Increasing Ransomware Resiliency

Gain complete infrastructure awareness with APTARE IT Analytics

VERITAS

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 cost estimates for companies afflicted by ransomware are reaching $20 billion. Figure 1 shows the significant effect ransomware is having—or will have—on organizations and the economy.

950

In 2019, over 950 U.S. organizations fell prey to Ransomware.

$20B

Ransomware will cost organizations across the globe over 520 billion by 2021.

$6T

In 2021, general cybercrime is expected to make a $5 trillion total impact.

Figure 1: Data points illustrating the impact of ransomware.

Like many organizations, yours likely maintains an increasingly complex IT environment that you must manage within the constraints of reduced resources. You want assurance your environment is safe and secure—capable of overcoming threats like ransomware—while also being able to lessen the day-to-day complexity of maintaining and monitoring 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, APTARE™ 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 APTARE—on-prem, in the cloud, data protection and storage—alerting and reporting is comprehensive and easy to set up. In the face of an attack, you'll have the insights needed to make informed decisions with these APTARE reporting options:

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

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. APTARE 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. APTARE 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, APTARE 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.

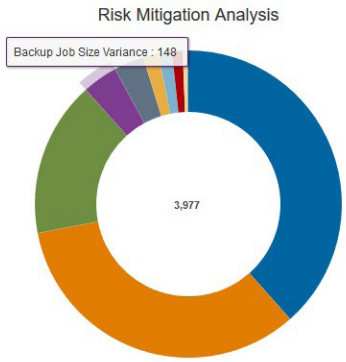

Figure 2: An example of a Risk Mitigation Analysis report in APTARE.

DISCOVERING HOSTS AND BACKUPS

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

Sources Consecutive Failure *Jul 1, 2020 7:06:22 PM*

Total Rows:57

Backup Server	Source Name	Source Type	Message	Today	Yesterday	Day 3 Status	Day 4 Status	Day 5 Status	Day 6 Status	Day 7 Status	Day 8 Status	Day 9 Status	Day 10 Status	Day 11 Status	Day 12 Status	Day 13 Status	Day 14 Status
effingham	five		Failed Backup Since Last 14 days	No Backup	Failed	Failed	Failed	Failed	No Backup	No Backup	Failed	Failed	Failed	No Backup	No Backup	No Backup	No Backup
everest	cheryll		Failed Backup Since Last 14 days	No Backup	No Backup	Failed	Failed	Failed	Failed	No Backup	Failed	Failed	Failed	Failed	Failed	Failed	Failed
latova	arrow		Failed Backup Since Last 14 days	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	No Backup	No Backup	No Backup
latova	ashley		Failed Backup Since Last 14 days	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	No Backup	No Backup	No Backup
latova	ashuelot		Failed Backup Since Last 14 days	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	No Backup	No Backup	No Backup
latova	auqlaize		Failed Backup Since Last 14 days	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	No Backup	No Backup	No Backup
latova	barkers		Failed Backup Since Last 14 days	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	No Backup	No Backup	No Backup	No Backup
latova	buffalo		Failed Backup Since Last 14 days	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	No Backup	No Backup	No Backup
latova	laqunitas		Failed Backup Since Last 14 days	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	No Backup	No Backup	No Backup
latova	marchington		Failed Backup Since Last 14 days	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	Failed	No Backup	No Backup	No Backup

Figure 3: An example of a Sources with Consecutive Failures report in APTARE.

APTARE 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, APTARE can interrogate CMDB systems like ServiceNow and provide similar results.

