



Attack Hardened™ Storage: Building Data Resilience from External and Internal Threats with the BlackPearl Platform

2021



CONTENTS

Introduction	3
Attack Hardened.....	3
The BlackPearl Family: Attack-Hardened Storage.....	4
Building Bricks of the Security Wall.....	4
Encryption	4
Snapshots and Data Immutability	5
Air Gap	5
BlackPearl’s Approach to Snapshots	6
Non-Traditional File Protection via BlackPearl Snapshots.....	7
Snapshots Used to Protect Backup Data Sets	7
Replication	8
Multi-Factor Authentication	9
Multi-factor Authentication as “Internal Gatekeeper”	10
Hardened but Versatile.....	11
Ransomware Resiliency – A Two-Part Story	12
Block, Manage, Protect.....	12
The Role of Tape in Attack-Hardened Storage	14

Copyright ©2021 Spectra Logic Corporation. All rights reserved worldwide. Spectra and Spectra Logic are registered trademarks of Spectra Logic. Amazon Glacier® is a registered trademark of Amazon Technologies, Inc. All other trademarks and registered trademarks are property of their respective owners. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. All opinions in this white paper are those of Spectra Logic and are based on information from Spectra Logic and other sources.





Introduction

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.

Ransomware has been steadily on the rise and is increasingly making headlines in the news. Cases of ransomware attacks are cropping up right and left, such as at the Colonial Pipeline, Exagrid, and meat processing giant JBS. Spectra Logic even became the target of ransomware. Spectra's successful defense of that attack has led to multiple articles, white papers, and webinars. It also led to the company's deployment of even more robust storage solutions to help others avoid such a situation. That storage approach is at the heart of this white paper.

According to Check Point Research, ransomware attacks have seen a 102% increase this year compared to the beginning of 2020, and there are no signs of it slowing down. In many instances, companies opt to pay the ransom as a means of recovering their data and operations. Unfortunately, doing so does not guarantee that they get the key to unlock their data. In some cases where the key is obtained, ransomware has corrupted the data to the point that it is rendered unreadable.

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 and *Attack-Hardened* storage.

Attack-Hardened

Spectra Logic offers an approach to data protection that counters the challenges mentioned above and gives organizations greater leverage in avoiding the harrowing experience of negotiating with criminal elements of the underworld. We call it Attack Hardened™ Storage.

What does it mean to say that a storage solution is Attack Hardened? The process of hardening a material or substance is hardly new. The "fire-hardened" spear is one of the most iconic weapons of the Paleolithic era and dates back over 450,000 years. More modern approaches to hardening a substance include heat treating to harden metal. Before hardening, the crystal lattice structure of metal allows for a level of plasticity that is weaker. When metal is heated to a certain temperature, the elements in the metal become a more solid solution greatly reducing this weakness.

Attack-Hardened storage could be viewed in a similar light, in part based on Spectra's ability to prevail against a May 2020 "Netwalker" [ransomware attack against our internal IT systems](#). There are many different elements offered to protect storage. Spectra brings those elements together to offer a more solid solution capable of avoiding "give" when under attack. Some of the elements we work with in this approach are already known, some are enhanced, and some are new. By forging these features and approaches together, Spectra is able to offer storage that is made stronger, more efficient and better able to withstand the heat of attack from external threat actors, internal actors and even natural or man-made disasters.

The BlackPearl Family: Attack-Hardened Storage

The BlackPearl® Platform, with Attack-Hardened storage, is now available. The BlackPearl product family is most easily described as a storage platform. It starts as traditional NAS disk storage. It is the optimal platform for mid-tier (inactive) data as it provides self-protecting, flexible and affordable secondary storage for data that does not require continual backup. With BlackPearl OS V 5.4, Spectra is adding data immutability and other features to prevent destruction or encryption of files stored on the BlackPearl.



BlackPearl expands via hardware and software to include capacity and performance enhancements; offers multiple interfaces including CIFS, SMB, NFS, S3 or object storage interfaces; acts as a gateway to public cloud storage; and even offers upgrades to create on-premises glacier storage. Due to the tremendous versatility of the BlackPearl Platform, it typically sits in the middle of secondary storage, either as a target or an intelligent gateway to additional secondary storage.

