Migrating Legacy Applications to the Cloud for the Federal Market

Charles Hall, Roger Hockenberry, Dan Cybulski

All questions and enquiries regarding this paper should be directed to:
Charles Hall
Chief Operating Officer
Cognitio
chall@cognitiocorp.com

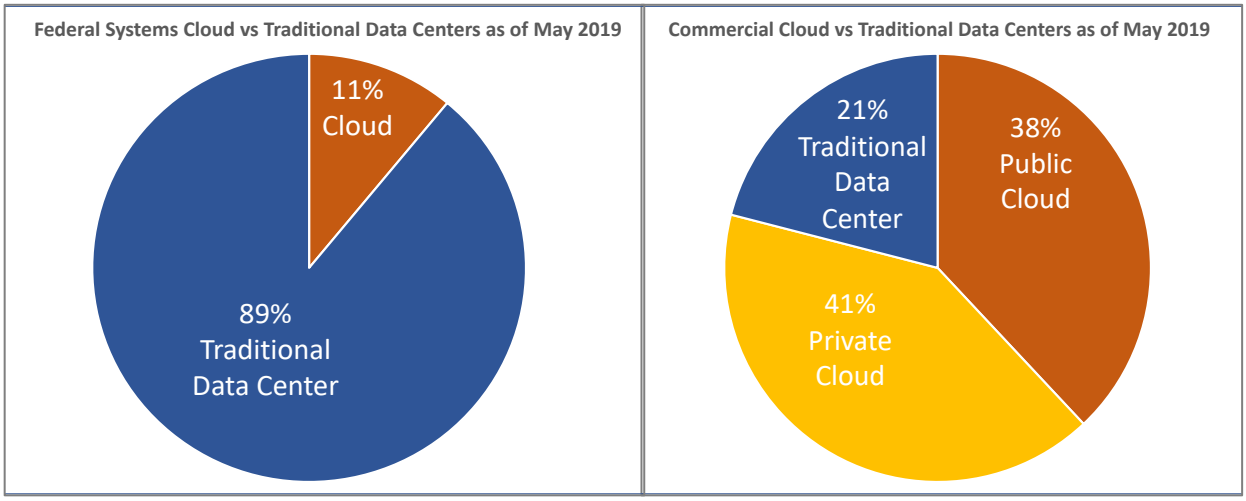
Table of Contents

Copyright © Cognitio 2019

Background

The federal government relies on many legacy applications for critical mission support. Unfortunately, these applications often reside on obsolete hardware that is past end-of-life and no longer supported by the manufacturer; the lack of easily obtained replacement parts increases the downtime and decreases the stability of these systems. Even the operating systems are often obsolete and unsupported, which means no more security patches are being created, increasing the risk that the system could be breached. Combined, these challenges can turn a critical mission system that should support a mission into a liability that can negatively impact the mission.

Further, these systems are not Cloud compatible because they are not X86 architectures, and prevent an agency from following the federal "Cloud First" mandate to move to the Cloud. Despite significant investments made in cloud solutions, mission elements have continued to maintain their own separate IT infrastructures for their most critical and sensitive workloads on these legacy systems, with only 11% of federal IT systems currently in the Cloud. Comparing the adoption rate of Cloud in the federal space, versus adoption in the commercial space, and we see an adoption rate in commercial of over seven times that of federal.



Federal[1] vs. Commercial[2] Cloud

This inability to move mission-critical legacy workloads to the Cloud, an effort intended to preserve the functionality of existing mission critical applications, is a detriment to their capabilities, as it fails to expose them to the rich, on-demand capabilities of cloud infrastructures,

[1] Corrigan, Jack. "Only 11 Percent of Federal IT Runs on the Cloud, Watchdog Says", NextGov.com, May 7, 2019, https://www.nextgov.com/it-modernization/2019/05/only-11-percent-federal-it-runs-cloud-watchdog-says/156816/. May 20, 2019.

