & Archive Repository

User File Shares & Home Directories

Online Archive

Computer Forensics

DevOps/SecOps

Electronic Health Records VNA / PACS

Manufacturing

Streaming Video & Surveillance

RACKTOP

Jumpstart Program: protect data immediately with the BrickStor SP Virtual Appliance

Promotional Offer

- Free for 90-days
- No paperwork, no strings attached
- No commitment software subscription
- Includes two BrickStor SP virtual appliances
- Includes free install and 24/7/365 full support
- Minimum of 4vCPU & 32GB of RAM required

https://www.racktopsystems.com/jumpstart

Multilevel Security (MLS)

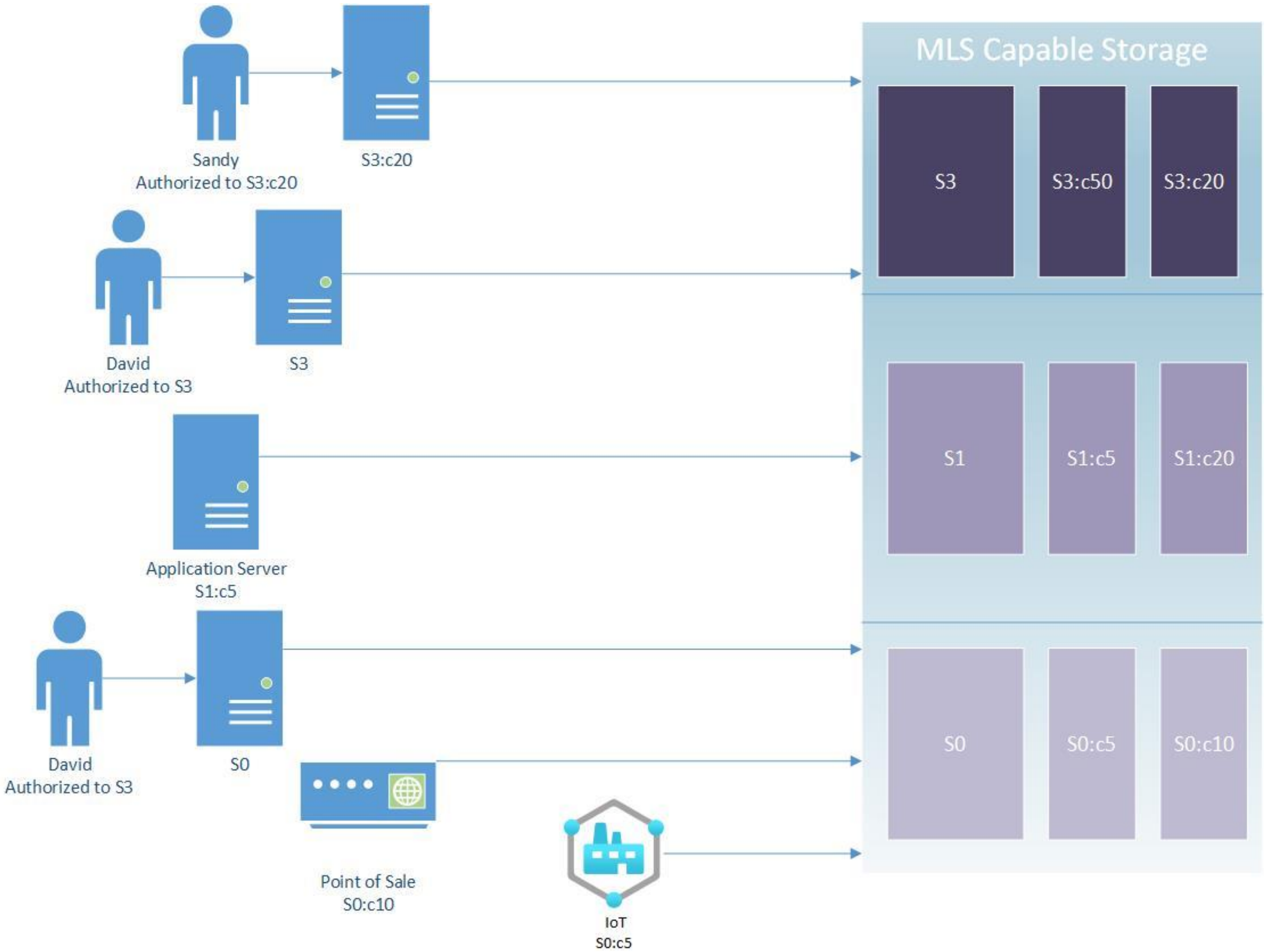
How any organization can leverage and benefit from MLS

Where Did MLS Come From?

- Confidentiality requirements around classified & compartmented data
- Bell–LaPadula model
  - To determine whether a specific access mode is allowed, the clearance of a subject is compared to the classification of the object (Sensitivity & Compartment)
    - 2 Mandatory Access Control Rule
      - User/Application cannot read an object at a higher sensitivity level
      - User/Application may not write an object at a lower sensitivity level ***
    - 1 Discretionary Access Control Rule
      - Normal Owner, Read, Write, Execute

MLS As a Concept

- User can access files based on a set of rules beyond simple ACL using Attribute Based Access Controls (ABAC)
- Access to file must satisfy all 4 questions
  - Is the machine used by user/application approved to access file Classification Level
  - Is the machine used by user/application approved for all caveats in the file
  - Is the user approved for the Classification Level of the file
  - Is user approved to access all caveats in the file
- Files that are above the classification level of the user role or machine are not accessible
- Files that have a compartment the user doesn’t have are not accessible
- Users and Applications can browse down and write same as their role
- Administrative rights doesn’t provide access to sensitive information



MLS Capable Storage

S3

S3:c50

S3:c20

S1

S1:c5

S1:c20

S0

S0:c5

S0:c10

Sandy
Authorized to S3:c20

S3:c20

David
Authorized to S3

S3

Application Server
S1:c5

David
Authorized to S3

S0

Point of Sale
S0:c10

IoT
S0:c5

MLS Restaurant Demo

User	Sensitivity	Compartment
Vegan	S1	
Vegetarian	S2	
Carnivore	S3	

Item	Sensitivity	Compartment
Vegan Items	S1	
Dairy and Animal Derived Products & Fish	S2	
Meat	S3	
Non-alcoholic Drinks	S0	
Alcoholic Drinks	S0	C100

2022 FORTRESS CYBER SECURITY AWARD

CYBERSECURITY BREAKTHROUGH AWARD 2022

2021 FORTRESS CYBER SECURITY AWARD

SECURITY today GOVIES 2020 Government Security Awards

NVTC CAPITAL CYBER AWARDS 2022 FINALIST

2022 GLOBEE AWARDS GOLD WINNER CYBER SECURITY GLOBAL EXCELLENCE

STRATUS 2022 AWARD

FINALIST 2021 CISO CHOICE AWARDS Data Security RACKTOP SYSTEMS

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2022

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2021

RACKTOP