RFP GUIDE

Ransomware Protection

PURESTORAGE®
Uncomplicate Data Storage, Forever

Table of Contents

Overview

What Is Ransomware?

Ransomware is a type of malware that encrypts your files and requires payment of a ransom in return for restoring access to your data. There's no guarantee that a perpetrator will honor the terms of the ransom, however, so preventing ransomware through cybersecurity best practices and routine snapshots is your best option.

How Does Ransomware Work?

Like all malware, ransomware must be downloaded onto your machine or network for it to gain access to your data. The most common way to contract ransomware is through a downloadable attachment delivered via a phishing email, but thumb drives, compromised apps, and infected websites are also viable attack vectors.

Once downloaded and executed, ransomware encrypts the host system's files, and renders it computationally inaccessible without the right decryption key. Typically, a ransom note is presented to the owners of the compromised system with details on how to make payment to have their files released. More sophisticated ransomware, such as NotPetya, can deliver its payload without relying on human error, but instead, it exploits critical software vulnerabilities in your system.

Are Attacks Increasing?

Ransomware attacks have become such a common occurrence today that it's no longer a matter of how many cyberattacks happen per day—it's now measured in attacks per second. What was once a problem for only large and prominent organizations is now a problem that every organization needs to prepare for, no matter their size.

According to research conducted by Cybersecurity Ventures, 2021 saw a ransomware attack every 11 seconds. And by 2031, it is expected that an attack will occur every 3 seconds, ballooning the total damages caused by malware, including downtime costs, recovery time, and lost revenues, to grow 15% per year over the next five years.

How Do You Prevent Ransomware Attacks?

Common methods to prevent ransomware attacks include:

- Keeping your operating system and technology stack up to date to stay ahead of known exploits and vulnerabilities
- Investing in cybersecurity (e.g., InfoSec training, network security audits, and vulnerability testing)
- Controlling access to secure files and data through admin rights and privilege management
- Backing up files through frequent snapshots and other data protection methods

In an age where organizations are so dependent on their systems and data to operate, being able to recover what you need—when you need it—is essential. When your systems and data are offline, every minute and every second count. It is important to think out and plan for what happens when a disaster or ransomware does occur.

There are a variety of ransomware solutions in the market today. Typically, these solutions fall into three categories:

- **Prevention and Alerting:** These solutions prevent unauthorized access to your networks and systems. They may also prevent the installation of malware and notify IT of an alert.
- **Eradication:** These tools and functions help isolate and remove malware. They may also help close access points that enabled unauthorized access to the systems and network.
- **Remediation and Mitigation:** These solutions restore and recover systems and data that have been infected or encrypted.

In this guide, we'll focus on ransomware remediation and mitigation.

Data Protection Is Not Enough

While most organizations have some sort of backup and recovery or data protection solution in place today, it may not be enough. Not long ago, it was possible to simply restore a backup over an infected or encrypted file or system and resume business as usual.

But hackers have caught on and modified their tactics. Today, hackers frequently penetrate an environment weeks or months before launching an attack. The hackers are known to target backups and archives and corrupt and destroy them before they launch their encryption attacks. This greatly increases the chance that a ransom will be paid to decrypt a system.

Being able to ensure your most critical data and applications are recoverable is the best insurance you can have.

Why should you evaluate your ransomware remediation and mitigation plans and solutions?

- Concern over ransomware is the number one driving factor now and for the foreseeable future. Backups need to be protected.
- The ability to restore data and applications quickly to avoid costly downtime. Any recent recovery event that did not go as planned can drive quick action (e.g., a database recovery took far too long). Ransomware concerns also drive the need for faster recovery.
- Many organizations experience dissatisfaction with their current backup product. When combined with the need for a ransomware solution, this presents an excellent opportunity to bring in a new backup solution and change the entire environment, both software and storage.

Understanding What Matters for Your Organization

Before you begin reviewing different solutions, it is important to perform a self-assessment to determine what data is critical to the business, how much data is deemed critical, what applications are most important for the organization, and what service level agreements (SLAs) your organization has set for recovering after an outage.

