



Advertisement

Defense program acquisition news, budget data, market briefings

Contact ▾

Subscribe ▾

Log in ▾



#### Archives

[MIL](#)

[BIZ](#)

[GEO](#)

[DAY](#)

#### **Aircraft**

#### **Electronics & IT**

#### **Land Equipment**

#### **Logistics & Support**

#### **Military Overall**

#### **Naval Equipment**

#### **Ordnance & Guns**

#### **Space**

#### **WMD**

#### **White Papers & Events**

#### **Table of contents**

Try this quick tour to discover our time-saving article tools. [×](#)

## The Virtual Armed Forces: US Military Turns to Virtualization

Aug 15, 2011 08:59 UTC by Defense Industry Daily staff



USS Abraham Lincoln  
going virtual  
(click to view full)

The US Department of Defense (DoD) and the individual services are turning more and more to virtualization to improve the efficiency and flexibility of their IT networks. This technology allows multiple virtual machines with different operating systems to run side-by-side on the same physical machine. The main benefit is a decrease in needed hardware, space, and power to perform the same IT operations, thus saving money and weight on military IT systems and platforms.

At the same time, virtualization raises security concerns because traditional IT security products, such as firewalls, do not work in the virtual environment.

[Virtualization: What Does It Mean?](#)

[DISA Out in Front](#)

[GD's TVE Project](#)

[Navy's Virtual Strike Force](#)

[Air Force Goes Virtual Early](#)

## Virtualization: What Does It Mean?



Virtualization means

fewer of these

(click to view full)

Virtualization is the creation of a virtual version of an operating system, a platform, a storage device, or a network. Its advantages are that it reduces the need for physical hardware and software because the functionality is created virtually.

Traditional computer hardware is designed to run on a single operating system and a single application. Virtualization enables organizations to run multiple virtual machines on a single physical machine.

Software is used to “virtualize” the hardware resources of a computer—including the CPU, RAM, hard disk, and network controller—to create a virtual machine that can run its own operating system and applications.

Virtualization works by inserting a thin layer of software directly on the computer hardware or on a host operating system. This contains a virtual machine monitor known as the hypervisor that allocates hardware resources dynamically and transparently.

An entire virtual infrastructure can be constructed by scaling across hundreds of interconnected physical computers and storage devices using a virtualization platform. Hardware resources are dynamically allocated when and where they are needed within a private cloud (see this on [DoD’s cloud computing efforts \(/defense-cloud-computing-06387/\)\)](#)).

“Virtualization is the first step toward cloud computing,” explained Aileen Black, vice president of the public sector at VMware. “By being able to separate your usage of IT and being able to put in the virtual paradigm as opposed to the physical paradigm, you can bring up all that capability, services, and applications, and have it separate so you can create a virtual environment... across all of your data centers.”

Through virtualization, organizations can cut their IT costs in half and consolidate scores of data centers into a handful. The advantages in an era of tight defense budgets are obvious.

Black told DID that VMware’s customers have been able to consolidate as many as 25 servers down to one server through virtualization. By consolidating servers, costs are cut, energy is saved, and space requirements are reduced, she noted.

## DISA Out in Front



The Obama administration has been pushing government agencies to consolidate their data centers. It has set a goal to close 800 of the US government's 2,094 data centers by 2015, which is expected to save \$3 billion annually.

Leading the way for the Department of Defense (DoD) is the Defense Information Systems Agency (DISA). Henry Sienkiewicz, the agency's chief information officer, said (<http://gcn.com/articles/2011/02/07/interview-disa-sienkiewicz.aspx>) in a February 2011 interview that he expects the agency to be a completely virtualized organization by the end of the year:

"I think there is definitely a lot more optimization [through virtualization] that we can gain. I don't know what the final upper limit is. I know also that there are certain categories of applications – command and control systems and PKI for instance – that you really can't virtualize. So we're actually going application by application to figure out which applications are completely appropriate to be virtualized and which ones are not. Except for a few outliers, we will be very much a completely virtualized organization by the end of the year."

To accomplish this goal, DISA has been working with a number of contractors, including HP, VMware, and General Dynamics.

DISA has an eight-year capacity services contract (five-years with three option years) with HP for the agency's Windows and Linux environments. VMware is a subcontractor that provides the virtualization services under that contract.

The agency buys capacity as a service, which includes the virtualization service, explained Alfred Rivera, computer services director at DISA. The agency does not own the hardware or the software, but it buys the service through the HP contract, he told DID.

Rivera said that the agency is working on an acquisition strategy for the follow-on contract, which is expected to be awarded in 2014. This will follow the same contract model of purchasing virtualization as a service.

