

# Protection Storage Architecture: The What, Why, and How

## GOT PROTECTION STORAGE ARCHITECTURE?

A Protection Storage Architecture has the following three core components. Be wary of impostors.

- **Protection Storage:** The anchor of the architecture is highly durable, capacity-optimized storage that can support a continuum of data protection services, including backup and recovery, archive, disaster recovery, and data availability.
- **Data Source Integration:** Leverages both the optimized data flows and user interfaces of data sources, including hypervisor, application and storage, to deliver the performance and visibility internal customers want.
- **Data Management Services:** A catalog of services (e.g., policy and storage management, monitoring, analytics, discovery, etc.) the data protection team offers to improve business efficiency, productivity, and agility.

Over the next few years, IT will be faced with a new set of data protection challenges, centered on delivering multiple data protection services, including backup and recovery, archive, disaster recovery and data availability, across the organization. Traditional backup architectures lack the flexibility, agility, and scale to meet these requirements. That's where a Protection Storage Architecture comes in. This transformational architecture not only enables backup teams to solve immediate tactical challenges but also helps IT teams keep business applications running and, importantly, evolve to support strategic services-oriented business models. Isn't it time your organization redefined data protection?

## GOOD-BYE ACCIDENTAL ARCHITECTURES, HELLO INTEGRATED DATA PROTECTION

If your backup team is unable to solve critical protection performance challenges from your application, virtualization, and storage teams and have deployed silos of point products on their own to address these issues, you have an accidental architecture. It's accidental because no organization would intentionally plan for a half-dozen unconnected data protection tools with no central oversight or cost control.

The good news is you can gain control of your environment by integrating data protection with a Protection Storage Architecture.

## PROTECTION STORAGE ARCHITECTURE TO THE RESCUE

From a technology standpoint, a Protection Storage Architecture is comprised of three components: Protection Storage, Data Source Integration, and Data Management Services. Together, these modules provide a platform that can evolve with business and technical requirements, including cloud and Big Data, while minimizing lock-in.

### PROTECTION STORAGE ARCHITECTURE



HANDOUT

EMC<sup>2</sup>

# WHAT MAKES GOOD PROTECTION STORAGE GOOD?

A well-designed Protection Storage platform differs from other types of storage in important ways:

- **Durability.** Since protection spans backup and recovery, availability, disaster recovery, and archive, organizations need storage that ensures data will be there for years or decades to come.
- **Multi-use.** Your organization can't afford the CAPEX and OPEX costs of purchasing and maintaining separate silos. Scale easily, reduce CAPEX and OPEX costs and meet business objectives by unifying backup and recovery, availability, and disaster recovery, and archival on a single platform.
- **Capacity and cost-optimized.** Price matters. The first step toward cost optimization is capacity optimization—reducing the number of copies, the overhead of storing multiple copies, and the footprint of each copy. The second step is developing software to leverage lower-cost hardware components. This includes scaling performance with CPU and capacity with low-cost, large-capacity storage—while not compromising data durability and capacity optimization.

## PROTECTION STORAGE

This is the anchor of the architecture: storage built for protection. It is highly durable, capacity-optimized storage (see sidebar) that can be pooled, or consolidated, to support a continuum of data protection services (e.g., disaster recovery, backup, data availability and archive). To avoid creating silos of protection storage, the storage platform must support multiple protocols (e.g., VTL, NAS, OST, and deduplication) and integrate with multiple data sources (e.g., applications, hypervisors, storage, and backup applications).

## DATA SOURCE INTEGRATION

Customers want three things from their data protection team: performance, availability, and visibility. Done right, data source integration enables the highest level of all three by optimizing data flows between and views of virtual and physical, application, and storage environments. A Protection Storage Architecture leverages both the optimized data flows and user interfaces of the data sources (hypervisor, application, and storage), tracking data as it changes (e.g., VMware Changed Block Tracking, array snapshots, etc.), not after the fact like traditional backup agents do. The user interface (e.g., VMware, vSphere®, Oracle RMAN, EMC Unisphere™) displays protection status in that team's preferred native interface.

## DATA MANAGEMENT SERVICES

This is the *value* component of the architecture. It is a catalogue of services the data protection team offers to improve business efficiency, productivity, and agility. What types of services should be included? Senior management wants to ensure data protection meets SLAs and compliance regulations as cost-effectively as possible; they need analytics and reports for compliance, policy and infrastructure utilization; and customers want to be able to retrieve information quickly and easily.

