Hitachi Vantara

eBook

Protect Smarter, Recover Faster:

Your Guide to Data Protection as a Service (DPaaS)

Introduction

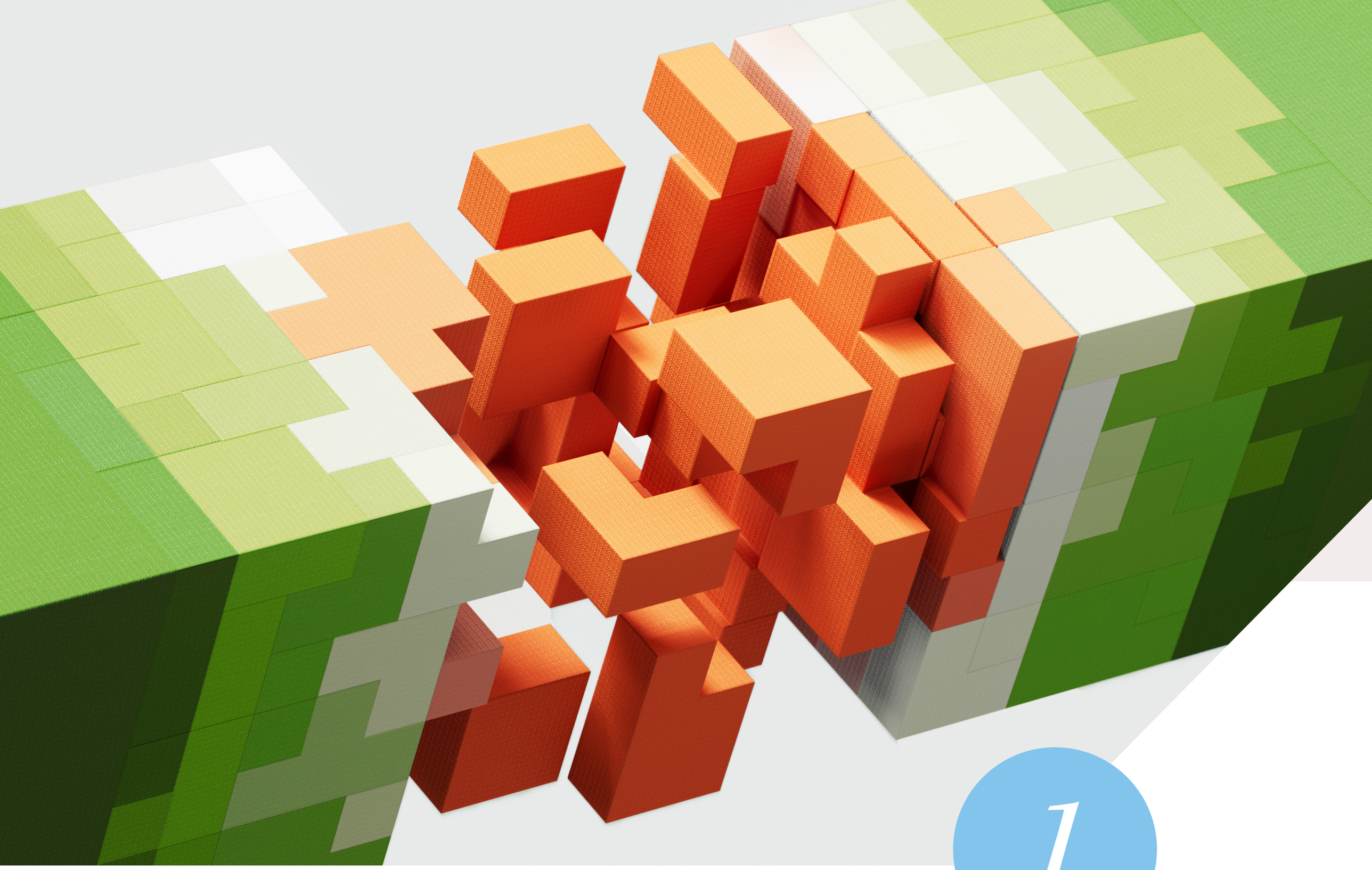
Why It's Time to Rethink Data Protection

Hybrid cloud has transformed how we deliver infrastructure. But data protection? It's lagging behind.