VMware provides the hardware, but DISA personnel manage it. VMware's "responsibility includes giving us the physical platform and [ensuring it meets] our security standards, which means putting the operating systems at our security levels. We take management control," he said.

"We are seeing a lot of underutilized infrastructure, both communications and servers. On average, we see utilization on the physical level of about 10% or less. So at DISA we are making a concerted effort, as part of our technical refreshes in the server and communications infrastructure, to virtualize where we can," Rivera said.

"Cost is a big driver in virtualization. But I think the other thing is improving the use of the data center itself in terms of power and air conditioning", he said. For one of its DoD customers, DISA virtualized 96 application servers and cut operating and software costs in half.

DISA is working with VMware to implement its virtualization program across its data centers. Rivera said that DISA recently implemented Enhanced VMotion Compatibility (EVC) and Dynamic Resource Scheduler (DRS) to improve VMotion across DISA's virtual machine clusters. VMotion enables the migration of virtual machines from one server to another in a way that is transparent to the user. This allows the performance of hardware maintenance with no downtime, re-routing of traffic from failing or underperforming servers, and allocation of resources for optimal hardware utilization.

"By implementing those two products under VMotion, we can move virtual machines across clusters seamlessly, so that we don't have downtime when we upgrade software patches or operating system upgrades, as well as implementing new hardware," Rivera said.

## GD's TVE Project



TVE in Action

(click to view full)

In addition, DoD has contracted with General Dynamics to deploy its [Trusted Virtual Environment](http://www.gdc4s.com/content/detail.cfm?item=35a995b0-b3b7-4097-9324-2c50008b3a75) (<http://www.gdc4s.com/content/detail.cfm?item=35a995b0-b3b7-4097-9324-2c50008b3a75>) (TVE) that uses virtualization technology to enable one desktop computer to access different security classification networks. General Dynamics first deployed the TVE platform in 2008.

Usually, each level of classification – unclassified, secret, and top secret – is separated physically and has its own access point, i.e., a separate work station. This provides greater security but also results in higher costs and reduced productivity.

"TVE is a trusted virtualization product that allows users to access information at multiple security levels from a single computer. It utilizes trusted virtualization developed under a government program," explained David Muchi, secure computing lead for General Dynamics C4 Systems.

The TVE product enables a single desktop to access both the unclassified and the secret network or both the secret and the top secret network using virtualization technology. This reduces the cost of equipment and as well as improves worker productivity since the user does not have to go to a separate terminal for each network.

"We have been able to collapse multiple desktops and go from a scenario where a user might have 4 desktops and having to go monitor to monitor in order to go between the different domains, whereas today they are able to use a single monitor, keyboard, and mouse, and view all that information from a single monitor", Muchi told DID.

TVE creates virtual machines within a single computer using VMware. Each virtual machine can run different operating systems – such as Windows, Linux, and Solaris – and at different security levels in separate

windows on a shared computer and monitor.

"Using the VMware software along with the hardware capabilities of the newer Intel chipsets allows us to get a higher assurance of separation between these [classification] domains than we had been able to 5 or 10 years ago", he said.

In addition to VMware, General Dynamics has worked with Intel in developing the TVE platform, which uses Intel's vPro technology to provide hardware-based information security that ensures the classified networks are kept separate.

In addition to the different classification levels, the DoD has different "caveats" that restrict who can access certain information. There are caveats, for example, for different coalition partners. Without TVE, each classification level and each caveat would require a physically separated terminal.

"You can imagine an intel analyst with 4 computers at their desk having to move back and forth between these computers in order to access information they need to put together a report. TVE allows them to use a single interface to access this information and to view all the information at the same time as well," Muchi said.


General Dynamics C4 Systems plans to release the next-generation TVE product, TVE 2.0, by the end of 2011.


## Navy's Virtual Strike Force



Lincoln & friends  
(click to view full)

The US Navy has expanded the US military's virtualization effort to include aircraft carrier strike groups.

In 2010, the USS Abraham Lincoln (<http://www.cvn72.navy.mil/>).  (CVN-72) strike group conducted sea trials using a common computing environment (CCE), under the Application Integration Early Adopter Initiative (AIEAI). This enabled the strike group to use virtual machines to provide communication flexibility in case one part of the network was disrupted.

Lt. Cmdr. David White, Abraham Lincoln's combat systems information officer, explains ([http://www.navy.mil/search/display.asp?story\\_id=52820](http://www.navy.mil/search/display.asp?story_id=52820)). 

