SNIA STORAGE SECURITY SUMMIT

Wednesday, May 11, 2022 • Virtual

Importance of Cyber-Resiliency for next data decade

Key trends around cyber resiliency & how to design cyber resiliency strategy

Presented by: Anay Pathak

A SNIA Event

Agenda

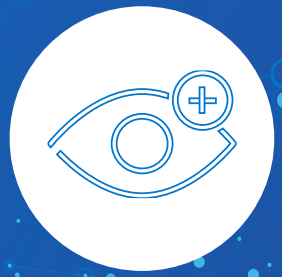
- ✓Understating Cyber Resiliency
- ✓Trends and why it is important to be resilient in today's connected world
- ✓Cyber Resiliency: Key requirements from customers
- ✓Best Practices and how to design CR strategy

Digital Risk

The greatest facet of risk that an organization faces when transforming

Successfully Manage the Risk

CHALLENGE: SECURE DATA BACKUP AND RECOVERY	CHALLENGE: THREAT AND VULNERABILITY DETECTION AND RESPONSE	CHALLENGE: SUPPLY CHAIN INTEGRITY



Dell Safeguard and Response powered by VMware Carbon Black

PowerProtect Cyber Recovery

VMware NSX Network Virtualization Platform

Dell Technologies Managed Detection and Response

Supply Chain Security and Integrity

Gain the confidence, control and scale you need to address security challenges from Dell Technologies.

Cyber Attacks – A threat to IT Transformation

Data-driven Society

Data has immense value, offers insights and transfer's leverage. Data fuels global economies and our professional, social and individual lives

Inadequate Protection for Critical Data

Cybercrime and cyber warfare are outpacing preventative solutions and are terminal threats to businesses, governments and all data-driven entities

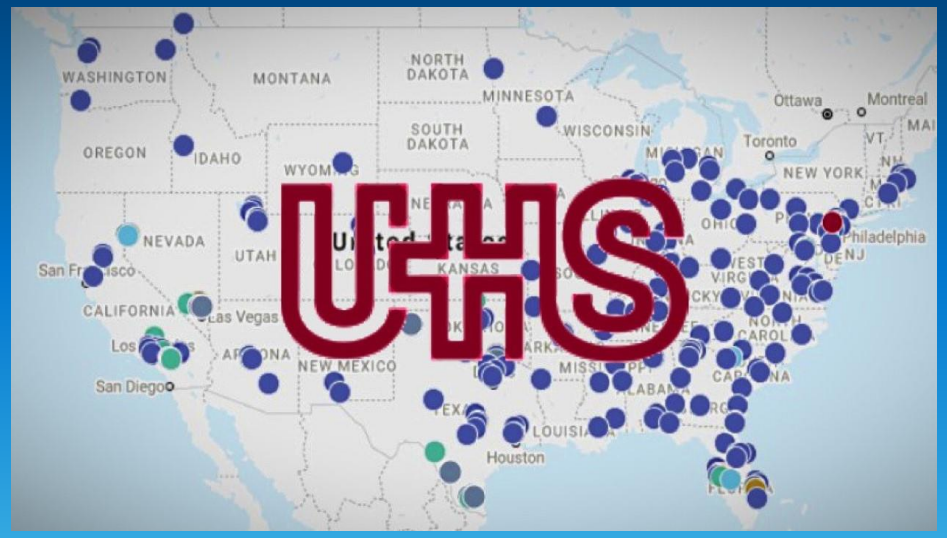
Cyber Recovery is an Enabler of Security Transformation

Modern threats require modern protection, isolation and intelligence to enable recovery in wake of successful ransomware or cyber attack

Cyber attacks are increasingly sophisticated

Source: SolarWinds, Jan 2021

Source: Wired, Oct 2020



Source: HealthITSecurity.com, Oct 2020

SNIA STORAGE SECURITY SUMMIT

"69% of global IT decision-makers lack confidence their organizations could reliably recover all business-critical data in the event of a cyber attack. "

Global Data Protection Index Survey 2020 Snapshot

HOBBLED —

four-day service meltdown was caused by ransomware

Anticipates $50-70 Million Loss Following Ransomware Attack

ICS Threat Snake Ransomware Suspected in Attack

An attack targeting the automaker reportedly infected internal servers and led to the suspension of production at plants around the world.

Dell EMC commissioned Vanson Bourne for the Global Data Protection Index, which was conducted between September and November 2019.

