InterAct
White Paper

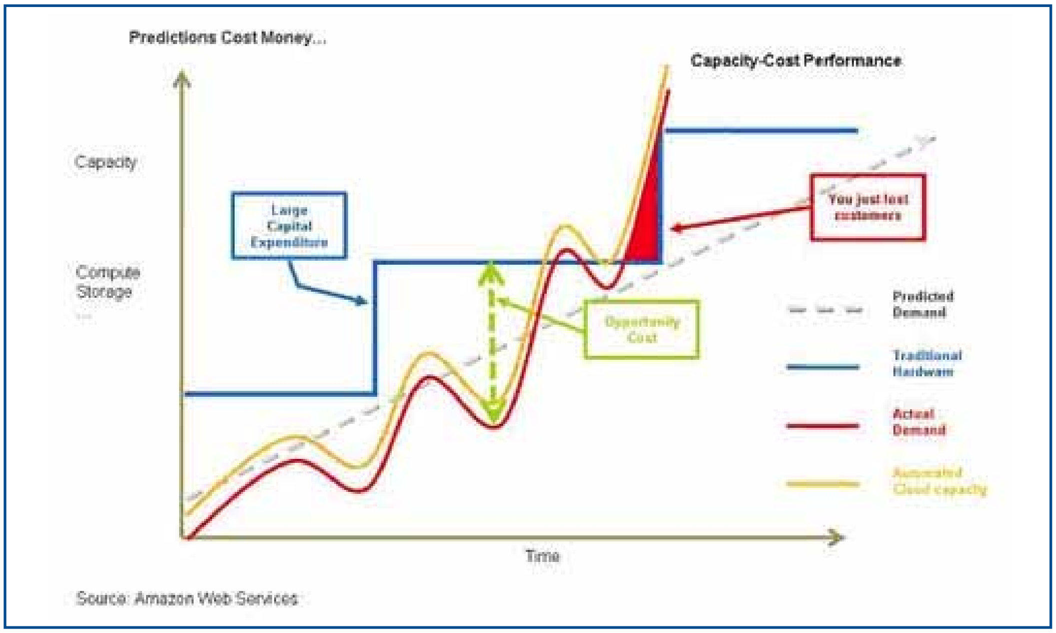
Business Intelligence

Cloud Computing in Public Safety

Cost Benefits are Only The Beginning of Cloud Superiority

Introduction

The U.S. Federal Government has adopted a "cloud first" policy that requires agencies default to cloud-based solutions whenever a secure, reliable, cloud option exists. The National Institute of Standards and Technology (NIST) has issued a three volume Cloud Computing Technology Roadmap and initiated a standards acceleration program so that best practices from the private sector can be used for government systems immediately, without a protracted standards process.



Source: Amazon Web Services

Figure 1 – The Cloud Eliminates the Costs of Both Excess and Insufficient Capacity

Cloud Economy of Scale

The motivation for this unprecedented initiative is clearly economic. Figure 1 shows the cycle of excess and insufficient capacity inherent in premise-based systems, versus how cloud based infrastructure scales quickly to meet, but not exceed, demand.

A Booz Allen Hamilton Study (Figure 2) compared the cost of 1000 premise based servers with equivalent capacity in public, hybrid, and private cloud environments.Their findings show that shared infrastructure alone results in 50-70% life cycle cost savings. Furthermore, the cost of the cloud itself is decreasing dramatically. The cost to run a basic Internet application on LoudCloud in 2000 was $150,000 / month. Running the same application on Amazon today costs $1500 / month, two orders of magnitude less. It is a conservative expectation that we will see still another order of magnitude reduction within the current decade.

All of these cost benefits accrue from the migration of systems infrastructure from premise to cloud, or Infrastructure as a Service (IaaS). Even greater savings and benefits are possible when platforms and applications are migrated to the cloud.