*"In the past, my days were filled with phone calls telling me which telephone lines were down, the status of email backlog and slowness of the Internet. This time, users were never aware when we dropped a satellite shot because we never lost connectivity...we were truly operational 24/7."*

The CCE enables combat systems information officers to manage hardware virtualization, software updates and patches, information security, and training. It provides a single set of hardware to support virtual applications that can be installed as software.

Installing software from disks, as opposed to hardware racks dedicated to specific applications, reduces the number of hardware racks on board ships. Virtualization provides the ship's network with central processing resources, dynamic resource allocation, and near instantaneous data recovery.

During the sea trial, the Lincoln experienced no satellite communications interruptions and data back-ups were conducted automatically, without having to manually manage tape libraries, while servers remained in use.

"Historically, we would work past liberty call and have significant downtime during the satellite and pier cut over. We always had to worry about restoring services. This was not the case this time. It took only five minutes to cut over the pier. Our IT specialists were on liberty with the rest of the crew during liberty call," White said.

Coordinated by the Tactical Networks Program Office (PMW 160), AIEAI is an effort to enable the deployment of a secure, reliable, common network infrastructure for the Navy fleet. The Lincoln Strike Group was the first to implement AIEAI, which will continue through full implementation of the Navy's next-generation afloat tactical network, the Consolidated Afloat Network and Enterprise Services (/US-Navy-to-Lean-on-CANES-to-Integrate-Shipboard-Networks-06221/). (CANES).

The CANES program will replace 5 shipboard legacy network programs to provide the CCE on board for command, control, intelligence and logistics. The primary goal of the CANES program is to build a secure shipboard network required for naval and joint operations.

In addition to bandwidth performance improvement and equipment reduction, the virtual AIEAI network provided \$5.7 million in fiscal year cost savings for the USS Lincoln, the USS Cape St. George (CG 71), and the USS Shoup (DDG 86).

A precursor network to CANES is the Integrated Shipboard Network System (ISNS), which has a CCE with virtualization and hosting of applications that allow removal of several racks of equipment. The ISNS incorporates blade servers and disk-to-disk storage capabilities that enhance the network operator's ability to manage, back up, and recover their systems.

Additionally, the Automated Digital Network System (ADNS) increment III provides ships with the ability to harness increased bandwidth provided by broadband satellite communication systems.

ADNS provides surface, submarine, shore, and airborne platforms access to the tactical wide area network for Navy IP network operations. ADNS increment III ([https://www.fbo.gov/index?search=opportunity&mode=form&id=f5a020965b6f754c87f326645247ef61&tab=core&\\_cview=0](https://www.fbo.gov/index?search=opportunity&mode=form&id=f5a020965b6f754c87f326645247ef61&tab=core&_cview=0)) will provide an all IP voice, video, and data network; 25-50 Mbps data speeds; and dynamic bandwidth management.

"The combination of CANES and ADNS will allow the Navy to change the game in shipboard communications and greatly enhance the war fighter's ability to dominate in the information intensive environment that they

operate in today and tomorrow,” commented Capt. Joe Beel, PMW 160’s deputy program manager.

## Air Force Goes Virtual Early



2007 CWID Exercise  
before virtualization  
(click to view full)

Back in 2009, the Air Force’s Electronic Systems Center (ESC) launched a [virtualization pilot project \(http://www.hanscom.af.mil/news/story.asp?id=123181414\)](http://www.hanscom.af.mil/news/story.asp?id=123181414) at its C4ISR Enterprise Integration Facility (CEIF), which is used for hosting exercises such as the Coalition Warrior Interoperability Demonstration (CWID).

The pilot, led by prime contractor NPLACE and subcontractor Jackpine Technologies, enabled Microsoft, Solaris and Linux operating systems to run on the virtualization software.

A factor in the decision to test virtualization was the speed with which vendors such as VMware and Red Hat had advanced the technology, explained Ray Smith, an administrator on the ESC’s virtualization implementation team.

For the ESC’s virtualization project, the hypervisor was loaded onto operation center computers. It then reported data on performance and functionality back to a central management console. An administrator, monitoring this server via the management console, was able to see all the resources available and allocate those resources on a per-customer basis.

The pilot enabled CEIF users to take their home computer with them to the center. “A user can walk in with a disc image that he’s already built using this software. That gives him a way to just bring one DVD and start working,” Smith explained.

Plugging in the DVD – a copy of the user’s own hard drive – the user could boot up and run the exact system he would be running at his home location. Previously, he would have had to build and configure the system from scratch in the CEIF.

