BlackPearl's Attack-Hardened™ Network Attached Storage

BlackPearl Attack-Hardened NAS

BlackPearl NAS with a scale-up architecture provides expandable enterprise-grade NAS storage. It can be deployed as either a standalone system or combined with additional software extensions as part of the BlackPearl platform. BlackPearl NAS is designed to provide secure, scalable storage for a variety of use cases, including backup, online shared storage, capacity offload, and more.

Benefits of BlackPearl NAS

Enterprise-grade data protection

- Attack-hardened security improves ransomware resiliency
- Self-encrypting disks and multi-factor authentication provides additional security

Flexible for many workloads

- Designed for unstructured data
- Extensible to S3 storage with optional tape-out

Easily expandable bulk storage

- Scale-up architecture allows low-cost expansion and growth
- Over 20PB in a single rack, expandable to hundreds of PB

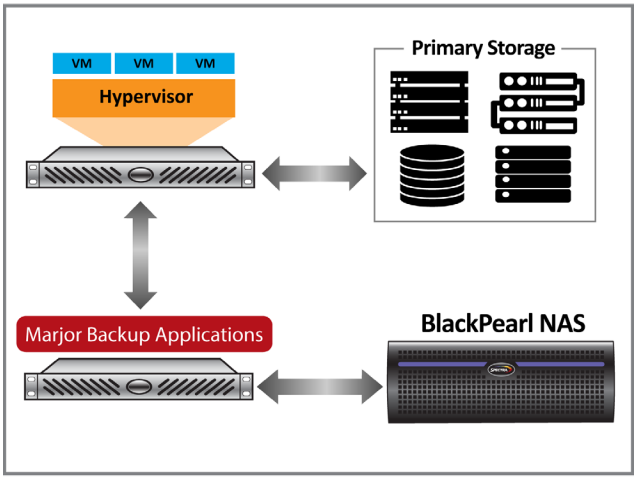
BlackPearl Attack-Hardened Use Case

The Challenge:

Finding a platform that was able to protect data and grow with their organization. Beginning with a simple NAS backup target for their existing software that has the ability to be a simple shared storage resource for both backup and archive.

The Solution:

Spectra's BlackPearl NAS has been qualified with all major backup applications to provide a tight integration ensuring full functionality with their backup environment. Additionally, BlackPearl's Attack-Hardened capabilities create a ransomware resilient storage solution by utilizing scripts to perform triggered snapshots at the completion of each job or group of jobs, providing the ideal time to create snapshots to protect data from ransomware attacks. With the ability to scale to over 20PB in a single rack, the BlackPearl solution was a perfect fit for not only backup data but also provide shared online storage for archival data that needs to be accessed quickly. With built-in data protection and easy scalability, the BlackPearl NAS easily fits into their existing environment providing secure and affordable secondary storage for back-up and archival data.



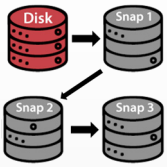
BlackPearl® Attack-Hardened™ NAS is the ransomware resilient storage solution for the modern data center

BlackPearl Attack-Hardened Storage

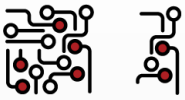
Constant threats loom against data. Whether they be external from an outside threat actor, such as ransomware, or internal, from a disgruntled employee, or accidental from human error, data must be protected equally so that business continuity can be maintained. The best defense is to avoid having to deal with bad actors and to be able to restore data and infrastructure back to pre-attack state using best practices.

BlackPearl is offering an approach to data protection that will counter the challenges mentioned above and give organizations greater leverage in avoiding the harrowing experience of negotiating with criminal elements of the underworld.
We call it Attack-Hardened Storage.

BlackPearl Attack-Hardened Features



Triggered Immutable Snapshots:
Snapshots, or point-in-time copies of a volume, let you restore a volume to the state it was in when the snapshot was created. BlackPearl interfaces with backup software via pre and postscripts. After the snapshot is complete, Spectra provides code to be used to make the target volume read only.



Multiple Types of Air Gap:
- **Virtual Air Gap** - Replication inside BlackPearl unit
- **Remote Air Gap** - Replication to a remote BlackPearl
- **Offline Air Gap** - Tape copy of data

Multi-Factor Authentication:
BlackPearl works with Google Authenticator to confirm the identity of any user trying to log into the BlackPearl system.

Tape Storage for Offline Storage:
BlackPearl has full integration with Spectra automated tape libraries and can provide a fully protected, offline copy of your data to ensure no outsider threat can access that offline data.

Multi-Site Replication:
BlackPearl can replicate to another volume in the same BlackPearl system, a separate system located in the same onsite location, a different offsite location, or a remote cloud target.

Self-Encryption:
BlackPearl can be configured with self-encrypting drives (SED).
This is excellent protection of the data if a drive is being sent back for repair or being disposed of at end of life.

*Amazon Glacier® is a registered trademark of Amazon Technologies, Inc.

About Spectra Logic Corporation

Spectra Logic develops a full range of Attack Hardened™ data management and data storage solutions for a multi-cloud world. Dedicated solely to data storage innovation for more than 40 years, Spectra Logic helps organizations modernize their IT infrastructures and protect and preserve their data with a broad portfolio of solutions that enable them to manage, migrate, store and preserve business data long-term, along with features to make them ransomware resilient, whether on-premises, in a single cloud, across multiple clouds, or in all locations at once. To learn more, visit www.spectralogic.com.

GSA 47QTCA20D0064

V1-060922

Toll Free: 800-833-1132 • 303-449-6400 • 6285 Lookout Road • Boulder, CO 80301 USA

SPECTRALOGIC.COM