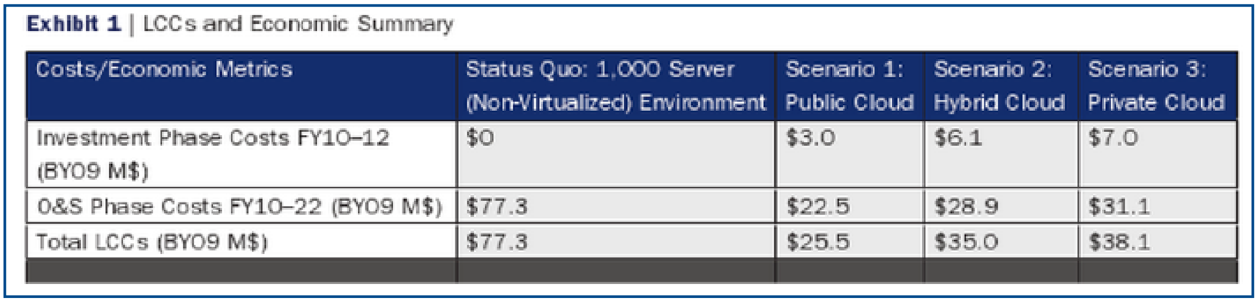


Exhibit 1 | LCCs and Economic Summary

Costs/Economic Metrics	Status Quo: 1,000 Server (Non-Virtualized) Environment	Scenario 1: Public Cloud	Scenario 2: Hybrid Cloud	Scenario 3: Private Cloud
Investment Phase Costs FY10–12 (BY09 M$)	$0	$3.0	$6.1	$7.0
O&S Phase Costs FY10–22 (BY09 M$)	$77.3	$22.5	$28.9	$31.1
Total LCCs (BY09 M$)	$77.3	$25.5	$35.0	$38.1

Figure 2 - Savings Approaching 80%

Software as a Service

Over and above the IaaS benefits described in the preceding are those of Software as a Service (SaaS). In the SaaS model, a vendor takes responsibility for not only infrastructure, but also for all of the processes required to manage an entire application solution (patches, upgrades, backups, database management, systems tuning, performance management, etc.). Because SaaS vendors manage many customers on a small number of application instances, they can amortize infrastructure costs over many customers. In other words, the inherent savings of IaaS are compounded when many agencies share a single system.

The terms Cloud and SaaS are sometimes (incorrectly) applied to hosted applications that are not multi-tenant. The benefits described here accrue from sharing resources. Simply hosting a dedicated system is insufficient. As traditional on-premise solution vendors move to the cloud, they learn that multi-tenant architecture is very difficult, if not impossible, to retrofit into legacy applications. InterAct's Online Applications are multi-tenant from the ground up, designed to take full advantage of scalable cloud based infrastructure.

The software architecture of such shared systems is called multi-tenancy because a single instance of the software application serves multiple client agencies, referred to as tenants. Databases and configurations are partitioned so that each tenant's user experience is identical to having a dedicated (rather than shared) system.

Because multi-tenant SaaS applications run on shared infrastructure, the incremental cost of deploying an additional customer is far lower. There is no hardware, operating system or database to purchase, no site preparation, no staging, and no delivery. By contrast, premise-based systems require an initial investment that leaves vendors no choice but to "front-load" costs. The SaaS model opens the door to pay-as-you-go subscription pricing. Of course, there are discounts for pre-payment and for multi-year contracts.

Hurwitz Group estimates that the four-year total cost of ownership (TCO) for SaaS based applications is about one third of the cost of a comparable premise based application. But the cost-benefit of SaaS is even greater. Upgrading premise-based systems is expensive. A vendor may release new versions of an application several times per year, but most customers only upgrade when the version they have deployed approaches end-of-life, or when a new version has features that justify the upgrade cost. Except for a short time after initial installation and occasional upgrades, customers are deprived of the benefits of the newest features. Furthermore, because upgrades almost always skip multiple releases, they are disruptive and require retraining.

SaaS applications are upgraded more frequently and in smaller increments. Most such improvements require little or no retraining. All customers get the benefit of all upgrades the moment they are applied, and there is no upgrade cost.

When most customers do not take advantage of most upgrades, vendors are encouraged to put most of their development effort into features that will enable them to acquire new customers. In the SaaS model, vendors' profits depend on keeping their subscribers happy, largely through new features that benefit existing customers.

The SaaS model ultimately provides the same type of products as a software licensing model - but with a better economic model, one that is lower in cost to the customer and structurally inclined to keep getting better for the customer with every new release.