While systems get faster and more flexible, recovery remains slow, risky, and fragmented. That gap isn't just inconvenient—it's dangerous. It threatens resilience, compliance, and business continuity.

Here's what's changed:

- Ransomware attacks are more frequent and destructive.
- Compliance requirements are tougher and less forgiving.
- Backup windows are shrinking as data volumes explode.
- Infrastructure is distributed across cloud, on-prem, and edge.
- Skilled staff are stretched thin, with limited bandwidth to manage growing risk and complexity.

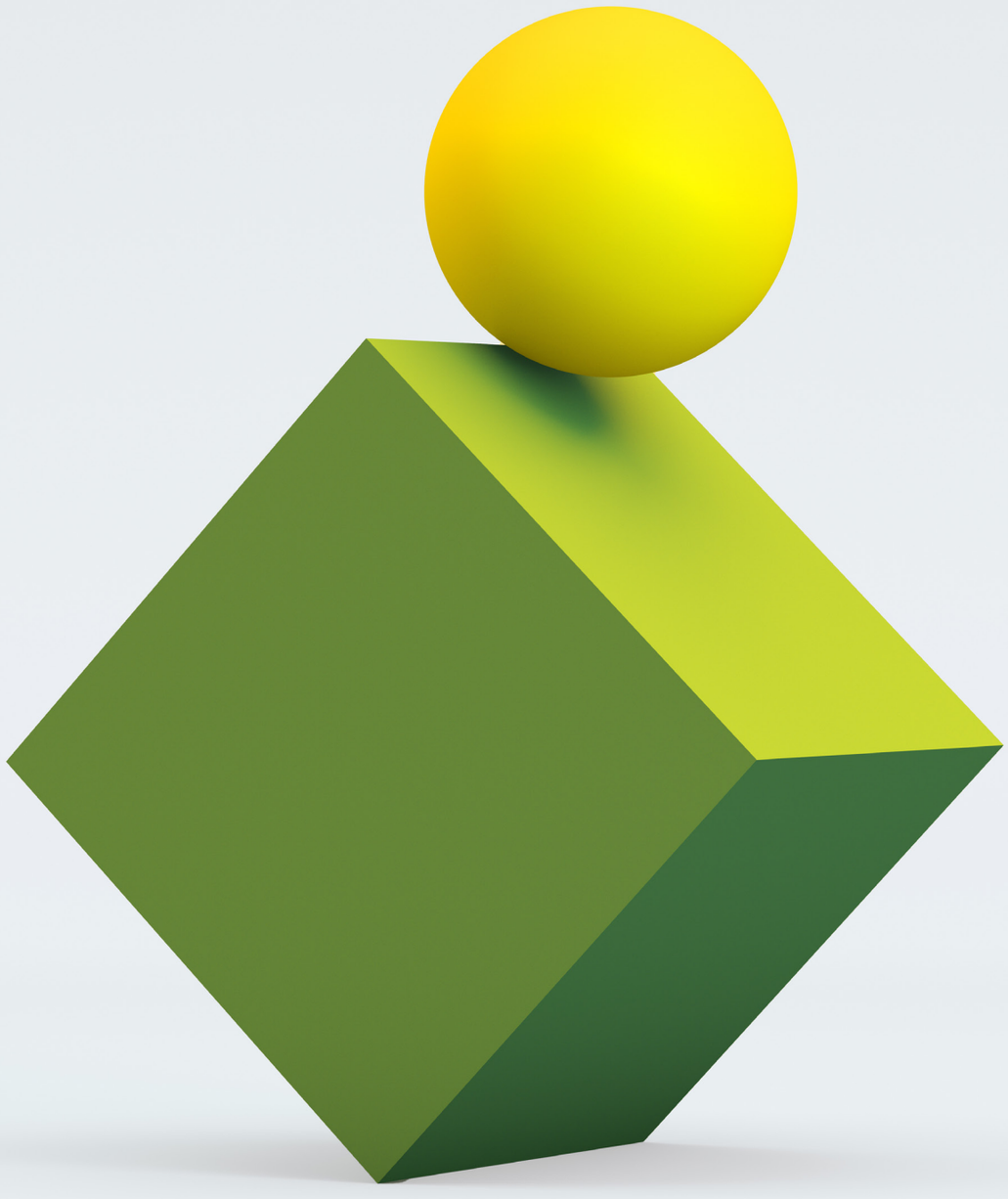


1

Data protection isn’t optional anymore. But traditional backup tools weren’t built for today’s demands. Many teams are stuck with outdated systems that create more stress than security. That’s why organizations are shifting to “as-a-service” models that reduce operational burden and deliver outcomes. Just like Infrastructure-as-a-Service (IaaS) revolutionized hybrid cloud infrastructure, Data Protection as a Service (DPaaS) is transforming how we protect data in hybrid cloud environments.

DPaaS combines backup, recovery, and resilience into one scalable, outcome-driven solution, allowing organizations to protect their critical data across hybrid environments without overloading internal teams or compromising control. It brings together automation, compliance support, and trusted recovery under a single, outcome-based model.

If your current data protection approach is falling behind and you’re ready to advance, this eBook serves as a roadmap forward.



2

The Cost of Standing Still

Every day organizations delay modernizing protection, risk compounds.

Here's what teams are dealing with:

- **Fragmented tools and disconnected processes.** Teams often manage separate backup systems for cloud, on-prem, and edge environments with no centralized visibility.

- **Shrinking backup windows.** Data volumes are growing faster than most infrastructure can accommodate. Traditional tools can't meet shrinking Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).

