A New Era
Cloud Ushers in Insight-Driven Defense

High performance. Delivered.
# Table of contents

How will cloud computing change the game for defense agencies? 2  
Entering the era of insight-driven defense 3  
Mapping a path to cloud maturity 6  
Six ways cloud computing will change the game in defense 7  
The future provisioning model for cloud in defense:  
The cloud services broker 15  
Building a platform to seize the cloud computing opportunities 19  
References 21
How cloud computing will change the defense industry

A fast-changing and unpredictable world...

Defense agencies across the world are facing unprecedented change in military threats and requirements. Whether they are collaborating with allies to tackle a sudden threat in remote and hostile territory, defending their systems against cyber attacks, or delivering humanitarian relief, the pace, agility and coordination of operations are increasingly important.

Meeting these needs critically depends on an ability to control, share and access data, without compromising information security in any way. And agencies must achieve all this at a time when defense budgets—both in the US and globally—are tighter than at any time in recent history, and are likely to tighten even further.

...demands new ways of managing, sharing and securing information

In response, growing numbers of defense agencies worldwide are investigating the potential of cloud computing to transform way they organize and manage their information, operations and relationships. And they are identifying ways to seize the benefits of cloud while maintaining the highest standards of security over classified and mission-critical data.

Different defense agencies are at different stages on their journey to cloud computing, and taking different routes to their destination. We believe the direction of travel is clear—and that the momentum will continue. In the defense world, cloud computing is a concept whose time has come. It’s going to change the game.
Across all the activities undertaken and overseen by defense agencies—from intelligence gathering on emerging threats to platform readiness and sustainment; from battlefield operations to supply chain logistics; from disaster relief to collaboration with allies—there is an increased need for timely, accurate and comprehensive data.

Effectively managing each area of operations critically depends on defense agencies’ ability to manage, understand, share and secure information, and to use it to drive and apply accurate and actionable insights. But in seeking to achieve these goals around data, defense agencies face significant hurdles in the sheer volume, diversity and sensitivity of the information they hold.

Effectively managing each area of operations critically depends on defense agencies’ ability to manage, understand, share and secure information, and to use it to drive and apply accurate and actionable insights. But in seeking to achieve these goals around data, defense agencies face significant hurdles in the sheer volume, diversity and sensitivity of the information they hold.

Proliferating data, declining budgets

Defense agencies have a complex organization-wide matrix of different types of data for different purposes—back-office, operational, intelligence, personnel, finance, logistics, and more. Each item of information has its own specific security sensitivities and requirements, ranging from top-level classified and mission-specific intelligence, to publicly available communication and recruitment information.

The complexity is compounded because individual personnel generally have multiple clearance and access levels for different data sets. Some data is specific to one of the armed forces, some shared across them, and some shared externally with other government agencies or even coalition partners.

As well as being diverse, defense agencies’ data is also expanding exponentially in volume, driven by advances in areas such as, remote electronic sensors, cybersecurity, and surveillance by satellite and drones. To manage and store these rising volumes of data, and then generate the detailed insights they need, defense agencies require increased storage capacity and analytical processing power, imposing greater costs. Yet agencies need to meet these demands against a background of declining budgets, requiring them to drive operational efficiency upwards and deliver “more for less.”

The US Department of Defense (DoD) starts its cloud migration

The US DoD has begun a transformation to cloud computing by launching a set of initiatives aimed at achieving improved mission effectiveness and cybersecurity in a reengineered information infrastructure. The result of this new effort will be the Joint Information Environment (JIE)—a robust and resilient enterprise that delivers faster, better-informed collaboration and decisions enabled by secure, seamless access to information regardless of computing device or location.

According to “Hype Cycle for Smart Government, 2012” published by Gartner, Inc., this migration, “the DoD is setting up private or community clouds with high levels of security to enable efficiencies and intelligence-sharing.

The DoD has developed private cloud-like services at the Defense Information Systems Agency (DISA) for infrastructure as a service (IaaS), limited platform as a service (PaaS), enterprise email and SharePoint.” Pilot cloud efforts are under way across DoD, and savings are being realized. In the 2011 financial year, the DoD exceeded its target by closing 55 data centers.

The DoD’s hybrid cloud computing strategy, announced in July 2012, is centered on using cloud to contribute to three key DoD objectives:

1. Reduced costs and increased operational efficiencies by consolidating systems, using resources on an as-needed basis, and leveraging existing DoD cloud computing development environments

2. Increased military mission effectiveness by improving business continuity, warfighter mobility and the real-time exploitation of big data

3. Increased cybersecurity, including leveraging the Certification and Accreditation process supported by FedRAMP and standardizing and simplifying identity and access management

Entering the era of insight-driven defense
Initial moves into the cloud

The challenges mentioned are seeing defense agencies worldwide move away from an expensive, device-centric view of computer information systems (CIS), towards a more efficient view centered on information, applications and the people who use them. This is the view of the world enabled and empowered by cloud computing. As a result, more and more defense agencies—initially in the US, but increasingly in other countries are piloting and implementing cloud-based solutions, drawing on demonstrated expertise and knowledge developed in private sector, commercial and other government clouds. Further impetus is being provided by the wider moves into cloud computing being made by governments worldwide.

