

COHESITY

Gain greater resilience
with a modern data
operating model



Traditional ways of managing and securing data aren't necessarily built for the cloud era. Data is often stored across multiple clouds, on-premises, and at the edge. Both data volumes and cyber security threats continue to explode exponentially – not to mention the ever-expanding tool stack to manage it all.

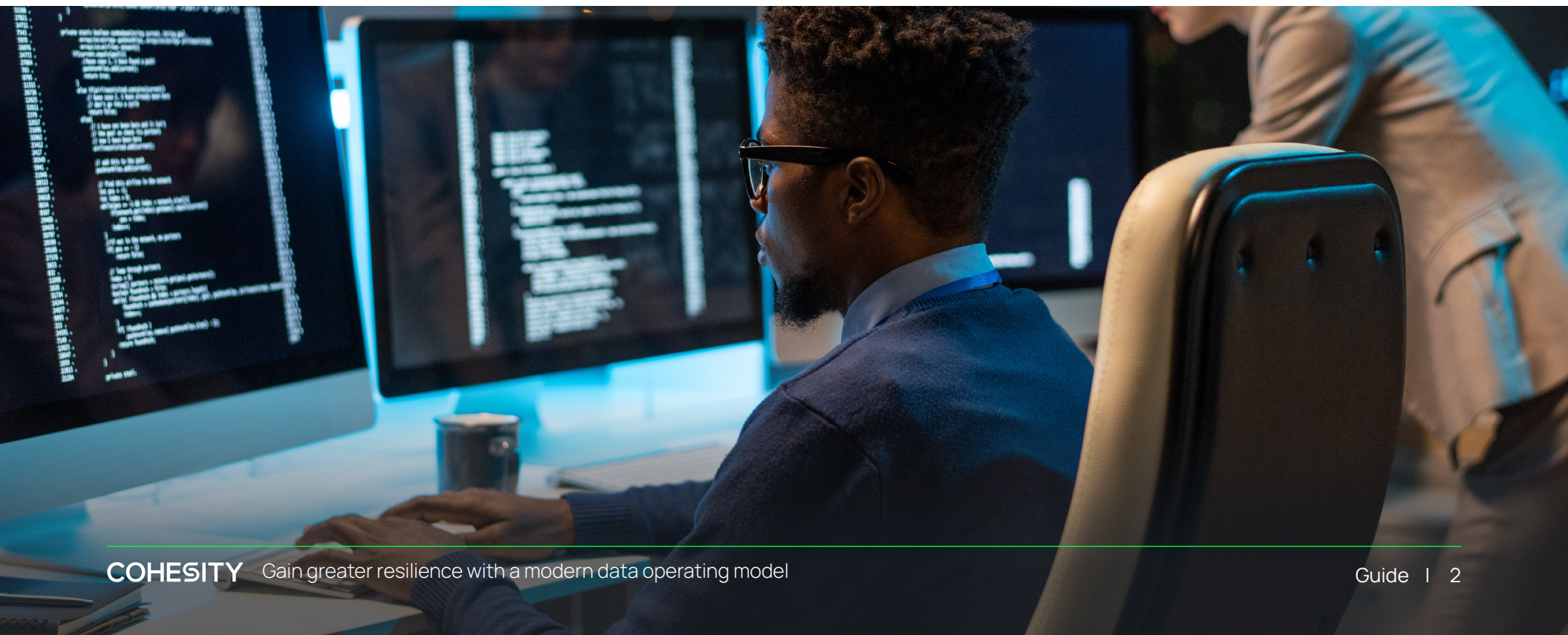
All this change has compounded over time. A new reality is setting in: the processes, products, and single-purpose tools of the past decade just can't keep up with today's priorities.

In the following pages, we'll discuss these challenges in more depth, the three levels of resilience that all organizations should pursue – and the most important step you can take to tackle and tame your data estate.

67%

of IT and Security Operations leaders lacked confidence that their company could recover data and critical business processes in the event of a system-wide cyber attack.¹

¹ All data points, unless otherwise noted, are from Cohesity's *The State of Data Security and Management Report 2023*.



Examine your status quo to understand the path forward

Technology modernization efforts must include rethinking how your people work, the processes they follow, and the tools they use. In the past, the impacts of these challenges were seen as IT's problem and not inherently affecting operations. Today, however, data management and security are increasingly recognized as mission-critical functions for keeping organizations operational and thriving.