- **Operational and staffing pressures.** Many teams are spread thin, with limited resources and growing skill gaps around modern data protection practices.

- **Compliance demands.** Regulations like HIPAA (Health Insurance Portability and Accountability Act), GDPR (General Data Protection Regulation), and DORA (Digital Operational Resilience Act) require more than just storing data—they demand demonstrable integrity, immutability, and audit readiness.

At the same time, the shift to "as-a-service" models creates new fears:

- What if we lose visibility?
- How do we ensure control and compliance?
- Can we trust a third party with our recovery requirements?

These challenges require evaluation of alternative service delivery models that maintain control while reducing complexity.

3

What Is DPaaS, and

Why It Matters

Data Protection as a Service provides outcome-based backup, recovery, and resilience management across hybrid IT environments. Rather than purchasing and managing protection infrastructure, organizations subscribe to guaranteed protection outcomes delivered through managed or co-managed service models.

As more organizations adopt hybrid cloud strategies, there's a clear shift toward managed services for backup and disaster recovery. Disaster Recovery as a Service (DRaaS), for example, is gaining traction as ransomware and operational complexity grow. DPaaS is part of this broader trend—bringing together backup, disaster recovery, and compliance-readiness into a single, automated model.

A modern DPaaS solution:

- Works across on-prem, hybrid, and multi-cloud architectures.
- Provides immutable, air-gapped backups to defend against ransomware and insider threats.
- Delivers SLA-based recovery time and integrity guarantees.
- Offers centralized management and reporting.
- Integrates with compliance workflows and provides audit-ready logs.
- Uses pay-as-you-go pricing to align cost with consumption.

Crucially, DPaaS aligns with Zero Trust principles by enforcing strict access controls, ensuring backup immutability, and monitoring usage patterns across environments. In a Zero Trust world, data protection isn't just a safety net, it's part of the architecture.