[2] Flexera. "RightScale 2019 State of the Cloud Report", Flexera.com, 2019, https://media.flexera.com/documents/rightscale-2019-state-of-the-cloud-report-from-flexera.pdf. May 20, 2019.

Copyright © Cognitio 2019

and further increases the risk to mission. It also increases the cost for the agency, as space in legacy data centers continues to be used for these mission critical systems.

There are ways to overcome these issues. It is possible to use an emulation product to create a virtual machine, replacing the aging hardware with a modern system using standard x86 technology. The operating system and application remain intact, while the troublesome, unsupported hardware goes away. There's no need to modify or re-validate the application, as it continues to exist intact, in its same operating environment, on new hardware.

Some such emulation products even allow a move to the Cloud, by using virtual machines that can be built in any of the various Cloud environments, such as AWS, IBM, Azure, or Oracle. This allows the transition from a legacy data center to a cloud environment, with many benefits. Let's take a look at one such solution, the Charon product from Stromasys.

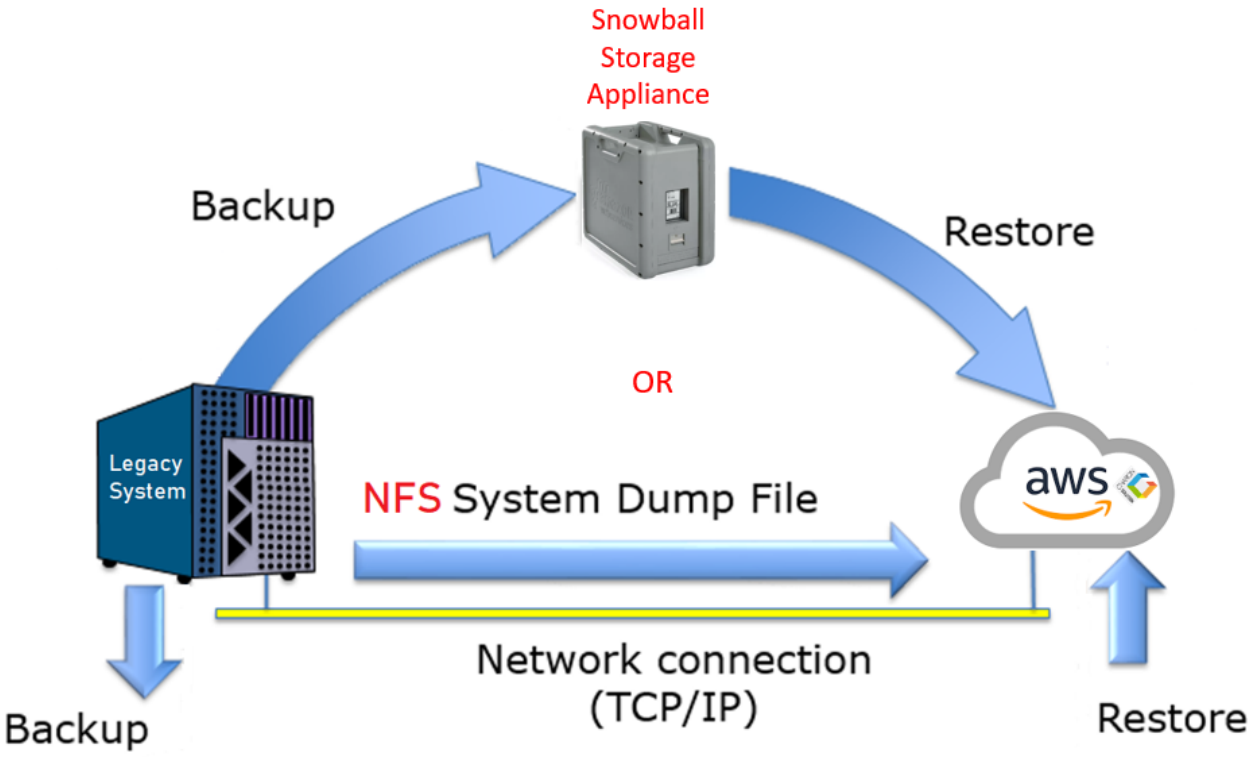
Using Charon to Migrate Legacy Systems

Stromasys's Charon product emulates legacy hardware (HP 3000 or 9000, DEC VAX, PDP, and Alpha, and Sun SPARC) on modern x86 systems. It allows legacy applications to be migrated from old hardware that is beyond its end of life, to an emulated version of the old hardware on modern hardware. It is Cloud-enabled, and will run on any Cloud system, such as AWS, Oracle, Azure, or IBM.

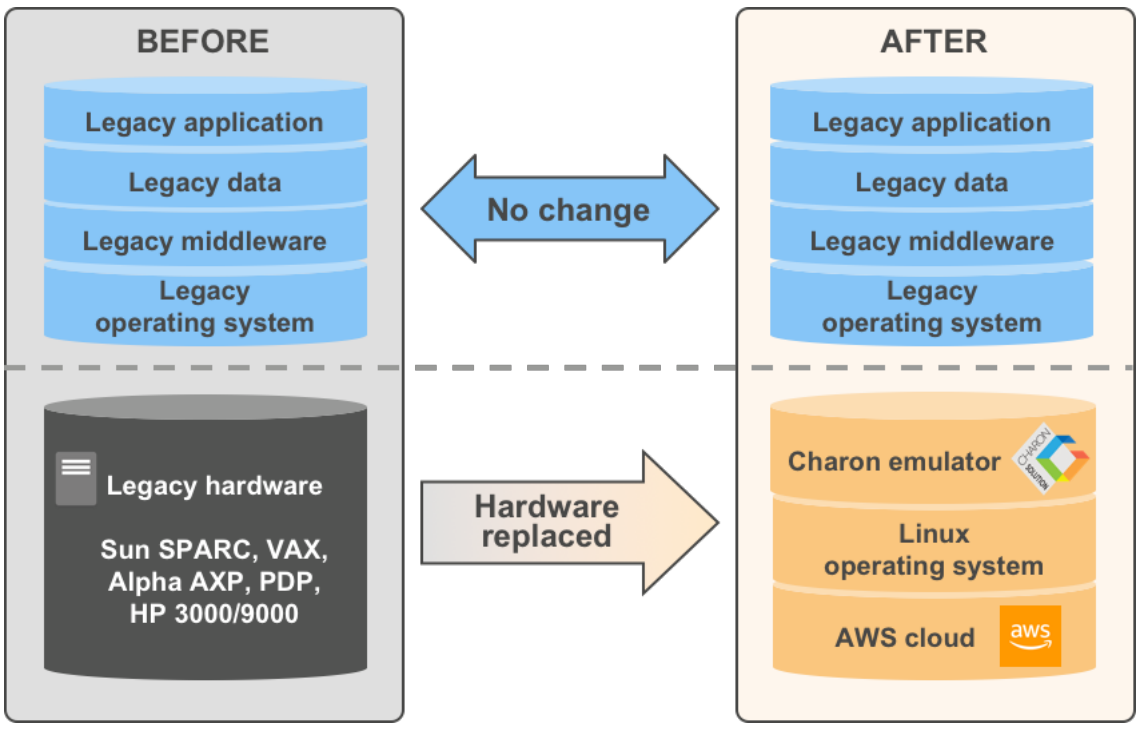
The process for migrating an application to Charon is simple. A Charon instance is spun up, which emulates the hardware to be replaced. The legacy application and its operating system are restored from a backup onto the new emulated hardware. Then the application is brought up as normal. Users will see no difference in the application, and there's no need to re-engineer, re-code, or re-validate the existing functionality.

