

SOLUTION BRIEF

Simplified and Automated Cyber Recovery with Pure Protect

Right-size your cyber recovery

Don't put your business at risk. Traditional cyber recovery tools are complicated, expensive, and can disrupt the core of your business. And they definitely weren't designed for modern threats like ransomware. The traditional approach involves multiple vendors, complex integration projects, and months of deployment time just to achieve basic functionality. Many organizations manage a patchwork of solutions that creates more problems than it solves—backup systems that don't integrate with recovery orchestration, disaster recovery sites that require manual intervention, and testing procedures so complex they're rarely executed properly.

Cyber recovery shouldn't require a dedicated team of specialists or consume enormous portions of your IT budget to be effective. Companies need a simple, cost-effective, and modern solution, delivered as a service, that gets business back up and running quickly when cyber events or disasters strike.

Uncomplicated cyber recovery

The use of cyber recovery tools and services has become complicated, costly, and even unpredictable when protecting against disruptive events like ransomware. Cyber recovery strategies may involve co-locations, secondary sites, cloud, or a hybrid approach. All of these strategies cost time and are expensive to set up, maintain, and test, as older tools do not provide flexibility and ease of use. To combat modern threats, legacy solutions often create bottlenecks that inhibit the rapid provisioning required for instant recovery and secure isolated recovery environments (SIREs), also known as clean rooms. The recovery of virtual machines (VMs) needs to be easy so critical applications and services can be returned to operations rapidly and reliably. With ransomware strikes and natural disasters happening daily, it is essential for companies to have a cyber recovery solution to help protect their business.



On-demand cyber recovery

Pure Protect® puts you in control of your VMware cyber recovery spend.



Fully orchestrated

Pure Protect makes failover and failback simple with fully orchestrated management through Pure1®.



Complete control

Pure Protect uses your AWS or VMware site, so you're always in control.

Flexible deployment for hybrid architectures

Pure Protect® offers flexible deployment options for cyber recovery, supporting both cloud environments through Amazon Web Services (AWS) and on-premises VMware-to-VMware replication:

- **Cloud:** Your recovery solution should not be complicated or a black box of mystery—you need to be in control of the solution and your data. Pure Protect leverages your existing AWS organization, so you maintain control over your systems and data. Management is performed through Pure1®, so you can manage your cyber recovery and failover anywhere you have internet connectivity. Management capabilities include the fully orchestrated provisioning of a virtual private cloud (VPC) landing zone and orchestration of VM failover. This allows for the automated provisioning of a recovery VPC, which can serve as a cyber recovery environment.
- **On premises:** Many organizations cannot leverage cloud deployments for security and privacy concerns. The Pure Storage® VMware-to-VMware cyber recovery capability enables fast and efficient recovery of VMs from one VMware environment to another in case of an outage, data loss, or site failure. Pure Protect replicates VMs from a primary site to a secondary recovery site with all the functionality of a cloud solution.

Advanced recovery capabilities

Pure Protect provides advanced recovery capabilities, including a SIRE for safe data validation and seamless failback options to your primary location:

- **SIRE:** In the event of a malicious attack, Pure Protect can automatically provision a complete, virtualized, and isolated recovery environment—including compute, networking, and storage. This clean room allows you to safely restore and validate data using immutable snapshots before bringing systems back online, ensuring you recover without reintroducing the threat. The entire environment is orchestrated to reduce staff overhead and accelerate the restoration of mission-critical applications.
- **Failback:** With any deployment option you choose, Pure Protect always gives you the option to fail back your workloads to a primary location. The ability to quickly restore services following a failure and seamlessly transition back to the primary environment is essential. With this capability, Pure Protect minimizes downtime, maintains data integrity, and supports business continuity without prolonged reliance on secondary systems.

Predictable, cost-effective, and reliable outcomes

Accelerate cyber recovery

Unlike other cyber and disaster recovery solutions, Pure Protect fully orchestrates layered resilience and recovery provisioning. With predefined workflows, automatic target provisioning, and regular testing, Pure Protect lets you minimize downtime and ensure business continuity. Automated recovery on demand and the ability to test a failover in different scenarios is critical to a successful and rapid cyber recovery strategy. The isolation capabilities in Pure Protect enable routine testing and validation of VMs to help identify potential gaps in coverage without interfering with production systems. This same orchestration capability can be used to create a SIRE in the event of a malicious incident. In a cyber recovery scenario, immutable and indelible snapshots are used to rapidly restore data and VMs to the SIRE. With scale-down capabilities, systems can be powered on and tested with minimal resources, thus saving money.

Maximize your budget with consumption-based VMware cyber recovery

Pure Protect is a cost-effective solution that provides simple, on-demand orchestrated failover of workloads should you need them for testing or recovery. You don't have to bear the massive recurring expense of a secondary data center or co-location for cyber recovery readiness. By leveraging both on-premises VMware infrastructure and native Amazon EC2 instances from AWS, organizations can maintain a flexible, cost-efficient strategy.



Reduce complexity

Pure Protect reduces complexity by centralizing and automating VMware data protection across hybrid and multicloud environments. With policy-based automation, an intuitive user interface, and rapid recovery capabilities, Pure Protect eliminates the need for multiple backup policies and manual processes. This streamlined approach reduces operational overhead, improves consistency, and accelerates protection workflows—empowering teams to manage data resiliency more efficiently.

Critical capabilities

Pure Protect simplifies recovery from cyberattacks so you can get your business back online quickly—without having to maintain costly infrastructure and complex configurations. Pure Protect allows you to fully orchestrate the failover of applications and business systems from on-premises VMware vSphere to your organization's AWS site or a secondary VMware site.

Pure Protect provides:

- On-demand cyber recovery that's right-sized for your business.
- Pure Protect Recovery Zones that automatically provision complete virtualized recovery environments (compute, networking, and storage) to isolate, remediate, and recover from malicious attacks.
- Provisioning of your target location, including isolated cyber recovery environments, so the recovery of your VMs is fully orchestrated.
- Cyber recovery testing in isolated environments, allowing you to find gaps in coverage without risking your production systems.
- VM point-in-time recovery, enabling clean data restoration after ransomware attacks and other disasters for faster business recovery.

Additional resources

- Learn more about [Pure Protect](#).
- Explore Pure Storage [cyber resilience](#) solutions.
- Learn more about how Pure Storage helps you build an [Enterprise Data Cloud](#).
- Experience the power of the [Pure Storage platform](#).

purestorage.com

800.379.PURE