Scott Sehlhorst, Pragmatic Marketing,
The Economics of Software as a Service (SaaS)
vs. Software as a Product - http://goo.gl/T75dQ

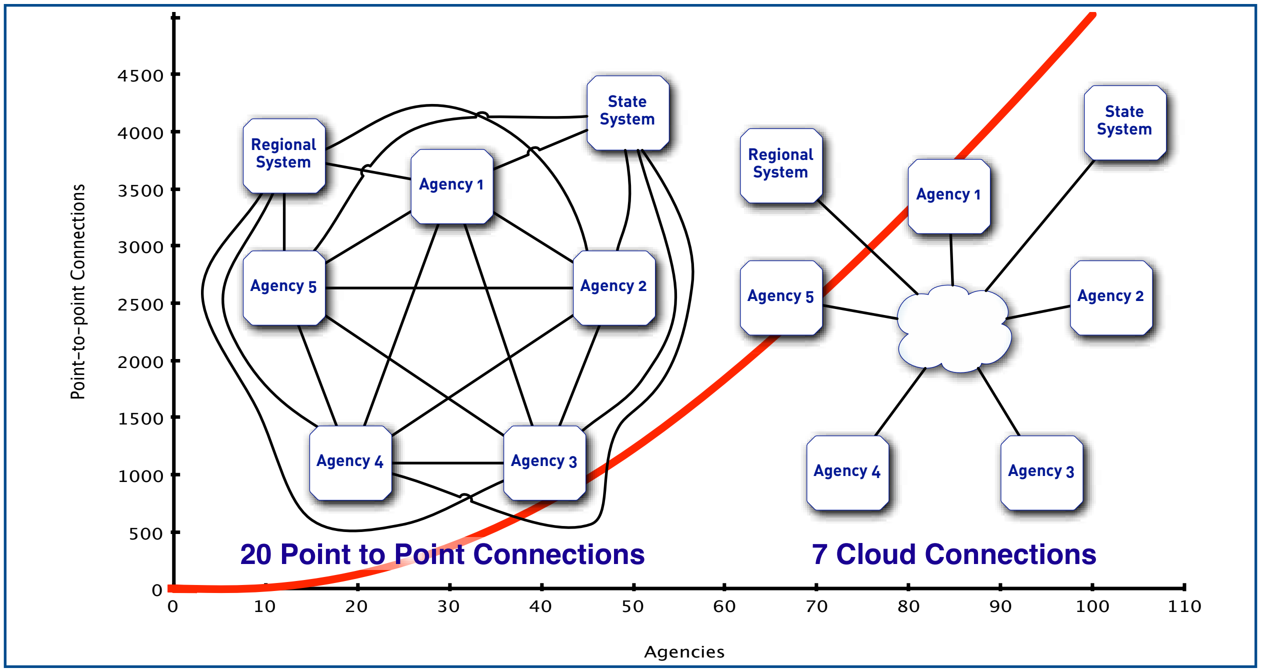


Figure 3 - Greater Connectivity with Fewer Connections

Cloud Benefits for Public Safety

Ironically, cloud adoption by public safety has lagged many industries for which the benefits are not nearly as great. The nature of public safety applications is such that the advantages of shared systems are greater in both cost and utility.

Interagency Integration and Intersystem Interfaces

Public safety applications are increasingly interconnected to inter-agency, regional, state, and national systems and databases. Each premise-based system must be individually connected to each external system. Every point-to-point connection takes network engineering, interfacing, monitoring, maintenance, support, and may require time-consuming certifications and audits. Shared systems come with shared external connections, live and pre-certified.

Figure 3 shows a nearly 60% reduction in the number of interfaces required for 5 agencies to share information and to acquire data from 2 external sources. For 20 agencies, the improvement approaches 90%.

As new data sources and applications become available, the cloud model makes it possible to amortize the investment required (to make third-party plug-in services available to users) over the entire user population. With lower integration costs come greater incentives for the creation of new, innovative technologies. As the cost-benefit of supporting third party services is enhanced by lower up-front costs, support for the add-on marketplace becomes a competitive advantage.