When using a Cloud instance, the biggest hurdle can be migrating the backup of the operating system, application, and data to the Cloud prior to restoration to the new emulated hardware. It can take a while to move large amounts of data over a WAN connection. Each Cloud provider has alternate methods for migrating data which can help with the process. One option is to use a physical device to transfer files to the Cloud provider for restoration, which is much faster than using a WAN connection.

Copyright © Cognitio 2019



The following diagram shows the migration from obsolete hardware onto a Charon instance running in the AWS cloud:



Copyright © Cognitio 2019

Benefits of Approach

There are many benefits to using this approach to migrate legacy systems to the Cloud, such as stability of the application, extended application lifetime, improved performance, enhanced security, and better disaster recovery.

One of the most frustrating things about running an application on hardware that is past its end of life is the lack of spare parts. When a part fails, the system can be unavailable for an extended period while increasingly sparse parts are located and brought in to complete the repair. This downtime is frustrating to users and represents significant risk to mission. Add to this the amount of time and effort required by agency personnel to source these parts and perform needed maintenance, and costs quickly become overwhelming. Moving to emulated hardware eliminates the obsolete hardware, and creates a much more stable environment, reducing risk to mission and ongoing costs.

At some point, there will be no more spare parts for these systems. Most are no longer supported by the manufacturer, and the supply of parts dwindles as it becomes less and less economically viable for third parties to make parts. When no more parts are available, the application will no longer run. Migrating to new hardware that is still supported by the manufacturer extends the life of the application beyond the lifetime of the aging hardware.

Performance is another issue with these legacy systems. Modern systems run at faster clock speeds, with architectural improvements like cache memory and faster system buses that improve overall performance. The emulated system takes advantage of these advances, as it sits on top of faster hardware, with a more modern architecture. While there is some overhead associated with the emulation, the speed benefits of the new system more than compensates. Users may see a significant performance boost, allowing mission critical results to be obtained faster.

Security is often a major concern with legacy systems. In most cases, the vendor no longer provides operating system or firmware patches for these systems. This increases the cybersecurity risk associated with the application. The emulated system sits on new hardware, on top of a modern operating system. The manufacturer provides firmware and operating system patches, and the emulated hardware inherits benefits from the native security features of Cloud, such as Security Groups, Access Control Lists (ACLs), and, optionally, adding other services such as Web Application Firewalls (WAFs), that help to lower the cybersecurity risk.

Disaster recovery and business continuity are important considerations for any mission-critical system. Stable hardware provides a better operating environment, but disasters and downtime can still occur. Using features of the Cloud, it is possible to have more than one instance of a legacy system available, and to have these in geographically diverse data centers managed by the cloud provider. If a tornado, flood, fire, or other disaster should take down one of the instances, another instance will be available to service users. It's also possible, with some engineering work, to keep the backup instance in sync with the live instance, further improving

Copyright © Cognitio 2019

the Restore Time Objectives and Restore Point Objectives used to determine effectiveness of a disaster recovery solution.

Replacing the legacy application with a new application requires that the new application go through an accreditation process. Migrating a legacy application to a new emulated hardware platform should require very little in the way of re-accreditation, if any at all, because the legacy code is not touched. That saves considerable time and effort over replacing the application with a new one.

Options to Consider Before Migration

Migrating the application to the Cloud is fairly straightforward. An instance of the Charon product is started, and a backup of the operating system, application, and data are restored to it. However, there are still many options to consider while building out the emulation in the Cloud. Among these options, a cloud provider must be chosen, the characteristics of the emulated hardware must be defined, a method for transferring and restoring the backup must be selected, user connectivity must be established, testing of the application in its new environment must be conducted, and recovery options must be considered.

Finding the right cloud provider is made easier by the fact that Stromasys' Charon product is provider agnostic. Consider costs, existing relationships with cloud providers, security options, and agency requirements when choosing a provider.