Sources with No Recent Backups *Jul 1, 2020 7:07:55 PM*

Total Rows:1,530

Source Name	Source Type	Product	Primary IP Address	Host Type	Days Since Last Backup	Last Backup	Job Status	Job Type
cahaba		Veritas NetBackup	[redacted]	Other	47	May 15, 2020 2:40:53 PM	Failed	Full Backup
chilikadrotna		Veritas NetBackup	[redacted]	Other	44	May 18, 2020 7:00:54 PM	Failed	Full Backup
macao		IBM Spectrum Protect (TSM)	[redacted]	Other	28	Jun 3, 2020 11:37:42 PM	Successful	Incr Backup
lucia		IBM Spectrum Protect (TSM)	[redacted]	Other	28	Jun 3, 2020 11:55:05 PM	Successful	Incr Backup
opasatika		IBM Spectrum Protect (TSM)	[redacted]	Other	15	Jun 16, 2020 10:26:11 PM	Successful	Incr Backup
crooked		IBM Spectrum Protect (TSM)	[redacted]	Other	15	Jun 17, 2020 2:45:41 AM	Successful	Incr Backup
virgin		IBM Spectrum Protect (TSM)	[redacted]	Other	12	Jun 19, 2020 7:12:06 PM	Successful	Incr Backup
stroudwater		IBM Spectrum Protect (TSM)	[redacted]	Other	11	Jun 20, 2020 3:41:27 PM	Successful	Incr Backup

Figure 4: An example of a Sources with No Recent Backups report in APTARE.

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 APTARE, your company can build dashboards to view the restorability of every single application.

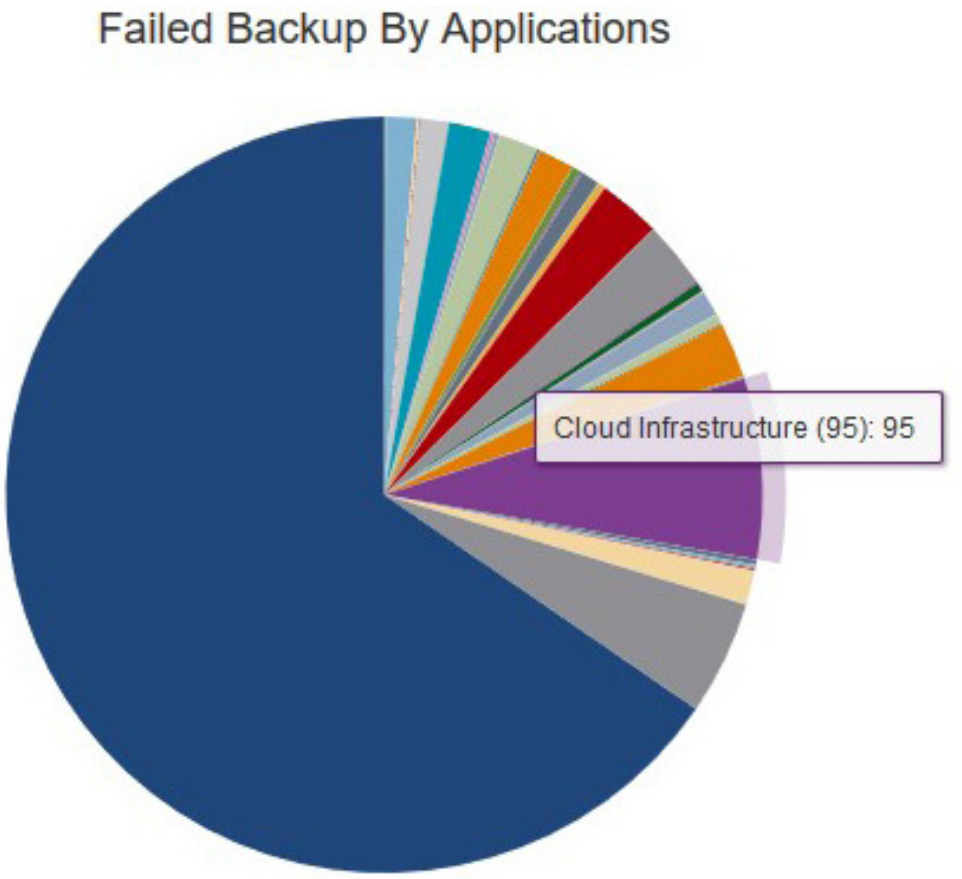

Figure 5: An example of a Failed Backup by Applications report in APTARE.

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. APTARE IT Analytics can support your recovery and detect future occurrences. Interested in learning more about APTARE IT Analytics? Check out www.veritas.com/aptare.

ABOUT VERITAS

Veritas Technologies is a global leader in data protection and availability. Over 50,000 enterprises—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.

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

For specific country offices and contact numbers, please visit our website.
www.veritas.com/company/contact

VERITAS

V1061 07/20