The cloud eliminates field service, enables vendors to do the work once for the immediate benefit of all customers, and the subscription model gives them a powerful incentive do so. In theory, Service Oriented Architectures make plug-compatible open interfaces possible in premise-based client/server environments, but in practice, the need to support multiple installed versions of each such interface with a field service workforce makes most cross-vendor integrations financially unattractive, so they are only done when necessary to acquire new business. The investment must be repeated for each new version of each interface for each customer, and when customers aren't up on the newest version of primary product, they can't take advantage of the newest plug-ins.

Connectivity to the Public

In the same sense that state or national CJIS databases are resources, so are citizens who adopt public-facing collaborative apps, and the complexity and cost of connecting agencies and responders to such applications is orders of magnitude less when agencies use shared multi-tenant online systems.

Security

It has long been the opinion of old school IT people that the most secure systems are those housed within the walls of the enterprise. And when the external "surface area" of those systems consisted of a few dial-back modems for systems engineers debugging batch jobs on 3rd shift, they were. But today, useful information systems are not so isolated. They present themselves to users through web and wireless interfaces, and they make use of a myriad of network (a.k.a. cloud) resources. Yet it is still the conventional wisdom that the cloud computing and SaaS applications, are somehow more vulnerable than premise-based client/server or in-house web based (intranet) systems. The truth is the exact opposite!

Cloud computing infrastructure is, in nearly every respect, more secure that its premise-based equivalent. An Aberdeen Group study states, "Compared to companies using on premise web security solutions, users of cloud-based web security solutions had 58% fewer malware incidents over the last 12 months, 93% fewer audit deficiencies, 45% less security-related downtime, and 45% fewer incidents of data loss or data exposure."

AlertLogic, a security monitoring service provider analyzed 2.2 billion security events, classified 62 thousand as credible incidents, and determined that the frequency of incidents for every significant category is lower for systems operated by service providers.

Hundreds of millions of dollars worth of financial transactions are conducted on the public Internet every day. Trade secrets and confidential data are exchanged. Even organizations that don't deploy their business applications in the cloud rely on its secure infrastructure to conduct crucial business activities.