This is the storage dedicated to backup, replication or migration. It's also the storage that is relied on to overcome adverse events, be they from external actors, internal actors, natural disasters, or technical mishaps. For this reason, the BlackPearl Platform is created with a relentless focus on data security which will be detailed below.

While BlackPearl works as a standalone Attack-Hardened solution, it can also be paired with front-end partners such as backup or migration software applications, or back-end partners such as Arctic Wolf to enhance security even further.




Building Bricks of the Security Wall

Rather than focus on a single, large lock to safeguard data, the BlackPearl approach is to create multiple locks or “building bricks” to prevent destruction or theft of data. BlackPearl incorporates encryption, immutable snapshots, replication, and multi-factor authentication to create an unbreachable wall between an organization’s data and the threats which are constantly surrounding that data.

Encryption

While encryption may seem too obvious to mention, it's for that very reason that we mention it first. Ransomware is most well-known for encrypting an organization’s data and extorting a ransom for the decryption key. Ransomware attacks are also capable of opening “back door” access to networks, making data available to third-party conspirators who want to profit from the use of an organization’s data.



One of the most notorious ransomware viruses, *Netwalker*, acts in this very manner. In addition to facing ransom, data loss and/or arduous rebuilds if attacked by Netwalker, an organization may deal with more traditional data breaches which require notification to any affected parties, public disclosure and often loss of public faith or their customer base.

The simplest approach to encryption is to encrypt via the backup application. As an additional hardware-level security, if organizations are working with applications that don't offer encryption, or if that feature is not activated, Spectra's StorCycle® storage lifecycle management software (version 3.6 and beyond) can encrypt infrequently accessed files and move them to immutable BlackPearl storage. This effectively reduces the "attack surface" of a hacker, virus, or ransomware. Many governmental laws and industry regulations do not view the theft of encrypted data as falling under the same mandates as the theft of unencrypted data which can easily be read and manipulated.

For those requiring device-level 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. It doesn't replace the above-described functions of encryption.

Snapshots and Data Immutability

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. A snapshot only consumes the space of the changed blocks, which makes them very space-efficient. BlackPearl snapshots can be generated automatically (hourly, daily, or weekly); or snapshots can be created on demand.

Snapshots are not a new approach to data protection and easy restoration. Snapshots have been around for a while and are often the "go to" for restoring data from many types of loss. The real appeal of snapshots is that they restore a system to an earlier state in rapid manner. Petabytes of data can be restored (or re-accessed) in minutes.

Because snapshots are accessible across the network, however, they are not considered to be "offline Air Gap" protection, which is found in fully offline storage such as tape. It's helpful to have a working definition of Air Gap and the several different ways it's defined.

Air Gap

The term Air Gap means different things to different people. For the purposes of this paper, we'll talk about three types of Air Gaps: virtual Air Gap, remote Air Gap and offline Air Gap.

- *Virtual Air Gap* consists of immutable snapshots, which protect the data path, and can be achieved with replicated snapshots to another volume on the same BlackPearl.
- *Remote Air Gap* employs the replication of data to a remote site/location on another BlackPearl system, to the cloud or to tape, providing protection against insider threats and local environmental disasters.
- *Offline Air Gap* operates when the BlackPearl is used to send data to tape – in this instance of offline, tape is then ejected or moved to an inaccessible area, either into a vault or into a cold partition on a tape library.

BlackPearl's Approach to Snapshots

The BlackPearl Platform has created an approach that offers the convenience of snapshots along with a *Virtual Air Gap* to bring it closer to the protection offered by tape. We refer to it as "Air Gapped NAS." The game-changer comes from creating "immutable" snapshots.