As the development of "g-clouds" gains momentum, some defense agency clouds are already up and running, while many more are at the pilot stage. As with government clouds generally, the cloud models being used in defense differ widely, and additional models will emerge over time, but there is consistent focus on tapping into the scale, agility and pay-per-use basis of cloud-based solutions to deliver a set of operational and cost benefits. For example, agencies are finding that formerly complex and time-consuming tasks become simple and routine, costs are reduced, operational efficiency rises, military mission effectiveness is enhanced, and cybersecurity can be strengthened.

As cloud implementations gain momentum, other benefits are becoming clearer. These include a reduced risk of vendor lock-in, since cloud enables an agency to drop a poorly performing provider and move on to a better one while content remains unaffected in the cloud. Looking forward—as we will highlight in this paper—the capabilities of cloud computing can enable transformational benefits, impacting virtually all areas of defense agencies’ activities and operations.

But despite the benefits already being achieved, concerns remain—especially around security. Common fears in moving to cloud computing include the risks of unauthorized access to classified information; loss of vital data, requiring robust disaster recovery features; people changing or modifying data either maliciously or inadvertently; and people accidentally or deliberately posting classified information onto systems not designed to hold it.

More broadly, there are concerns over "Big Data" within and outside the organization. In today's data-rich world, there are concerns that adversaries might gather large volumes of public or semi-public information and join the dots to gain unauthorized insights. This risk demands rigorous tracking and audit trails of anyone who has accessed data, whether in the cloud or on traditional systems.

Balancing cost, effectiveness and control

The good news is that cloud computing architectures have the capabilities needed to address these concerns. The goal for defense agencies is to realize the types of efficiency available from a public cloud, but to do so in a secure environment. The key to achieving this goal is to choose the model of cloud computing that provides the appropriate balance between cost, effectiveness and control for each use case and application, given the sensitivity of the data and insights involved.

As we summarize on page five, four main deployment models for cloud computing exist, each with different cost and security implications. To date, private clouds or virtualization has proved the most attractive option for defense agencies conducting cloud computing pilots and implementations, since it provides significant cost benefits while the data remains under close internal control.

However, our view is that community cloud models will also emerge over time, as they provide close control within a distinct and carefully-selected group of users. In the next few years, community clouds will emerge across governments, across defense agencies (including the various armed forces), across different arms of defense intelligence, and even across international coalitions.

We also believe that agencies’ cloud landscape will expand to include some usage of public cloud, creating a hybrid model. While the most sensitive and classified data is likely to remain on in-house systems, including private clouds, their more public-facing applications such as recruitment could move to public cloud—always with the proviso that appropriate security thresholds are met. To source, manage and provision the resulting mix of in-house and legacy services with various forms of cloud, agencies will move to a ‘cloud services broker’ model for IT. We describe this concept in more detail on page [x].

Governments take various routes into cloud computing

Governments’ cloud strategies across the world range from mandating some level of use of cloud computing by government departments and agencies, to ensuring that individual government organizations have the necessary decision frameworks—including procurement guidance—to venture into cloud computing.

In mature markets, most governments have cloud strategies in place and have begun investment in shifting public administration IT to cloud computing architectures. In contrast, governments’ cloud readiness in emerging markets varies greatly, with most countries still in the planning stages.
Gartner predicts cloud computing as a delivery model to shape buying and prioritization of security

In January 2013, Gartner made three predictions about the security solutions industry for 2013 and beyond:

• “By 2016, public cloud infrastructure will include and be mandated to critical national infrastructure regulations by the US.”

• “By 2015, 10 percent of overall IT security enterprise product capabilities will be delivered in the cloud.”

• “By 2015, 20 percent of the VPN/firewall market will be deployed in a virtual switch on a hypervisor rather than a physical security appliance.”

Cloud computing: a quick primer for defense agencies

Cloud computing is a proven model for providing and sourcing IT hardware and software services on a pay-per-use basis using internet technologies. Cloud services are configurable, adaptable and scalable, and generally require less up-front investment and ongoing operating expenditure than traditional IT models. Clouds generally take one of four forms (or a combination of these forms)—private, public, hybrid, and community—each bringing its own implications for data control and security.

Private clouds are dedicated to a single organization for private use, and thereby offer the highest level of internal control over data and applications. They can either be built within its own data center, or located off-premise and provided by an external third party to deliver virtualized application, infrastructure and communications services for internal business users. Public clouds are owned and provided by external third parties over a network, meaning that control and oversight over data must be handled by the external provider. Hybrid clouds offer a mixed degree of control, blending the benefits of public and private clouds by enabling an organization to retain confidential information in a private cloud, while providing access to the wider choice of applications available in public clouds.

