Increasing Ransomware Resiliency

Gain complete infrastructure awareness with NetBackup IT Analytics.

Overview

Ransomware is a growing threat for enterprises, and media headlines reflect its devastating impact. Company data is being held hostage by cybercriminals, and stakeholders are forced to choose between paying the ransom or having their company's data erased or exposed. The global cost estimate for companies afflicted by ransomware will soon exceed $20 billion. Figure 1 shows the significant effect ransomware is having—or will have—on organizations and the economy.

950 U.S. organizations fell prey to ransomware in 2019

$20B Ransomware will cost organizations globally over 20 billion by 2021

$6T Cybercrime is expected to make a $6 trillion impact in 2021

Figure 1: Data points illustrating the impact of ransomware.

Like many organizations, yours probably maintains an increasingly complex IT environment you must manage within the constraints of reduced resources. You want assurance your environment is safe, secure and capable of overcoming the threat of ransomware while being able to reduce the day-to-day complexity of monitoring and maintaining backup and storage configurations.

At Veritas, we recommend a three-part approach to reducing the threat of ransomware—protection, detection and recovery. There are numerous solutions on the market to help organizations detect and prevent the infiltration of ransomware, but what happens if ransomware makes its way past your organization's frontline defenses despite your best efforts? What if you pay the ransom and don't receive the decryption key?

You need a recovery plan that ensures you can reliably restore data to the last known good backup if and when ransomware strikes. This includes the ability to effectively visualize your organization's entire infrastructure to focus on critical applications.

End-to-End Infrastructure Awareness

In five minutes or less, NetBackup™ IT Analytics can help your company understand the breadth and depth of a ransomware attack so you can recover strategically. With the correlated environmental insights of NetBackup IT Analytics—on-premise, in the cloud, data protection and storage—alerting and reporting is comprehensive and easy to set up. You'll have the insights needed to make informed decisions in the face of an attack with these NetBackup IT Analytics reporting options:

- Risk Mitigation Analysis (see Figure 2)
- Sources with Consecutive Failures (see Figure 3)
- Sources with No Recent Backups (see Figure 4)
- Backup Failures by Application (see Figure 5)

In addition, NetBackup IT Analytics Ransomware Scorecard measures ransomware resilience and readiness of data protection and recoverability.

When the worst does happen, are you sure you have a good backup? If so, how do you know? As good as vendors have made their backup software, most are not 100 percent reliable for three reasons:

1. There are false positives; backups appear successful but wouldn't result in a full restore
2. There could be hosts your backup software knows nothing about
3. Most organizations have multiple solutions comprising a data protection strategy on-premises and in the cloud; to know if a backup is successful (or not), you must query every data protection solution

Identifying False Positives

Just because a backup job is successful doesn't mean you can restore the image when it's needed. NetBackup IT Analytics creates a baseline of known successful backups and compares future backups to the discovered baseline. The analytics software automatically spots false positives like job duration variations, image size variations and policy/configuration changes. NetBackup IT Analytics then displays these anomalies in high-level summary graphs to help you assess the size of the risk or in more detailed, actionable tables to help you clean up the environment. To make the process more efficient for you, NetBackup IT Analytics automates the process of creating anomaly tickets. You can then review these tickets in order to pinpoint if, when, and where an incorrect backup occurred, reducing the likelihood of experiencing a failed restore.
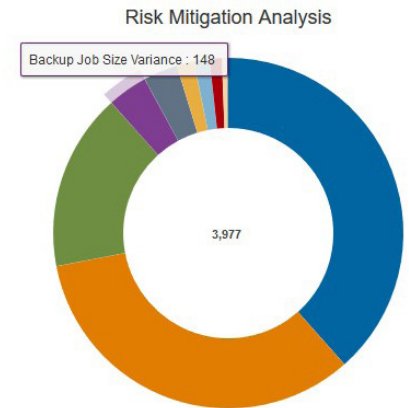
Risk Mitigation Analysis

Backup Job Size Variance : 148

3,977

Figure 2: An example of a Risk Mitigation Analysis report in NetBackup IT Analytics.

Discovering Hosts and Backups

Backup software can't find failures for hosts or virtual machines (VMs) that aren't configured. NetBackup IT Analytics discovers all hosts from your infrastructure and automatically compares all discovered hosts with the hosts known by the backup software.

Figure 3: An example of a Sources with Consecutive Failures report in NetBackup IT Analytics.

NetBackup IT Analytics flags hosts that are completely missing from the backup solution(s) as potential risks. It can also show any hosts with no recent backups (see Figure 4). In both scenarios, NetBackup IT Analytics can interrogate CMDB systems like ServiceNow and provide similar results.

Figure 4: An example of a Sources with No Recent Backups report in NetBackup IT Analytics.

Classifying Data by Importance

It's also important to be able to classify backups by application and importance to your business. You need to know every single host and database that encompasses each application. With NetBackup IT Analytics, your company can build dashboards to view the restorability of every single application.
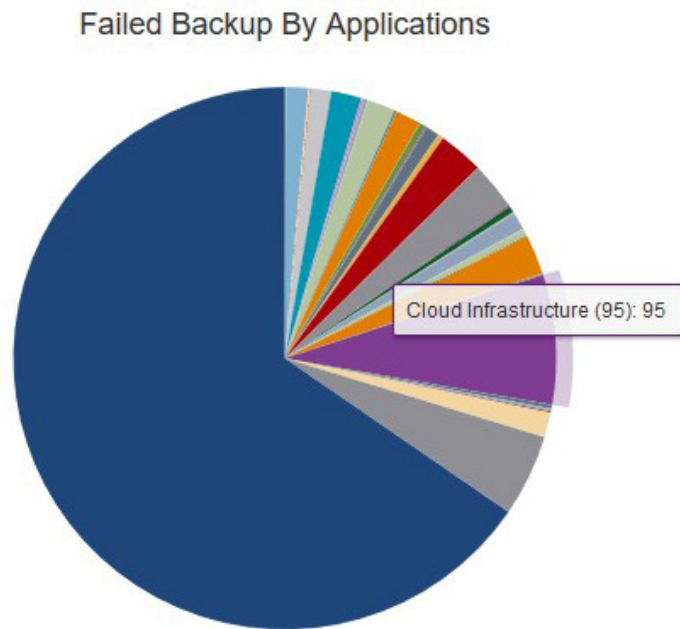
Failed Backup By Applications

Cloud Infrastructure (95): 95

Figure 5: An example of a Failed Backup by Applications report in NetBackup IT Analytics.

Summary

Although we hope your company never experiences a ransomware attack, we want to ensure you're ideally prepared to take on the threat with confidence in recovery in the event you do. NetBackup IT Analytics can support your recovery and detect future occurrences.

Interested in learning more about NetBackup IT Analytics? Check out www.veritas.com/netbackup-it-analytics.

About Veritas

Veritas Technologies is a global leader in data protection and availability. Over 80,000 customers—including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact
information visit:
veritas.com/company/contact