Configuring the emulated hardware is another consideration. This configuration influences the cost of the emulated system, as it uses resources. Selecting the CPUs, memory, storage, and other options should be done with care, to ensure that the new system is capable of handling the load imposed by the mission. Rather than just configuring the emulated system exactly like the legacy system, this is a time to right-size resources, adding or subtracting to get the best performance while containing cost.

As we discussed earlier, migrating the backup to the Cloud for restoration on the new platform requires careful thought. Some of these systems have large data sets, which can take significant time to transfer over a WAN connection. Look at options and choose one that will meet project objectives and timelines.

Making sure users can connect to the application is vital. Ensure that the security requirements of the organization can be maintained, and that the pathways needed for connection to the Cloud provider can be met. Consider the number of users and available bandwidth, as well, to ensure satisfactory performance of the application.

Once the new system is live, make sure that it works as planned. Before migration begins, define a test plan that will be followed to ensure that functionality continues to perform as expected. Create test cases based on common and uncommon functions that users must perform,

Copyright © Cognitio 2019

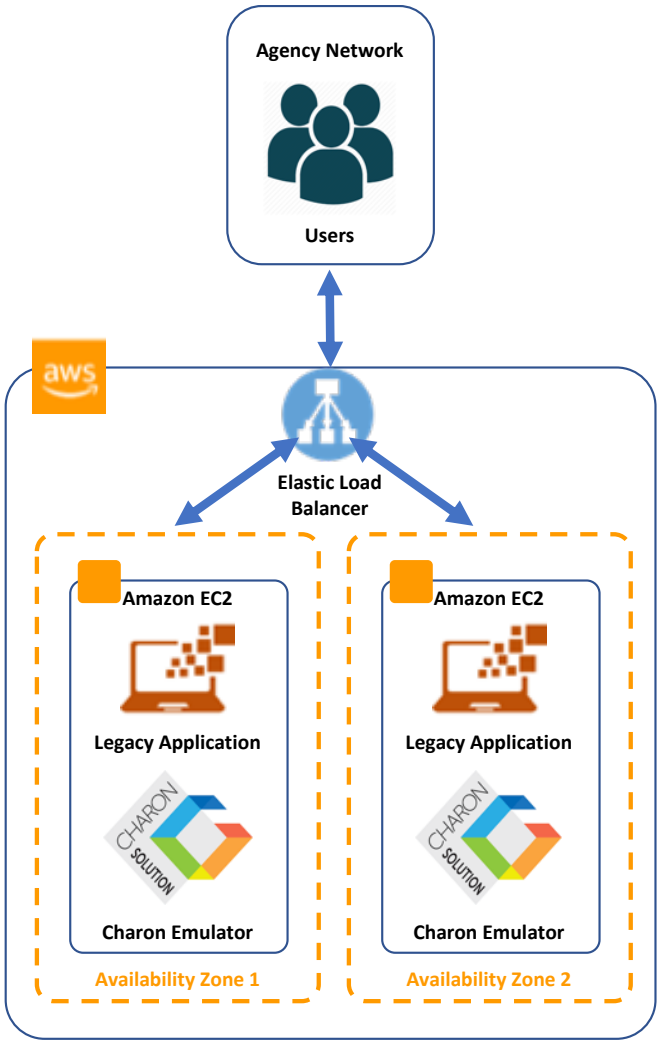
document how those cases can be tested, perform the test on the original system before migration, then conduct the tests on the new system and compare results.

Migrating to the Cloud, as previously discussed, can provide many new options for disaster recovery and business continuity. Consider these options and incorporate the ones that make sense to ensure mission success and continued system viability.

Reference Architecture

To help visualize the emulated system, let's consider a reference architecture. For our example, we'll assume that this will be built using AWS. We'll size the new system exactly the same as the old, under the assumption that it was scaled correctly to begin with. We'll create 2 instances in 2 different Availability Zones, to provide some measure of disaster recovery.

