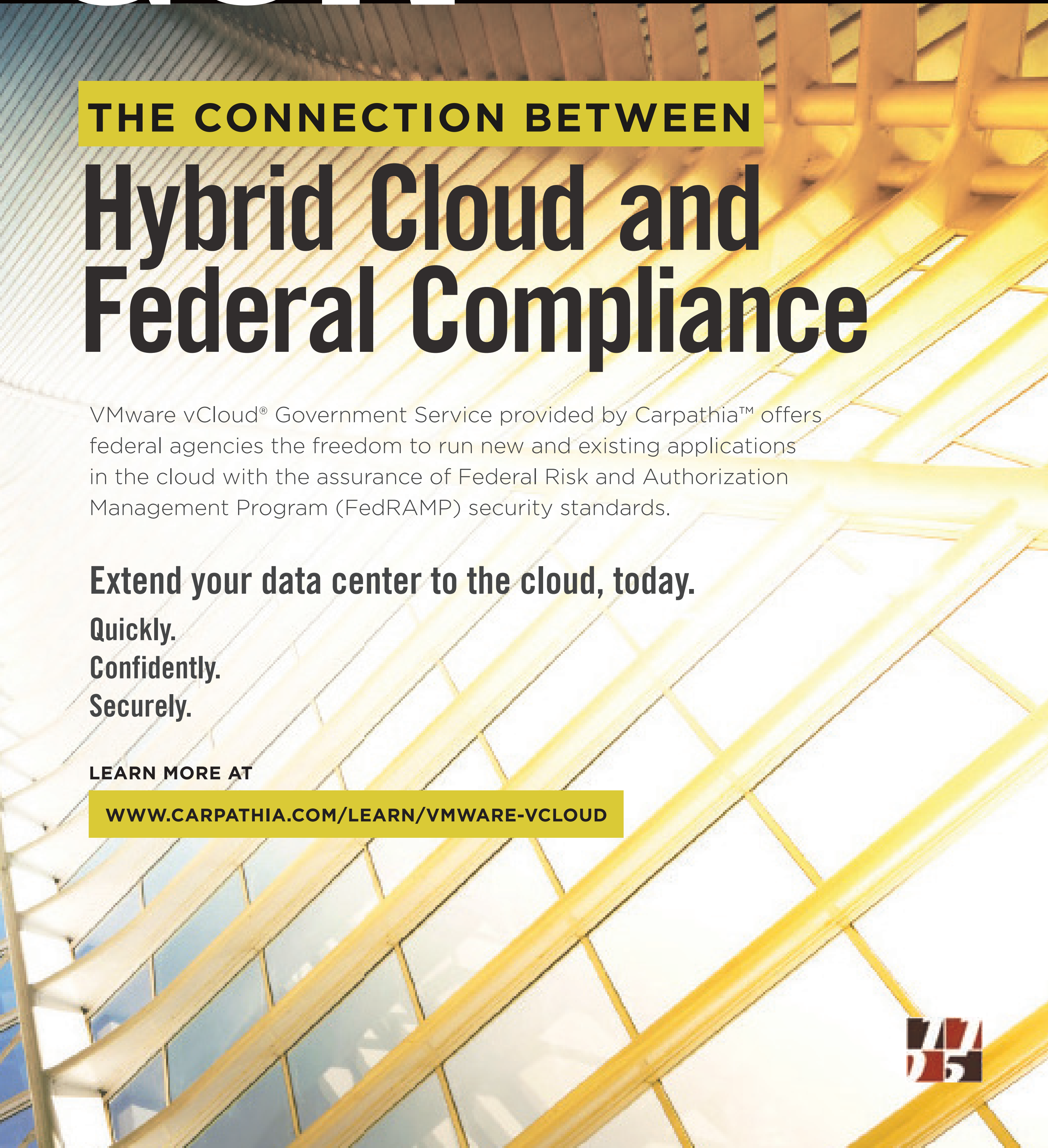
GCN

JANUARY 2015 VOLUME 34, ISSUE 1

Technology, Tools and Tactics for Public Sector IT



The Fastest Path to Cloud *for* Federal Organizations

Overcome your lingering obstacles to cloud adoption with VMware vCloud® Government Service provided by Carpathia™, an enterprise-class hybrid cloud service built on the same platform used in many federal data centers today.

- Test & Development
- Packaged Application Hosting
- Backup & Disaster Recovery
- Web Hosting & Customer Service
- On-Demand Data Center Expansion

LEARN MORE AT

CARPATHIA.COM/LEARN/VMWARE-VCLOUD

carahsoft | vmware

CARPATHIA

GCN

JANUARY 2015 VOLUME 34, ISSUE 1

Technology, Tools and Tactics for Public Sector IT

REAL-TIME DATA MODELING ON YOUR DASHBOARD

PAGE 31

PUBLIC SECTOR TECH FORECAST

New tools for the automated enterprise

Page 22

Energy recasts EA in cybersecurity role

Page 12

GCN

Technology,
Tools and Tactics
for Public Sector IT

SALES CONTACT INFORMATION

MEDIA CONSULTANTS

Ted Chase
Media Consultant, DC, MD, VA,
OH, Southeast
(703) 944-2188
tchase@1105media.com

Bill Cooper
Media Consultant, Midwest, CA, WA, OR
(650) 961-1760
bcooper@1105media.com