The hardware being used for the pilot was three-year old equipment left idle by a moribund program. The virtualization project took all the capability offered by this equipment, which might otherwise have been discarded, and extended its useful life, Smith noted.

Also in 2009, the Air Force Weather Agency (AFWA) experimented with virtualization of its weather forecasting infrastructure.

The AFWA implemented virtualization to refresh 26 aging development servers; replacement of the servers was estimated to cost \$182,000. Instead, Capt. Brian Woolley and Roy Ashcraft of the agency’s 2d

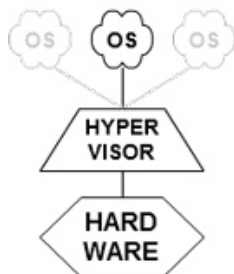
Systems Operations Squadron decided to use virtualization to reduce the number of servers.

They decided to deploy a four-node virtual machine clusters that only cost \$72,000. Testing revealed that the system would support 48 virtual machines, thus delivering a realized value of \$336,000.

At the same time, the virtualization solution introduced an added layer of complexity and information security challenges. The AFWA addressed those issues by putting in place policies and procedures governing the system's physical architecture, as well as the configuration of virtual network switches and virtual machines operating within the infrastructure.

"The virtual environment adds no new vulnerabilities to the network. In fact, the virtual environment infrastructure itself is invisible on the network, with only the virtual servers being exposed, identically to a traditional server. The virtual hosts reside on a private VLAN [virtual local area network], isolated from the standard networks. This prevents all attacks on the actual virtual environment," SAIC analyst Ashcraft explained.

## Security Challenges/Benefits



Is the hypervisor the weak link?

Virtualization's security risks can be broken down into three categories: attacks on virtualization infrastructure, attacks on virtualization features, and compliance and management challenges, according to an ISACA white paper called [Virtualization Benefits and Challenges](http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Virtualization-Benefits-and-Challenges.aspx) (<http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Virtualization-Benefits-and-Challenges.aspx>).<sup>4</sup>

There are two primary types of attacks on infrastructure: hyperjacking and virtual machine jumping. Hyperjacking is still a theoretical attack scenario, but it has earned media attention because of the damage it could cause.

One example of hyperjacking is inserting a rogue hypervisor into the virtualization system. Traditional security measures are ineffective against these threats because the operating system, which runs above the hypervisor, is not aware that the machine has been attacked.

Virtual machine jumping involves exploiting vulnerabilities in the hypervisor that enables malware or a remote attacker to compromise virtual machine protections and gain access to other virtual machines or



even the hypervisor. These attacks are often conducted once an attacker has gained access to a less secure virtual machine.

There are also two types of attacks on virtualization features: virtual machine migration and virtual networking functions. Insecure virtual machine migration can expose a virtual machine to both passive sniffing and active manipulation attacks. There are also security issues with the networking features and support typically used by virtualization infrastructures. Other examples include differing ways in which media access control address assignment, local routing, and layer 2 traffic can be exploited.

In addition, the white paper noted that VM sprawl and dormant VMs make it a challenge to get accurate results from vulnerability assessments, patching updates, and auditing, which are compliance and management challenges.

ISACA offers the following recommendations to improve security in a virtual environment: patch and harden the hypervisor and the guest it supports; use physical, network, and virtualization-based separation to segment VMs and systems; use transport encryption to secure VM migration; and implement virtualization-aware management products and services.

While virtualization poses security risks, the DoD has looked at virtualization as a way to improve network security. According to a [2009 request for information \(https://www.fbo.gov/index?s=opportunity&mode=form&id=34ba3f4de5d4e40e7fe14a73431b93c1&tab=core&cvview=1\)](https://www.fbo.gov/index?s=opportunity&mode=form&id=34ba3f4de5d4e40e7fe14a73431b93c1&tab=core&cvview=1), the DoD asked for research on how virtualization could improve network security in the following ways: network provisioning via virtual infrastructure; reduced-risk Internet exposure via virtual machines; creation of a trusted enclave via virtual machines; and employer-subsidized computers replacing employer-supplied computers.

DoD was particularly concerned about threat posed by operating systems in traditional data centers:

*"The attack surface of modern operating systems and many applications is too large to effectively secure. It may be that the era of monolithic general purpose operating systems is nearing its end and could be replaced by a cluster of modules or virtual appliances acting in concert to perform services traditionally supplied by operating systems."*

So the future challenge for the US military will be to take advantage of the efficiencies and cost savings of virtualization, while ensuring that any additional security risks are dealt with effectively. Only time will tell if a benefit/security balance can be struck.