Common data management and security challenges include:



Difficulty ensuring consistent security measures and efficient backup/recovery processes across a dynamic IT estate.



The inability to scale and adapt to keep up with growing data volumes, types, and sources, as well as new innovations like AI and remote access.



Outdated security measures that leave organizations susceptible to vulnerabilities and exploits.



Tool sprawl and unintegrated security controls that cause gaps in coverage.



Cultural/people issues like process bottlenecks, skill shortages, and a lack of collaboration between IT and cyber.

130+

The average enterprise cyber security team works with more than 130 different security tools – all operating with siloed data views.



A new way forward

Given the complexity of these challenges, many IT leaders have turned to a **data operating model** to guide modernization efforts. This framework outlines how an organization manages, secures, shares, and uses data to achieve its overarching goal: resilience in the face of the unexpected and the unknown.


There are three types of resilience that organizations must build and foster: data, cyber, and business. Each level of resilience results from an increasing mastery of the five layers of a modern data operating model. Let's look at each.

Baseline maturity: Data resilience	
Goal	The ability to maintain the availability, integrity, and accessibility of data in the face of unexpected events, disruptions, or failures.
Method	Data protection The implementation of robust data backup, redundancy, and recovery strategies.

Intermediate maturity: Cyber resilience	
Goal	The ability to prepare for, investigate, respond to, recover from, and generally withstand cyber attacks.
Method	Data security The integration of data resiliency systems with cyber resiliency capabilities to protect against complex attacks and improving metrics like Mean Time to Detect, Mean Time to Respond, and Mean Time to Contain.

Cohesity + Google Cloud: Key Benefits

- ✓ **Manage** data on Google Cloud and hybrid cloud efficiently.
- ✓ **Consolidate** backups for VMs, NAS, databases, and more on a single platform.
- ✓ **Backup** and protect Google Cloud and Google Cloud VMware Engine.
- ✓ **Runs** on and natively integrates with Google Cloud.
- ✓ **Eliminate** tape and reduce long-term retention and storage costs.

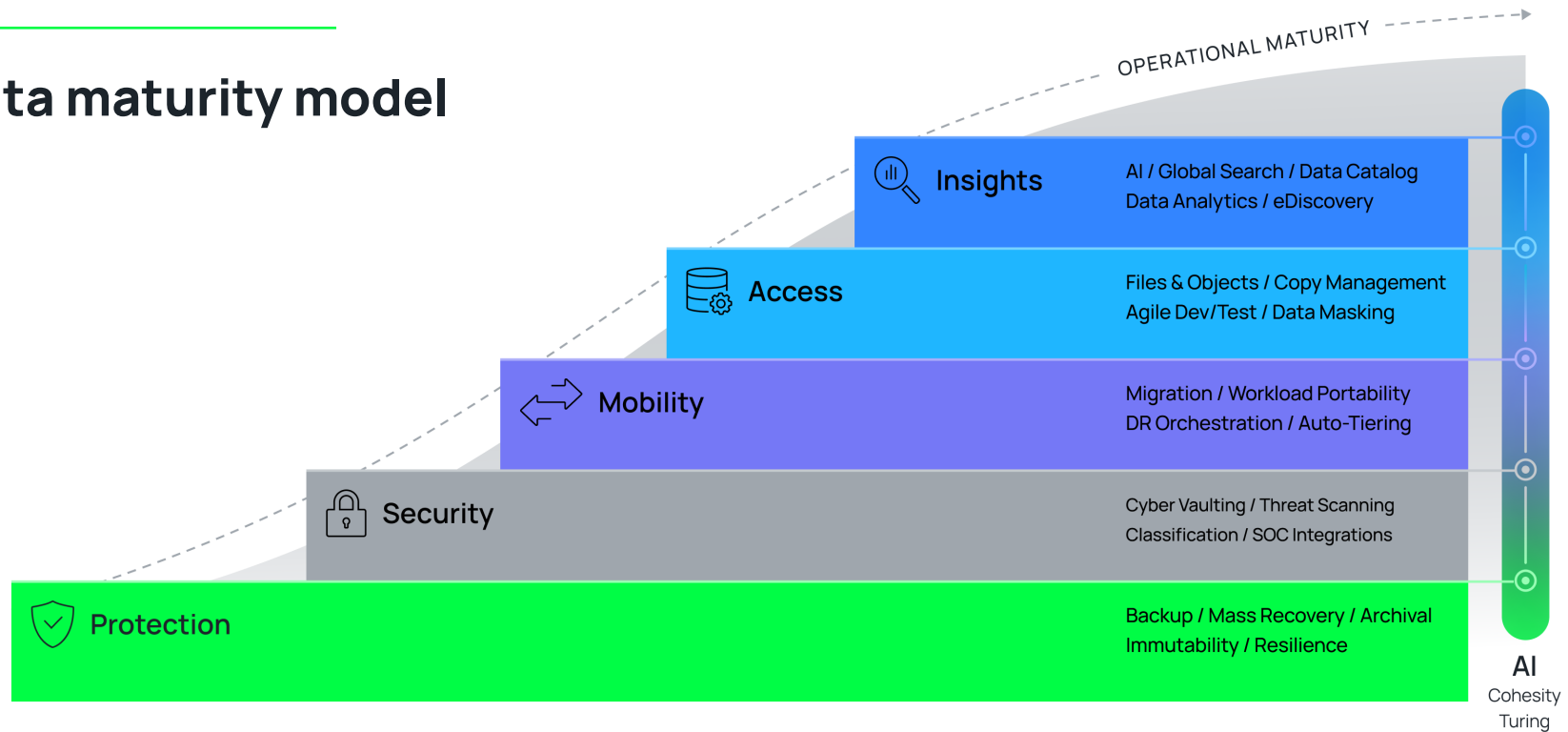
Advanced: Business resilience 	
Goal	The ability to respond and adapt quickly to any disruption or significant change that threatens the business, as well as to drive business value from data and resilience efforts.
Method	<p>Data mobility The ability to move data seamlessly across locations, such as multiplex clouds, data centers, and applications, without compromising consistency, security, and integrity.</p> <p>Data access The governance of data access so that authorized users and applications can retrieve and interact with data without security or compliance compromises.</p> <p>Data insights The ability to gain value from backup and secondary data via innovative AI capabilities and analytics.</p>

