BACKUP VALIDATION

VALIDATION REPORT

RECOVERYPOINT

Protecting Performance

Recovery Point's Backup Validation Report informs you of the **risks associated with your backup data**.

The Backup Validation process takes the most recent backup copy that Recovery Point has of your systems, rehydrates it into an isolated environment, and confirms the restore process was successful. Once restored, the file system is scanned for malware and other indicators of compromise (IOC).

Infected Systems

These are systems that were restored correctly and, upon scanning, were **found to have malware or suspicious activity** flagged within their file systems.

Next Steps: Provide the report to your security team for further analysis with Endpoint Detection & Response (EDR) or other tools.

System	Status	Threat Type	File
MAILSRV01	Infected	Malware	C:/mail.zip
BACKUP03	Infected	Malware	E:/file1.trz

Failed Recovery

These are systems that failed the restoration test and were **not able** to have the contents scanned for malware.

Next Steps: Verify locally that the backups or replicated image exists, and can be successfully recovered within your environment.

System	Status	Technology
CRMWEB01	Failed	Veeam Backup
PRINTSRV03	Failed	Veeam Backup

Passed Validation

These are systems that were restored correctly and, upon scanning, **no malware or suspicious activity** was found.

System	Status	Technology
APPSRVR01	Clean	Veeam Backup
ERPDBS01	Clean	Veeam Backup

Recovery Point's **Backup Validation** service provides information that can help you to make **informed decisions**.

In the event of a Cyber Security Incident declaration, if you are supported by the Recovery Point Systems *Managed Resiliency*, we will work closely with both you and your chosen Cyber Response partner to help you recover your IT systems as quickly as possible.