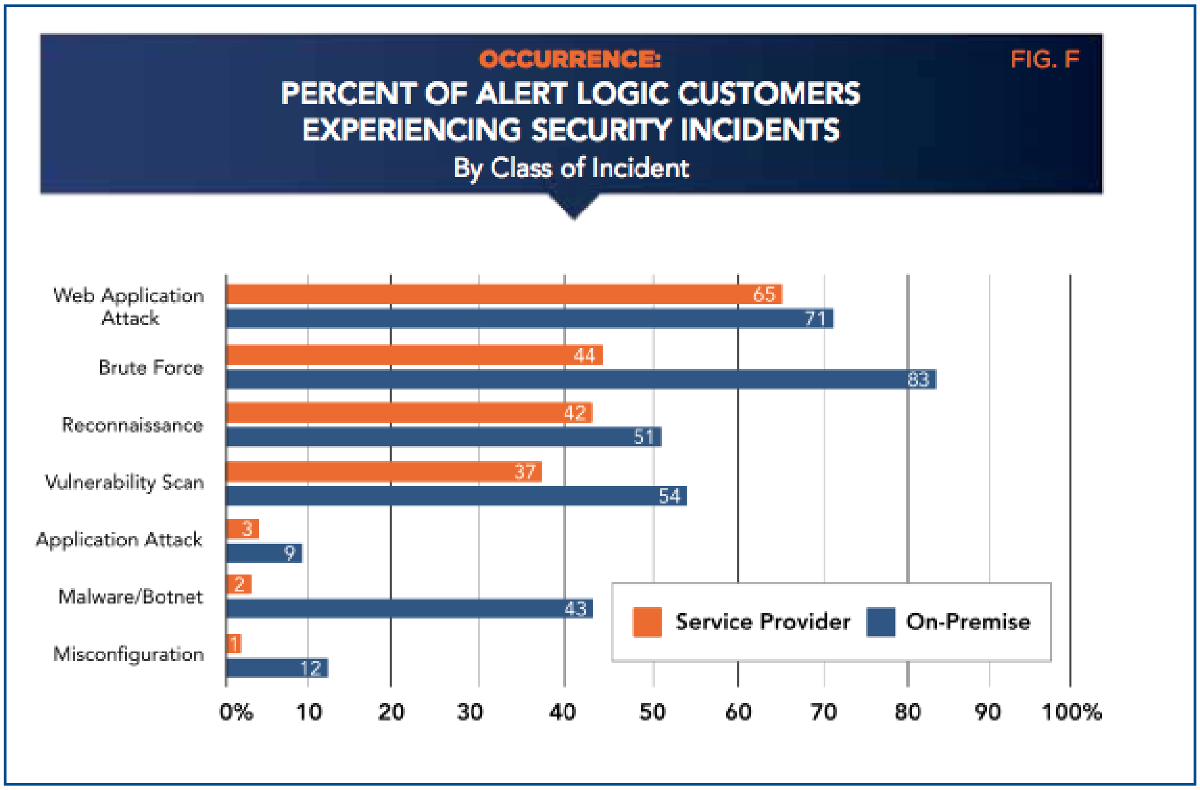


Figure 4 - Fewer Security Incidents with Cloud Based Systems
Source: AlertLogic

Since their inception, online service providers have been exposed to the open Internet, and have consequently learned to be far more diligent in application of best practices for security. Note for example that misconfiguration incidents are twelve times more common for on-premise systems. Misconfiguration is the online equivalent of leaving your car unlocked with your keys in the ignition. Either security options are not turned on, or default userids and passwords are left unchanged (e.g. admin/admin).

A search of LinkedIn for the keyword CISSP (Certified Information Systems Security Professional) yields about 60 thousand hits, .04% (one in 2500) of which work for government agencies in public safety.

Mobility

Public safety activity is inherently mobile. The majority of the workforce operates in the field. A typical responder's need for instant access to a broad range of information far exceeds that of a typical field service practitioner, and they are the source of diverse and complex data that may be of immediate value to others.

Early mobile data systems for queries and dispatch preceded ubiquitous commercial data networks by many years, and relied on proprietary data transmission piggybacked on land mobile radio (LMR) systems. Because data transmission was painfully slow and often unreliable, applications were optimized to minimize data traffic and tailored to tolerate high error rates and intermittent connectivity. A class of mobile applications evolved that was (and is) entirely separate from those used by dispatchers and records clerks who worked in offices.

As commercial networks were developed and the Internet flourished, a different approach to mobile applications was propelled by consumer demand for mobile access to the utility and pleasure of the Internet. In order to deliver the web to mobile devices, the problems of data compression, error corrections, and tolerance of intermittent connections had to be solved in the network layers. Wireless vendors tweaked the infrastructure, and web development frameworks and techniques were optimized within the constraints of wireless networks. Today's modern web applications need only to adapt to the form factors of mobile devices. Essentially the same applications run in the back office and on mobile web browsers.

Despite the advancement of commercial networks, and their adoption by most public safety agencies, most mobile applications for public safety are still deployed on traditional mobile data systems, with their fat clients and proprietary message switches. The big disadvantage is, ironically, the lack of mobility. Responders are tethered to their vehicle-mounted ruggedized laptop computers, and version upgrades

