Ransomware – Pure's Unique Mitigation Solution

Welcome to Part two of a series on the ransomware landscape and how Pure can help. If you didn't read Part 1, I'd recommend reading it first as it covers the ransomware landscape and general defense principles. Today we'll continue with more defense principles and how Pure can help.

Having spent a lot of time over the last few years presenting on the ransomware landscape and attack mitigation, I'm really excited by what Pure is announcing – a unique ability to mitigate the impact of ransomware attacks.

Simply put, Pure is now offering an industry-unique combination of Immutability Plus, simplicity, and high speed restore which can have a powerful impact on your ability to recover from ransomware attacks. This is possible due to FlashBlade™, Pure's purpose-built file and object platform that natively scales out and is built for throughput.

So, what's new? Immutability Plus via FlashBlade SafeMode is the key. This offers the ability to prevent backups stored on FlashBlade from being compromised by attackers, thus acting as a force multiplier on FlashBlade's existing simplicity and Rapid Restore capability.

Ransomware Attack Impact Mitigation – What Matters

Two recovery capabilities are key in mitigating the impact of a ransomware attack – reliability and speed of backup.

First, your data needs to be backed up AND your backups need to be protected from intentional, malicious deletion. To do this, the system receiving your backups needs to be simple and reliable (not requiring constant care and feeding) as well as immutable. In this case, immutability refers to the ability of a system to prevent changes or deletion of an object after it is created. Immutable Plus refers to the ability to prevent backup compromise even if your admin credentials have been compromised.

Second, your backup system must also be able to restore rapidly. In other words, if you can't restore backups fast enough to avoid major impact, do those backups exist from a practical perspective? Can your backup system restore rapidly enough to avoid a major organizational or financial impact in the event of a ransomware attack requiring large swathes of your datacenter to be restored from backup?

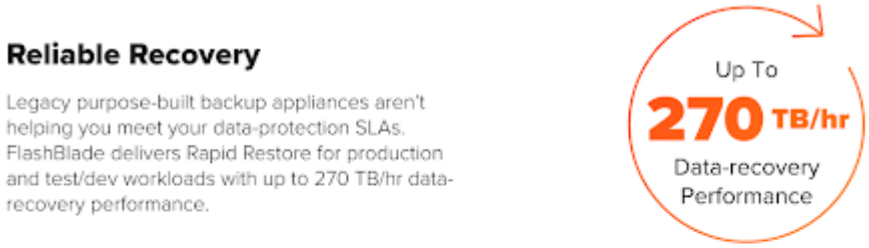
Let's make it a bit more real, albeit possibly painful. When is the last time you restored a large amount of data? How long did it take? One customer I spoke with recently had a restore after a ransomware attack that was going to take 60 days – not 60 hours, but 60 days. Clearly, this is unacceptable to business continuity.

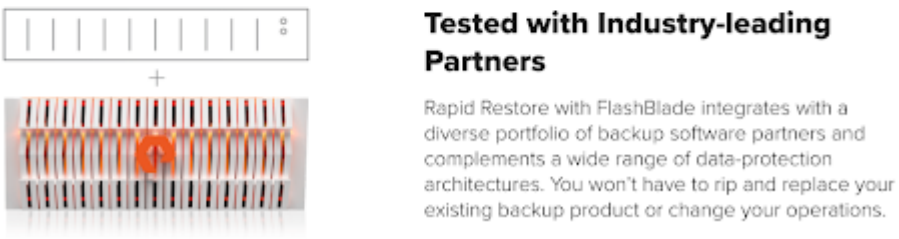
Where Does FlashBlade Fit?

To put it simply, FlashBlade brings a unique combination of:

- **Simplicity** – easy to set up, manage, expand, and integrate with backup software such as Commvault, Veeam, and Veritas NetBackup.
- **Immutability Plus** – to ensure your backups aren't compromised by attackers even in scenarios where admin credentials have been compromised.
- **Speed** – to restore quickly enough to actually matter.

Note: There's already a lot of great material on FlashBlade's simplicity and restore speeds so I won't go into depth. One fun speed anecdote – we've seen FlashBlade increase database restore speeds by 76x (yes, this is a real customer). This is an order of magnitude speed difference from alternative solutions and gives customers the ability to know they can restore quickly enough for their backups to actually matter.





However, I'd like to focus on Immutability Plus via FlashBlade's SafeMode – the capability which has direct impact in ransomware scenarios and is a force multiplier on FlashBlade's simplicity and speed. As

mentioned above, attackers are now targeting backup data – this is only logical.

SafeMode on FlashBlade is a direct answer to this issue and prevents ransomware attackers from deleting backups stored on FlashBlade. After being enabled, it takes an automated FlashBlade-wide snapshot that is kept for a customer-specified period of time and cannot be deleted by the customer or even anyone with admin access to the FlashBlade system. If you're concerned about running out of space, we're happy to discuss, along with how to handle unplanned high change rate scenarios (that aren't ransomware attacks).

Note: if you're concerned about ransomware/attack gestation period, let's chat – it's a legitimate concern but not one where what I'm describing here can help.

We've even specifically collaborated with several leading backups vendors to show how SafeMode would integrate for our joint customers. Even better, this is a capability that can be turned on without requiring re-architecture. We have video walkthroughs demonstrating this which we'll post soon.

Of course, this will require additional space on a FlashBlade system to maintain the snapshots over the amount of time you specify – we're happy to help with sizing to provide clarity around space required and resulting costs.

Am I being a bit vague here? Absolutely – there are doubtless many people around the world reading this blog post, maybe some with ill intent. If you'd like a more detailed walkthrough of how SafeMode works, how it is enabled, and protections against it being disabled, please reach out to your local Pure Storage sales team. They'd be happy to walk you through it in more depth.

What Next?

Right now, I truly believe FlashBlade has a unique combination of simplicity, Immutability Plus, and speed which has specific applicability to ransomware recovery scenarios. This is both based on my own experience and what I'm already hearing from customers.

If you'd like to learn more, listen to the Pure Report podcast or webinar which dives deeper into this topic.