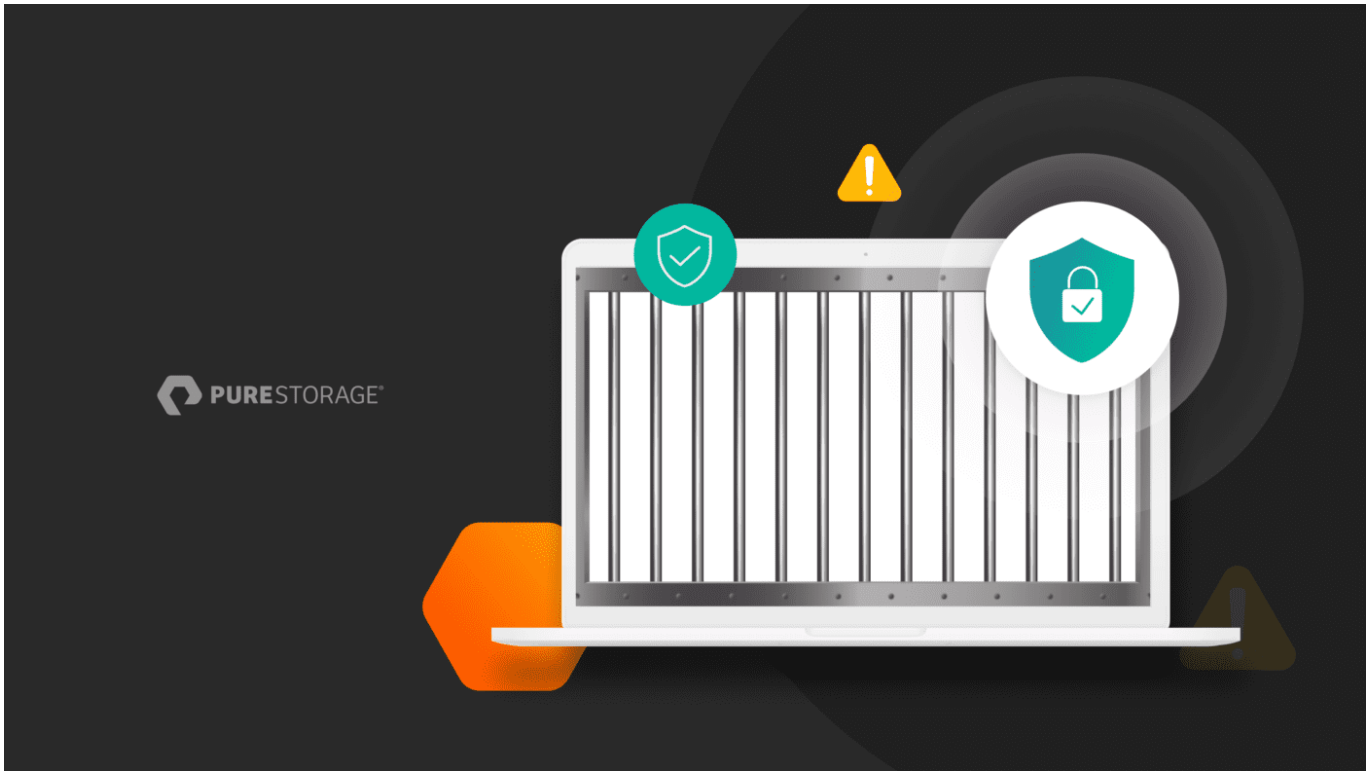
Escaping Ransomware Jail: Protection Before, During, and After an Attack



Ransomware isn't a new threat, but it's certainly having a moment. Blockchain analysis company Chainalysis reports that ransomware victims in the United States paid out nearly $602 million to attackers in 2021. In its 2022 Cyber Threat Report, SonicWall reported 623.3 million ransomware attacks in 2021 worldwide – up 105% from 2020 and more than three times since 2019.

Cryptocurrency is another factor for ransomware's skyrocketing climb. Ransomware operators, like many criminal actors, prefer the blockchain-based currency as a method of payment. Cryptocurrency transactions can happen quickly. And because cryptocurrency is pseudonymous, these transactions are difficult—although not impossible—to trace.

The volatile political state of affairs worldwide is also prompting ransomware attacks. Costa Rica fell victim to multiple attacks this year, potentially related to the Russian-Ukraine war. The attacks crippled government services, caused international trade issues, and led the president to declare a state of emergency.

Another reason for the increase in attacks? Ransomware campaigns are easy to carry out. The dark web is home to many Ransomware-as-a-Service (RaaS) "vendors"—like REvil, who was behind the July 2021 global attack that hit up to 1500 global businesses. These groups sell or lease malicious software kits and services to anyone who wants to launch a cyberattack, making the RaaS business model an efficient launchpad for

any enterprising cybercriminal looking to start his or her own ransomware campaigns. TrendMICO recently reported a jump in the number of for-hire RaaS and extortion groups, such as LockBit, Conti, and BlackCat, up 63.2% in Q1 2022 from the same period in 2021.

