CLABBY ANALYTICS

Research Report sponsored by IBM

New Emphasis on Resiliency, Recovery and Cybersecurity in the COVID-19 World

Executive Summary

Due in part to the COVID-19 pandemic – as enterprises continue to adjust to greater demand for remote services, new security threats, and increased eBusiness transaction rates – information technology (IT) budgets are changing. From our perspective, in 2021, ***IT executives will likely see greater spending on remote support tools, on IT operations and performance, on cyber-security, and on resiliency/recovery to respond more quickly to cyberattacks as well as to maintain business continuity.***

This report takes a closer look at this final category (resiliency/recovery) and particularly focuses on IBM's newest offering: IBM Z Cyber Vault. The IBM Z Cyber Vault (which operates on IBM z14 and IBM z15 mainframes) combines IBM Z hardware and software, IBM storage, and integrated services. It is designed to help enterprises recover more quickly from outages due to corrupted logical data – the data that includes entities (tables), attributes (columns/fields) and relationships (keys) – the logic that drives a database. It can also help IBM Z customers identify cyberattacks aimed at logical data – and help enterprises respond/recover more quickly from data breaches. As a result, IBM Z Cyber Vault should be of high interest to IT executives who are dealing with concerns about data loss/corruption and corrupted data from security breaches.

In 2021, IT executives will likely see greater spending on remote support tools, on IT operations and performance, on cybersecurity, and on resiliency/recovery to respond more quickly to cyberattacks as well as to maintain business continuity.

The COVID-19 Effect: Spiceworks Ziff-Davis 2021 Survey/Report

The Spiceworks, a Ziff-Davis company, recently published its 2021 State of IT Report on projected IT buying patterns. Its survey of 1,073 information technology executives shows that COVID-19 has acted as a major catalyst for business transformation. As a result, enterprises have had to increase spending to support remote workforces, adopt new digital workflows, optimize business operations, and find new ways to meet the needs of a changed computing market, including a substantial increase in

Business-to-business eCommerce; significant shifts in consumer buying behaviors; and a large (7X) increase in phishing scams, as well as several large-scale ransomware attacks

The Spiceworks report further shows that in response to COVID-19, 44% of the enterprises surveyed have planned to accelerate their digital transformations. It also shows that enterprises are highly concerned about security: 33% plan to improve security, risk and governance; 32% are very concerned about providing users with standardized, secure and easy-to-use tools for remote access; and 27% plan to adapt their disaster recovery plans to account for new and additional scenarios.

IBM has decided to tackle this logical data protection problem with its new IBM Z Cyber Vault logical data corruption protection offering.

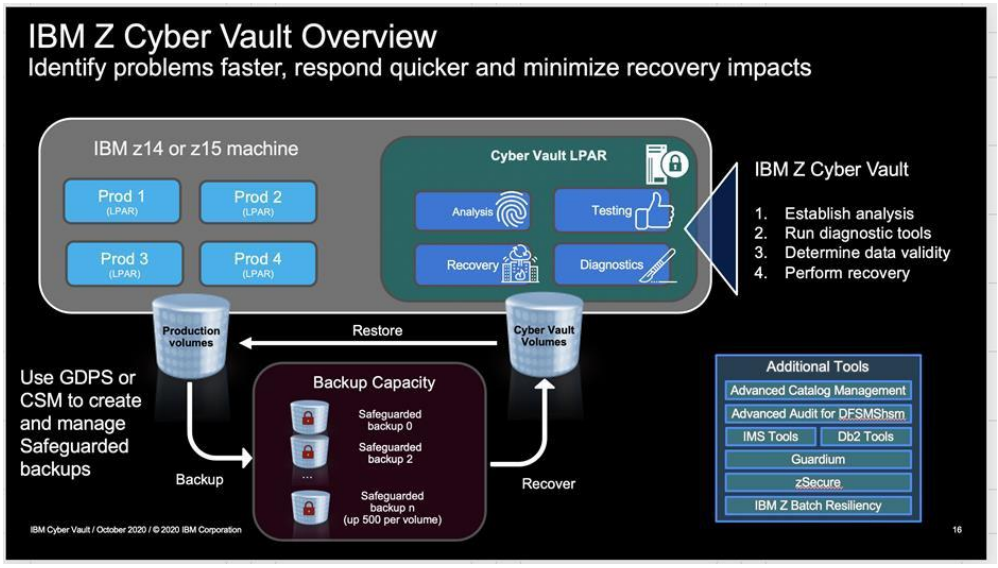
A New Recovery Scenario – and How IBM Z Cyber Vault Addresses Corrupted Logical Data

To date, the computing industry has largely focused on protecting access to and utilization of physical data (via authentication, authorization, encryption, data masking, etc.) to protect physical data records. Protecting logical data structures (the structures that describe the relationships between various entities in a database) from being corrupted, however, has been a labor-intensive problem involving strict adherence to backup procedures, as well as, ultimately, recovery from another known and trusted backup source.

