COHESITY

NETNORDIC TECHNOLOGY UNIVERSITY

Chris Dyer – Principal Channel SE, NEUR

COHESITY

Cohesity + Veritas: The Leader in AI-powered Data Security

Our Mission:

To protect, secure & provide insights into the world's data.
The largest organizations in the world rely on us for their Resilience.

Our Focus:

Data Protection
- Broad Workloads
- Enterprise Scale
- Flexible Consumption

Data Security
- Ultrafast Threat Detection
- Posture Management
- Automated Cyber Recovery

Data Insights
- GenAI for Unstructured Data
- Search & Analytics
- Operational Insights

What We Bring:

$1.7B Revenue[1]	**100+ EBs** Data Protected	**1600** Patents
2x R&D of Nearest Competitor	**19.4%** Market Share[2] (Leader)	**140** Global Locations
12000 Customers	**3000** Partners	**Leader** Gartner MQ

Notes: 1. 2023 pro forma metrics after acquisition of Veritas data protection business
2. Analyst and Company Research, Proforma 2023 Backup and Recovery Market Share

Delivering Business Outcomes That Matter

05 min

to restore email, down from 4 days.

INCREASE RESILIANCE

$0 paid

during a ransomware attack

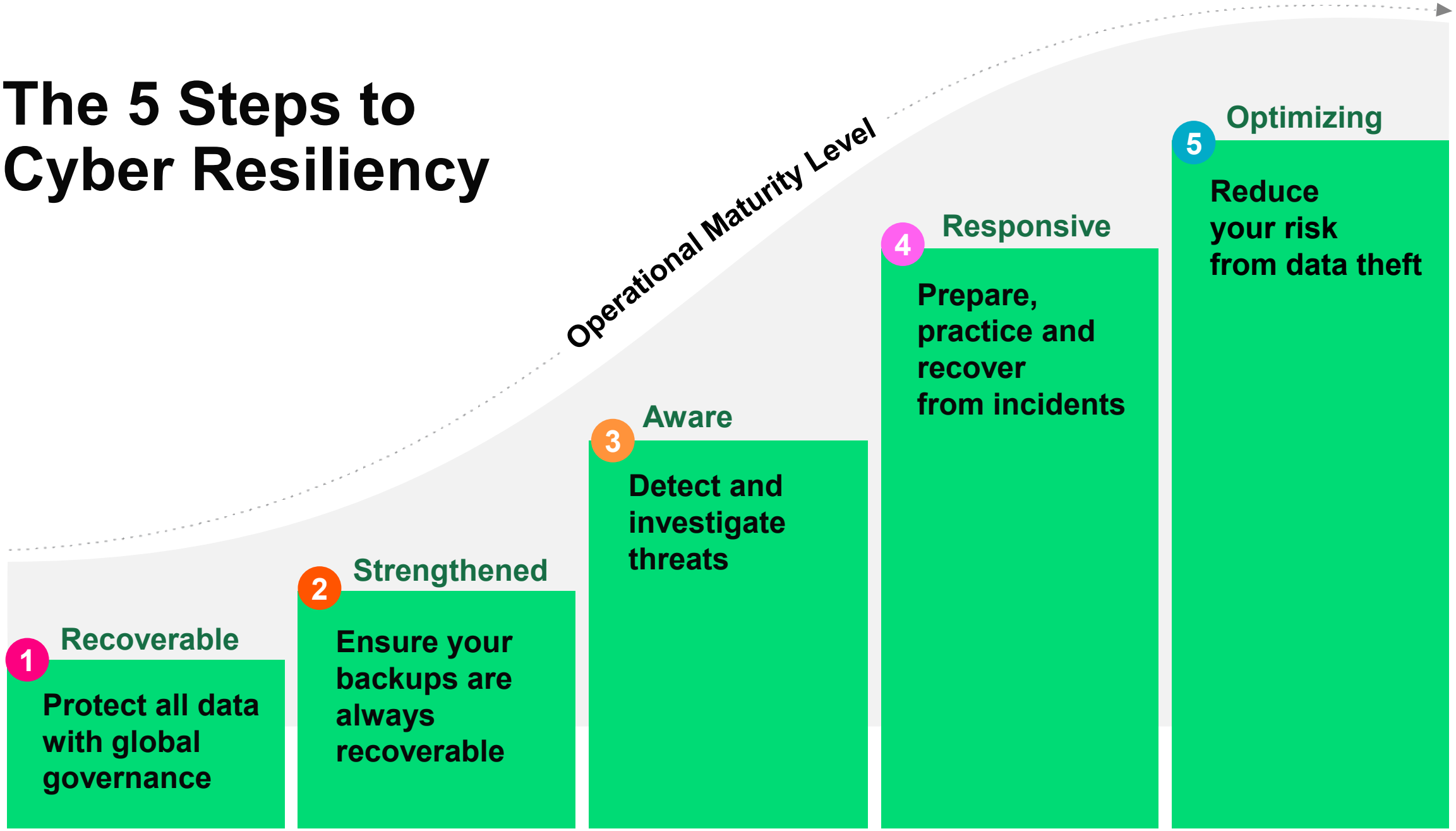
REDUCE RISK

$2 Million

annual savings after upgrading to Cohesity

LOWER COSTS

The 5 Steps to Cyber Resiliency



1 PROTECT ALL DATA with global governance

Identify unprotected data – your biggest security risk

Physical servers VMs Containers	Databases Unstructured data NAS	SaaS	1000+ data sources

Cohesity Data Cloud

Unified UI + APIs | Common SLAs | Compliance | Reporting | Policies | AI-Powered Operations

Critical Success Factors

Storage Efficiency | Scale-out Performance | Global Search | Flexible Deployment Models | Consistent Licensing

KEY OUTCOMES

- Enhanced security
- Risk reduction
- Improved compliance & governance