Community clouds — again mixed in terms of data control — are collaborative resources shared between a number of organizations with common requirements and interests, which are often in the same industry, with the costs spread across the users. Like private clouds, community clouds can be hosted internally or by external third parties.

All four forms of clouds can provide on demand computing at one or more of four levels.

• At the infrastructure level, companies use infrastructure-as-a-service, or IaaS, offerings to source raw computing resources, processing power, network bandwidth and storage on an on-demand basis. IaaS is generally an organization’s first step into the cloud.

• At the platform level, cloud-based platform-as-a-service, or PaaS, offerings provide companies an environment that supports rapid evolution for key business application development that needs continuous change, helping to foster ongoing business innovation while controlling costs.

• At the application level, cloud-based applications—generally known as software-as-a-service or SaaS—are available via standard browsers, supporting device independence and anywhere access. Some SaaS offerings, such as the customer relationship management cloud on salesforce.com, have achieved widespread adoption across many industries. Both SaaS and PaaS have established themselves as ways of delivering new functionality quickly.

• At the business process level, cloud-based solutions known as business process outsourcing platform-as-a-service (BPaaS) or platform-based business process outsourcing (BPO) offer an internet-enabled, externally-provisioned service for managing an entire business process. This differs from application clouds in that BPaaS provides end-to-end process support, covering not just software but also people processes, such as contact centers.

Cloud computing + mobility + analytics = game changer

As defense agencies move to pilot and adopt cloud solutions, cloud technologies are converging rapidly with mobility and analytics to open up new vistas of opportunity in all industries. Defense is no exception. We believe agencies will increasingly apply these three technologies in combination, often with game-changing impacts. We’ll now look at six ways in which we think cloud computing and these other technologies will change the game.
Mapping a path to cloud maturity

Figure 1. Leading defense organizations will use cloud’s unique characteristics based on a well formed cloud strategy, assessment, and migration plan

Examples

- Governance is in place to adopt new cloud capabilities as they mature
- Employs advanced capabilities regarding cloud security, advanced integration, highly secure environment support
- Basic IT functions plus Integrated Acquisition and Maintenance, Force Generation (Preparation, Analytical and Operative Insights) and Deploy, Operate and Sustain
- Employs hybrid cloud integration or enterprise integration
- Focus on unique systems – limited, if any integration
- A push towards basic IT functions: email and collaboration functions

Leading defense organizations will be

- Realizing all the available value from level 1
- Proactively and systematically exploring opportunities at level 2
- Preparing for level 3 as the cloud matures – depth and scope of cloud market increases

As defense organizations increase their utilization of cloud, they are on a journey toward using cloud’s unique attributes as an ever greater enhancer of key defense capabilities. Accenture has devised a cloud maturity model (see Figure 1) to help defense organizations map their path to cloud maturity. It will help defense leadership pinpoint their organization’s stage in the journey, assess the upcoming opportunities and plan their best next steps. The model divides the journey to cloud maturity into three main phases. The journey starts with selected back-end functionalities within branches, enhancing collaboration capabilities and increasing storage. At stage two, the scope can expand across branches in select functional areas (e.g. HR, Finance) to increase analytical capacities, reducing costs and making complex and time-consuming tasks routine. The third and final step includes shared functionalities across branches with all levels of security classification to produce real-time intelligence and exploitation of big data, increase operational efficiency, enhance mission effectiveness and strengthen cyber-resilience.

At the same defense organizations progress from a focus on costs to ad-hoc strategic enablement, before finally making cloud an integral part of the strategy. Each of these objectives addresses a different defining factor of the defense context that we described earlier. Clearly, different organizations will move into the cloud at their own pace, reflecting the unique characteristics and mission objectives. However, our industry experience and insights indicate that to get the most out defense cloud, defense organizations will be:

- Realizing all the available value from level 1.
- Proactively and systematically exploring opportunities at level 2.
- Preparing for level 3 as the cloud matures— as the depth and scope of the cloud ecosystem increases.
Six ways cloud computing will change the defense industry

Here are six ways we believe cloud computing—combined with the converging forces of mobility and analytics—will change the way defense agencies operate.
Defense agencies are already realizing significant cost and agility benefits from cloud technologies. Initially, the cost savings have come mainly from moving from traditional data centers to IaaS under private clouds or virtualization models. The savings can be significantly larger if IaaS is outsourced to a third party, but to date, due to security considerations, most agencies have chosen the in-house route.

Some agencies are gaining additional cost benefits from “thin provisioning” of storage capacity, where the available storage capacity is constantly realigned with need. Intelligence agencies in particular are facing a situation where they’re “maxed out” in terms of data storage, and are bearing rising server costs as a result. Thin provisioning can provide opportunities for significant savings, by using “shared compute, shared storage” architectures to balance and meet storage needs while maintaining capacity buffers.

