September 30, 2014

Hybrid Computing:

Collaboration with “need to know” access control reduces costs

Healthcare, Government, Finance, Retail Industry value

This report was prepared by

VICOM Infinity

Premier Business Partner IBM

Performance Disclaimer

All performance data contained in this publication was obtained in the specific operating environment and under the conditions described below and is presented as an illustration. Performance obtained in other operating environments might vary and customers should conduct their own testing. The information contained in this document is distributed AS IS, without warranty of any kind.

Overview

The need: Businesses/Agencies want to share data with consumers, business partners or other agencies on a "need to know" basis. They'd like to ensure that only the "right people" see "the right data" and those users may not know that any other data exists. Most important, they'd like the administration to be simple and reliable.

The solution: There is system infrastructure, running across a variety of hardware and software platforms, enabling a level of compartmentalization of data, applications and users on a need to know basis. IBM and Vicom Infinity, an IBM Premier Business Partner, have jointly developed a Proof of Concept lab that can demonstrate the value of collaboration for a wide variety of business problems and across many industries. Multiple vendor products (middleware and applications) are supported within this infrastructure to meet business needs, government certifications and business-defined regulations.

The benefit: Savings, simplicity and security. By sharing data, an organization can reduce the number of data copies and in turn, reduce the time necessary to deploy the data, the network bandwidth and additional servers necessary to process those copies of data. In addition, end users, partners, etc, will be working with a view of the data vs. having the data copied to them. This can reduce data leakage, theft and misuse of the data. With this infrastructure, the system becomes responsible for the access control of the data. As a result, a wide variety of applications and middleware can be deployed without adding complicated security infrastructure and access control logic within the application. This dramatically simplifies deployment of new applications, as internal reviews of code are not as critical toward security success.

The goal of this paper is to demonstrate that a hybrid solution can:

- **Reduce acquisition costs by taking redundant costs out of the solution**
- **Save money by reducing operational costs (hardware, software, environmental, labor)**
- **Reduce operational and deployment risks, while meeting the original schedule**
- **Protect profits via the security and resilience of the deployed solution**
- **In addition, looking forward, show investment protection and continued cost benefits through future technology deployment**

The Proof: The lab is available to prototype a wide variety of applications, middleware and data types. If your business needs mandate a private network implementation please discuss with us and we'll determine if a local implementation is feasible. Regardless, we believe that when over 250 servers are being proposed as your solution, we can help reduce the deployment bill by $1 million or more.
Don't hesitate to contact us to try a free proof of concept or see a demo.

Patterns for Success – end to end Hybrid Computing Pattern

There are data patterns that are common across several business models. Most important, they can take advantage of a hybrid deployment model and some unique infrastructure characteristics that can result in a dramatic reduction in operational and security overhead and simplify compliance to a wide variety of government, industry and business regulations. It's all based on a shared data model and collaboration across end-to-end technologies.

There are three critical business oriented data operations: update a record, read a record and analyze a collection of records. There are also management operations: backup/archive, migration/recall and disaster recovery. We're going to focus on the business-oriented aspects for this post.

Let's consider three different scenarios.

1. A national intelligence operation that is processing satellite and other electronic information
2. A health care environment that processes medical records and data from medical devices
3. A Criminal database containing wants, warrants and criminal records

Each of these has a data ingest process that comes from individuals or individual devices. Satellite data is beamed to earth, typically to an x86 based server and then transmitted and loaded into a "System of Record" which might be considered the master database.

Medical records can be updated by a medical professional and patient via an end user device or portal. Input can be received from medical devices e.g. EKG, MRI, XRay, etc. All of this information is then loaded into a master database.

BOLO's (Be On the Look Out), Criminal Records, Wants and Warrants are input by various police agencies and transmitted to a master record database that can be accessed by other police departments to see if someone they've stopped or is in custody may be wanted by other jurisdictions.

The "Need to Know"

Each of these scenarios has something special about them – a need to know. A doctor or nurse can't "troll" a medical database looking for any data. That's against HIPAA policy. They should only be looking at records associated with patients they are working with.

Intelligence analysts may only be able to see certain satellite or ELINT (electronic intelligence feeds) based on their security clearance.

Police in one jurisdiction cannot query or update records in other jurisdictions unless they are pre-approved for a particular case.

This Need to Know can also be called Compartmentalization or labeling of data. Our infrastructure includes technology known as Multi-Level Security (MLS) that allows data to be hidden from users and applications that don't have a need to know. The best part of this technology is there doesn't need to be any change to an application. The need to know criteria is established between security administrators and database administrators. As a result, when multiple users attempt to query an entire database, if they are in different compartments they'll get completely different result sets without knowing the full breadth of the database.

Medical Collaboration – Doctor, Patient, Hospital, Insurance

So let's look at a Medical System that has multiple hospitals scattered across a broad geography. Each hospital has specialty areas: Orthopedics, Oncologists, Pediatrics, etc. There is a Primary Care Physician (PCP) for each individual patient. There is the Patient. There are a bunch of different medical test devices: MRI, CTScan, EKG, etc. At some point, a Patient Care Record is created. A PCP is identified to that Patient. They may order tests on behalf of the patient. Test data is captured, stored and linked to the patient's record. A Cardiologist may see and annotate information associated with the EKG. Any other Cardiologist at the hospital may also see that EKG and annotate it. An Orthopedic surgeon may look at it, but not annotate it. A doctor at another hospital may not even know that the patient exists unless they are invited to look at it by a peer or via the patient requesting a second opinion.