After a disaster, the main objective should be to restore the business-critical data and applications first so business can resume quickly. Non-critical data and systems need to have different SLAs than the business-critical items.

Ransomware Solutions

While many vendors will try to bundle different feature sets and tools together in an attempt to create an end-to-end solution, this may not be the best strategy. Look for vendors that offer differentiated solutions in prevention (stopping an attack from happening), eradication (stopping an attack after it has begun or spread ransomware, and removing it from your environment), and remediation or mitigation (restoring and recovering after an attack).

Look for solutions that your IT staff can understand and operate to help you meet your organization's SLAs. Once you have selected your solutions, create plans, document the steps and procedures, and practice them.

In this guide, we will focus on recovering after an attack. Questions about what you will be able to recover, how, and within what time frame should be part of every discussion when choosing a ransomware remediation solution. This is a serious subject and needs careful consideration for all organizations, regardless of the size.

Integration with Data Protection Solutions

Backups safeguard critical data against common scenarios such as natural or human-made disasters, data corruption, or accidental deletions. However, ransomware attacks can stress existing data protection infrastructure that may be built on legacy architectures, such as disk and tape, more than expected.

If you're already struggling with meeting recovery SLAs, a ransomware attack can exacerbate the situation with additional downtime. Next, your backup systems and data can be compromised, which could require you to reinstall and reconfigure your backup solution, before even contemplating data recovery. According to Enterprise Strategy Group (ESG), 87% of organizations are concerned their data backup copies could become infected or corrupted by ransomware attacks.

Recovery Strategy

While recovering from an attack, there are two key considerations: are there valid, usable data copies that were safe from the attack that can be used for backup? And what is the fastest possible recovery? After an attack occurs, the best way to remediate the damaged or compromised data is to restore backups over the infected systems and data. When planning out a recovery plan, two capabilities are key in mitigating the impact of a ransomware attack: reliability and speed of recovery.

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, why do those backups exist? Can your backup system restore quickly enough to avoid a major organizational or financial impact in the event of a ransomware attack? How does it hold up to restores involving large swathes of your data center? Can your storage and network handle a large-scale recovery?

If your organization has an SLA measured in hours or days, you may want to calculate how long it would take to recover from a large-scale attack to determine if your infrastructure can achieve its SLA goals.

Questions to consider:

- When was the last time you restored a large amount of data?
- How long did it take?
- What are your SLAs for recovery?
- Where is the bottleneck in your infrastructure?
- Can you achieve SLA targets with your solution?

A good RFP helps create a level playing field among the different solution choices and vendors and makes comparison and selection easier. A common challenge in developing an RFP is to know what questions to ask to help match your requirement with vendor offerings.

To help you through that process, we've designed a set of criteria that you can add to your RFP process for ransomware remediation or mitigation. They are based on real-world experience with proven ransomware architectures. These questions can help you highlight a storage system.

Use the vendor responses to weigh future needs, both known and unknown, against vendor claims and capabilities. This guide is not meant to be exhaustive, but to help the key requirements of a ransomware remediation solution.

Sample RFP Questions

Section 1: Data Protection Solutions

Describe the system's data protection abilities.

- Describe the components of your solution.
- What data protection applications can you integrate with?
- Do you offer role-based access control (RBAC)?
- How do you stand up disaster recovery copies?
- Does your solution replicate?
- Is your solution on-prem, hybrid, or cloud-based?
- What purchasing models do you offer?
- What upgrade or trade-in programs do you offer?
- What reporting is included in the solution?
- What certifications are part of the solution?
- With what is your solution compliant with?
- With what protocols does your solution work with?
- Does your solution require specific hardware?
- How are updates installed?
- How do you protect against deletion, ransomware, and intentional deletion?
- With what third-party ransomware detection providers can you integrate with?
- Does your solution provide orchestration for recovery from zero-day attacks?
- Can your solution provide snapshot, clone, and replication capabilities to capabilities to secure data from malware, accidental deletion, data corruption, technology failure, or site failure?
- Does your solution provide backup immutability?
- Describe options for creating snapshots, replicating data, and managing malware.
- Describe any additional security capabilities that differentiate your solution.