- Lower costs & improved ROI
- Increased IT efficiency

2 ENSURE YOUR BACKUPS are always recoverable

Harden your platform + add a cyber vault

1000+ data sources

On-Prem | Cloud | SaaS | Edge

Cohesity Data Cloud

Immutability | MFA | Separation of Duties | RBAC | 3-2-1-1 | Threat Containment | DataLock

Cyber Vault

Physical & logical isolation

Critical Success Factors

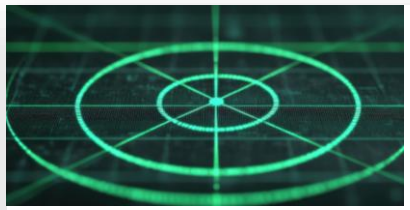
Backup Restoration Performance | Cyber Vault On-Prem or Cloud | Cyber Vault Key Management & Immutability

KEY OUTCOMES

- Faster & more secure recovery
- Stronger protection against attacks
- Audit readiness
- Zero trust alignment

3 DETECT AND INVESTIGATE threats

Regularly conduct threat scanning & threat hunting



Threat scanning

Threat hunting

Ecosystem integrations
(SIEM/SOAR)

Cohesity Data Cloud

Automated & On-Demand Scanning | AI-Powered Anomaly Detection | Threat Intelligence | Hash Index | Forensics

Critical Success Factors

Built-In & BYO Threat Feeds | 100,000s Indicators of Compromise | YARA Rules | Open & Extensible Platform

KEY OUTCOMES

- Early threat detection & mitigation
- Backup integrity assurance
- Faster incident recovery and reduced downtime
- Shared context for IT & InfoSec teams

4 PREPARE, PRACTICE, AND RECOVER from incidents

Automate cyber recovery: initiate, investigate, mitigate

Digital Jump Bag™

Orchestration

Clean Room

Rapid Recovery at Scale

Cohesity Data Cloud

Secure File Storage | Cyber Recovery Orchestration | Clean Room Solution | Forensic Threat Hunting | IR Ecosystem

Critical Success Factors

MVRC | Incident Analysis Timeline | Instant Mass Restore | CERT (Cyber Event Response Team)

KEY OUTCOMES

- Faster & safer recovery
- Improved RTO
- Lower risk of re-infection
- Reduced disruption & financial risk