BlackPearl's ZFS file system creates immutable snapshots – snapshots which cannot be overwritten or altered. This prevents snapshots from being encrypted after they've been written. This makes snapshots very desirable for recovering from many variants of ransomware attack as shown in Figure 1.1

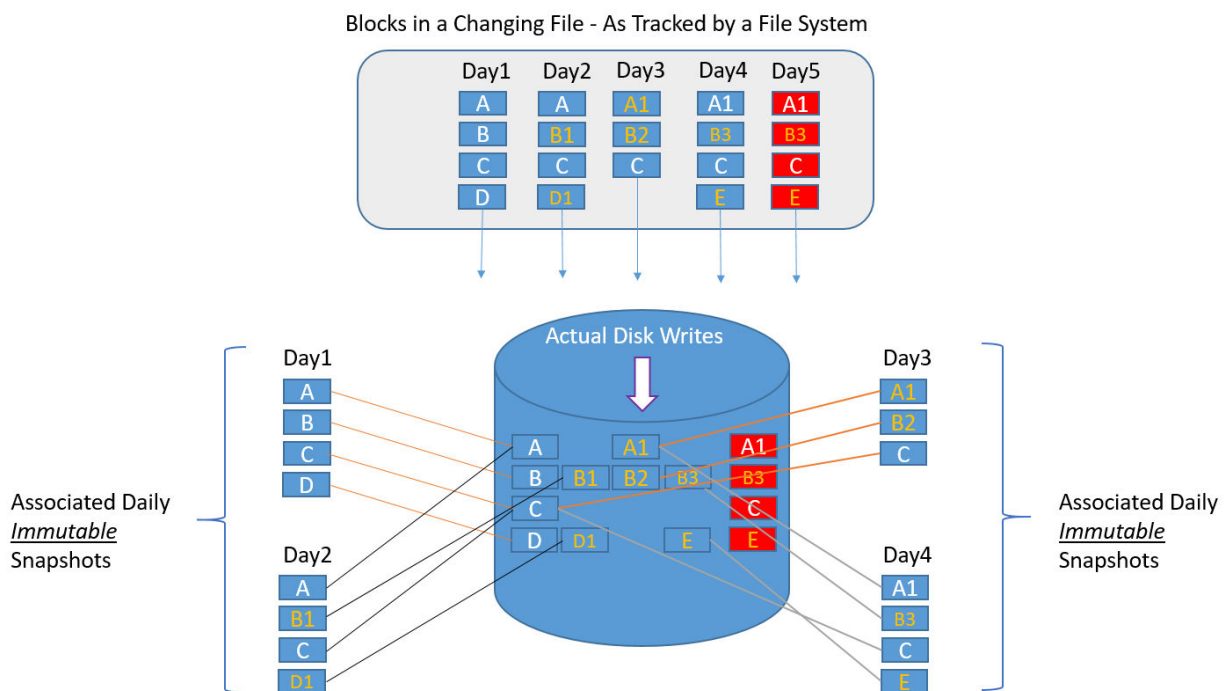


Fig 1.1

On Day 5, a ransomware attack encrypts files. Administrators can reclaim the unencrypted files from any time period in which they have a snapshot. Because BlackPearl creates immutable snapshots, they cannot be encrypted by the attack that encrypted the original data. For simplicity, this example shows daily snapshots. Snapshots can be taken at any time, i.e., hourly, daily, weekly, on-demand, etc.

Administrators can create a snapshot at any time and can create as many snapshots as desired. This is especially important when files are being created that aren't typically protected by traditional backup software. This method can be used in many different scenarios to assure information is protected.



Non-Traditional File Protection via BlackPearl Snapshots

Some aspects of IT infrastructure are not protected by traditional backup software, such as network configuration images, server settings, data images, etc. Administrators can drag/copy data to BlackPearl for long-term storage, then make snapshots of this information for immutability.

Zoning and programming switches is an arduous task. While this is not often “redone,” complete reconfiguration is often required after a disaster or cyberattack. BlackPearl makes it easy for system administrators to simply drag and drop or copy network configuration files to BlackPearl and implement a snapshot. Each new configuration is kept along with prior versions.

Virtual machine configuration is another good use of BlackPearl’s snapshot capability. There is no reason to run a backup every time a VM is created or changed. Again, a simple copy to BlackPearl assures an application snapshot for easy rebuilds whenever necessary.

Likewise, individual employees may have data on a local laptop or system that isn’t being curated by backup software. This is often the case with remote work or large project files. Anyone who has content, data, or information they are concerned about protecting can use the snapshot feature of BlackPearl to assure data security.