DPaaS also shifts the burden from internal teams to a trusted partner, letting your staff focus on innovation and transformation while knowing your data is protected.

What Does "Zero Trust" Really Mean?

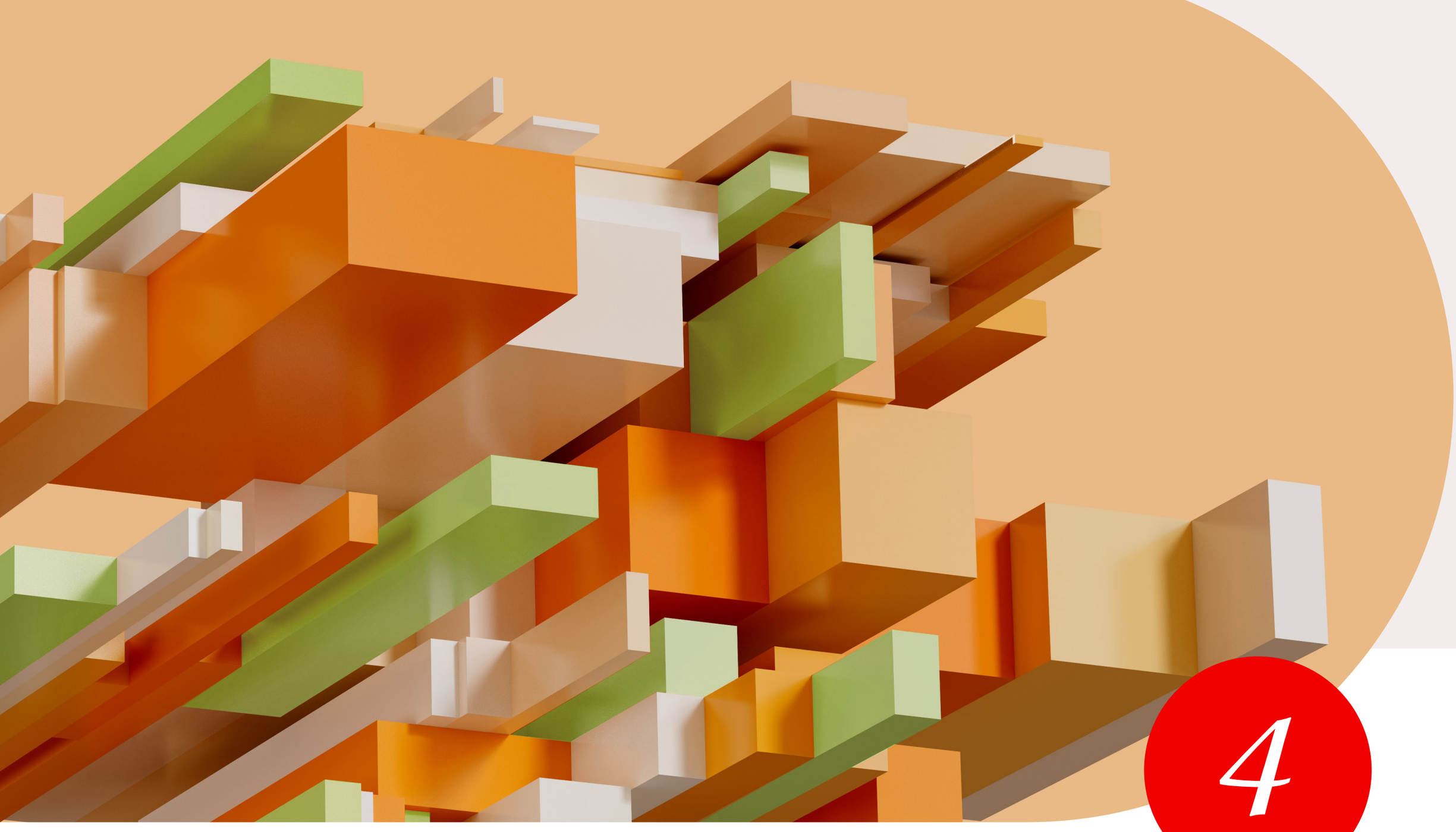
Zero Trust is a modern security approach built on one core principle: *Never trust, always verify.*

That means no user, device, or system is trusted by default—even inside your network. Every access request must be authenticated, authorized, and continuously validated.