5 REDUCE YOUR RISK from data theft

Optimize your data security posture

Assess incident impact

Identify unprotected critical data

Data classification

DSPM ecosystem
Data discovery & classification

Cohesity Data Cloud

Large Pattern Dictionary | Context Recognition | Name Entity Recognition | Ensemble Learning Models | DSPM Integration

Critical Success Factors

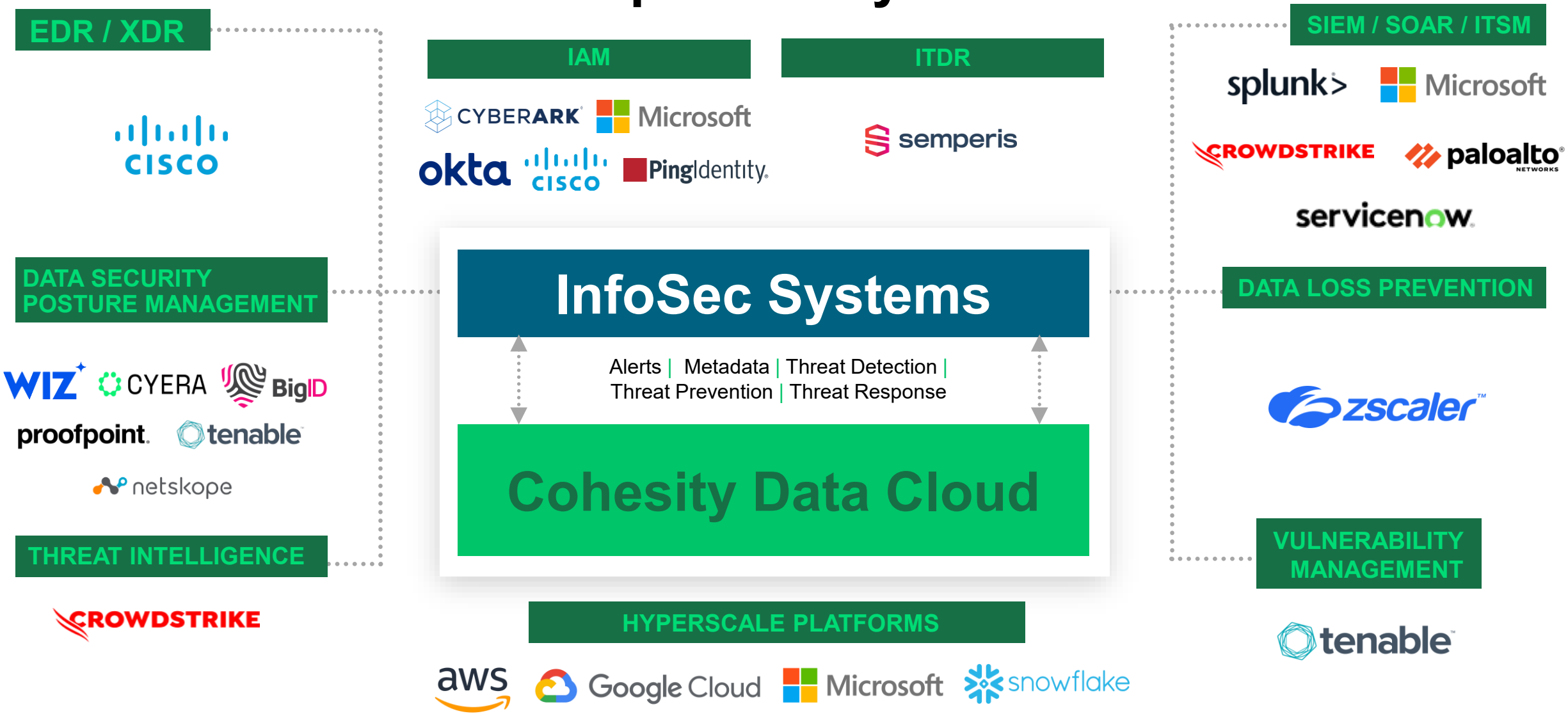
230+ Data Classifiers | Choose the Right DSPM Solution