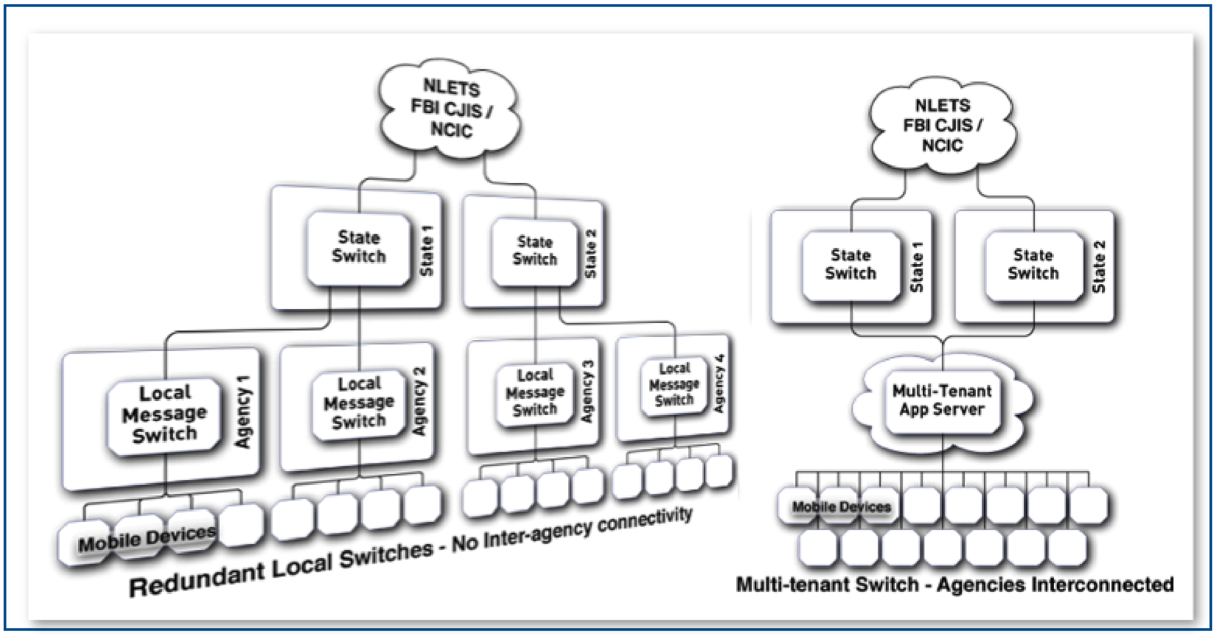


Figure 5 - Cloud Based Mobile Systems Require Less Redundant Hardware

are even more problematic than for back-office client/server apps.

The server side of mobile data client/server apps is an even bigger opportunity for improvement. Client/server based mobile systems require each agency to deploy a local message switch, interfaced (through no small effort) with a state CJIS network. Cloud deployed multi-tenant app servers could easily replace hundreds of these servers per state, along with the lifecycle costs of purchasing, installing, operating, maintaining, and auditing them. Figure 5 shows a single multi-state server. State CJIS administrators, who are charged with security and regulatory compliance, do not yet universally accept this architecture, but obstacles are being overcome, and a multi-state service has the big advantage of interstate connectivity for data sharing and messaging.

There is no reasonable doubt that modern web apps will make mobile fat client solutions obsolete. In the absence of wireless infrastructure constraints, the portability, device support, elimination of massively redundant server infrastructure, and ease of deployment make online applications too attractive to pass up. It is only a matter of time for vendors and customers to make the necessary investment. There will be a few applications for which installed smart client applications offer advantages, but even these will utilize cloud based services and deployment models.

The Shape of Things to Come

In the private sector, largely as a result of experience gained in consumer applications, there is a nascent understanding that user satisfaction is correlated with simplicity and usability, which are inversely related to the number of features in a product. In simple terms, "Consumers think they want all the bells and whistles—until they actually use what turns out to be a very complicated product ."

> Customers are most satisfied with products that get the job done with the fewest possible features, functions and options.

Multi-tenant online systems offer huge economic advantages over traditional systems. But they can't be customized individually for each customer. They are not inflexible, but to take advantage of their benefits, customers must rethink the relative value of usability and features. Since customer satisfaction is more strongly correlated with usability than with the number of features, this turns out to be a benefit rather than a limitation.

In a Harvard Business Review summary of their research , Roland Rust et al suggest:

"Particularly in cases where a company has packed one model with many features to address market heterogeneity, consumer satisfaction might be greatly enhanced by tailoring products with limited sets of capabilities for various segments.

… This makes the decision process more difficult for consumers, forcing them to think carefully about which features they actually need. Moreover, our empirical results suggest that people will be tempted by products that offer greater capability."

Among the reasons public safety has been underserved is that these behaviors have been reinforced by formal procurement processes that require complete pre-specification of requirements, and consultants who cross-pollenate requirements from one project to the next rather than helping users to carefully choose the features they really need.

SaaS adoption cycles are far shorter and up-front costs are far lower, enabling hands-on trials to replace protracted pre-specification. As vendors move toward simpler solutions, tailored to homogeneous subclasses of users, buyers will adopt less costly procurement vehicles that are appropriate for lower risk purchases.

