



THE MOST SECURE STORAGE
ON THE PLANET

???

ADV CYBER XCHANGE CONFERENCE

DATENHOHEIT
DATENSICHERHEIT

Peter Hermann
Alfred Grossler



Agenda

1. WAS IST DATENHOHEIT?

1. Definition
2. 4 Faktoren
3. Datensicherheit
4. Datenspeicherung
5. Datenschutz

2. WELCHEN BEITRAG NETAPP LEISTET

1. Unsere Lösungen
2. FY'26 Big Bets

3. Partnership Check-In

4. Next steps together

DATENHOHEIT - Definition

Beschreibt das Prinzip, dass digitale Daten den Gesetzen und der Kontrolle des Landes unterliegen, in dem sie erfasst oder gespeichert werden, und dass die Dateninhaber die volle Hoheit über diese Daten haben.

DATENHOHEIT

Nationale Kontrolle:

Die Regierung hat die Befugnis, die Erhebung, Speicherung und Verarbeitung von Daten zu regeln, die innerhalb ihrer Grenzen generiert werden.

Anwendbarkeit von Gesetzen:

Digitale Daten unterliegen den Datenschutzgesetzen der Gerichtsbarkeit, in der sie sich befinden.

Kontrolle über Daten:

Volle Kontrolle über den Zugriff, die Nutzung und die Verwaltung der eigenen Daten.

DATENHOHEIT

1

Datenhoheit ist
direkt mit
Datensicherheit
verlinkt

2

Datenhoheit wird in
der jetzigen
geopolitischen Lage
immer wichtiger

3

Organisationen sind
immer mehr
international verlinkt

DATENHOHEIT



4 Faktoren:

DATENSICHERHEIT

DATENSPEICHERUNG

DATENSCHUTZ

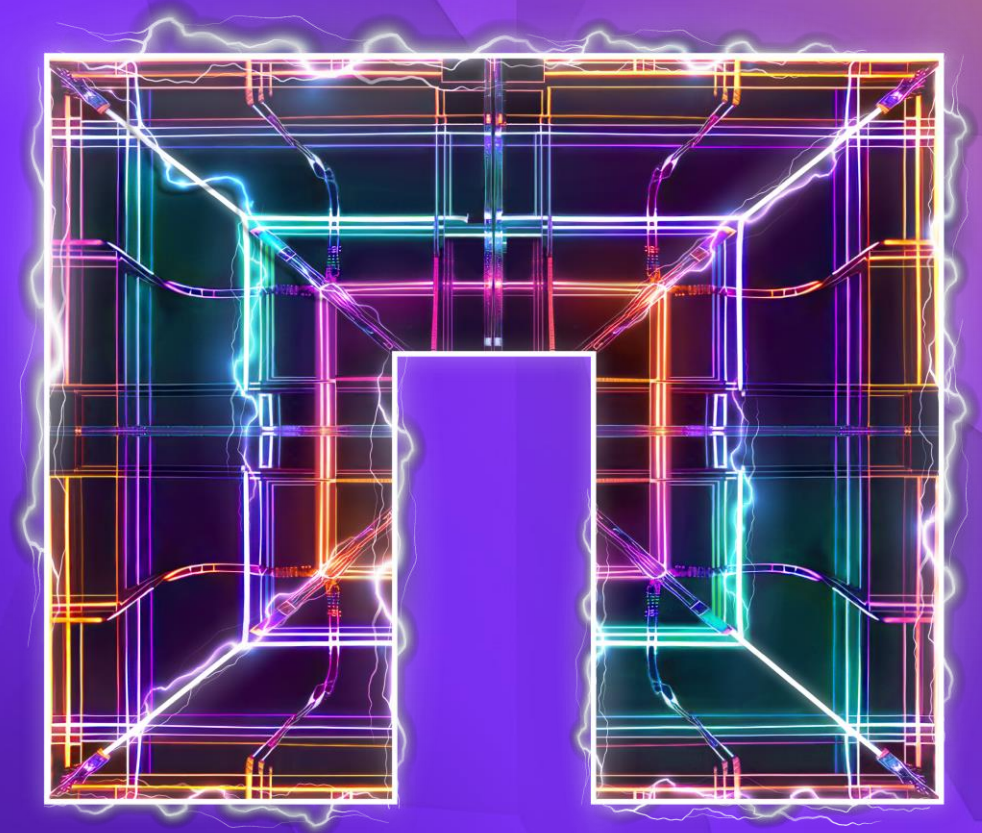
DATENHOHEIT

DATENSICHERHEIT

Wie widerstandsfähig ist unsere digitale
(Storage- und Datenmanagement)
Infrastruktur wirklich ?