KEY OUTCOMES

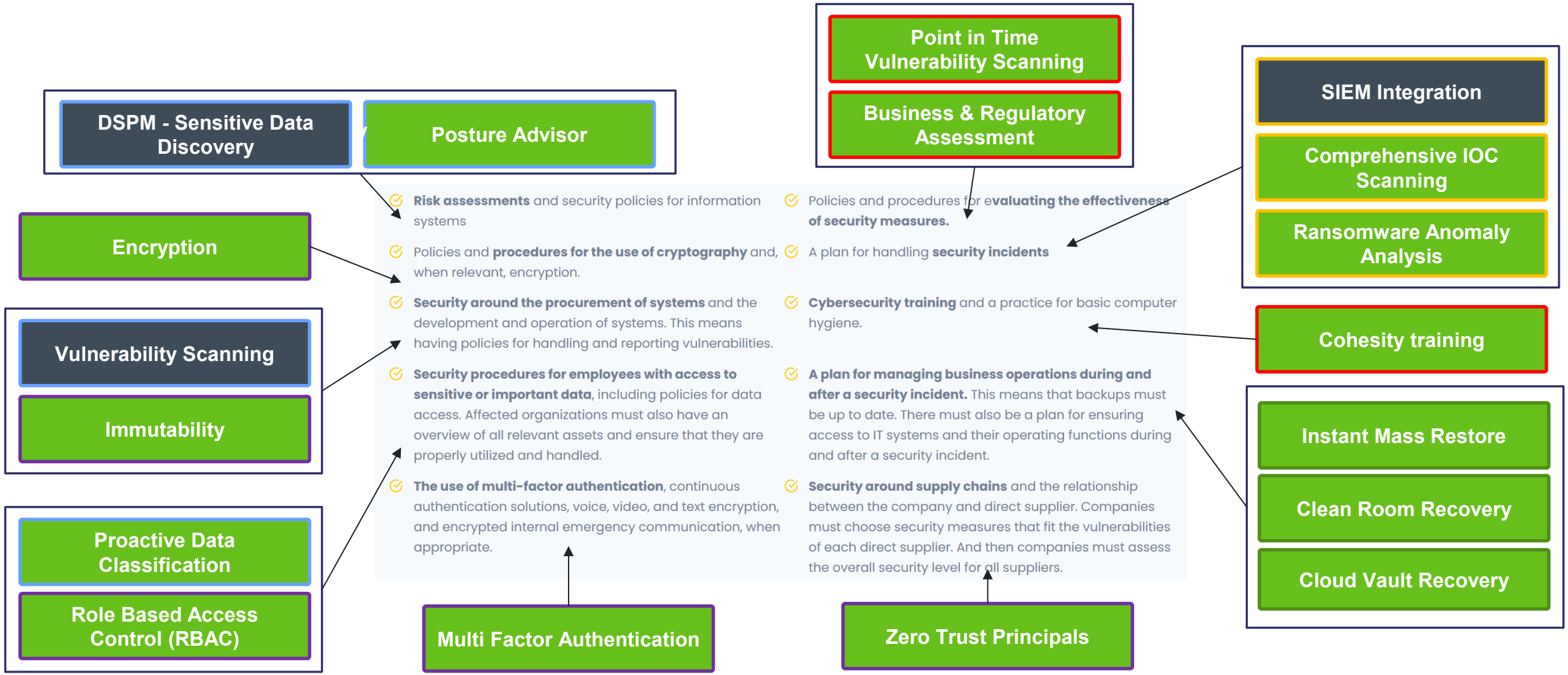
Enhanced data visibility & classification

Proactive risk identification & mitigation

The Industry's Most Secure & Open Ecosystem



EU NIS 2 Directive



Introducing the Destructive Cyberattack Maturity Model

5 Steps to Cyber Resiliency

Describes an increase in functionality

1. Ensure backups are always recoverable
2. Protect all data with global governance
3. Detect and investigate threats quickly
4. Prepare, practice and recover from incidents quickly
5. Prevent data theft by continuously mitigating data risks

Destructive Cyberattack Maturity Model

Measures the prospect/customer's operational capability that those features enable