When the cost of procurement and adoption fall, the tendency to overload procurements is reduced. In the past, the costs of issuing and evaluating RFPs coupled with up-front software fees and custom implementation have encouraged customers to "throw the kitchen sink" into their RFPs. When the cost of a shopping trip is very high, customers are encouraged to purchase everything they could possibly need in

Figure 6 - Feature Bloat

the foreseeable future every time they shop. When up-front costs are reduced, customers can purchase what they need when they need it and eliminate the need to pay for features they will probably never use just in case they might need them in the future.

Product Versus Platform

One of the benefits pitched by the purveyors of complex monolithic products is "integration". Ostensibly a suite of products that share a database should work together seamlessly. Information is passed from module to module and is always readily accessible. While it is true that tightly coupled systems are inherently integrated, tight coupling is not the only way to achieve a high level of integration between modules. And, tight coupling has significant disadvantages, not the least of which is the feature-bloat described above. It is also difficult to decouple tightly coupled systems. Customers are forced to make all-or-nothing decisions, and may be forced to replace systems that are working well.

In a properly implemented Service Oriented Architecture (SOA) loosely coupled modules utilize simple externalized open interfaces to achieve tight integration between applications, modules, and subsystems. Components may be supplied as part of an integrated system or suite, or configured to exchange standardized information packages with external customer-supplied and third party systems. Standards based data exchanges such as NIEM and others dramatically reduce the complexity and attendant cost of configuring data exchange interfaces.

The greatest benefit of loosely coupled SOA is extensibility. An extensible system is one that includes mechanisms for expanding or extending features and functions without changing the baseline system. Loosely coupled SOA allows completely separate processes, running on geographically separate systems to exchange information and request services as though they were modules in a single executable program. To the extent that interactions are based on standards, setting up interfaces requires only configuring each process to be aware of the other.

Conclusion

There is no credible reason to doubt that the cloud will be the predominant platform for public safety applications. Even legacy on-premise systems will be interconnected with a myriad of cloud-resident services including the NG9-1-1 communications backbone of emergency response. The benefits of scale and connectivity are not only economic but also functional. Shared multi-tenant systems really do enable public safety providers to do more with less.

Like all technology revolutions, migration to the cloud will take time. One of the benefits of cloud applications is that they are not an all-or-nothing proposition. Through service oriented architectures and standards based data exchanges, cloud and legacy technologies can and will coexist for some time. The benefits of the cloud will drive an urgent but orderly and methodical migration.

No technology is perfect. There will be challenges along the road, but the destination is clear: collaboration, information sharing, interoperability, and engagement are central to the mission of public safety. The cloud has been proven beyond any trace of doubt to be the enabling technology for all of the above. The revolution has begun.

Author

Mark Fetherolf
Chief Technology Officer
InterAct
email: mark.fetherolf@interact911.com

Sources

[1] Federal information technology shared services strategy - http://goo.gl/fNdFK

[2] NIST Special Publication 500-293, US Government Cloud Computing Technology Roadmap, Release 1.0 (Draft), Volume I High-Priority Requirements to Further USG Agency Cloud Computing Adoption - http://goo.gl/CPmQR; NIST Special Publication 500-293, US Government Cloud Computing Technology Roadmap, Release 1.0 (Draft), Volume II Useful Information for Cloud Adopters - http://goo.gl/qLebx; NIST US Government Cloud Computing Technology Roadmap Volume III - Technical Considerations for USG Cloud Computer Deployment Decisions (First Working Draft) - http://goo.gl/skV2Q

[3] Booz Allen Hamilton, The Economics of Cloud Computing - http://goo.gl/wPSLE

[4] Hurwitz Group - The TCO Advantages of SaaS… http://goo.gl/Ofdg8

[5] Web Security in the Cloud: More Secure! Compliant! Less Expensive! Derek Brink, Aberdeen Group, May 2010, http://goo.gl/XZeDI

[6] Removing the Cloud of Insecurity, State of Cloud Security Report, Spring 2012, AlertLogic Inc., http://goo.gl/QMK1N

[7] Journal of Marketing Research, November 2005, Thompson, Hamilton, and Rust, Feature Fatigue: When Product Capabilities Become Too Much of a Good Thing

[8] Harvard Business School, Working Knowledge for Business Leaders, Archive, 5/8/2006, Rust, Thompson, Hamilton, Feature Bloat: The Product Manager's Dilemma