IDC LINK
Real-time IDC Research® opinion on industry news, trends and events

IBM Announces a New Layer of Security with Secure Service Containers

October 04, 2018

By: Peter Rutten

IDC's Quick Take

IBM announced that it has embedded new capabilities at the core of its IBM Z and LinuxONE product lines in the form of Secure Service Containers that help protect an organization's data in new and powerful ways, shielding it against both internal and external threats. Secure Service Containers provide encrypted data in, encrypted data out, and encrypted data at rest; fully isolated and protected memory with no sharing; a secure boot sequence; and no command-line access for administrators – plus organizations benefit from an also just announced pay-as-you-go pricing model.

Product Announcement Highlights

Today, line-of-business (LOB) executives and senior executives are much more aware of IT security issues than they were just a year or two ago. Despite accelerated efforts to beef up security systems, tremendous vulnerabilities continue to plague many organizations. It is not uncommon for employees or contractors, for example, to have access to sensitive data, even if there is no good reason for it. Take VM administrators, for example. With the way many organizations work today, and because of technology limitations, VM administrators are sometimes given administrative authority to environments that house extremely sensitive information —the infamous example, of course, being Edward Snowden who managed to snapshot a few VMs and walk away with a large amount of NSA data.

What organizations need is the ability to protect data, not just from peer environments but also from the administrators above those environments that have authority over them. IBM calls this "vertical isolation." The IBM Z has provided for EAL5+ levels of isolation between peer environments for quite some time at the LPAR level. If adjacent LPARs are used by different parties, this level of protection ensures that it will be impossible for one party to access the other party's LPAR. This is especially critical for managed service providers (SPs) and cloud service providers. However, this type of LPAR protection does not address the issue of an administrator who operates above the LPAR level.

When a company is looking to move sensitive data off-premise, there are significant cultural and resource implications. Moving sensitive data from the datacenter managed by an organization's employees to an external entity with employees that the organization has no direct HR control over and has not performed background or security checks on is a major leap of faith, even as clauses in the contracts with service providers intend to protect the organization from such risks. Much sensitivity remains around this issue, with no complete technical solution.

IBM says that this is one of the reasons why it developed Secure Service Containers, which ensure that an administrator has no access to either the data or the execution within the Secure Service Container environment. These "containers" are not to be confused with, for example, Docker containers. Secure Service Containers are a special kind of LPAR that can hold thousands of VMs, with each of those VMs running hundreds of Docker containers in them. Intel and AMD have secure enclaves, SGX and SEV, respectively, but IBM believes that its Secure Service Containers have the advantage of no application

code changes required and access to much more memory (10TB) compared with Intel's SGX, which is limited to 128MB — not enough for a database, for example.

IBM believes that CISOs and CIOs prefer simple push-of-a-button security approaches and dislike complicated strategies based on best practices and human reliability, which is why the company created the concept of a "secure box" that guarantees that data inside the box is inherently secured by the platform technology. The company developed a special kind of LPAR that is secured in a trusted boot sequence in firmware before it gets to the software level. This ensures that it is a known and good image that has not been corrupted or manipulated as it is booting up. All memory in this environment is completely isolated and not shared with any other virtualized environments. It is impossible for another environment in a virtualization scheme to get access to the address, for example, in case it is overcommitted. All of the data on disk is fully encrypted as is all of the data going in and out through network channels.

Furthermore, Secure Service Containers feature level 4 encryption key security on the FIPS PUB 140-2 regulatory standard. The most common encryption key protection is level 2. Some solutions have level 3, which means that, if a tamper proof enclosure is compromised, a proactive notification is issued. With level 4, zeros are automatically written over the data to protect the keys and ensure that they can't be appropriated. IBM says that, with this combination, it has created a "lockdown environment where a whole LPAR with up to 10TB of memory has been holistically and completely protected as a black box. And any workload you put in that box receives the full benefit of that security."

But perhaps the most radical aspect of Secure Service Containers is that administrators cannot simply log in via Secure Socket Shell (SSH) or Telnet to a command line and then do whatever they want on the system — that would break the entire security model. With Secure Service Containers, no one has open command-line access with administrative authority. IBM essentially turned off the ability to remote administrate via a command line by turning off SSH, Telnet, and other remote access features. Instead, every administrative operation that is approved for that operating environment is white-listed by being exposed as either a RESTful service or a web interface.

IBM has developed a software development kit (SDK) that helps customers create such an administrative interface for their Secure Service Container environments. This means that whatever goes into a Secure Service Container environment is essentially a software appliance, with a software appliance interface, and all administrative activities that are appropriate are managed through that software appliance, not through the command line. Every workload inside a Secure Service Container has to have its administrative operations exposed through this SDK as a web page or RESTful service.

IBM has already done this for its blockchain service, which runs on LinuxONE in the IBM Cloud. IBM expects that ISVs will soon be able to create such experiences for their software, and eventually, customers will create their own administrative interfaces for their LOB-created apps. The solution is not just suitable for service providers but also for large organizations that are worried about employees or contractors in their datacenters.

IBM says that it regards Secure Service Containers as a good example of its strategy to provide unique differentiation versus server infrastructure running on Intel processors. The immediate market opportunity consists of workloads that customers are not comfortable moving to the cloud yet. Furthermore, IBM believes that managed SPs and cloud SPs are eager to differentiate themselves with solutions such as Secure Service Containers versus hyperscale giants such as AWS and Azure.

New Container Pricing Model

IBM also announced a new container pricing model. IBM Z software pricing has traditionally caused customers to religiously monitor million service units (MSUs) on their systems, especially when new software or new business usage patterns are introduced, since this can lead to significant increases in software billing. IBM has recognized that, as a result, customers are very careful to bring new workloads to the platform that do not necessarily require typical IBM Z environments like CICS, IMS, MQ, or DB2.

IBM Z software is priced based on what's called the "peak rolling four-hour average" measured in MSUs, not on a software product's individual contribution. If that product causes greater utilization during the four-hour peak or if it causes a new four-hour peak, pricing for all software on the platform will be disproportionally higher. IBM has tried to offset this effect with new models but never to complete customer satisfaction. With the new container pricing model, IBM hopes to provide full transparency and fair software pricing at last.

According to IBM, Container Pricing allows IBM-approved solution workloads on z13 and z14 to scale from collocated solutions within existing LPARs through to separate LPARs, up to multiple LPAR solutions, without directly impacting the cost of unrelated workloads. Solutions that benefit are:

- **Application Development and Test Solution —** This is standalone pricing for development and test workloads.
- **New Application Solution —** Customers can add new workloads, such as CICS TS or WebSphere applications, that are not currently running on any Z platform.
- **Payments Pricing Solution —** This new “per payment” price metric ties directly to payment volumes based on IBM Financial Transaction Manager (FTM) software.

IDC's Point of View

IDC believes that IBM continues to strongly differentiate its LinuxONE and IBM Z platforms with these new security capabilities. After the introduction of pervasive encryption with the launch of the latest generation of IBM Z and LinuxONE, Secure Service Containers provide a much-needed additional layer of security by completely shielding LPARs from each other and by eliminating command-line access for administrators. Managed SPs and cloud SPs can tell their customers reliably that, with Secure Service Containers, simply no one can access their data, regardless of authority level within the managed SP and cloud SP. The same is true for organizations that run the platform in their datacenters. They also know that it will be impossible for rogue employees or contractors to access the data. Moreover, the new pricing model promises fewer worries about cost when adding new workloads to the containers.

Subscriptions Covered:
Servers and Computing Platforms