PURESTORAGE®

WHITE PAPER

Secure Your Data with Pure Storage Layered Cyber Resilience Architecture

Bolster cyber security with visibility and resilience

Today, ransomware attacks, including double extortion schemes that combine encryption with data exfiltration, have become the norm across all industries, representing the most prominent and damaging cyber threats organizations face. However, going forward, these threats are evolving into much more destructive forms such as wiperware, which completely destroys a company's IT systems and renders them useless. In addition, nation-state threat actors from China, Russia, Iran, and North Korea are actively targeting critical national infrastructure (energy, water, transportation, financial, and healthcare) and lying in wait to attack when "the time is right."

Government agencies in the United States and other countries, including the National Security Agency (NSA), Federal Bureau of Investigation (FBI), Cybersecurity & Infrastructure Security Agency (CISA), Government Communications Headquarters (UK), Federal Office for Information Security (BSI - Germany), and Cyber and Infrastructure Security Centre (CISC - Australia), all recommend taking action across two domains: **visibility and resilience**.

Their recommendation is that **visibility** should be the first line of defense. However, they also recognize the difficulties and costs associated with developing an effective visibility program. So, if companies can't make the necessary investments to get the right levels of visibility to stop a threat actor before they can do bad things, then, companies need to be able to recover quickly from an attack. There is no in-between. This is where **resilience (recoverability)** comes into play. Companies need layers of recoverability throughout their infrastructure to get their business back online as fast as possible when the attack occurs. Pure Storage® plays a role in both visibility and resilience.

Visibility

In the above context, **visibility** is the notion of **cyber threat hunting**. This includes analytics tools to ingest data (Splunk, Elastic, LogRythm, QRadar, etc.), and correlation tools (Darktrace, EDR tools, Cisco AMP, SentinelOne, etc.) to make sense of the data. Cyber threat hunters are members of the security team who respond to a very specific threat using the output from these tools. The purpose of the **visibility platform** is to enable cyber threat hunters to precisely point to a specific area and take immediate action to **stop a threat actor before they can elevate privilege in an environment** and start laying malware payloads, stealing data, or taking other potentially destructive actions.

So Where Does Pure Storage Come Into Play?

Fast Storage Platform

Multiple Layers of Storage

Speed for an analytics platform is critical because when hunting for threat actors, time is of the essence. Analytics platforms ingest data from various sources and correlate that data to feed the cyber threat hunters.

In many cases, the storage platform becomes a bottleneck between the ingest and correlate activities. This is because most storage platforms leverage SSDs in their architecture. Those SSDs all have individual controllers that often create a scenario whereby the platform can either ingest data quickly or correlate data quickly, but not both. Pure Storage storage platforms can ingest and correlate data as fast as possible without bottlenecking the system.

Further, a customer could put a GPU in front of a Pure Storage array, and that GPU could reach its maximum utilization without the storage limiting the compute capabilities. This is critical since machine learning and AI are becoming central to the correlation piece of the architecture, and organizations are using GPU processing power to catch the bad actors. The net here is that the faster the analytics can run, the more likely the threat hunters can take action to stop the threat before it becomes a really big problem.

Storage data temperature tiering also becomes a critical component of the analytics process because most analytics platforms reside on three tiers of storage: hot, warm, and cold. A hot tier is the fastest and most expensive tier. Most organizations will only keep 30-90 days of hot data due to cost. The warm tier is less expensive than the hot tier and not quite as fast. It houses more historical data—think 90-180 days. The cold tier is the least expensive tier and where historical data is kept the longest.

Many organizations keep years of data in cold storage. When searches take place for correlation, they often span multiple tiers. Where the storage is slow, searches can take a very long time to execute and return a result, thus dramatically slowing down the threat hunting process and possibly creating a scenario where the results come in too late to take appropriate action. This is especially true where the public cloud (think AWS Glacier) is used for the cold tier. Pure Storage can solve this problem for customers by offering hot, warm, and cold storage tiers on flash storage. All-flash storage in your data center or colo yields the fastest searches, allowing the cyber threat hunting team to take the necessary action(s).