Costs can be further reduced by combining the IaaS solution with more efficient and responsive allocation of IT staff, freeing up skills for higher-value activities. Agencies are also finding that the savings increase the further up the IT stack they take their cloud provisioning, from their starting point with virtualization and—IaaS to PaaS and SaaS solutions.

“When we combine infrastructure as a service, continuous delivery automation and the agile development approach, this is a game-changer.”

Robert Vietmeyer, lead for cloud computing and agile development within the enterprise services and integration directorate at the Department of Defense office of the CIO

Generally, the higher up the IT stack, cloud computing’s benefits in terms of speed and responsiveness increase, along with the potential for agile development. With PaaS, for example, agencies can develop mission-critical applications far faster and more efficiently through reusable components and shared modules—thus helping to reduce the time taken to develop new capabilities from months or years, to hours or days—bringing new capabilities to the front line much faster. One way to boost application development speed and reduce cost is to apply the “burst” technique using public cloud services.

Further opportunities to act at higher speeds and lower costs can be realized from SaaS, especially when combined with secure mobile access. Going forward, many agencies may create an “app mall”—a bank of ready-made, standardized, reusable apps that can be shared, used, improved and repurposed across forces and missions. An app mall saves development cost, time and effort while also boosting the speed of delivery to operatives in-theater.

Using public cloud “burst” for application development

While security considerations often mean much of a defense agency’s data will remain in private cloud architectures, one viable use of lower-cost public cloud for agencies is rapid, iterative application development through the “burst” technique. Developers can use public cloud to develop and test the application at high pace and low cost, with the finished application then being “poured back” into the private cloud before being populated with sensitive data. As such opportunities demonstrate, one of the challenges for defense agencies going into cloud computing, is pinpointing the tipping-point at which to go for public versus private cloud. This means striking the right balance in every case between cost and security. An expert third-party cloud computing adviser can provide valuable input into these vital decisions.
Defense agencies have historically built their systems in-house, on a silo basis, with different armed forces—and even different missions—having an entire dedicated IT stack, from network to applications. One driver behind this approach is the fact that operational security (OpSec) is paramount and must never be compromised.

While the critical importance of OpSec will not change, one thing that we believe will change is the widespread misconception that cloud computing architectures are inherently less secure than in-house silos. Security in the cloud—as in other architectures—comes down to the rigor and consistency of the standards applied. Moving to cloud computing offers defense agencies an opportunity to implement the security capabilities in a near-greenfield environment—doing it right the first time and diminishing resource and capacity requirement hindrances.

The current silo approach can actually weaken security in some ways. One of the arguments for having data in multiple physical systems is that adversaries have to break into more than one system to be successful. But, at the same time, creating the IT stack in a separate silo for every mission multiplies the chances of human error (and possibly loss of life) in the silos. There is also a risk that having hundreds of silos creates myriad vulnerabilities and a huge electronic surface to defend, since attackers seek out the "weakest link."

Encryption and tokenization of data at rest, in transit and in process, is a cloud security technology solution capability that is prime for implementation.

Many vendors have raised the stakes regarding the cryptographic algorithms that they support—reaching into the defense domain’s toolbox to establish a lower acceptable threshold.

Cloud computing can strengthen overall security by reducing the risks of individual errors or weaknesses in each silo, while also maintaining consistent and rigorous security standards across the entire organization. And technical advances are enhancing cloud’s security capabilities. For example, sensitive data can now be made “self-protecting”, by having security and authorization access built into the metadata integrally attached to the data itself. This enables security to flow with the data as it moves across cloud services, networks and devices—which helps make sure it is only readable by authorized individuals, whether at base or in-theater.
Exploratory Security Analytics: fighting cyber-attackers on their own ground

Whether they are teenage hackers or governments, the adversaries seeking to penetrate defense agencies’ systems use cloud technologies to source the processing power needed to identify vulnerabilities and then develop and launch attacks. Exploratory security analytics is a cloud-driven tool that enables defense agencies to track and model the activities, motivations and behaviors of their cyber adversaries, and to use this intelligence to anticipate emerging threats and take proactive actions to head them off. The scale and processing power needed to support these tools means the cloud is the only viable and cost-effective environment in which to run them.

Advances in exploratory security analytics permit the evaluation of security hypotheses to validate assumptions and provide more accurate and near real-time situational awareness. Visibility across cloud platforms, service providers and traditional IT environments the hybrid world we are now inhabiting permits security decisions to be made better, faster, cheaper – with a higher degree of accuracy [and lower risk exposure] for agencies.