Oder:

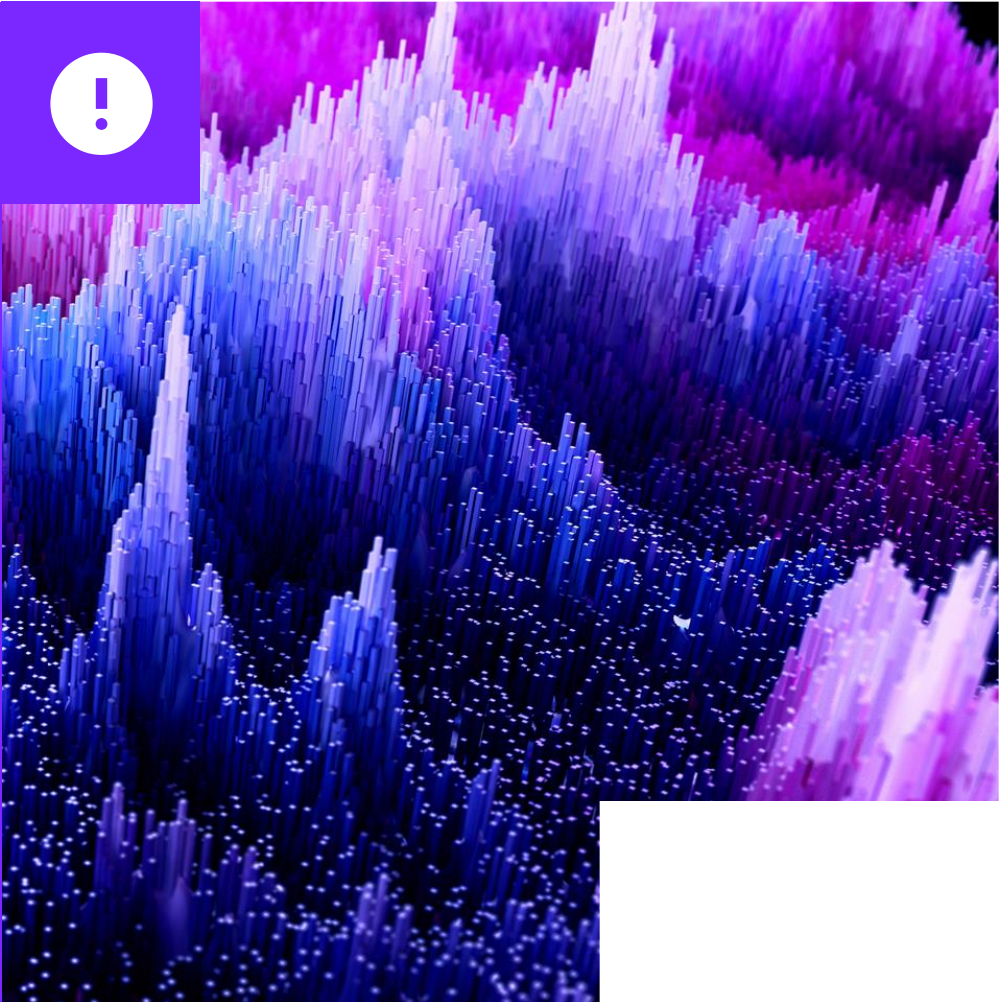
„NetApp = The most secure storage on the planet ?“



We are in the “Era of data”

But companies need to overcome some big hurdles

Data is increasing in complexity and highly fragmented across on-premises and hybrid multi-cloud environments	Data is costly to store and manage, with increasing pressures to cut costs, capex, and demonstrate ROI	Data is the crown jewel and constantly under threat
Complex and fragmented 	Costly to store and manage 	Under threat 
Data fuels AI workloads, but data management and operational bottlenecks make it hard to scale	Data and applications infrastructure needs to responsively scale to demand	Data-related operations need to be more sustainable to meet rising expectations
Hard to scale 	Scale to demand 	Sustainability 





NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

Guidelines to manage and reduce cybersecurity risk and threats.