How DPaaS supports Zero Trust:

- Limits who can access backup systems and data
- Maintains immutable, tamper-proof backups
- Enables full audit trails and compliance reporting

By aligning with Zero Trust principles, DPaaS helps ensure your data is protected—not just from outsiders, but from insider threats and accidental misuse too.



4

Why Buyers

Are Making the Shift

Despite spending on backup tools, most organizations still struggle with recovery, largely due to limited testing and orchestration. DPaaS flips this script—emphasizing automation, tested runbooks, and fast, SLA-backed recovery across environments.

Organizations adopt DPaaS to address operational challenges while enabling strategic business objectives.

Key benefits include:

- **Freeing up internal teams:** Offload manual, repetitive tasks like patching, reporting, backup testing, and troubleshooting.
- **Filling critical skills gaps:** Access specialized expertise without hiring or retraining—especially valuable as technologies evolve faster than talent pipelines.
- **Reducing risk:** Ensure consistent protection and rapid recovery through immutable backups and verified SLAs.
- **Architectural alignment:** Integrate protection services with Zero Trust security frameworks and governance policies.
- **Scalability management:** Extend protection to new workloads, locations, or cloud platforms without re-architecting your strategy.
- **Improving cost predictability:** Shift from CapEx-heavy tools to predictable OPEX pricing aligned with usage and business growth.

IT organizations can focus on revenue-generating initiatives while maintaining superior protection posture.

How Different Industries

Are Using DPaaS Today

From finance to healthcare, organizations are adopting DPaaS to solve pain points unique to their sectors:

- **Finance:** Automate audit-readiness and secure high-value transactional systems
- **Healthcare:** Protect clinical data with immutable backups and SLA-backed recovery
- **Public sector:** Offset staffing shortages while meeting compliance demands
- **Manufacturing:** Protect critical production and customer data
- **Technology:** Streamline dev/test data across hybrid clouds

The Business Case for DPaaS

	Legacy Backup Tools	DPaaS Model	Benefit
CapEx vs. OpEx	• High upfront costs for hardware/ software	• Subscription-based, pay-as-you-go	• Improved budget flexibility
Staffing Costs	• Requires dedicated team for maintenance, patching, testing	• Offloads routine tasks to provider	• Frees up internal resources
Downtime Risk	• Higher risk due to manual processes and fragmented systems	• SLA-backed recovery guarantees	• Reduced business disruption
Compliance Overhead	• Manual audits, limited visibility	• Automated logging, audit-ready reports	• Lower risk of fines and penalties
Scalability	• Requires re-architecture for new workloads	• Elastic scaling across environments	• Faster time-to-value

Watch Video →

How DPaaS Provides a Complete Solution for Your Multicloud Environment

5

Overcoming Barriers

And Choosing the Right Partner

Even when the benefits are clear, it's natural to hesitate. Even organizations that know their legacy approach is failing often hesitate to make the leap.

Here are some common concerns and how to reframe them:

"We'll lose visibility or control."
A modern DPaaS provider doesn't put up walls. Instead, the best solutions offer full transparency through dashboards, audit-ready reporting, and granular controls that allow your team to monitor protection status, performance, and compliance outcomes at any time.

"I'm not sure I can trust an outside vendor with our SLAs."
That skepticism is valid, especially for organizations bound by strict RTOs, RPOs, or regulatory timelines. That's why outcome-based SLAs matter. Instead of vague uptime guarantees, look for agreements tied directly to recovery times, data integrity, and compliance needs. Bonus: Many providers automate recovery runbooks and DR testing to build confidence over time.