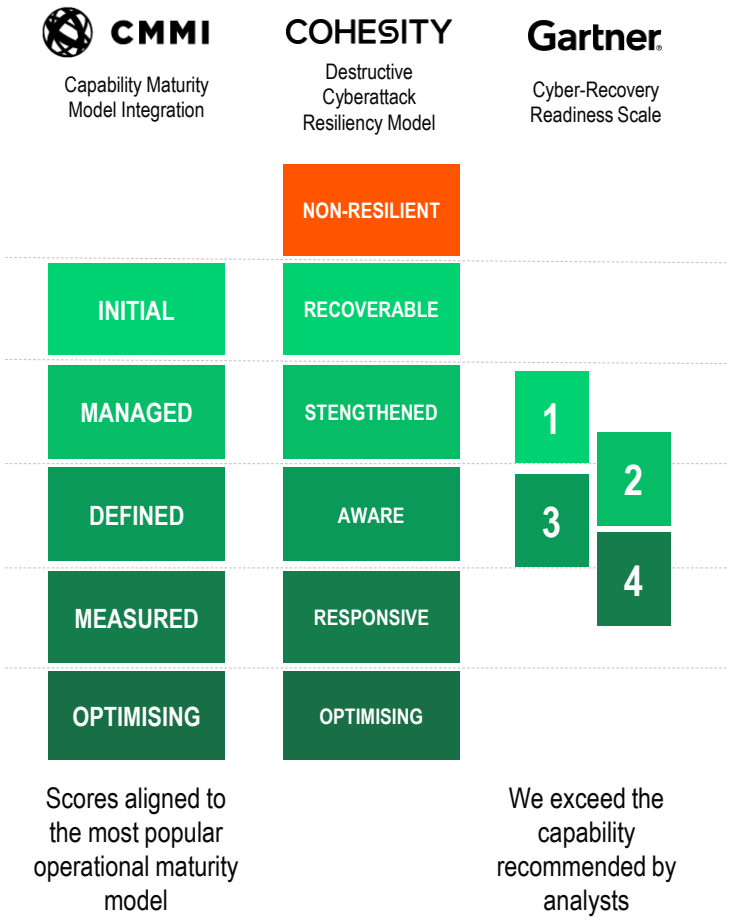
0	Non-Resilient
1	Recoverable
2	Strengthened
3	Aware
4	Responsive
5	Optimising