NIST
CSF 2.



Was ist “NIST CSF” und deckt sich das mit EU-Richtlinien ?

Das NIST Cybersecurity Framework (CSF) ist ein US-amerikanischer Standard, der weltweit Anerkennung findet – auch in Europa. Obwohl es kein offizieller EU-Standard ist, lässt sich das NIST CSF gut mit europäischen Richtlinien wie der **DSGVO**, der **NIS2-Richtlinie** und dem **Cyber Resilience Act** in Einklang bringen. Hier ist ein Überblick:

🇪🇺 Vergleich: NIST CSF vs. EU-Richtlinien

NIST CSF Funktion	Entsprechung in EU-Richtlinien
Identify	Risikomanagementpflichten (Art. 20 ff NIS2)
Protect	Datenschutzmaßnahmen (DSGVO Art. 32), technische und organisatorische Maßnahmen
Detect	Pflicht zur Erkennung von Vorfällen (NIS2, Cyber Resilience Act)
Respond	Meldepflichten bei Vorfällen (DSGVO Art. 33, NIS2 Art. 23)
Recover	Wiederherstellungspläne und Business Continuity (NIS2, Cyber Resilience Act)
Govern	Governance-Strukturen (NIS2 Art. 7–10), Verantwortlichkeiten und Strategien



Source: Copilot



THE MOST SECURE STORAGE ON THE PLANET

???



**Der einzige validierte Enterprise
Storage Hersteller für die
Speicherung von
NSA Top-Secret Daten!**



FIPS 140-3



Common Criteria



U.S. Department of Defense
Information Network (DoDIN)
Approved Products List
(APL)



Commercial Solutions for
Classified (CSfC) Program
Component List

CYBER RESILIENCY

for any
workload

hosted
anywhere

SECURE BY DESIGN

Only enterprise
storage validated by
NSA CSfC to store
top-secret data



Policy engine

Automatically block
known malicious
file types



WORM primary data and tamper- proof snapshots

Prevent data
destruction with
immutable and
indelible
snapshots



AI-powered autonomous ransomware protection

Real-time detection
and response on file,
block, native cloud
and user behavior



Multi-admin / multi-factor verification

Block rogue
admins and
malicious users



End-to-end encryption

Secure data
at rest, in transit
and in use



CYBER RESILIENCY



AUTONOMOUS RANSOMWARE PROTECTION

Detection and response
embedded in the storage layer.

