



IBM Storage – New Cyber-Resiliency Functionality

By Jean S. Bozman

IBM added more cyber-resilience capabilities for its already-extensive IBM Spectrum portfolio of data-protection software. The data-resilience features of products in the IBM Spectrum portfolio have been extended – and IBM announced expanded data-protection support for two widely-used enterprise workloads: SAP HANA and Salesforce.

Taken together, the new features address customer demand for cyber-resilience in the face of malware and ransomware that can harm, or delete, enterprise data. For large enterprises, these types of outages can cause millions of dollars of downtime for each incident.

IBM added an expanded set of [cyber-resilience features](#) to the IBM Spectrum portfolio on September 20. All of these will see general availability in September and October. The moves are aligned with IBM's strategy to support customers who are migrating traditional enterprise applications to the hybrid cloud.

Background

Cyber-resilience features for distributed data, cloud-native data, [SAP HANA and Salesforce SaaS](#) applications reflect customers' accelerated migrations of enterprise applications, following the onset of the COVID-19 pandemic in 2020. Since then, customer concerns about cloud-security gaps have grown – driving their need to secure data in-flight and at-rest in hybrid clouds.

The tasks of identifying, addressing, and recovering from any such attacks is exacerbated by the rapid pace of moving data-center enterprise workloads to the hybrid cloud. This acceleration in cloud migrations is accompanied by concerns in the CXO community (e.g., CISOs, CIOs, CEOs) that applications and data will come under increasing threats as they are moved into Cloud and Edge deployments, throughout this decade.

Detecting Attacks, and Restoring from Isolated Resources

IBM Spectrum Protect software has long protected enterprise workloads – which is why IBM is adding protection for data-optimization “blueprints” that protect data across multiple cloud resources. Customer worries center on the long period of time it



generally takes to discover than a cyberattack has taken place – and concerns that valuable business data might be ransomed, or lost altogether, as a result of such an attack.

IBM customers already use IBM QRadar and IBM Guardium to detect cyberattacks – but customers are stepping up their use of “immutable copies” of enterprise data – data that has been replicated in a format that cannot be changed by malware or ransomware. Even when attackers demand a ransom, data that is protected and isolated can be restored from its backup resource, without change, preserving business continuity.

The recent IBM Spectrum announcements will provide wider support automated data replication; the use of immutable copies; and air-gapping – to create more barriers to data loss via cyberattacks or ransomware.

IBM Spectrum Announcements

Key Points of the IBM Storage Announcements, made on Sept. 20, 2022, include:

- IBM Spectrum Scale V 5.1.5 supports immutable snapshots (data that cannot be updated or changed), and leverages policy-based controls originally designed for scalable data resources managed by IBM DS8000 storage systems. This brings IBM’s Safeguarded Copy capability to a broader user base, allowing IBM Spectrum Scale customers to use logical air-gapping on unstructured data sets.
- IBM Spectrum Virtualize 8.5.2 supports asynchronous, policy-based data replication. The new version adds support for cloud-native applications using AWS ROSA (Red Hat Open Shift on AWS), combining a bring-your-own-license approach for IBM customers with a customer’s move to hybrid computing. Red Hat OpenShift users can use ROSA, which is an AWS managed service, to build, scale, and manage containerized applications on AWS.
- IBM Spectrum Sentinel software, which identifies security issues, is now available for SAP HANA workloads. It provides automated data snapshots and automated recovery orchestration. This approach acknowledges the widespread use of SAP HANA in-memory databases by a broad base of enterprise customers.
- IBM Spectrum Protect Plus Online Services will now be available to support Salesforce (SaaS) workloads. This adds data-protection for Salesforce applications that are not currently replicated automatically; it can also be used in place of third-party backup/recovery software. As was reported last year, Salesforce had changed its Data Recovery Service for cloud-native services in



2020, and ending support in 2021, causing customers to move to third-party software.

- IBM added asynchronous data backup to IBM Spectrum Virtualize. Using policy-based asynchronous replication, Spectrum Virtualize synchronizes data stored on IBM FlashSystem all-flash arrays, and data stored on IBM Spectrum Virtualize appliances.

Cloud Architects Analysis: Key Takeaways

Cyberattacks and ransomware have become more frequent in recent years – and many types of attacks target both enterprise applications and cloud-native applications. Customers' data "estate" is more extensive than ever before, as enterprise workloads become more distributed, and more widely exposed to threats across the hybrid cloud – from data center to Cloud to Edge locations.

The firewalls and perimeters of the traditional data center no longer stop attacks, unless policies are updated, and an organization's cyber-resilience is strengthened. A multi-layered approach to achieving better security, addressing it at many layers of an organization's infrastructure, is sometimes referred to as a tiered defense or a defense-in-depth strategy.

That's why customers in large enterprises, SMB companies and governments are realizing that their former approaches to data backup/recovery are no longer sufficient to ensure business continuity. The adoption of hybrid clouds is bringing about a new era when "the rubber meets the road" – when enterprise applications "meet" cloud-native applications, running side-by-side on the same cloud infrastructure. That situation demands new approaches to data-protection.

Data-protection and data-management are top priorities for customers, spanning large, medium, and small businesses with vastly different budgetary resources. Clearly, IBM knows that it must compete with some long-time data-protection companies – while it partners with others to provide data-protection solutions across the global marketplace. Support for SAP HANA and Salesforce software, via the IBM Spectrum software announcements, underscores this point.

We expect that this expanded approach to data-protection will grow the worldwide ecosystem for data-protection software by 2025, bringing a co-opetition model along with it. The most recent set of IBM Spectrum Protect announcements reflects IBM's



deep understanding of cyber-security and data-protection issues, informing the new set of IBM Spectrum data-protection capabilities.

Copyright @ 2022 by Jean S. Bozman