Cyber Threat Actors

Different Motivations, Techniques, & Goals

CRIME	INSIDER	ESPIONAGE	HACKTIVISM	TERRORISM	WARFARE
					
Theft & extortion for financial gain	Trusted insiders steal or extort for personal, financial, & ideological reasons. Increasingly targeted because of privileged access to systems	Corporate or Nation-state actors steal valuable data	Advance political or social causes	Sabotage & destruction to instill fear	Nation-state actors with destructive cyber weapons (Not Petya)

Cyber Threats 2021: The facts

39s

Every 11 seconds

a cyber or ransomware attacks occur.*

71%

86%

of breaches are financially motivated.

verizon

$13M

$24.7M

Avg. cost of cybercrime for an organization.

accenture

$1T

$6T

Total global impact of cyber crime in 2021.

Cybersecurity Ventures

43%

48%

of breaches involved small business.

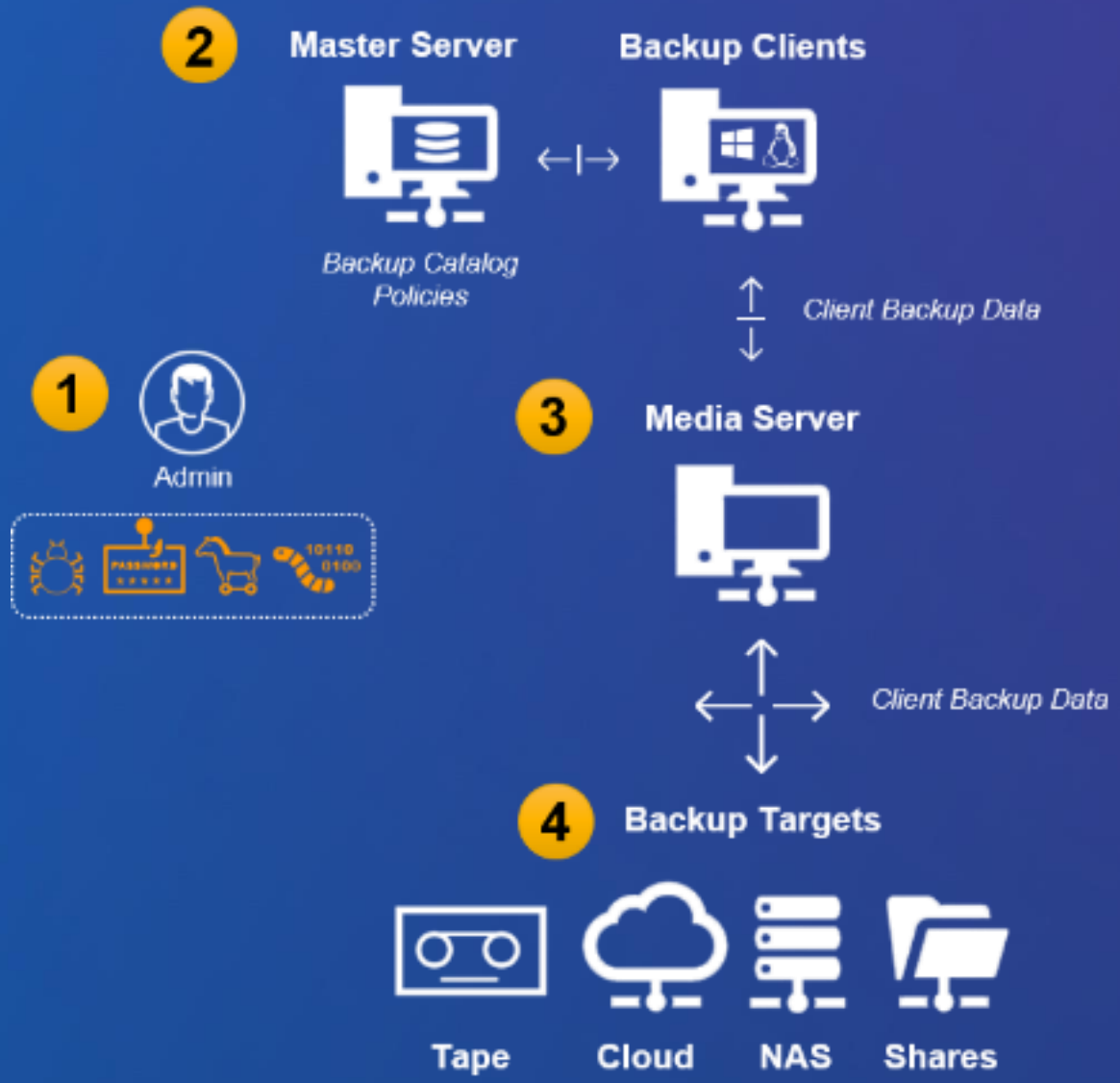
verizon

Banking	$18.4M
Utilities	$17.8M
Software	$16.0M
Automotive	$15.8M
Insurance	$15.8M
High Tech	$14.7M
Capital Markets	$13.9M
Energy	$13.8M
US Federal	$13.7M
Consumer Goods	$11.9M
Health	$11.9M
Retail	$11.4M
Life Sciences	$10.9M
Media	$9.2M
Travel	$8.2M
Public Sector	$7.9M