Snapshots Used to Protect Backup Data Sets


An excellent use of snapshots is to protect traditional backup data. While offsite backups to tape are considered the gold standard for assured data recovery, the restoration of large data sets can be tremendously time consuming. As mentioned earlier, snapshots can turn days of restoration into minutes. BlackPearl excels in this area. In addition to administrators manually initiating snapshots via the BlackPearl user interface, backup software can be configured to automatically initiate snapshots.

BlackPearl interfaces with backup software via pre-scripts and post-scripts. Any application which supports pre and post commands can be configured to take advantage of the BlackPearl’s immutable snapshots as well as “lock/unlock” data at the volume level.

Backup applications which are capable of issuing commands before and after they initiate a backup job can instruct BlackPearl to take a snapshot as soon as backups are complete (post command). After the snapshot is complete, Spectra provides code to be used to make the target volume read-only. If any outside threat actor tries to overwrite or encrypt those snapshots, the volume will be protected as read-only. The pre command can be used to “open” the volume or turn it back to read/write before the next backup job is scheduled to run. The process then repeats itself with the post command.

This unique approach creates a “one-way valve” so to speak – preventing any access to the finished backups via any application other than the backup application. Now, not only are the snapshots immutable, but the data itself is immutable due to its read-only status.





Snapshots are, however, still limited in two ways. They do not offer disaster recovery protection from fire, flood, earthquake, or other natural disasters if the disk systems they reside on or point to are compromised in that event. Likewise, snapshots are not effective against ransomware or internal actors if they are intentionally deleted. Unfortunately, this has become a common feature of ransomware – searching for and deleting backups and snapshots before encrypting data.

BlackPearl's Replication and Multi-Factor Authentication are the keys to making immutable snapshots bullet-proof.

Replication

Creating a *Virtual Air Gap* with immutable snapshots is an excellent approach to avoid paying a ransom after a cyberattack. It does not, however, offer protection against disaster recovery if the onsite storage system is destroyed by natural or man-made disaster. One of the easiest ways to add redundancy for disaster and attack harden a storage system is by using replication to create a *Remote Air Gap*.

As previously mentioned, a *Remote Air Gap* requires making a direct second copy on an independent system which is, ideally, geographically separated from the first.

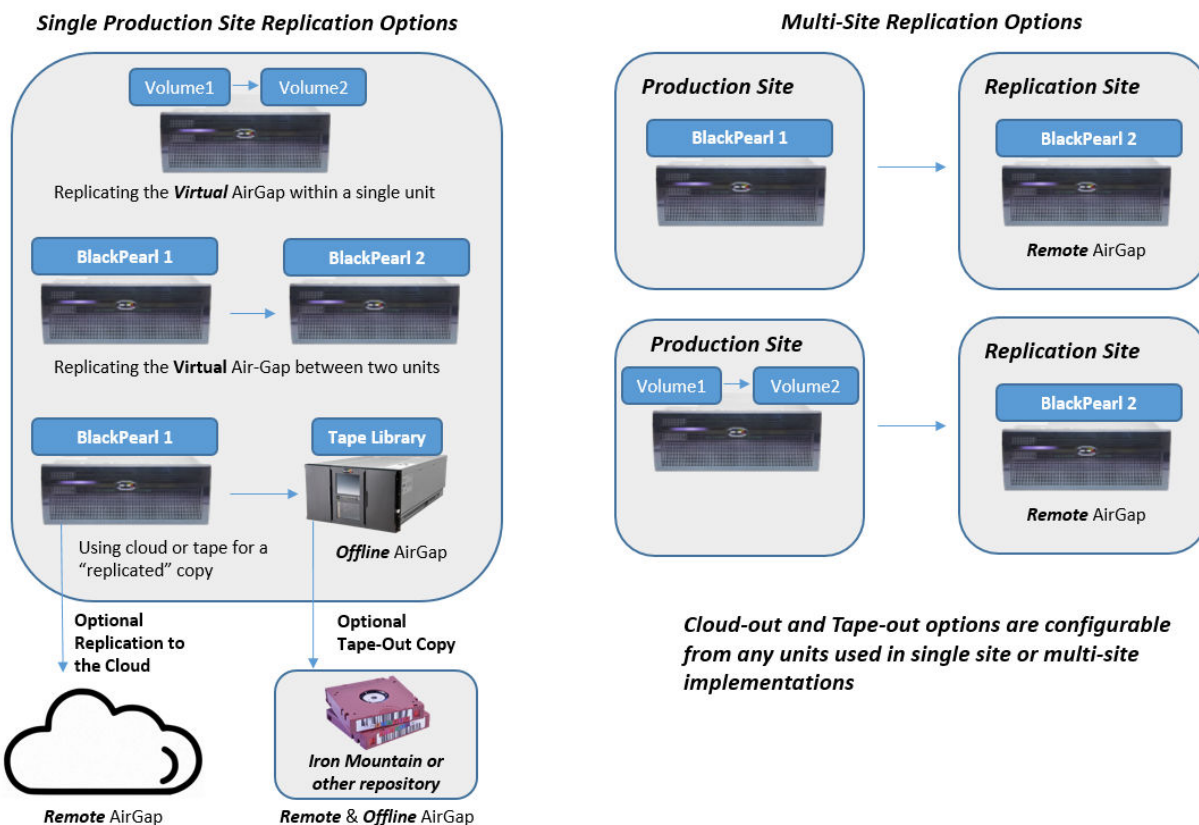
The BlackPearl ZFS file system includes the ability to take snapshots of data on a scheduled basis. Volumes can then be replicated to another BlackPearl NAS system over a switched network. Set up is straightforward and can be tailored to meet workflow needs by customizing snapshot timing and frequency.