So, when you hear a security team complaining that their Splunk (or other) queries are taking too long, Pure Storage can help. Pure Storage offers an economical storage platform that helps organizations solve this problem while improving search performance.

Resilience

Resilience focuses on an organization's ability to recover after an event. At this point, visibility has failed, and the threat actor has successfully launched their attack. The company's goal now is to get the business back online as quickly as possible. Speed is of the essence. In fact, speed is the only thing company executives will care about. With stress levels through the roof, security and IT teams struggle with prioritization. The teams quickly find that recovering from backups doesn't work the way they had been promised. Businesses don't operate on infrastructure alone. They operate via applications. Applications have dependencies, and a general order of operations is required to get them back up and running. Starting a restore of every server doesn't lend itself to getting back up and running quickly. There are several instances where companies had their backup data, but paid the ransom anyway because it would have cost them more to be out of business for the time it would

Pure Storage Plays a Vital Role in the Recovery Process

Pure Storage SafeMode™

Organizations can implement resilience through three (or possibly four) layers and leverage **Pure Storage SafeMode** to create a guaranteed point of recoverability post-event.

The first thing to understand about recovering during a cyberattack is that an organization should always begin its recovery from the point closest to the attack as possible. Regardless of what other vendors say, there is no way of knowing a "perfect point in time" to recover to. In this context, we leverage SafeMode to protect the data on the primary storage arrays and create Layer 1 of the Pure Storage layered resilience architecture.

Recovery Process

When beginning the recovery process, the company will start from the primary storage array and take the following steps:

1. Start by rehydrating the most recent snapshot, prior to noticing the cyber event, into an isolated sandbox environment (generally a new Pure Storage array). For most organizations, they can focus on their most critical data and applications first.
2. Allow an incident response (IR) team to come in and clean any known indicators of compromise (IOCs) that can quickly be identified. These IOCs will likely be rootkits or running malware.
3. At this point, the organization can bring its mission critical applications back online in a degraded state, so the organization can operate at a minimum level.
4. The team can move on to a deeper dive forensic review and additional cleanup as they go.

After the initial recovery is complete for the most critical assets, the deeper dive review can be completed via Layer 2 of the Pure Storage layered resilience architecture, which is a snapshot offload layer. In Layer 2, the organization should copy the snapshots from the primary layer and keep them as long as it can afford to (preferably 6-12 months). After the initial recovery in Layer 1, the company can create as many copies of a given snapshot as needed for the IR team, instantly, with no additional space overhead, to allow the responders to begin running their tools and identifying additional cleanup activities or changes that may need to be made.

This is of huge benefit because normally the storage team would need to make “n” number of copies of data onto external media for “x” number of responders. In most incidents, especially in a large organization, there may be 10 or more responders, so this can result in significant time savings. In addition, Layer 2 “could” be used to run a workload if needed albeit in a less performant manner. In reality, most businesses would rather be up and running while less performant than down entirely.

Backup Layer

The third and final layer of the Pure Storage layered resilience architecture is the **backup layer**. Nowadays, legacy backups should be considered for long-term data retention and compliance. Most organizations should not consider recovering their entire estate from backups due to performance concerns and the urgent need to restart critical operations as soon as possible. Even with Pure Storage as the archive layer for legacy backup platforms, the recovery is much slower than recovering from the SafeMode Snapshots in Layer 1.

In addition, legacy backup platforms are vulnerable to attack and often a target for the threat actor. Where the backup layer can run on Pure Storage, the organization can use SafeMode to protect the indexes or catalogs associated with the backup solution and/or the backups themselves. This is why Pure Storage advocates a multi layered cyber resilience strategy. If a company is relying on a single resource such as legacy backups alone to recover from a cyberattack, they remain vulnerable.

Summary

With the increasing and evolving threat of cyberattacks, government agencies advise organizations to bolster their defenses by leveraging a visibility platform and implementing resilience. Pure Storage plays a vital role in both by providing a fast storage platform, multiple layers of storage, and features like SafeMode that can help businesses get back up and running quickly.

Learn more about how Pure Storage cyber resilient storage safeguards your data and your operations.

PS2732-02-en 05/25