Section 2: Backup

Describe the system's backup capabilities

- Describe how the solution will protect your organization from a ransomware attack.
- What workloads can be protected?
- What type of machines can you back up?
- Do you use full, incremental, or differential backups?
- Do you use deduplication? What type is used?
- How is data backed up?
- How do you ensure recoverability?
- How often are backups or snapshots executed?
- Can your solution create immutable backups?
- How do you ensure immutability?
- Does your solution offer automated recovery?
- Does the solution offer immutable backups or snapshots?
- What is the process for creating an immutable backup or snapshot?
- Do the immutable snapshots reside inside or outside of the IT environment?
- Does your solution offer any testing of backups?
- Does your solution tier backup data?
- How do backups get safeguarded from tampering or deletion?

Section 3: Recovery

Describe the solution's recovery abilities.

- What recovery time objective (RTO) can your solution offer?
- Does your solution offer automated failover?
- Does your solution offer instant recovery?
- How does an immutable snapshot or backup get recovered?
- How does deduplication affect the recovery times?
- How is the data restored?
- How do you recover your immutable copies?
- What is the restore rate you expect to see?
- How much data can the system restore per 24 hours?
- What level of granularity of restore is offered? (file, point in time, incremental, differentials, etc.)
- How do you failover to cloud-based storage?
- For cloud-based storage, is there an egress charge to migrate data back on-premises?

Section 4: Infrastructure

Describe the infrastructure of your solution.

- To achieve a mass restore, what type of storage does your solution need? What speed network is required?
- Where are backups stored? Can they be stored in the cloud?
- What amount of storage is needed?
- What amount of storage is needed for immutable backups?

Other Resources

About Pure Storage Ransomware Solutions

Pure has always been a pioneer, from the all-flash data center to the most modern data protection solutions, and our Evergreen™ subscription models.

Pure offers everything-as-a-service for flexible consumption and cloud economics. Simple cloud mobility lets you seamlessly extend your data services into the cloud.

Pure delivers simple setup, effortless operations, and expansive integrations. But it's the white-glove treatment of customers and partners that sets Pure apart.

According to ESG, 79% of organizations experienced at least one attempted ransomware attack within the last 12 months. More incredible, 86% of organizations victimized by an attack failed to recover all their data after paying a ransom. It's time to prepare. Identify your vulnerabilities and see how Pure can help. Are you ready to fight back?

Backups safeguard critical data against common scenarios like disasters, data corruption, or accidental deletions. But ransomware can stress existing data protection infrastructure even more. Pure Storage SafeMode™ Snapshots, available with both FlashBlade//S® and FlashArray™, provide immutability to protect data backups from ransomware attacks.

Secure Backups Against Ransomware: SafeMode Snapshots protect backup data and metadata by creating a secure copy.

Ransomware can't eradicate, modify, or encrypt SafeMode Snapshots, even with admin credentials. In an unpredictable world, you're covered 24×7×365.

Snapshots with All-flash Storage Simplicity: Snapshot scheduling and retention are fully customizable and easy to deploy. Expand and upgrade without disruption. And there's no need to change your backup software. Simply set it and forget it.

Move at the Speed of Business: Legacy disaster-recovery solutions are slow. FlashBlade smashes your recovery-point and recovery-time targets with petabyte-scale data-recovery performance for production and test/dev workloads.

Get Multi-protocol Support: The addition of native Server Message Block (SMB) support makes backups faster and more efficient. SMB support delivers high performance for Windows applications and gets greater coverage for business needs and use cases.

For More Information

- Learn more about ransomware protection.
- Discover how to mitigate the effects of ransomware with SafeMode.
- Read how the City of New Orleans and COCC depend on Pure to prevent damage from ransomware.

purestorage.com

800.379.PURE

PURESTORAGE®
Uncomplicate Data Storage, Forever