The escalating cybersecurity threat from cloud-powered attackers is underlined by increasing action from governments worldwide to counter the threat. During his State of the Union address in February 2013, US President Barack Obama commented: “We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy.” The following week, the President signed an executive order designed to protect critical national infrastructure (CNI) in both the public and private sectors against cyber attacks, by developing voluntary standards and sharing classified threat data between companies and the US’ defense and intelligence agencies. Comparable steps are being taken by several other governments worldwide. The UK Government has put in place a £650 million (US$983 million) National Cybersecurity Programme, focusing on threats including state-supported espionage and attacks on UK CNI. In January 2013, UK Members of Parliament on the Defence Select Committee published a report on cybersecurity in relation to the Ministry of Defence and the Armed Forces, highlighting the risk that a successful cyber attack could potentially result in the armed forces’ ability to operate being “fatally compromised.” Meanwhile, at a European level, the European Commission is working to launch a new cybersecurity strategy, along with a directive calling for each EU member state to set up ‘CERTs’ — Computer Emergency Response Teams — to deal with hacking and malware crises. The Australian Government launched its new cybersecurity strategy in January 2013, aiming to enhance the country’s ability to respond to all cyber issues.
Security considerations mean defense agencies and forces have historically sought to keep data to themselves, at times exhibiting a reluctance to share it with other organizations, including other government organizations. However, the resulting silo approach can cause widespread fragmentation across data, applications and devices, acting as a drag on speed, efficiency and interoperability. Cloud computing can enable secure sharing of data across missions, between forces and among allies, boosting the ability to respond quickly and effectively, and enhancing interoperability, coordination and collaboration.

When combined with mobility, cloud computing opens up further opportunities in the “BYOD” (bring-your-own-device) arena. Defense agencies are facing the same trend towards the consumerization of IT as commercial organizations, with personnel expecting to use the types of devices they are most familiar and comfortable with. Cloud solutions will enable agencies to select and adapt the most appropriate and usable device for each situation, such as a hardened tablet with added security features. A good example of this model is Accenture’s own approach with cellphones. While the individual employee owns the handset, Accenture installs layers of security on the mobile device to make it usable for sensitive work purposes. Whether owned by the agency or the personnel, other devices such as laptops and tablets can be managed and configured in a similar way.

A further opportunity presented by cloud computing is the ability to gain constant feedback from across the armed forces on how to improve operations. The UK Ministry of Defence implemented such a system in the cloud in 2012.

With access to cloud technologies via secure devices, interoperability will also be improved, due to the ability of different missions and forces to ‘plug in’ with secure ID authentication to cloud apps and data from various devices and locations. This will improve collaboration not just in military operations but also in disaster relief missions, which require rapid and responsive coordination with governments locally and with NGOs.

**Israeli Army adopts cloud computing**

The Data Center and Computer Systems unit that lead’s the Israeli Army’s automation process, is preparing to implement a new server system which will shift to cloud computing in 2013. The change reflects the need to maintain the Israel Defense Force’s computer systems at the highest level of readiness, and to provide an appropriate degree of defense in cyberspace should the computers come under an attack.

**UK Ministry of Defence (MoD) taps into the UK G-Cloud program**

In November 2012 the U.K. Ministry of Defence (MoD) became the latest UK central government department to tap into the UK government’s G-Cloud program, when it rolled out an online suggestion box app for its staff through the G-Cloud framework. GEMS Online will allow personnel from both the MoD and the Armed Forces to make suggestions on how to improve the organizations’ daily functioning.
4. More secure, efficient logistics and supply chains

Defense agencies manage extremely complex supply chains in which any delays or security lapses are unacceptable. The risk of counterfeit parts getting into the supply chain can be a particular challenge, posing a threat to equipment maintenance, operational effectiveness and even service personnel’s lives. Agencies must also track sensitive materials and equipment that cannot be allowed to go astray, whether these be parts for nuclear devices or airplanes carrying weapons.

Cloud computing solutions, combined with mobility, powerful analytics and sensor technologies such as Radio Frequency Identification (RFID) can transform the efficiency and security of supply chains, giving unprecedented control and visibility into what supplies are where, and immediately highlighting any shortages or bottlenecks. The risk of counterfeits can be tackled by tagging and tracking genuine parts from manufacturer to theater.

Cloud computing, mobility and analytics can also support smart, data-driven automation to make the supply chain more accurate and self-correcting. For example, when providing ‘meals ready to eat’ (MREs) to front-line personnel, it has traditionally been impossible to track consumption in real-time, meaning the most commonly used option has been to oversupply MREs. However, combining supply-chain control with constant visibility into soldiers’ frontline consumption data from on-body, cloud-connected sensors can help ensure the right type and volume of MREs are provided at the right time.

NATO plans out its cloud strategy

The North Atlantic Treaty Organization (NATO)—the intergovernmental military alliance of 28 countries including the US and UK—is planning how it will seize the cloud opportunity, including using “cloud-in-a-can”, a turnkey product for private cloud deployments. Information in the NATO cloud will come from its diverse member nations, all of which must agree how it is handled. NATO’s IT operations in Virginia have already been moved into a private cloud to help NATO smooth out command, control, surveillance, and intelligence projects, and improve decision-making on the ground.
5. Enhanced situational awareness, visibility into the 'last tactical mile' and in-theater decisions

In the future, cloud capabilities will combine with mobility and analytics to take situational awareness to a new level. We believe data will be shared and accessed on the front line from a vast array of sources—including satellite, air and ground reconnaissance devices, climactic condition sensors, geopolitical and military intelligence, command center insights, allied forces, and devices and on-body sensors worn by in-theater personnel. Data from all these sources will be fed into portable private cloud ‘containers’ on the battlefield, and accessible only under strict ID authorization protocols. Ultimately the data could potentially be integrated into service personnel’s heads-up displays.