REAL-TIME DETECTION AND RESPONSE

AI-powered ransomware detection and response for file

Real-time file
anomaly detection
- respond with
automatic
snapshots



AI-powered ransomware detection and response for block

Real-time vm
anomaly detection
- respond with
automatic
snapshots



Ransomware detection and response for native cloud

Real-time file
anomaly
detection for
FSx - respond
with automatic
snapshots



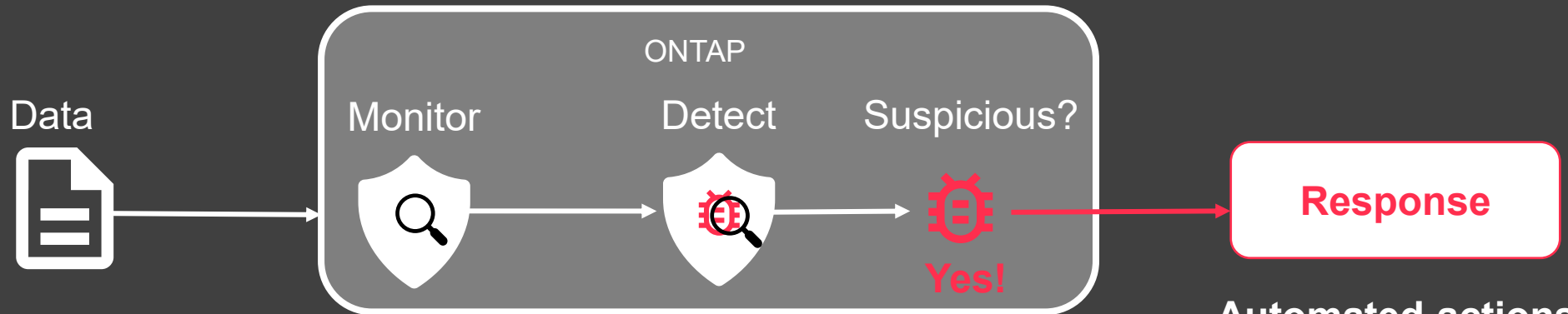
AI-powered detection for user behaviour

Real-time user
behaviour anomaly
detection with
automatic
snapshots



On-device anomaly detection (ARP/AI) simplified

World's first on-box, AI-powered, real-time ransomware detection and response



Monitor for signals

- Data Entropy
- Encrypted file content
- Encrypted file headers
- File metadata signatures

We do NOT open the files!

Automated actions

- Mark current snapshot for hold
- Create evidence
- Generate alerts

Customer actions

(May require additional software)

- Investigate
- Block user
- Take system offline?

Ransomware Recovery Guarantee

No data loss. We guarantee it.

TRUST IN NETAPP'S ABILITY
TO **RECOVER DATA** EVEN AFTER
A RANSOMWARE ATTACK



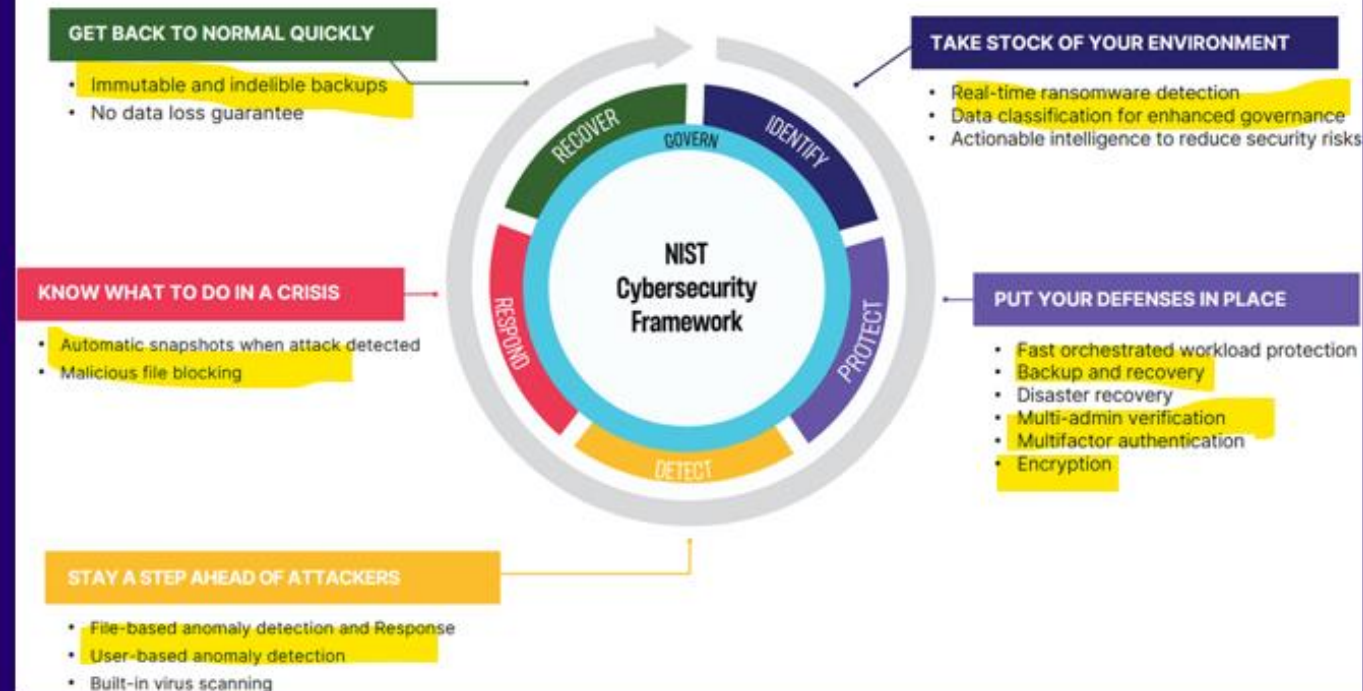
The NetApp Ransomware Recovery Guarantee*
for enterprise primary storage

*Guarantee covers tech deployment and service engagements. T&Cs apply.