Using these assumptions, the architecture might look something like this:



Copyright © Cognitio 2019

Note that, depending on the capabilities of the legacy application, we can scale resources up or down as needed by dynamically allocating additional instances of the emulated application. An Elastic Load Balancer (ELB) can be used to allow distribution of workloads amongst these application instances. Native Cloud security features, such as Security Groups and ACLs, should be used to dramatically improve overall application security. If applicable, and if the architecture of the legacy application allows, other security options can be added, such as WAFs, which can inspect network traffic going to a website front end and filter out known cyber exploits, while also allowing finer control over allowed traffic to and from the application.

Summary

Getting legacy applications off aging hardware and into a stable environment is vital to the success of the mission for any agency. Moving to the Cloud is an important additional step. The "Cloud First" mandate compels agencies to consider Cloud, and overall, it is a strategy with many benefits, undeniable for any enterprise. Utilizing Charon enables the transition of critical systems to a cloud-based architecture with low risk, and allows agencies more time to better plan, execute and operate replacements for aging technology.

Copyright © Cognitio 2019

About the Authors

Charles Hall – COO

Chuck is Cognitio's Chief Operating Officer. He is a strong technology leader with extensive experience in legacy systems, and understands the finance and insurance industries through his work as CTO and VP of IT with organizations such as Wells Fargo and Marsh & McLennan. He learned much about the healthcare business, including data protection and compliance with regulations, as Senior Director for Enterprise Technologies at The Advisory Board, which provides guidance and products for the health care industry.

Dan Cybulski – CTO

Runner-up for Central Intelligence Agency (CIA) Technologist of the Year in 2014, Dan is recognized as a proven technologist, leader, and decision maker. Prior to joining Cognitio as CTO, Dan spent over ten years supporting the High Performance Computing (HPC) mission at the CIA, including serving as both an engineering lead and chief architect, before ultimately serving as acting chief prior to his departure from the Agency. In this capacity, Dan developed broad-based experience and hands-on technical skills supporting every aspect of this unique HPC infrastructure.

Dan's experience includes building, deploying, and supporting operational technical infrastructure including complex heterogeneous High Performance Computing grid systems, high performance networks, and multi-petabyte storage subsystems. Finally, Dan is recognized for his broad understanding of computing hardware and software including the evaluation of leading edge technology against known and anticipated requirements.

Roger Hockenberry – Cofounder – Partner – CEO

Roger is a proven technologist and business executive with over twenty years of experience working with all aspects of IT to assist enterprises in better utilizing technology to create, deploy and operate unique and innovative solutions and provide mission and competitive advantage. He is the former CTO for the National Clandestine Service of the Central Intelligence Agency where he helped shaped mission capabilities across a broad spectrum of activities.

Prior to this, Roger served with the Agency's CIO to help create and realize the community cloud capabilities, future desktop and field architecture, large data initiatives, and served as the Agency's Chief of Cyber Solutions. Prior to government service, Roger was a Managing Partner at Gartner responsible for several practices, including their security practice across their North American consulting business.

Copyright © Cognitio 2019

About Cognitio

Cognitio is a Senior Leveraged Consulting firm focused on several key practice areas including Cyber Security, Research and Influence, Government Services, and Technology Discovery and Innovation. Our partners are senior leaders with a wide array of government, Intelligence Community, and commercial experience, enabling us to bring both technology and business perspective to client engagements. Additionally, our engineering team boasts extensive experience designing and building high performance computing (HPC) and advanced analytic systems for the U.S. Intelligence Community (IC). With its broad experience, Cognitio is adept at driving impactful change, helping clients see clear paths to success, and helping to change perspectives in order to drive higher value for their enterprises.

For Questions please contact:

Charles Hall | COO
Cognitio Corp. | 1750 Tysons Blvd, Ste 1500 | McLean, VA 22102
Office: 703.738.0068 | Mobile: 571.426.0231 | Fax: 877.428.4728
chall@cognitiocorp.com

Copyright © Cognitio 2019