80%

of IT and SecOps leaders expressed concern about their organization's cyber resiliency strategy in the face of today's challenges and threats.



Data maturity model



Adopting a data operating model is a useful method for reducing risk and optimizing business outcomes.

90%

of IT and SecOps leaders agreed their organization would benefit from a data security and management platform that provides insights on their overall security posture and cyber resilience.

The 6 elements of a modern data platform

Taken in isolation, each of these layers (along with their related challenges) can seem overwhelming. Thankfully, there is a sweeping approach that IT leaders can take to ease the path to advanced data management and security maturity.

To guide modernization efforts, deliver across-the-board resiliency, and ease operational burdens for IT, organizations are migrating from incumbent data management systems to a **modern data platform**.

What makes a modern data platform? Six architectural elements leap to mind:

1. Scalability



4. AI readiness



2. Simplicity



5. Extensibility



3. Security



6. Performance and cost



1. Scalability



- Handles petabyte scales of data.
- Scales horizontally and vertically to manage increasing volumes of data and users.
- Supports a wide range of data sources, including structured and unstructured data.

2. Simplicity



- Easy to use with common UX patterns and best practices.
- Doesn't require specialized training or expertise for basic use.
- Online training is sufficient to instruct users on basic, intermediate, and advanced use.

3. Security



- Protects data under management as well as identifies data that needs protecting, and supports attack detection and cyber incident response through platform capabilities and integration with other security tools.
- Offers role-based access controls.
- Encrypts data at rest and in transit.
- Applies Zero Trust principles.

4. AI readiness



- Breaks down data silos to enable organizations to extract insights and value from their secondary and backup data.
- Supports SQL-based analytics, machine learning, and natural language processing (NLP).
- Prioritizes AI innovation and partnerships for a future-ready product roadmap.

5. Extensibility



- Built to be API-first.
- Supports straightforward integration with other systems, including native integration with cloud hyperscalers, to ease data ingestion, processing, and analyzation.
- Reduces manual data-related tasks to increase efficiency.

6. Performance and cost



- Automatically moves data between storage tiers based on patterns and importance.
- Optimizes performance and cost by placing frequently accessed data on faster storage and less-used data on more economical options.

The first step to data modernization

Once you have a unified, cloud-first data management and security platform in place, you are well-positioned to begin your modernization journey in earnest.

For a deeper look at the modern data operating model, read our [*Executive's guide to modern data security and management*](#).

To learn more about the joint Cohesity and Google Cloud solution, visit <https://www.cohesity.com/solutions/cloud/google/>.