IBM's Distributed Data Security for the Edge Leverages zSystems Encryption

Status is online

By Jean S. Bozman

IBM is extending highly secure data from customers' IBM z Systems mainframes, across IBM Cloud – and out to remote edge locations. Edge locations now covered by core-to-edge data security links include sites like retail stores, factories, bank branches, regional insurance offices, and oil/gas refinery locations.

The new end-to-end solutions leverage data security software and hardware-enforced pervasive encryption on IBM z15 mainframe systems, IBM Data Privacy Passports software and IBM Cloud services to support hybrid multi-cloud and edge-device security.

The data on the IBM zSystems servers and the IBM Cloud is protected at the highest data security level -- the FIPS-140-2 Level 4 standard for 256-bit encrypted data.

On a business level, IBM plans to leverage end-to-end data security to fuel continued digital transformation and cloud migrations by IBM's customers. Many of these customers are modernizing older applications for born-on-the-web operations – and containerizing legacy applications for re-use on the cloud. IBM's services groups will work directly with customers to develop and deploy modernized applications for distributed computing.

Building Core-to-Edge Data Security

Just a decade ago, this extension of IBM-secured data capabilities out to edge devices would have been unthinkable, even within IBM. Even the word "distributed" was once freighted with meaning for IBM, which then saw the world of small x86 servers growing up around the data center as incapable of supporting the very highest levels of data security.

That vision has dramatically changed, with new revelations at the May 2020 THINK conference providing new details about IBM's core-to-edge data security solutions. These solutions leverage the IBM z15's hardware-enforced pervasive encryption, as well as IBM Data Privacy Passports software and the IBM Cloud Pak

for Data, to secure the data throughout its hybrid cloud journey across private and public clouds.

The Mainframe and the Cloud

Pervasive data encryption – a capability that has been enforced by the IBM zSystem's on-board processors since 2017 – is now an essential part of the broader edge-to-core IBM data security offerings.

It is the presence of the IBM z Systems and the IBM Cloud that will protect data-in-flight and data-at-rest – all along the pathways to the edge, which is at the heart of this security innovation. We note that IBM storage and IBM Spectrum software support this end-to-end data security software.

End-to-End Data Protection and Data Security

The IBM mainframe's data security (FIPS-140-2 Level 4) can travel with data-in-flight, using IBM Data Privacy Passports software, for hybrid cloud and edge devices. IBM storage systems will also play a strong role in supporting data-privacy, data protection and high-availability. Taken together, that's much of the portfolio-based innovation that will stand behind the end-to-end encrypted data, and its business value proposition.

The IBM z15 mainframe system – located in the customer's data center or inside the IBM Cloud – supports hardware-enforced pervasive encryption, at the FIPS-140-2 Level 4 standard for 256-bit encrypted data.

Yet, the IBM Cloud's end-to-end data-security solution now applies to cloud-enabled applications running on any Linux-enabled platform, including a new air-cooled IBM z15; the IBM LinuxONE III, mid-range IBM Power Systems; and on hundreds of brands of Linux x86 system platforms sold by other systems vendors worldwide. This reflects the diversity of Linux systems that can connect with end-to-end data security delivery.

Surrounding Products and Technologies

IBM and Red Hat products support an open-source-based software stack aimed at distributed computing on the hybrid multi-cloud. They include: IBM Red Hat Enterprise Linux (RHEL 8), Red Hat OpenShift 4.4 containers, industry-standard

Kubernetes orchestration software, IBM Data Privacy Passports software, IBM Cloud Paks for cloud-certified applications, IBM Spectrum software-defined storage management and IBM storage systems.

Earlier this year, IBM extended the end-to-end high levels of encryption with its IBM Edge Application Manager (APM) 4.0 – and IBM is expected to enhance that software with its APM 4.1 release, due to ship in Q220.

This combination of IBM products, IBM Cloud services and IBM data-security software will extend data-center security to regional data hubs – and to thousands of edge systems across major geographic regions in the IBM Cloud worldwide. This capability is becoming even more important as 5G telecommunications networks bring high-speed bandwidth to edge devices, where new corporate data is being generated, and replicated.

Customer Control of Data Access Plays an Important Role

Customers' ability to control access is what allows extension of this solution out to the edge of the network.

At IBM's THINK conference, IBM said that its customers could deny access to specific users – including IBM personnel – even though the solutions are running on the IBM Cloud. This ability to provide granular access controls is why IBM is now comfortable selling the end-to-end, core-to-edge data security across the hybrid multi-clouds that now surround customers' enterprise data centers.

A version of this end-to-end data security is shipping with IBM's FS (Financial Services) Cloud – which began deliveries to banks and financial institutions in fall, 2019. Based on IBM THINK presentations, we expect that FS Cloud capabilities will be enhanced and extended in 2020.

Why Is IBM Doing This Now?

As IBM expands its end-to-end data security to edge locations, what's changed in IBM's approach to distributed computing at edge sites? IBM is taking full advantage of the Red Hat developers' toolkits, and its own IBM Garage development and deployment resources. The IBM Garage services support customers' collaboration with IBM developers to update and secure aging mission-critical workloads that are migrating to the hybrid cloud.

IBM's priority is to work with customers who are migrating key applications and data to hybrid clouds in what IBM calls "Chapter Two" digital transformation projects. As it does so, IBM Cloud may also capture more upside revenue for its IBM Cloud enterprise business, to gain share from cloud competitors AWS, Microsoft Azure and Google Cloud Platform.

Additional relevant research and consulting services are available. Interested readers should contact Client Services to arrange further discussion or interview with Ms. Jean Bozman, President of Cloud Architects Advisors.