Exciting defense-relevant apps under development

As of May 2011, 25 large US federal agencies had identified 78 services suitable for migration to the cloud. While email and web hosting/analytics topped the list of cloud services, the pipeline also includes a number of exciting apps with clear relevance to defense, and specifically to situational awareness. These include:

- **The US Army is investing in portable, private-cloud containers that can be used on the battlefield.**
- **The National Oceanic and Atmospheric Administration is looking to store geospatial data in the cloud.**
- **NASA’s Khawaja Shams, manager of data services at Jet Propulsion Labs, talks of “earth-orbiting cloud computing centers.”**

Data flow in the other direction—from front-line fighters to command center and home base—will be data from on-body sensors and visual capture devices, automatically sending back information on key factors such as their tactical situation, health and physiological status, ordinance needs, and food consumption. Evaluated through real-time analytics, this data will help inform decision-making and tactical actions, and support the end-to-end supply chain.

At the same time, cloud-enabled in-theater access to health records will boost the speed and accuracy of treatment and evacuation. Experience shows that stabilizing the physical condition of wounded operatives within the first few minutes has a hugely positive impact on survival rates.

However, there are clear provisos in this scenario. To function effectively and continuously, cloud-based services need high-capacity networks to be available. This is not always the case on the tactical edge, where, in some areas, not even electricity is available. So in-theater cloud applications and devices need to be robust and durable enough to withstand being disconnected for long periods of time and interrupted regularly.

**US Army develops situational awareness in the cloud**

In August 2012, the US Army Communications Electronics Research, Development and Engineering Center (CERDEC) announced the Command & Control Tactical Cloud Computing Environment. Its goal is to enable warfighters on the forward edge of the battlefield to use cloud computing to access situational awareness information using data radios, wearable computers, rugged laptop computers, and other rugged mobile computing devices.
Bringing together cloud computing, mobility and analytics with advanced biometrics will enable defense agencies to automate and integrate ID and access management globally. They will be able to verify that someone is who they say they are anywhere in the world, by authenticating each individual’s security credential and clearance levels in real-time across multiple applications and authorizations, helping to enhance speed and security in all forces and geographies.

This parallels capabilities being developed in the commercial and civilian fields, ultimately leading to each individual having a single personal credential with multiple authorizations in different systems. Some civilian airports—especially in Europe—are already using automated, biometrics-enabled ID recognition border control and immigration systems. Defense agencies are likely to use similar technologies for site and system access both in the homeland and in-theater, even integrating biometrics into heads-up displays to help ensure security of data during military action.

Identity & Access Management gets personal

Cloud-based systems under development at Accenture's technology labs will enable each individual to have one unified personal credential containing multiple levels of ID recognition and authorization across multiple systems. The unified credential could be recognized by a wide range of secure systems such as banking, health, driver’s licensing and personal taxation. But each authorization event will have no visibility into the others, thereby minimizing the security exposure in the event of a security breach. This capability has clear applicability for defense agencies, given their need to allocate and manage multiple authorizations and clearances globally for each individual. It will enable them to automate the same individual’s security access and authorization profile across data, applications and devices worldwide.
The future provisioning model for cloud in defense: The cloud services broker

In the coming years, as adoption of cloud services by defense agencies accelerates and more third-party cloud offerings are developed to meet their needs, we believe that agencies’ IT provisioning will move towards the model of “cloud services broker.” This is a centralized organization that oversees the process of selecting, procuring, provisioning, governing and managing cloud services, and offers an orchestration platform and value-added cloud services to support adoption.

The role of cloud services broker can be played either by the internal IT function or an external provider. Either way, it is responsible for meeting IT needs across the agency by integrating and offering a wide range of cloud services—from IaaS to PaaS and SaaS, and from private to public cloud solutions—in combination with legacy in-house systems. The benefits of this model generally include delivery of the right applications solutions to the right users at the right time, stronger and more consistent governance and security, and lower total costs of ownership.

The model is already emerging in defense agencies. The US Department of Defense’s (DoD) has designated the Defense Information Systems Agency (DISA) as its “cloud services broker” (see information panel). At the same time, public cloud services brokers are applying to FedRamp for accreditation to supply the US Federal Government, to help fill the need for increased cloud brokering in government bodies.
The US Defense Information Systems Agency (DISA) sets out its “next generation” cloud strategy

The US Department of Defense’s (DoD’s) announcement in 2012 that it was designating DISA as its “enterprise cloud service broker” was a groundbreaking move in government—especially given the US General Services Administration’s description of brokering as a “next-generation cloud acquisition model.”