*Source: Cybersecurity Ventures

SNIA STORAGE SECURITY SUMMIT

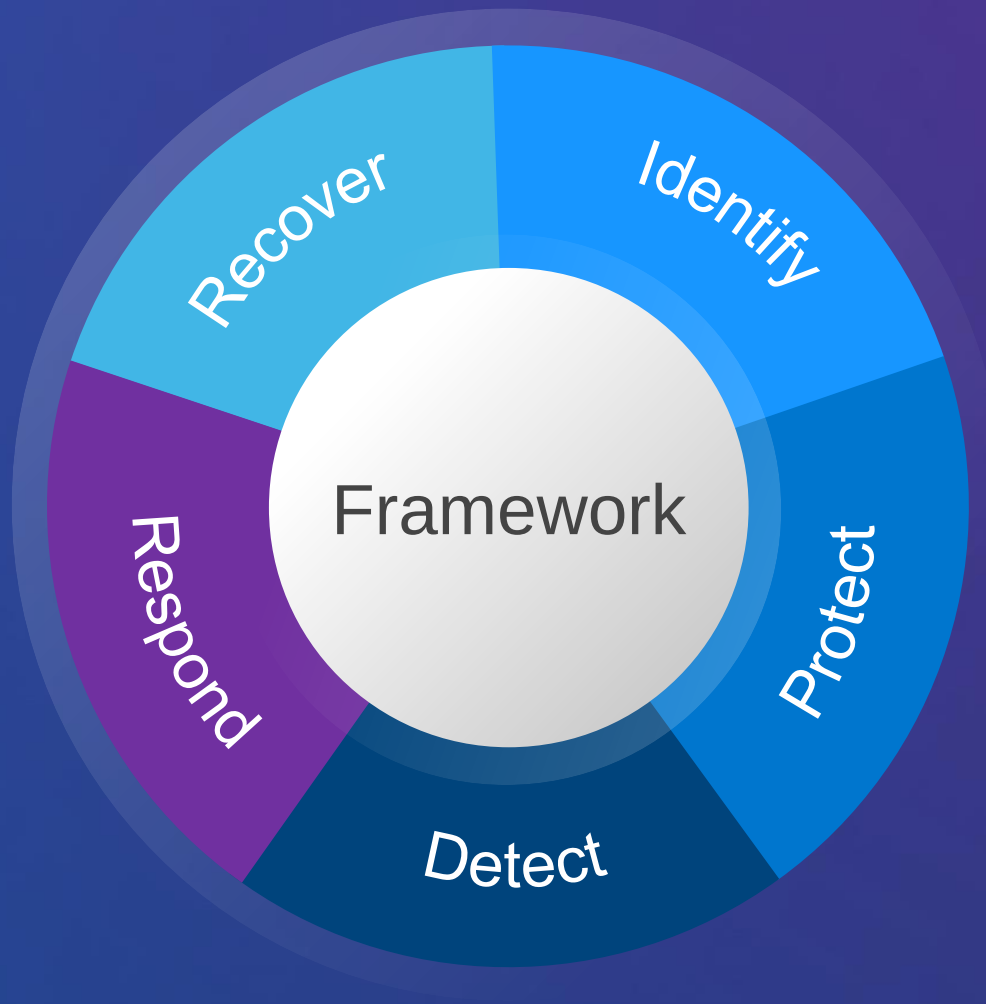
Attackers Target Primary Backups



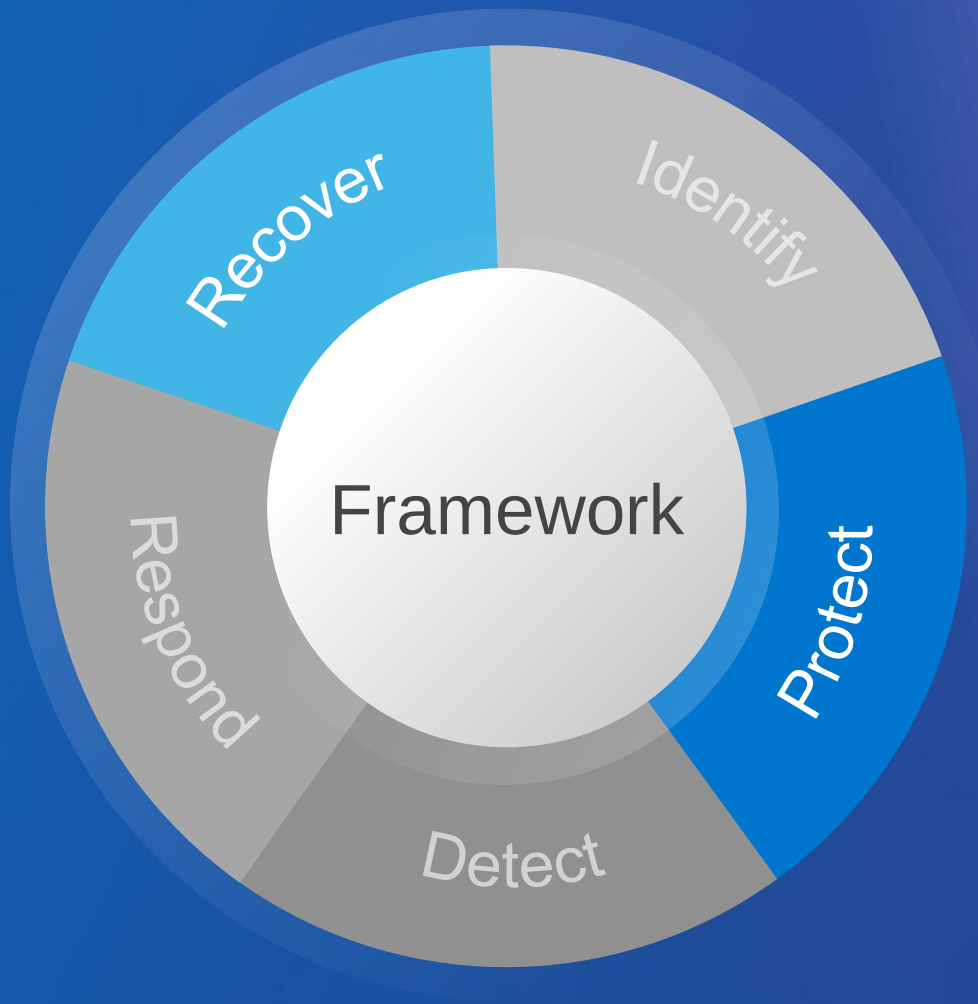
Cyber resilience is a strategy.

A high-level holistic strategy that includes cyber security standards, guidelines, people, business processes and technology solutions.

Example: NIST Cybersecurity Framework



Source: https://en.wikipedia.org/wiki/Cyber_resilience



Cyber recovery is a solution.

A data protection solution that isolates business-critical data away from attack surfaces.

Critical data is stored immutably in a hardened vault enabling recovery with assured data availability, integrity and confidentiality.

Source: https://en.wikipedia.org/wiki/Cyber_resilience

Cyber Recovery Requirements

Modern threats require modern solutions

Isolation

Physical & logical separation of data

- Air gap with physical isolation
- Logical isolation – not just separate from production
- Automation and control from secure side
- Secure during “unlock” phase
- Certification to a standard (Sheltered Harbor)

Immutability

Preserve original integrity of data

- A capability, not a solution
- Compliance with a standard (eg 17a-4)
- No admin or security overrides
- NTP Hardening
- Single point of failure / platform dependence

Intelligence

ML & analytics identify threats

- Answers the question: “Could this data be used for recovery?”
- Full content, not just metadata
- Resides and operates in the air gapped vault for security
- Reporting used to inform root cause and recovery

Please take a moment to rate this session.

Your feedback is important to us.

Key Data to Protect by Industry

Healthcare

Electronic Medical Records, scheduling, payment and billing systems

Financial Services

Payments, Core Banking, Trading, Treasury, Sheltered Harbor data

Life Sciences

Research and development, drug discovery & Clinical trial data

Retail

Point of sale, inventory, shipping

Legal

Document management, conflicts checking, billing, email

Oil & Gas

Seismic & geographical exploration data

Government

Property records and taxes, justice systems, payment collection, licenses

Manufacturing

Plant manufacturing and scheduling, ordering systems, inventory

