Ransomware Is Getting Smarter. Here's How to Be Ready

Just the mention of *ransomware* is enough to send shivers down the spine of the most seasoned IT professional. Ransomware attacks are increasing at an unprecedented rate while the level of their sophistication continues to rise. This includes the use of credential-stealing methods and multi-stage attacks that can cause widespread disruption from a single initial exploit.

Ever-morphing to evade detection, these stealth attacks are now successfully targeting the last line of defense for organizations: data backups.

Attacks Continue to Surge

Unfortunately, cybercriminals haven't slowed this year. In fact, they've ramped up efforts, using a variety of methods to lure unsuspecting employees to click on malicious links or provide sensitive data to access systems. Remote teams and the use of non-business networks have expanded vulnerabilities, with the impact of attacks becoming more disruptive and costly.

With employees working from home, remote admins are under pressure, being tasked with ensuring physical devices, including mobile devices, are kept secure. Aware that these devices offer a unique opportunity to catch unsuspecting targets, attackers are increasingly targeting SMS login-verification tokens on both desktop and mobile.

In 2021, the average ransomware payment was $541,010, up from 2020's $312,493 average. Because the productivity and revenue loss from an attack can be far more costly than the ransom itself, many organizations simply choose to pay up and hope the attacker provides a key to unlock the data.

Fortunately, there's another option, and that's protecting your most precious assets: backups.

Backups Are Your Last Line of Defense

With no sign of ransomware attacks decreasing, safeguarding critical data has become more important than ever. However, even if you have a multi-layered defense in place, skilled hackers now have the capabilities to access backup data, backup catalogs, and even storage array snapshots.

So, you may be asking if there's anything else you can do other than throw your hands up in frustration? The simple answer is yes.

It starts with backing up data and protecting those backups from an attack with a system that is simple to use, reliable, and perhaps most importantly, immutable. Along with protecting data from deletion, you also need a rapid way to restore it once an attack has occurred. This is where Pure FlashBlade®'s SafeMode™ snapshots fit in.

In this on-demand session, learn how Pure FlashBlade can enable you to:

- Gain simplicity, speed, and immutability to mitigate data loss from ransomware attacks.
- Prevent attackers from deleting, modifying, or encrypting snapshots of your backup data.
- Speed up data recovery, even if both your data and data backup are attacked.

FlashBlade is an innovative approach to mitigating data loss from ransomware attacks. With SafeMode snapshots, a built-in FlashBlade feature, your data is safe. Even administrators can't delete the SafeMode snapshots. Policies can only be modified with an authorized designee working with Pure Support. Put another way, even if a ransomware attack encrypts your data and your data backup, FlashBlade SafeMode snapshots have you covered with valid, usable data copies. And unlike legacy backup appliances that are

slow at recovery, FlashBlade dramatically speeds recovery.*

Bringing It All Together

While it’s important to have layers of defense to prevent a ransomware attack, it’s also crucial to have the ability to effectively recover if you are attacked. With FlashBlade’s SafeMode snapshots, you get a simple, yet effective way to protect your data and rapidly restore it—just what you need in a ransom scenario.

Learn how Pure can protect your data from ransomware.

**Restore speeds may vary based on your network.*