Zusammenfassend: NetApp bietet Sicherheit “per Design AND out of the box” um NIST CSF Frameworks & NIS2 + DORA Richtlinien umzusetzen.

Start fortifying your defense today

Aligning your cybersecurity strategy with the NIST cybersecurity framework enables you to build a stronger, more resilient solution. Wherever you are on your cybersecurity journey, NetApp® technologies and expertise can help you create a solution that adheres to NIST guidelines and helps you achieve your desired business outcomes.





IS THE MOST SECURE STORAGE
ON THE PLANET !!!

DATENSPEICHERUNG

DATENSCHUTZ

DATENSCHUTZ

Schutz personenbezogener Daten vor:

- Missbrauch
- Unbefugter Verarbeitung
- Ungewollter Weitergabe

Regelt wie Unternehmen und Organisationen

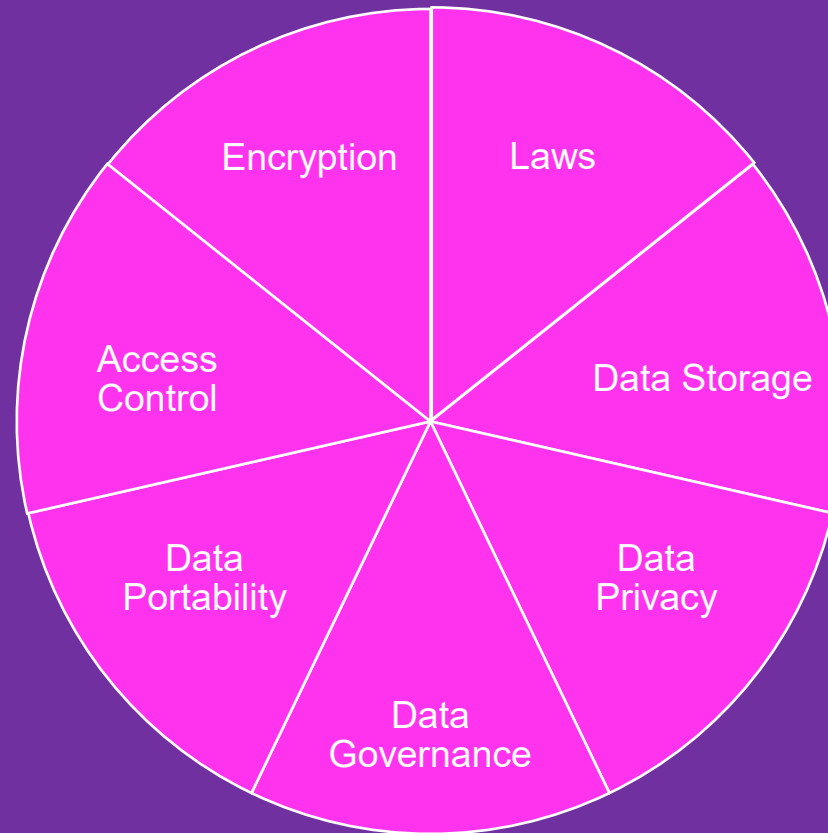
- Namen, Adressen, E-Mail Adressen, IP Adressen

sammeln, speichern und nutzen dürfen

Grundlage:

Datenschutz-Grundverordnung (DSGVO)

UNSERE LÖSUNGEN FÜR DIESE HERAUSFORDERUNGEN



NEXT STEPS

- **Verschlüsselt Daten und managed die Keys**
- **Aktiviert Ransomware Protection**
- **Managed die Daten**
- **Regelmäßige Security Assessments**
- **Regelmäßige Compliance Checks**

DANKE