Ransomware Operators Target Old Problems in IT Environments

Ransomware is a thriving and quickly maturing business. The White House has warned businesses that they need to buckle up and button down in anticipation of more ransomware activity to come. Lindy Cameron, the head of the National Cyber Security Centre (NCSC), recently issued a similar warning to organizations and citizens across the Atlantic. Cameron warned that ransomware is the top cybersecurity threat to the United Kingdom's national interests.

It's wise to heed these warnings because slowing the growth of ransomware, at least in the short term, is impossible. In a Pure Coffee Break Session, Escaping Ransomware Jail: Protection Before, During, and After an Attack, I talked prevention, defense, and mitigation with Pure's CTO, Andy Stone.

Ransomware competes with the core inefficiency of modern IT. No organization today, especially those with complex IT environments filled with legacy components, can say with confidence that they have everything buckled down and buttoned up. Especially when it comes to their data.

Ransomware, like most cyber threats, targets and exploits vulnerabilities and other security gaps in legacy, complex IT. Ransomware operators stealthily infiltrate systems, wait around about 40days on average to encrypt data, and then—bang!—demand their ransom. The savviest actors make it as difficult as possible for organizations to refuse payment by compromising backups, erasing snapshots, and more, as part of their attack.

Many of the basics, like updating and patching systems, segmenting networks, and creating and testing viable incident response plans, can help organizations avoid becoming imprisoned in ransomware jail. Good hygiene is a lofty goal. It's challenging and expensive, but you make yourself a much more difficult target. (Andy Stone covered a lot of these basics in his blog post on building a multilayered defense to protect against the ransomware threat.)

Another key security component is consistent logging across the entire environment. Recording events in a fast backend means accelerated analysis and mobilization of threat hunters before bad actors can launch a full attack, and an accurate restore point if they do get through.

But perhaps the most significant weapon an organization can wield against ransomware attackers is to execute a rapid recovery following an attack. While a ransomware attack will still sting and disrupt business, accelerating recovery will lessen the organizational, financial, and reputational pain that often follows an encounter with this high-impact threat.

The Keys to Rapid Recovery Include Simplicity and Immutability

If your business is hit with a ransomware attack, you want to be 100% confident that data protection is in place. You want zero chance that your backups or data protection methods have been compromised or deleted. That kind of confidence comes from implementing a modern data protection approach that

eliminates the complexity of keeping data safe. That foundation can help you expedite data recovery when needed and offer peace of mind that your critical data is actually protected.

With a tiered architecture, you'll build resiliency by protecting your data and enabling recovery throughout its lifecycle, lessening the impact of potential attacks. Immutability for your backup data and backup metadata is also essential for rapid recovery. With immutability, your critical data is always ready for restoration. Getting your data into an immutable state hinges on backing up your files frequently with snapshots that can't be modified, encrypted, or deleted.

SafeMode™ snapshots take Pure's core snapshot immutability even further. They prevent attackers from doing the final deletion of data on a storage array even if they've compromised administrative credentials. Think of SafeMode as a form of segregation of duties for your business-critical data. It provides a permissions "air gap," or a logical separation of key controls. And with just a few clicks, you can restore your data with speed and at scale. While backups can take time, snapshots can be recovered in milliseconds.

Keep in Mind: Cleanup Can Take Time

An hour of downtime can cost millions. While data backups and recoverability are essential to rebound from a ransomware attack, organizations still need to take proactive steps to ensure the recovery will be swift. If they can't move quickly after they've been hit, and can't afford to wait weeks or longer to recover, they could get desperate and actually pay the ransom. Sadly, even paying a ransom may result in receiving a decryption tool that takes days or weeks to run.

You don't want to do this. And the government doesn't want you to do it either. In response to the rising number of ransomware attacks, the U.S. Treasury Department and its Office of Foreign Assets Control (OFAC) advised businesses that ransom payments made to sanctioned ransomware operators are considered illegal. So, your business could potentially get *fined* by the government on top of paying the ransom to attackers. Ouch. If the ransomware attack is especially severe, you may need to go through the data restoration process a few times. Meanwhile, your security teams need to get rid of rootkits, address vulnerabilities, and shoulder through other cleanup tasks.

Thorough cleanup from a ransomware attack is an absolute must. A recent study found that among the 80% of organizations that paid ransom demands following a *second* ransomware attack, nearly half (46%) believed that the hackers responsible for the *first* attack had hit the business a second time.

Ransomware isn't going away anytime soon. It's "not if but when." Your organization needs to prepare for cyberattacks—and stay ready. The resilience you'll gain from a modern, simpler, and more robust and reliable approach to data protection can be a powerful antidote to ransomware disruption. And it can help your business stay out of ransomware jail.

And, stay out of ransomware jail with the Pure Storage Evergreen//One™ Ransomware Recovery SLA—the first STaaS solution to offer shipment of clean arrays after an attack.

Color orange–gradient

Color orange–gradient

Color orange–gradient

Color orange–gradient

Color orange–gradient