In the disk industry, many vendors support a form of replication from one system to another, typically for disaster recovery. This is usually found in enterprise-class tier 1 and tier 2 type NAS servers. BlackPearl's file system provides functionality to create a snapshot of the file system contents; transfers the snapshot to another machine; and extracts the snapshot to recreate the file system.

Administrators can create a snapshot at any time and can create as many snapshots as desired. By continually creating, replicating, and restoring snapshots, a protected copy of data can be created on a second BlackPearl system.

Many solutions require the entire storage array be replicated so it's not always realistic to use the storage as discussed above. Solutions which require the entire array to be replicated require two arrays for onsite replication and three full arrays to accomplish offsite replication. BlackPearl can accomplish replication with as few as one array for onsite replication or two arrays for offsite replication.

Replication and its Associated “AirGap” Levels



BlackPearl’s ability to replicate at the volume level makes it an ideal target for overcoming the traditional limits of snapshots and 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. Likewise, BlackPearl offers a tape-out feature so that snapshots can be offloaded to tape and located offsite. Making sure data is offsite in some manner assures recoverability in the event of a site-specific disaster.

BlackPearl’s ability to work on the volume level for read only as well as replication makes it an ideal solution for organizations desiring any level of Air Gap protection.

Multi-Factor Authentication

With the almost daily reporting of ransomware attacks, usernames and passwords are being used by external actors bent on destruction, disruption and ill-gotten gains. Clearly, a need exists to protect data more securely. The crowning jewel of Spectra’s approach to Attack-Hardened storage is Multi-Factor Authentication or MFA.

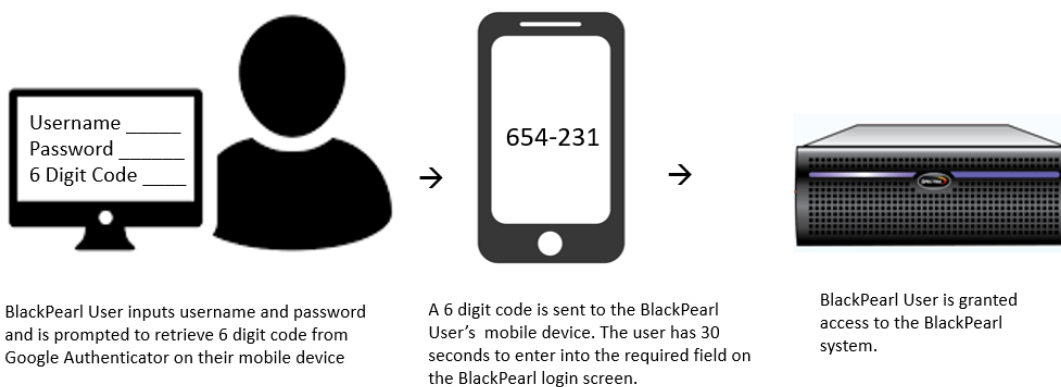
Multi-Factor Authentication is an added layer of security that assures the individual attempting to gain access to BlackPearl is authorized to do so. This approach prevents bad actors from accessing data even if they have access to your username and password – attack hardening the storage system.

