AvePoint

Ransomware Recovery Warranty - FAQs

What is AvePoint's Ransomware Recovery Warranty?

AvePoint's Ransomware Recovery Warranty for eligible customers covers up to $1 million in recovery incident expenses incurred while attempting to recover data protected by the eligible solution. When coupled with AvePoint's Cloud Backup Solution, the add-on Ransomware Warranty offers enhanced resiliency, making it easier to recover from a ransomware attack while also giving you peace of mind. AvePoint's warranty provides added assurance that your data is protected and secure.

Who qualifies for the AvePoint Ransomware warranty?

To be eligible for the warranty, a customer must purchase the AvePoint's Ransomware Warranty with a subscription to an AvePoint Cloud Backup service.

What expenses are covered by this warranty in the event of a Ransomware Incident?

Any fees and expenses directly related to the unsuccessful recovery, restoration, or recreation of customer data protected by the eligible solution, up to the Payment Cap, will be covered by the warranty in accordance with the Agreement.

How long is this offer covered for customers (i.e. contractual term)?

The warranty runs concurrently with the Eligible Solution's initial subscription term, unless terminated earlier in accordance with the Agreement. If the customer fails to comply with the Agreement, it will no longer be eligible for the warranty.

What is the warranty coverage?

Subject to the terms and conditions provided for in the Agreement, AvePoint will reimburse Customer's Recovery Incident Expenses directly resulting from the Recovery Incident in the amount of one dollar ($1.00) per gigabyte of unrestored customer data protected by AvePoint's Cloud Backup service, up to a maximum amount not to exceed one million dollars ($1,000,000.00) ("Payment Cap"), calculated based on the amount of data Customer protects using the Eligible Solution software.

What ransomware incidents could trigger this warranty?

Any event where a third party (not affiliated with or acting on behalf of the customer, i.e., not a customer's employee, contractor, vendor, etc.) results in the encryption of customer data residing in AvePoint provided storage with a demand for payment to decrypt the encrypted files where such customer data cannot be recovered. The customer must also be in compliance with the terms and conditions contained in AvePoint's Ransomware Recovery Warranty Agreement, including all of the data security best practices and other requirements provided for therein.

What are some examples of events that are not covered by the warranty?

The following events resulting in a ransomware incident are examples of what is not covered by the warranty:

1. Any fraudulent, criminal, negligent or malicious act by or on behalf of the Customer - for example: malware introduced by the Customer's employees, vendors, and contractors
2. Data Customer backs up using products other than the Eligible Solution will not count toward any Payment obligation under this Warranty

Are the terms and conditions of the warranty negotiable?

No. The warranty terms and conditions are non-negotiable. Read the complete Terms and Conditions here.

Are pre-existing events covered by the warranty?

No. Both the ransomware and recovery incidents must take place during the warranty period.

What are the data security best practices that need to be implemented?

Customers must utilize industry data security best practices to be eligible for coverage under AvePoint's Ransomware Recovery Warranty. As provided in the Agreement, this includes, but is not limited to, areas of data health, user access, data encryption, application access, and API security.

How do Customers process a claim?

If you are an existing AvePoint customer and purchased the Cloud Backup Ransomware add-on warranty and were hit by a ransomware attack, email warranty@avepoint.com and provide the associated tenant email address used for Cloud Backup. The AvePoint team will open a case and reach out to gather additional details related to the incident.