

InfiniSafe Cyber Detection: 7 Critical Post-Attack Insights

How to Enable Fast Recovery from Ransomware

InfiniSafe Cyber Detection is a key component in a post cyber attack recovery strategy. By having a clear understanding of the state of your data over time, you will have a clear vision of what was affected, and what good versions you can quickly recover to, nearly instantaneously. InfiniSafe Cyber Detection is a critical part of Next Generation Data Protection and Recovery capabilities that are built around cyber security and recovery first strategies. Aligning, orchestrating and automating storage cyber resilience is easy with InfiniSafe’s powerful capabilities.

1

When the alert was detected and what type was detected.

2

High-level description of what happened.

3

How many files and hosts are suspected to have been corrupted.

4

What files were added, deleted or modified alongside the attack.

5

When the selected files were modified.

6

Detailed listing of files that were impacted.

7

A view of Clean and Alert snapshots with the associated “Alert” for each suspect snapshot.

The screenshot displays the InfiniSafe Cyber Detection interface. At the top, there are navigation tabs for Alerts, Hosts, Snapshots, and Settings. The 'Alerts' tab is active, showing a 'New Alerts' section with 7 critical alerts. A table lists these alerts with columns for Severity, Start Time, Most Recent, Type, Status, and Policy Name. Below this, a detailed view of an alert is shown: '3/8/2024 3:36:45 PM: Infection found'. It includes a description: 'Infection was found in the backupsets. The file retains its original name and file extension, but the content has been encrypted.' and provides the Policy Name and Engine ID. The interface also shows 'Alert Configuration' and a summary of 78505 suspect files across 1 host. Three donut charts are present: 'Hosts' (1 host), 'Extensions' (listing various file types like .pdf, .jpg, .html, etc.), and 'Modified Times' (showing a peak on Wed Nov 15, 2023). A table below these charts shows a list of files with columns for Name, Host, Owner, Last Modified, Accessed, Size, Directory, and Last Known Snapshot ID. At the bottom, a detailed table shows snapshots for a specific host (ps-wt-108), with columns for Status, Host, ID, Type, Exceptions, Start of Snapshot, Start of Scan, Scan Duration, and Last Known Snapshot ID. The table shows a mix of 'Clean' and 'Alert' snapshots. A '7' is overlaid on the table to highlight the 'Alert' snapshots.