"Will this replace our internal team?"
Not at all. The goal of DPaaS is to offload repetitive, resource-intensive tasks—like monitoring, patching, compliance tracking, and recovery validation—so your team can focus on higher-value modernization efforts. In today's market, where skilled personnel are hard to hire and harder to keep, many organizations see DPaaS as a way to amplify their team, not replace it.

"What about vendor lock-in?"
This is a valid concern, especially with cloud egress costs on the rise. In fact, 70 to 80 percent of companies are repatriating at least some of their data back from the public cloud. That's why flexibility matters. Choose a provider that supports, integrates with your existing systems, and offers modular service tiers that scale without locking you in.

Three Questions

to Ask Your Team Before Evaluating a DPaaS Partner

- Which systems or data would cause the most business impact if they went down today?
- How confident are we in our current recovery time and when was it last tested?
- Do we have the internal bandwidth and skills to maintain protection across all environments?

These aren't just technical questions—they're strategic ones. Asking them now can help clarify your priorities before engaging providers. You don't need to make the shift all at once. Many organizations begin with a specific workload or compliance requirement, then expand once the value is proven. But success starts with a partner who understands your environment and your goals.

What to Look for

in a Trusted DPaaS Provider

- **Transparent, enforceable SLAs** that go beyond basic uptime to cover backup success rates, configuration compliance, and defined RTOs and RPOs for different workload tiers.

- **Strong recovery commitments.** For example, the ability to restore mission-critical workloads within an hour and recover data from points just minutes before an incident.

- **Consistently high backup success rates** with automated verification that policies are applied correctly, reducing the risk of silent backup failures.

- **Comprehensive coverage across hybrid and multi-cloud environments,** ensuring seamless protection and recovery whether workloads run on-premises, in public cloud, or in distributed edge locations.

- **Centralized visibility and self-service options,** with dashboards to monitor backup status, recovery readiness, and SLA performance.

- **Integration with compliance, audit, and reporting needs,** including immutable backups, policy compliance checks, and auditable logs for every backup and recovery event. Automated SLA and recovery reports should make it easy to demonstrate readiness to regulators and auditors.

- **Tiered services to match maturity and budget** from ultra-fast recovery for mission-critical systems to cost-optimized protection for less sensitive data.

- **Proven track record in similar industries or use cases.**

DPaaS isn’t just a tool. It’s a strategic partnership. And the right partner should be able to deliver trust and flexibility, but also stand behind their promises with measurable, verifiable outcomes.