## SAY "YES" TO THE ARCHITECTURE

Transformation will happen with or without [you](#). If you want your organization to "survive and thrive," data protection transformation is essential. Not only does a Protection Storage Architecture enable a clean, centralized protection service that will help accelerate business initiatives, but by taking on responsibilities that everybody deems necessary—but nobody wants to do—the data protection team will also elevate its status within the organization from one of cost center to business enabler.

### A NEW APPROACH: PROTECTION STORAGE ARCHITECTURE

EMC's innovative, reliable and powerful Protection Storage Architecture solves the challenges of backup and archive and lets your protection team make a real difference to your business. Three key components make it happen:

 <h1>489%</h1> <p>RETURN ON INVESTMENT OVER THREE YEARS</p> <p><b>The Right Protection Storage</b> Optimize scalability and performance. EMC is #1 in performance and scalability. Get 6-month payback consolidating backup and archive.</p>	 <h1>ZERO</h1> <p>SILOS</p> <p><b>Integration with Data Sources</b> Eliminate silos by integrating seamlessly with Oracle, SAP, Microsoft, VMware, Hyper-V, EMC Symmetrix VMAX, VNX, Isilon, and more.</p>	 <h1>81%</h1> <p>LESS BACKUP MANAGEMENT TIME</p> <p><b>Data Management Services</b> Ensure compliance, analyze data, add value—and quit fighting fires.</p>
---	--	--

## FOR MORE INFO

To learn more about the Protection Storage Architecture, EMC Data Protection solutions, and how to transform your business, visit [www.emc.com/protectionleader](http://www.emc.com/protectionleader) and check out Stephen Manley's six-part blog series: [The Right Architecture Is Priceless](#).

## FROM BLUEPRINT TO REALITY

A Protection Storage Architecture can guide the transformation of data protection to a clean, centralized service. However, each organization's blueprint will be unique to its business. Here are some guidelines to get started:

- **Step 1:** Find and implement the right Protection Storage for your environment. This is the single, fastest way to create worry-free protection without making changes to existing software or policies and without hiring new staff.
- **Step 2:** Start working with high-end application, virtualization, and NAS users. Understand their challenges, processes, and goals, and talk to them about how Data Source Integration will benefit them and your business.
- **Step 3:** Have some fun. Start adding Data Management Services and share them across your environment.

## PROTECTION STORAGE ARCHITECTURE AND EMC DATA PROTECTION SOLUTIONS

EMC offers a portfolio of market-leading software and hardware solutions to help you build out a Protection Storage Architecture:

- **EMC Data Domain® Deduplication Storage Systems** provide a scalable Protection Storage platform for consolidating backup and archive, data availability and disaster recovery. These systems feature EMC's market-leading deduplication and are integrated with EMC Data Protection™ Suite offerings.
- [EMC Data Protection Suite](#) is a key component of a Protection Storage Architecture. The suite includes EMC Avamar®, EMC NetWorker®, EMC Data Protection Advisor™, Mozy® and EMC SourceOne®.
- EMC RecoverPoint provides continuous data protection to restore applications instantly to any point in time, and EMC VPLEX provides data mobility and continuous availability across data centers.

### INNOVATIVE NEW SOLUTIONS

EMC delivers the capabilities you need for your Protection Storage Architecture:



Explore, compare, and get pricing for the latest Data Domain, Avamar, NetWorker, and Data Protection Advisor products in the EMC Store.



**EMC Data Domain Systems**  
Consolidate backup and archive storage requirements with the next generation of protection storage appliances. Part of the EMC Data Protection Suite, Data Domain systems are 4x faster—and 10x more scalable—than alternative



**EMC Avamar 7**  
Get instant VM access and deeper VMware integration. All with Avamar 7, part of the EMC Data Protection Suite.



**EMC NetWorker 8.1**  
Provide simplified, scalable data management services with NetWorker 8.1—part of the EMC Data Protection Suite.

EMC<sup>2</sup>, EMC, and the EMC logo, are registered trademarks or trademarks of EMC Corporation in the United States and other countries. VMware is the registered trademarks or trademarks of VMware, Inc., in the United States and other jurisdictions. All other trademarks used herein are the property of their respective owners. © Copyright 2014 EMC Corporation. All rights reserved. Published in the USA. 02/14 Handout **H12360.1**.

[www.EMC.com](http://www.EMC.com)

EMC believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

**EMC<sup>2</sup>**