DISA’s role for the DoD includes maintaining the certifications and accreditations that underpin cloud governance. As part of this role, DISA maintains the approval process as a whole, ensures the authorized cloud services providers to the DoD follow the required guidelines, and reviews their performance periodically.

In September 2012, DISA released a five-year strategic plan providing more detail on its evolving role. From a technological standpoint, the strategy includes plans to facilitate an increasingly enterprise-oriented DoD that shares IT resources across numerous services, relies heavily on cloud computing and mobile technologies, and continues to push the boundaries of cybersecurity.

The armed forces within DoD have the option to choose third-party providers rather than DISA, as long as they are lower cost and offer at least equal security. The US Army has been the most active adopter of DISA’s cloud brokering service to date, selecting DISA as its source for email in the cloud, and migrating Army email accounts to DISA-hosted Enterprise Email. The Army also plans to purchase enterprise collaboration services such as instant messaging and chat from DISA.

As Figure 2 shows, the cloud services broker—part process, part technology—fulfills its role by acting as the interface between external cloud providers and internal consumers. It undertakes activities which include selecting and negotiating cloud services from cloud service providers; aggregating, automating and integrating services; managing demand, workload and governance; and creating and maintaining a service catalog that cloud consumers can choose and buy from.

Below the level of the defense department in each country, some form of cloud services brokering capability will also be needed by each of the military forces, at least for the first few years of the migration to cloud. Provided that public cloud providers can meet their required security standards, we believe that many defense agencies will be leveraging public cloud solutions through cloud service brokering within the next few years.
A vision for European defense collaboration: cross-border community clouds

In Europe, there is the potential for the use of cloud computing in defense to take a particular form. Defense agencies and national security actors across Europe face shrinking budgets, combined with a growing need to collaborate, share resources and increase interoperability with each other. These requirements could lead to the creation of community clouds shared across borders between different national defense forces. The main barriers are national data protection laws specifying where data can be located, and the political will to make it happen. But it is a solution that would represent a logical response to the needs of Europe’s defense agencies.

In Accenture’s view, the journey to community defense clouds in Europe would involve three stages: first, the creation of national defense clouds shared between the various agencies and forces in a country; second, wider domestic collaboration between the various national security actors, such as defense ministries and interior ministries; and third, international collaboration in the cloud between different countries’ defense and security agencies. With horizontal cross-border integration of European defense forces already under way through shared processes and interoperability agreements, a community cloud would be the natural way forward.

The future evolution of the cloud broker in defense

Once a defense agency has established the role of cloud services broker, then the model can evolve through various stages, as shown in Figure 3. Starting from most IT departments’ legacy role of offering non-cloud infrastructure services, the role can mature through five further stages, taking it up to fully-fledged cloud integrator.

As an integrator, the cloud services broker could bring together multiple services to deliver an integrated outcome; introduce new functionality by integrating service data and processes; and support service models ranging from “one-to-many” (one service to many users) to “many-to-one” (many services to one user). Alongside the integrator role, the broker may also act as a “customizer”—including creating customized services around the original service, providing fully developed managed services, and introducing new functionality through customization.

Accenture is already helping some defense agencies create their cloud services broker strategies and operating models, and to investigate the future potential for moving up the maturity curve in the future.
Building a platform to seize the cloud computing opportunities

Cloud computing is coming of age in defense—and we believe it will converge with mobility and analytics to change the game in the ways we’ve described.

Different defense agencies and their IT functions will move at different speeds, balancing the cost and enablement priorities affecting them. However, they can all move now towards a platform for future cloud computing adoption, by rationalizing their IT environment to make it more homogeneous based on common infrastructure components.

This means defense agencies looking across their currently fragmented “silos of application excellence”, each of which may well have its own hardware configuration, and moving instead to a virtualized infrastructure environment standardized around one preferred storage provider, one database platform, one set of network monitoring tools, and so on.

Having taken this step, the agency’s IT function can work with each application team to plan how their apps can be aligned and integrated with this new environment. The benefits will then begin to flow: once the cloud data center is established, its scale will mean that each new component or application added to it will make it more efficient.

Defense agencies’ migration to cloud is likely to take several years. But we believe it will come, with game-changing implications. Now is the time to start planning the journey—and preparing the right IT architecture to begin the transition.
References


Find out more
The cloud-enabled future has begun— and is already starting to change the game for the defense industry. It is time to embark on the journey. To learn more about how Accenture can help your organization to seize the cloud computing opportunity to achieve high performance, please contact:

Matthew Coates
matthew.coates@accenture.com

Matthew Coates is the global lead for Accenture’s Cloud Sales and Strategy capability, with responsibility for sales and delivery of work to help clients understand the impact of cloud computing on their business and how to integrate this new technology into their existing business model. Prior to transitioning to this role, Matthew was a Managing Director in Accenture’s Information Technology Strategy practice, which focuses on helping clients’ IT organizations achieve high performance through focusing on their operating model, cost reduction and strategic planning and growth. During his career, he gained valuable experience while working in the Health, Revenue, Customs, Agriculture, Justice and Defense sectors for Accenture’s Health and Public Service practice.