IBM has decided to tackle this logical data protection problem with its new IBM Z Cyber Vault logical data corruption protection offering.

Figure 1 (below) provides a graphical overview of what IBM Z Cyber Vault is – and what it does. It is, essentially, a data recovery offering that runs within one or more logical partitions (LPAR) on an IBM Z server but it could also run on a separate server. The diagram shows an IBM z14 or z15 that constantly copies data volumes and active data to underlying IBM DS8000. The DS8000 safeguards up to 500 copies of the data (using IBM Safeguarded Copy technology in conjunction with IBM GDPS or IBM Copy Services Manager software, either is required).

Figure 1 – An Overview of IBM Z Cyber Vault



The IBM Z Cyber Vault uses immutable backup to protect data, and can present the captured backups for validation to identify corruption allowing for remedial action to be taken. The IBM TS7700 tape environment can also be used to backup data, creating an "air gap" between the backup data on the DS8000 and the TS7700 environments.

With the data safe and secure, the IBM Z Cyber Vault can, when needed, help analyze the data resident on IBM storage; it can help run diagnostics to determine data validity; and, when validity is determined, the Cyber Vault can initiate and perform the recovery process.

Now, consider how IBM Z Cyber Vault can be used to identify a security breach and quickly remedy the situation. Just suppose that enterprise data has been corrupted by an intruder. IBM Z Cyber Vault analysis tools can help identify a breach far more quickly than relying on human intervention alone. Using IBM Z Cyber Vault, the logical data within the DS8000 is protected from attack. Remember, the longer it takes to check the spread of malicious code or a cyber-attack, the longer it takes to rebuild a given environment. The IBM Z Cyber Vault is not only a recovery tool; it is also a cybersecurity response tool.

Summary Observations

The IBM Z Cyber Vault is a highly integrated system/software/storage/services option that can speed system/data recovery as well as help overcome the impact of malicious intrusions. Consider,

- Without IBM Z Cyber Vault a logical error can easily and quickly (sometimes instantaneously) replicate. IBM Z Cyber Vault uses scheduled point-in-time copy facilities to place copies in an isolated, secured location.
- Without IBM Z Cyber Vault, an IT administrator may not be able to immediately notice corruption when an outage occurs. With IBM Z Cyber Vault, data analytics can be performed regularly on the data to validate data consistency, giving administrators a heads-up in the event corruption has occurred.
- Without IBM Z Cyber Vault, there is only one recovery point (where the known-good copy lies – if indeed it can even be identified). With IBM Z Cyber Vault, there exists multiple recovery points to help identify the right point in time to restore from.
- Without IBM Z Cyber Vault, all systems, storage and tape pools participate in the same, open, logical system structure – making all attached devices subject to corruption. With IBM Z Cyber Vault, data can be protected by air-gapped storage systems that defend against logical errors and malicious intruders.
- Without IBM Z Cyber Vault, a system can be designed to provide continuous availability and disaster recovery from physical events. But with the addition of IBM Z Cyber Vault, analytics tools can provide forensic analysis of the data, allowing surgical or catastrophic recovery to occur significantly sooner from corruption events.

The COVID-19 pandemic has forced organizations to make numerous, often radical adjustments to their IT practices and IT budgets. For enterprises that run IBM Z servers (which are usually deployed in the most mission-critical environments), business continuity has become paramount to surviving the changes and pressures that COVID-19 has caused to businesses everywhere. With IBM Z Cyber Vault, IT executives can recover more quickly from corruption-induced outages while protecting logical data from the impact of malicious phishing and ransomware cyberattacks.

The bottom line here is that continuous availability and disaster recovery strategies focus on protecting against physical outages. IBM Z Cyber Vault has been architected to help enterprises recover from damage to their vital logical data resources.

Continuous availability and disaster recovery strategies focus on protecting against physical outages. IBM Z Cyber Vault has been architected to help enterprises recover from damage to their vital logical data resources.

CLABBY ANALYTICS

Clabby Analytics LLC
http://www.clabbyanalytics.com
Telephone: 001 (843) 297-5150

December. 2020

Clabby Analytics is an independent technology research and analysis organization. Unlike many other research firms, we advocate certain positions — and encourage our readers to fin counter opinions — then balance both points-of-view in order decide on a course of action. Other research and analysis conducted by Clabby Analytics can be found at www.ClabbyAnalytics.com.