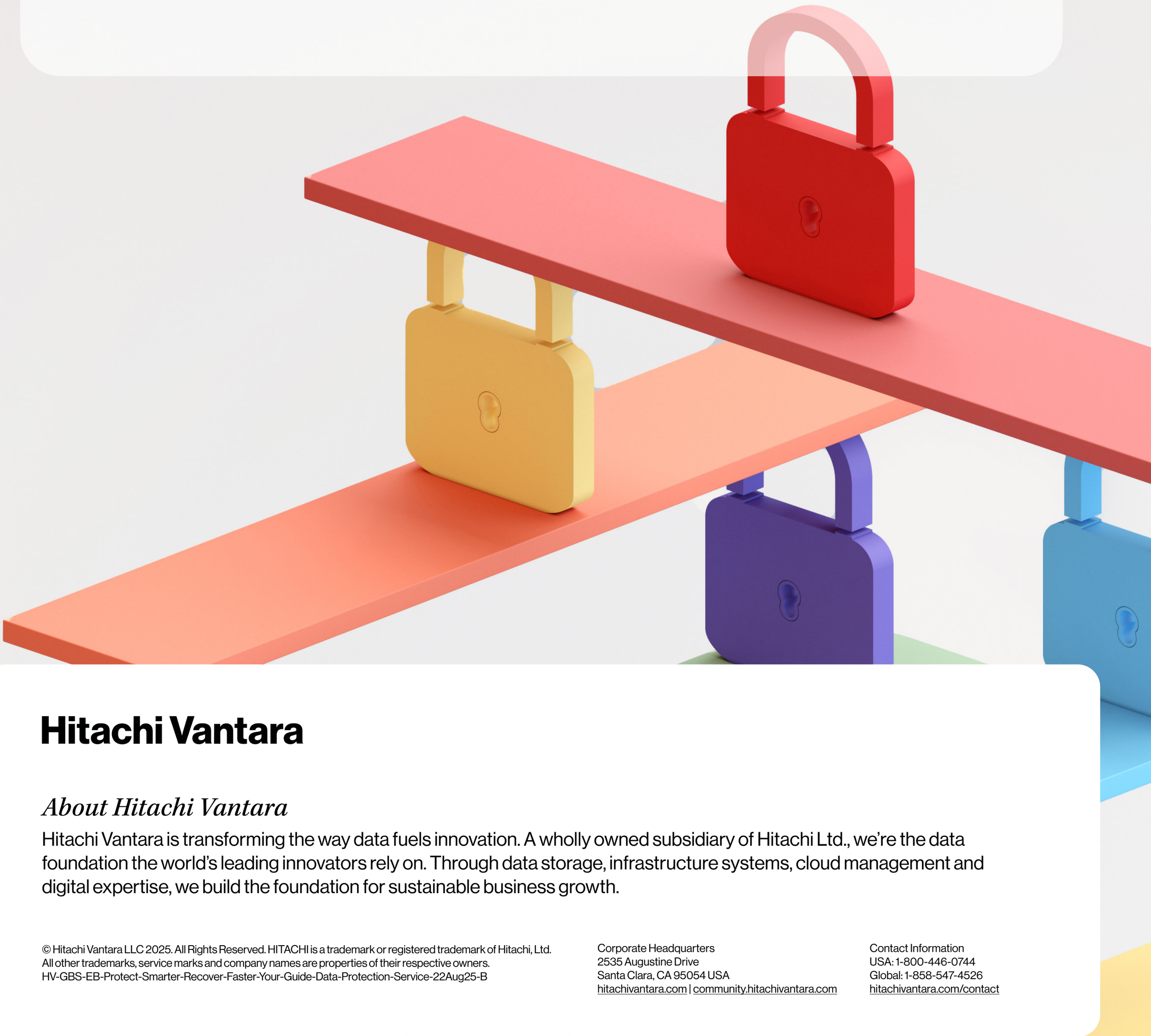
You Don’t Have to *Do This Alone*

If your data protection strategy feels like it’s stuck in the past, you’re not alone. Many IT leaders are finding that legacy tools no longer keep up with today’s threats and data complexity.

DPaaS offers a smarter path forward. You don’t need more tools. You need better outcomes. You don’t have to rip and replace. You can evolve with confidence. And you don’t have to do it all in-house. The right partner is ready to help.

Ready to take the next step toward simplified, resilient data protection? Hitachi EverFlex DPaaS delivers scalable, secure protection with cloud agility and fully transparent SLAs tied to your business outcomes. Discover how you can strengthen cyber resilience while reducing cost and complexity.

Resilience Simplified →



Hitachi Vantara

About Hitachi Vantara

Hitachi Vantara is transforming the way data fuels innovation. A wholly owned subsidiary of Hitachi Ltd., we’re the data foundation the world’s leading innovators rely on. Through data storage, infrastructure systems, cloud management and digital expertise, we build the foundation for sustainable business growth.

HV-GBS-EB-Protect-Smarter-Recover-Faster-Your-Guide-Data-Protection-Service-22Aug25-B

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA
hitachivantara.com | community.hitachivantara.com

Contact Information
USA: 1-800-446-0744
Global: 1-858-547-4526
hitachivantara.com/contact