Ahmed Hassan
ahmed.a.hassan@accenture.com

Ahmed Hassan is a Managing Director in Technology Consulting specializing in Infrastructure. Ahmed leads Technology Consulting for Accenture’s Australian Health & Public Service Operating Group, specializing in Revenue as well as Defense and Public Safety. Ahmed is one of the trusted advisors to Accenture’s Health & Public Service clients in the areas of Data Centre Solutions, Cloud Technology, Service Excellence and Mobility.

Chris Smith
christopher.l.smith@accenturefederal.com

Chris Smith is Accenture's U.S. Federal Chief Technology and Innovation Officer, bridging the federal market’s needs with Accenture's technology capabilities. Chris brings 25 years of experience in cutting-edge technology development to his role and is responsible for developing the technology agenda for Accenture's federal business portfolio. He oversees the services provided by Accenture to federal clients in strategic areas such as secure cloud computing, big data, logistics and supply chain and cost reduction. Prior to joining Accenture in 2012, Chris served as the chief information officer of the U.S. Department of Agriculture, where he led one of the largest federal government transitions to cloud computing. His federal government experience also includes senior positions with the General Services Administration, the Internal Revenue Service and the Air National Guard.

Dr. Valtteri Vuorisalo
valtteri.vuorisalo@accenture.com

Valtteri holds a Doctor’s degree from the Tampere School of Management, in which his focus area was the process and methodology of international crisis management capability development.

Keith Lippert
keith.w.lippert@accenturefederal.com

VADM (Retired) Keith Lippert started working for Accenture in Reston, Virginia, in October 2006. His last tour on active duty was as the 14th Director of the Defense Logistics Agency (DLA). Prior to coming to DLA, Vice Admiral Lippert was the Commander, Naval Supply Systems Command and 41st Chief of Supply Corps from August. He also served as Vice Commander, Naval Supply Systems Command. His personal awards include the Defense Distinguished Service Medal, Defense Superior Service Medal, three Legion of Merits, four Meritorious Service Medals, two Navy Commendation Medals, Navy Achievement Medal, and Submarine Supply Dolphins. His work at Accenture includes ERP implementations, business transformations, supply chain and cost reduction management, in the public and private sectors, both within the United States and internationally.

Dave Morales
dave.morales@accenturefederal.com

David Morales is a Managing Director and Executive VP of Defense Technology Solutions within Accenture Federal Services. He has over 25 years of System Integration, Technology Consulting & Technology Outsourcing experience and has served both public and private sector clients. He has worked in the Telecommunications, Product & Distribution, and High Tech industries, with his most recent experiences being in our Defense sector for the last 12 years.

James Menard
james.l.menard@accenturefederal.com

Jim Menard is a Managing Director within Accenture’s Defense Portfolio, with primary focus on the Intelligence Community.

Jim has 17 years of experience implementing complex information technology solutions. Currently, Jim is leading the delivery of a contractor owned and operated data center program within the Intelligence Community, providing infrastructure managed services, automated provisioning and business analytics. Jim also has responsibility for driving business growth in Infrastructure and Enterprise IT related opportunities across the Intelligence Community.

Additional Contributors

Laurie Henneborn
laurie.a.henneborn@accenture.com

Laurie Henneborn, based in New York, leads the global technology research team within Accenture Research – an inhouse network of professionals who have strong knowledge of various industries, geographies, technologies, and functional domains, as well as research methods and techniques. Laurie specializes in cloud applications-related topics.

Carla Kusel
carla.kusel@accenture.com

Based in Chicago, Carla Kusel is a H&PS researcher within Accenture Research where she is responsible for public sector research in North America. Upon joining Accenture in 1999, Carla spent a number of years with the technology research team before joining the H&PS research team. Prior to joining Accenture, Carla worked in the research practices of Hewitt/AON and William M. Mercer.
Accenture Enterprise Services for Defense

Accreture Enterprise Services for Defense provides Departments of Defense, defense forces and related defense agencies with key enablers for transformation, operational agility, and process management excellence, enabling clients meet future goals, mitigate risk and realize cost savings while ensuring mission success.

We provide leading services and methodologies that help departments of defense, the intelligence community and related federal agencies achieve operational excellence in support of the warfighter. We help improve the efficiency and effectiveness of mission and mission-support activities through our organizational performance and business process improvement strategies, information technology systems and other rapidly deployed solutions that reduce costs and increase efficiency to ensure mission success.

About Accenture

Accenture is a global management consulting, technology services and outsourcing company, with approximately 261,000 people serving clients in more than 120 countries. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world’s most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. The company generated net revenues of US$27.9 billion for the fiscal year ended Aug. 31, 2012. Its home page is www.accenture.com.