As mentioned earlier, immutable snapshots are one of two key elements in creating *Virtual Air Gap* protection on NAS. Although BlackPearl snapshots are immutable – they can't be written to or encrypted – the volume that the snapshots are written to could still be deleted by someone “posing” as a system administrator. Without addressing this threat, even replicated backups and snapshots can fall prey to the attacker.

BlackPearl works with Google Authenticator to confirm the identity of any user trying to log into the BlackPearl system. This type of technology is commonly used to confirm the identity of individuals logging into web portals with sensitive or personally identifiable information. Spectra Logic makes this approach available to BlackPearl users.

The process is straightforward. When a new system user is created, a QR code is generated for them. The user then scans their unique QR code in Google Authenticator to verify and set up their account. When the user logs onto a BlackPearl system, they will first enter their username and password per normal. At this stage they will be prompted to retrieve a unique six-digit code from the Google Authenticator application on their phone. The code must be entered at the login page within 30 seconds or it will expire and a new code must be generated. No connection to internet is needed. No connection between the phone and the BlackPearl servers is needed. No email messages are sent. This approach assures that no external actor can login as a system administrator.

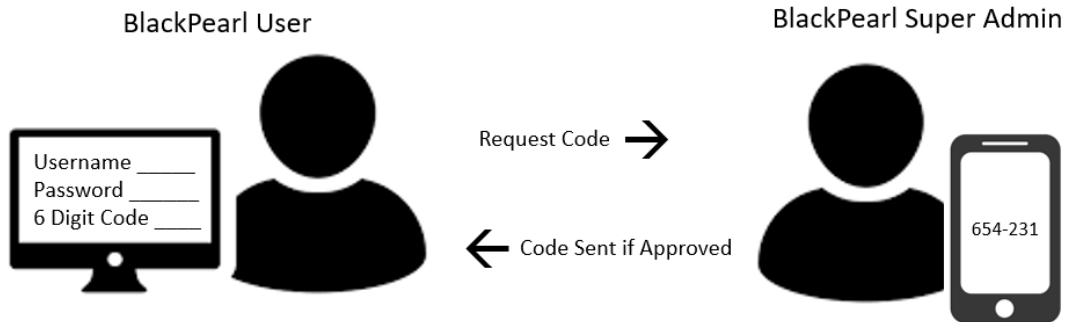
Multi-Factor Authentication to Prevent External Threats



Multi-factor Authentication as “Internal Gatekeeper”

Although not as widely publicized, internal actors can also become a threat. Accidental or unintentional data deletion happens. Likewise, disgruntled employees can create massive damage if that becomes their intention. And because it's impossible to predict who will make a mistake or act against the organization at some point in the future, this is an area of vulnerability.

Multi-Factor Authentication to Prevent Internal Threats



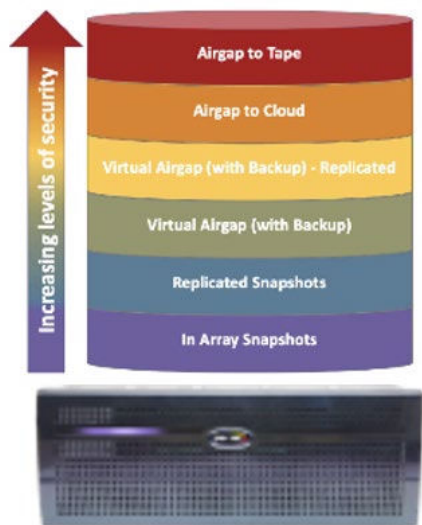
BlackPearl User is prompted to enter 6 digit code after entering their username and password into the BlackPearl login page. 6 Digit code is sent to *the one* team member that is designated the 'Super Admin'. The BlackPearl User contacts the 'Super Admin' to retrieve the code sent to the 'Super Admin's' phone to move forward.

BlackPearl Super Admin receives 6 digit code after BlackPearl User attempts to login. The BlackPearl Super Admin can either send the 6 digit code to the BlackPearl User to enter onto the login screen for access, or not send/deny the BlackPearl User access to the BlackPearl System.