## **Key Contacts as of August 2011**


Roy Aschraft, systems analyst, SAIC, tel: 402-293-5218, email roy.w.ashcraft @ saic.com


Aileen Black, vice president of government sales, VMware, tel: 703-466-4500


David Muchi, secure computing lead, General Dynamics C4 Systems; contact Carol Smith, tel: 480-441-0342, email carol.smith @ gdc4s.com


Alfred Rivera, director, Computer Services Directorate, Defense Information Systems Agency, tel: 301-225-7100


## Additional Reading


General Dynamics – [Department of Defense Creates a Secure, Virtualized Environment](#)  [PDF]


VMware – [Virtualization Basics](#) 


Government Computer News (July 28/11) – [Kundra: 'Golden source' of data center savings due in the fall](#) 


Defense Systems (April 1/11) – [Early success shows DOD what desktop virtualization can do](#) 


Defense Systems (April 1/11) – [Virtualization breathes new life into DOD health records system](#) 


Government Computer News (Feb 2/11) – [DISA's new focus: supporting mobility](#) 


DISA (July 29/10) – [Computing Services: Virtualization](#)  [PDF]


Air Force Institute of Technology (July 2010) – [Developing a Hybrid Virtualization Platform Design for Cyber Warfare Training and Education](#) 


Navy (April 24/10) – [Lincoln Strike Group Transitions to Navy's Virtualized Network](#) 


Air Force (Dec 9/09) – [Virtualization effort aims at more efficient management of computing power](#) 


Air Force (Sept 8/09) – [Team stands up a virtualized environment](#) 


Federal Computer Week (July 15/09) – [DOD: Can virtualization make security more manageable?](#) 

FedBizOpps.gov (July 10/09) – [Virtualization-based Security Tools \(Sources sought\)](#) 

Air Force Research Lab (May 2009) – [High Assurance Virtualization Engine \(HAVEN\)](#) [PDF] 

Marine Corps (Winter 2009) – [On Point: Virtualization links computers and Marines on the move](#)  [PDF]

DISA (April 28/08) – [ESX Server Security Technical Implementation Guide](#)  [PDF]

IBM (May 17/07) – [IBM Solution for ITES-2H Army Enterprise Thin Client Architecture Standardization](#)  [PDF]

**Categories:** [C4ISR](#), [Contracts - Awards](#), [Electronics - General](#), [General Dynamics](#), [IT - Cyber-Security](#), [IT - General](#), [IT - Networks & Bandwidth](#), [IT - Software & Integration](#), [New Systems Tech](#), [Pre-RFP](#), [Spotlight articles](#), [T&C - SAIC](#), [USA](#)

**Stay Up-to-Date on Defense Programs Developments with Free Newsletter**

DID's daily email newsletter keeps you abreast of contract developments, pictures, and data, put in the context of their underlying political, business, and technical drivers.

Subscribe now

© 2004-2022 Defense Industry Daily, LLC | [About Us \(/about/\)](#) | [Images on this site \(#\)](#) | [Privacy Policy \(/privacy/\)](#)

Contact us: [Editorial \(mailto:editorial@defenseindustrydaily.com\)](mailto:editorial@defenseindustrydaily.com) | [Advertising \(/ratecard/\)](#) | [Feedback & Support \(http://www.defenseindustrydaily.com/feedback-support/\)](#) | [Subscriptions & Reports \(mailto:subscriptions@defenseindustrydaily.com\)](mailto:subscriptions@defenseindustrydaily.com)

Follow us: [Twitter \(http://www.twitter.com/dodacquisition\)](http://www.twitter.com/dodacquisition) | [Google+ \(https://plus.google.com/110847360779127528432\)](https://plus.google.com/110847360779127528432)

## Stay Up-to-Date on Defense Programs Developments with Free Newsletter

DID's daily email newsletter keeps you abreast of contract developments, pictures, and data, put in the context of their underlying political, business, and technical drivers.

Subscribe now

### One-stop tracking

Our coverage for each program of record is centralized in one article to save time and provide comprehensive context.

### Catch up with new events

Recent updates are highlighted upfront to make it easy to stay on top of programs over their lifecycle.

### Table of contents

The table of contents can be moved on the side or folded to help you navigate within our reports.

### Exec summary

Quickly catch up with just the latest updates, main events and milestones by hiding more granular details.

### Media gallery

Each article comes with a gallery of relevant contextual images, charts, and videos.

### Clean printouts

Our articles print beautifully, without any of the clutter that often gets in the way on the web.

### Save as PDF

Exporting to the Adobe PDF format lets you read our content offline.

### Subscribe for more

Check out our [subscription plans](#) to access our extensive defense program coverage.