Business-to-Business Collaboration

The following diagram shows a Manufacturing business that gets a variety of "parts" from different suppliers. They allowed each of their suppliers to check the on hand inventory to allow for continuous manufacturing and improve the supply chain operations. The unintended consequence of this implementation was that each supplier could see another suppliers' inventory and price per unit. As a result, devious suppliers could undercut the competition or worse, collude with their competitors to raise prices.

By turning on the labeled security capabilities, the suppliers can only see their records. Employees of the manufacturing company can see all the records in the database. No applications were changed. The manufacturing company had to collect some additional security information for each supplier in order for this to work properly. You'll notice the inclusion of an internet address (IP @) as a security context. The manufacturer can "force" supplier updates to come from the supplier's site. It will not allow a supplier's employees to logon from home, for example. This could help inhibit a rogue employee of the supplier from compromising the Manufacturer's database.

Agency to Agency or Country to Country Collaboration

There are other examples of production systems leveraging MLS capabilities. Lockheed Martin has been operating a secure environment for multiple agencies for many years. This has been for the National Geospatial Intelligence Agency (NGA) and its mission partners.

An example of intelligence community usage could be for satellite processing. Some satellites may be Top Secret, so unauthorized users have no need to know that that particular satellite even exists. The System of Engagement requests sign on by the user first. They would not see the entire list of satellite's as that may have been excluded by an additional database query of accessible satellites for that user.

When comparing to medical devices, there is no secret that there are multiple imaging devices, but the results may not be visible to a user, based on the need to know. Many, many options exist. These are just examples to get the discussion started about new possibilities.

End user access is controlled via "stateless" sessions

But here's another important distinction from other models. The data operations are somewhat like the Eagle's song Hotel California:

"We are programmed to receive. You can check out anytime you like… but you can never leave".

That means if you are viewing the data, you are viewing the "System of Record". Where you are viewing from is called the "System of Engagement". By definition, the System of Engagement can overlay and complement the System of Record by transforming it. This is can be a stateless entity or read only. The Xray image, stored in a database, is just a collection of bytes. The end user may not have the proper viewer installed on their desktop. The System of Engagement will transform the image into something consumable and recognizable by the end user. The Hospital doesn't make a copy of the data and transmit it to other service providers. If they did, they'd have to ensure that those new data owners of the copy adhered to the same stringent privacy laws for which they are accountable. This becomes a logistics nightmare. Instead, the "user" being a patient or medical professional accesses a program (The System of Engagement), which could be a virtual desktop or web service, which in turn accesses the database and remotely presents the requested data to the end user. This is more like an image of the data, as the end user device is considered stateless. No local copy is saved. Because this is solely a remote presentation of the information, that device can be exempt from Privacy audits because it is understood that no local copy is made. This doesn't address an end user taking a picture or writing down information associated with the record being processed. There are other products that can be deployed to capture these breaches of privacy policy. Our infrastructure can handle that situation as well.

Compartments can be created that contain only a subset of the stored records, similar to a view. So analytic processing might be done across all database records, looking for patterns, fraud, opportunities, etc, but without including protected personally identifiable information. For example, analysis, such as disease outbreaks by region, trends, risks, etc, may only be done by someone with an authorized need-to-know.

Getting started can be easy as turning on a management feature

Some customers may already have the base infrastructure for the System of Record installed. There is a change in operations management required, but no additional software license charges required to implement this. Analytics can be provided, against this system of record, locally by bringing the analytic applications to the data, rather than copy it to the analytic application. Our infrastructure is capable of meeting the service level agreements of both the updates and queries of the database with very large scale and high availability.

The end user Systems of Engagement may be Linux or Windows systems running on Virtual Desktops or PC servers, as well as application servers running within our secure virtualization infrastructure. The end user access could be from kiosks (thin client terminals), Smart Devices, PC's or business specific devices e.g. Point of Sale, ATM, police cruiser access points, etc. These systems could be hosted in a public or private cloud. They could be part of an existing system infrastructure. Authentication and access control should be centrally managed across the entire operational infrastructure.

Many savings over non-shared implementations

The net of all this is a couple of examples of hybrid computing and collaboration across systems that can dramatically reduce the complexity and improve the efficiency of end-to-end business processes. If you are still compartmentalizing operations by server silos you may have the unintended consequence of missing some dramatic cost savings or better stated, cost avoidance. Compartmentalization on a need to know basis may initially lead a business toward separation of duties and separation/copying of data. But with the capabilities described, it's actually a form of consolidation and collaboration that enables a greater degree of sharing the System of Record. You might not have to spend more in systems deployment to solve some very complex problems.

Customer avoids over $1 million in costs

There were many considerations and differences in the pricing comparisons of their shared vs. non-shared infrastructure. In aggregation, the reduced cost of the shared deployment was over $1 million dollars less than the non-shared infrastructure. The shared infrastructure hardware was a bit more expensive than the non-shared servers. The biggest savings was in middleware charges. There were many more copies required in the non-shared infrastructure. There were a fraction of software copies necessary for the shared infrastructure. In addition, special pricing is available for disaster recovery or backup sites that further reduce the overall expense necessary in the shared environment.

The result for this agency was a rapidly deployable solution that met their current processing, could accommodate future growth in the same footprint, provided out of the box resilience and investment protection for their future computing needs.

Proof of Concept

Our lab is ready and willing to meet your collaborative infrastructure needs. Our offer stands to help you save over $1 million compared to alternative infrastructure deployments.

For more information

To learn more about **Hybrid Computing Collaboration** please contact your IBM marketing representative or Vicom Infinity.

400 Broadhollow Road
Suite 1
Farmingdale, NY 11735
631-694-3900
631-694-2640
Email: request@vicominfinity.com

Produced in the United States of America
09/2014

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.