BlackPearl's multi-factor authentication can help prevent this as well. By limiting multi-factor authentication to a single or very small number of trusted employees, authentication can be used as an obstacle to destructive acts, unintentional or otherwise. Users needing administrative access to the BlackPearl would contact the "super user" who is trusted to generate key codes for those individuals.

Hardened but Versatile

While designed to assure successful defense under attack, BlackPearl also offers tremendous versatility in working with other storage solutions. Certified by all major backup software solutions, BlackPearl offers unique interfaces to assure the backup partner you work with can take advantage of this Attack-Hardened approach.



Traditional NAS interfaces such as CIFS/SMB and NFS make BlackPearl a simple storage target for backup applications such as Commvault, Veeam, and others. BlackPearl can be upgraded to an S3 interface for applications such as Rubrik or Cohesity which can write to S3 storage targets.

Likewise, BlackPearl's S3 interface (in BlackPearl OS 5.4) can also be used to create onsite "glacier-like" storage for those who can't go to the cloud, desire a hybrid cloud solution, or want to reduce the cost of long-term storage. BlackPearl supports open formats in writing data and can itself target multiple forms of additional storage, including cloud, object storage disk and tape.

The versatility of the BlackPearl Platform allows organizations to configure any level of security needed to assure their data is being protected in the appropriate manner.

Ransomware Resiliency – A Two-Part Story

The full power of *Attack-Hardened Storage* is fully realized when combined with *Threat Reduction Software*. Combining the appropriate “threat-blocking” as well as “data movement” software with BlackPearl Attack-Hardened storage gives organizations an unparalleled level of *Ransomware Resiliency*.

Block, Manage, Protect

The first goal is to *block* any cyberthreats from coming into the organization. In full disclaimer, there’s no way to keep 100% of threats from entering your organization. Therefore, it’s important to *manage* (and survive) the threats that do get through. We also know that even managed threats occasionally hit their intended mark of disruption and possible data destruction. By moving, replicating and copying data, a *protection* layer can be created that is deployed in the unfortunate event of a successful cyberattack.

There are several levels at which software is deployed to achieve a powerful block, manage and protect approach.

Email is the greatest invention in communication since the telephone. It’s also the surest inroad for bad actors to deploy viruses and ransomware. Secure Email Gateways (SEG) are a mandate in today’s cyber environment. Manufacturers such as Barracuda, Cisco, Mimecast and Proofway are just a sampling of the vendors that provide SEGs. There’s a bit of a balancing act to deploy these solutions. At first, too much traffic may be blocked. Most have simple “release” mechanisms to add “trusted sender” emails and/or domains. Several will identify any email originating outside of your organization. This makes it easier for individual employees to identify emails being sent from someone impersonating a fellow employee.

Next in line is an Endpoint Protection Platform (EPP). Assuring that laptops, VPNs, and even phone systems are protected is equally important. An EPP is a solution deployed on endpoint devices to prevent file-based malware; detect and block malicious activity from trusted and untrusted applications; and provide the investigation and remediation capabilities needed to dynamically respond to security incidents and alerts. Sophos, McAfee, SentinelOne and CrowdStrike are examples of vendors providing such software solutions.

Threat-Reduction Software Applications

If the above precautions fail, the only viable answer to recovery is bringing back a protected copy of the original data. As already covered above, this can be accomplished via snapshots, backups and/or replicated copies of the original data. Software in the “backup” category includes Commvault, Veeam, Rubrik, Cohesity and Spectrum Protect, among many others.

Ransomware Resiliency



While these applications vary in their approach, they are all fully compatible with BlackPearl storage. They can interface to BlackPearl via traditional CIFS/SMB or NFS interfaces, and many offer S3 interfaces which are also supported. As mentioned earlier, BlackPearl further protects the data sets created by backup applications via immutable snapshots, replication and multi-user authentication.

As discussed, Spectra's StorCycle software is a storage lifecycle management solution that adds a more granular approach to data protection. StorCycle is used to *Identify, Migrate, Access and Preserve* infrequently accessed data. It's an ideal approach to creating project archives or disaster recovery copies of data.