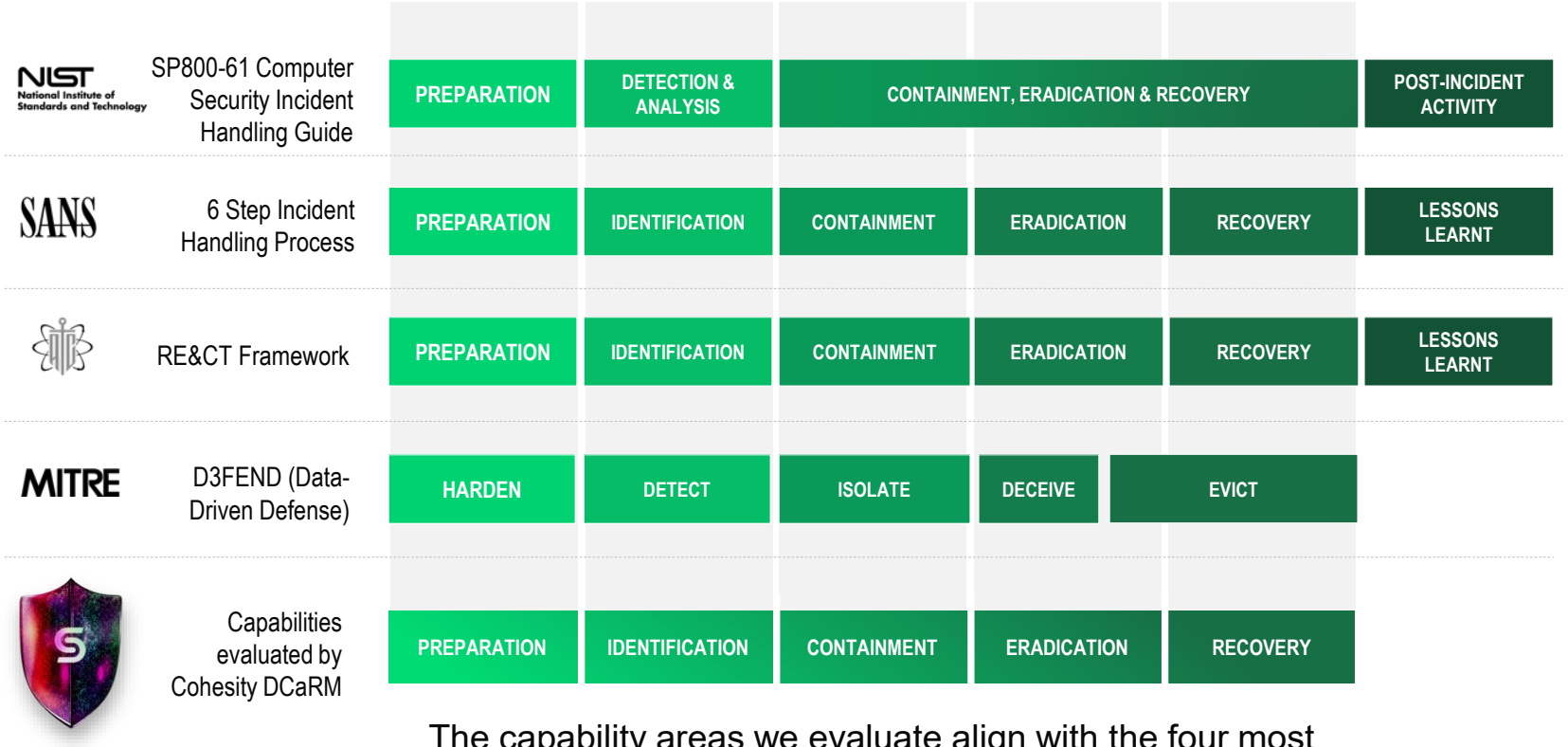
The 5 Steps achieve well-established cyber response best practices

The 5 Steps align with the most popular capability maturity scale

Cohesity model is defensible and validated by third parties

Why sell the value of a model when other people are doing it for you?





The capability areas we evaluate align with the four most popular cyber incident response and recovery frameworks

Five Steps to Cyber Resiliency - The Checklist

Protect All Data with Global Governance	Ensure Data is Always Recoverable	Detect and Investigate Threats	Practice Application Resilience	Optimize Data Risk Posture
❑ Physical Servers ❑ VM's & Containers ❑ Databases & Unstructured Data ❑ NAS ❑ Public Cloud - IaaS ❑ Public Cloud - PaaS ❑ Public Cloud - SaaS ❑ Active Directory / Entra ID ❑ <u>Governance:</u> consistent policies; Discovery of new workloads; Assurance of daily backups; Single tool everywhere	❑ Immutability / Encryption ❑ Multi-Factor Authentication ❑ Quorum ❑ Separation of Duties (Role Based Access Control) ❑ 3-2-1-1+ ❑ DataLock ❑ Leverage Vaults for Crown Jewels like the Digital Jump Bag and Minimum Viable Response Capability ❑ Active Directory backup on SmartFiles (immutability)	❑ Threat scanning & hunting with native & bring-your-own feeds ❑ Ability to detect Identity misconfigurations ❑ AI-Powered Anomaly Detection ❑ Hash based scanning and hunting ❑ SIEM/SOAR integration	❑ Digital Jump Bag ❑ Recovery Orchestration ❑ Automated Active Directory Recovery ❑ Clean Room ❑ Ability to Test Recovery at Scale ❑ Ability to practice/simulate Cyber Attack Response and Recovery	❑ PII data identified via external classifiers (DSPM integration) ❑ PII data alternatively identified via internal Data Classification ❑ PII data Assessed for protection & recovery capability ❑ Ability to determine if PII data is in an attack blast radius

THANK YOU

COHESITY