StorCycle now offers "ransomware snapshots." StorCycle integrates directly with Spectra's BlackPearl triggered snapshot feature mentioned earlier. When enabled, StorCycle initiates snapshots of BlackPearl volumes at the end of migration jobs. If the migration job is the only data written to a given volume, StorCycle will optionally turn that volume into read-only status so that files can't be overwritten or encrypted.

When StorCycle is used to move data again, a pre-API command will trigger BlackPearl to make the volume writable so that StorCycle can migrate the next set of files after which the volume will be turned to read-only status once again.



StorCycle naturally reduces the ransomware attack radius by moving less active data off of primary storage and into archive. But in addition to ransomware encryption, users must protect data from breach and theft. This is an area that StorCycle's Attack-Hardened approach can help with as well.

Archived data can be sensitive, such as Human Resources information. This information could be embarrassing or create liability if leaked. Likewise, archives may contain organizational intellectual property which could have devastating consequences if stolen.

StorCycle offers AES-256 encryption. Data migrated by StorCycle to other locations may be encrypted, then automatically de-crypted when brought back for usage. This feature provides a simple and secure way to assure that data can not be read by external bad actors. Highly confidential information can be kept accessible but not stealable.

New features of StorCycle such as versioning (due in 3.7, Dec. 2021) will assure that all versions of a file are kept even if the original data is changed and then "re-archived" or migrated.

Likewise, future releases of StorCycle will allow its powerful scanning ability to scan and identify the versions of snapshots created for protection. This will allow for an even quicker and more granular approach to using the correct snapshots for a speedy recovery.

Spectra's Vail® software brings the same file-based features of StorCycle to object storage. This powerful software will allow multi-cloud and hybrid cloud environments to view, access, share and protect data in

virtually any environment. The object-locking feature of Vail is similar to the immutable snapshot capability of BlackPearl storage.

Combining Spectra's Attack-Hardened storage with threat-reduction software will create one of the most secure environments possible while leaving data accessible to those authorized to access and use that data. This approach allows organizations to fully embrace the power of a cyber universe, while reducing the likelihood of disruption via disaster, hacking, viruses or ransomware.



The Role of Tape in Attack-Hardened Storage

As already mentioned, tape offers the only true "offline" air gap for data protection. But as ransomware viruses become more intelligent, it is not out of the realm of possibility that ransomware could implement tape load commands to delete, steal or encrypt data.

The Spectra® Stack Tape Library allows users to create a secure storage space not accessible by software. Human intervention would be required to move tapes from this secure area. The design is simple yet effective.



The Spectra Stack Tape Library can be configured with up to 560 tape slots. One or more partitions can be created for management of tape pools. Users can manually move tapes from a used tape partition into any licensed but unused slots in the tape library. This can be done via the Remote Library Controller (RLC), the front panel or a REST interface.

Once the tapes have been moved, the backup/archive application is instructed to perform an inventory. The tapes that have been moved will no longer show in the application's inventory. If a tape is needed for a legitimate restoration, an administrator can return the tape to the partition by the RLC, front panel or RESTful interface.

In the first half of 2022, Spectra will introduce a similar "safe partition" to its larger libraries. As these libraries can expand to tens of thousands of tape slots. Each "used" partition will be able to have a companion "cold" partition for safekeeping in the same manner as described above. Administrators will be able to use the RLC, front panel of the library or XML commands to execute the move to and from the cold partition in question.



These safe partitions assure that a rogue virus will not have access to any data moved into one of these extremely secure areas.

As ransomware and other malware viruses continue to evolve, Spectra continues to innovate. We will be adding a number of additional Attack-Hardened features to our storage and data management solutions in the coming quarters.

Spectra's approach to Attack-Hardened storage has been shaped by over 40 years in the storage industry as well as the recent ransomware attack the company successfully survived. By bringing these insights and innovations to our user base, we hope to help others say "No" to paying ransoms and recover from the crippling effects of a data breach.



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, protect and preserve their IT infrastructures with a broad portfolio of solutions that include ransomware resilient features to help them manage, migrate, store and preserve their data long-term, whether that data is located on-premises, in a single cloud, across multiple clouds, or in all locations at once.

To learn more, visit www.spectralogic.com.