Matt Lally
Media Consultant, Northeast
(973) 600-2749
mlally@1105media.com

Mary Martin
Media Consultant, DC, MD, VA
(703) 222-2977
mmartin@1105media.com

EVENT SPONSORSHIP CONSULTANTS

Alyce Morrison
(703) 645-7873
amorrison@1105media.com

Kharry Wolinsky
(703) 300-8525
kwolinsky@1105media.com

MEDIA KITS
Direct your media kit requests to Serena Barnes, sbarnes@1105media.com

REPRINTS
For single article reprints (in minimum quantities of 250-500), e-prints, plaques and posters contact:

PARS International
Phone: (212) 221-9595
Email: 1105reprints@parsintl.com
Web: magreprints.com/QuickQuote.asp

LIST RENTALS
This publication's subscriber list, as well as other lists from 1105 Media, Inc., is available for rental. For more information, please contact our list manager, Merit Direct. Phone: (914) 368-1000
Email: 1105media@meritdirect.com
Web: meritdirect.com/1105

SUBSCRIPTIONS
For questions on subscriptions or circulation, contact Annette Levee,
(512) 301-2632 (phone); (512) 301-3361 (fax);
alevee@1105media.com

REACHING THE STAFF
A list of staff e-mail addresses and phone numbers can be found online at GCN.com.

E-mail: To e-mail any member of the staff, please use the following form: *FirstinitialLastname@1105media.com.*

CORPORATE OFFICE
Weekdays 8:30 a.m.–5:30 p.m. PST
Telephone (818) 814-5200; fax (818) 936-0496
9201 Oakdale Avenue, Suite 101
Chatsworth, CA 91311

Editor-In-Chief Paul McCloskey

Executive Editor Susan Miller

Contributing Writers Kathleen Hickey, William Jackson, Stepanie Kanowitz, Carolyn Duffy Marsan, Patrick Marshall, Shawn McCarthy, John Moore, Brian Robinson

Vice President, Art and Brand Design
Scott Shultz

Creative Director Jeff Langkau

Assistant Art Director Dragutin Cvijanovic

Senior Web Designer Martin Peace

Director, Print Production David Seymour

Print Production Coordinator Lee Alexander

Chief Revenue Officer Dan LaBianca

PUBLIC SECTOR MEDIA GROUP

Chief Operating Officer and Public Sector Media Group President
Henry Allain

Co-President and Chief Content Officer
Anne A. Armstrong

Chief Revenue Officer
Dan LaBianca

Chief Marketing Officer
Carmel McDonagh

Advertising and Sales
Chief Revenue Officer **Dan LaBianca**
Director of Sales **David Tucker**
Senior Sales Account Executive **Jean Dellarobba**
Media Consultants **Ted Chase, Bill Cooper, Matt Lally, Mary Martin, Mary Keenan**
Event Sponsorships **Alyce Morrison, Kharry Wolinsky**

Art Staff
Vice President, Art and Brand Design **Scott Shultz**
Creative Director **Jeffrey Langkau**
Associate Creative Director **Scott Rovin**
Senior Art Director **Deirdre Hoffman**
Art Director **Joshua Gould**
Art Director **Michele Singh**
Assistant Art Director **Dragutin Cvijanovic**
Senior Graphic Designer **Alan Tao**
Graphic Designer **Erin Horlacher**
Senior Web Designer **Martin Peace**

Print Production Staff
Director, Print Production **David Seymour**
Print Production Coordinator **Lee Alexander**

Online/Digital Media (Technical)
Vice President, Digital Strategy **Becky Nagel**
Senior Site Administrator **Shane Lee**
Site Administrator **Biswarup Bhattacharjee**
Senior Front-End Developer **Rodrigo Munoz**
Junior Front-End Developer **Anya Smolinski**
Executive Producer, New Media **Michael Domingo**
Site Associate **James Bowling**

Lead Services
Vice President, Lead Services **Michele Imgrund**
Senior Director, Audience Development & Data Procurement **Annette Levee**
Director, Custom Assets & Client Services **Mallory Bundy**
Editorial Director **Ed Zintel**
Project Manager, Client Services **Jake Szlenker, Michele Long**
Project Coordinator, Client Services **Olivia Urizar**
Manager, Lead Generation Marketing **Andrew Spangler**
Coordinators, Lead Generation Marketing **Naija Bryant, Jason Pickup, Amber Stephens**

Marketing
Chief Marketing Officer **Carmel McDonagh**
Vice President, Marketing **Emily Jacobs**
Director, Custom Events **Nicole Szabo**
Audience Development Manager **Becky Fenton**
Senior Director, Audience Development & Data Procurement **Annette Levee**
Custom Editorial Director **John Monroe**
Senior Manager, Marketing **Christopher Morales**
Manager, Audience Development **Tracy Kerley**
Senior Coordinator **Casey Stankus**

FederalSoup and Washington Technology
General Manager **Kristi Dougherty**

OTHER PSMG BRANDS

FCW
Editor-in-Chief **Troy K. Schneider**
Executive Editor **John Bicknell**
Managing Editor **Terri J. Huck**
Staff Writers **Colby Hochmuth, Sean Lyngaas, Adam Mazmanian, Mark Rockwell**
Editorial Fellow **Jonathan Lutton**

Defense Systems
Editor-in-Chief **Kevin McCaney**

Washington Technology
Editor-in-Chief **Nick Wakeman**
Senior Staff Writer **Mark Hoover**

Federal Soup
Managing Editors **Phil Piemonte, Sherkiya Wedgeworth**

THE Journal
Editor-in-Chief **Christopher Piehler**

Campus Technology
Executive Editor **Rhea Kelly**

1105 MEDIA INC

Chief Executive Officer
Rajeev Kapur

Chief Operating Officer
Henry Allain

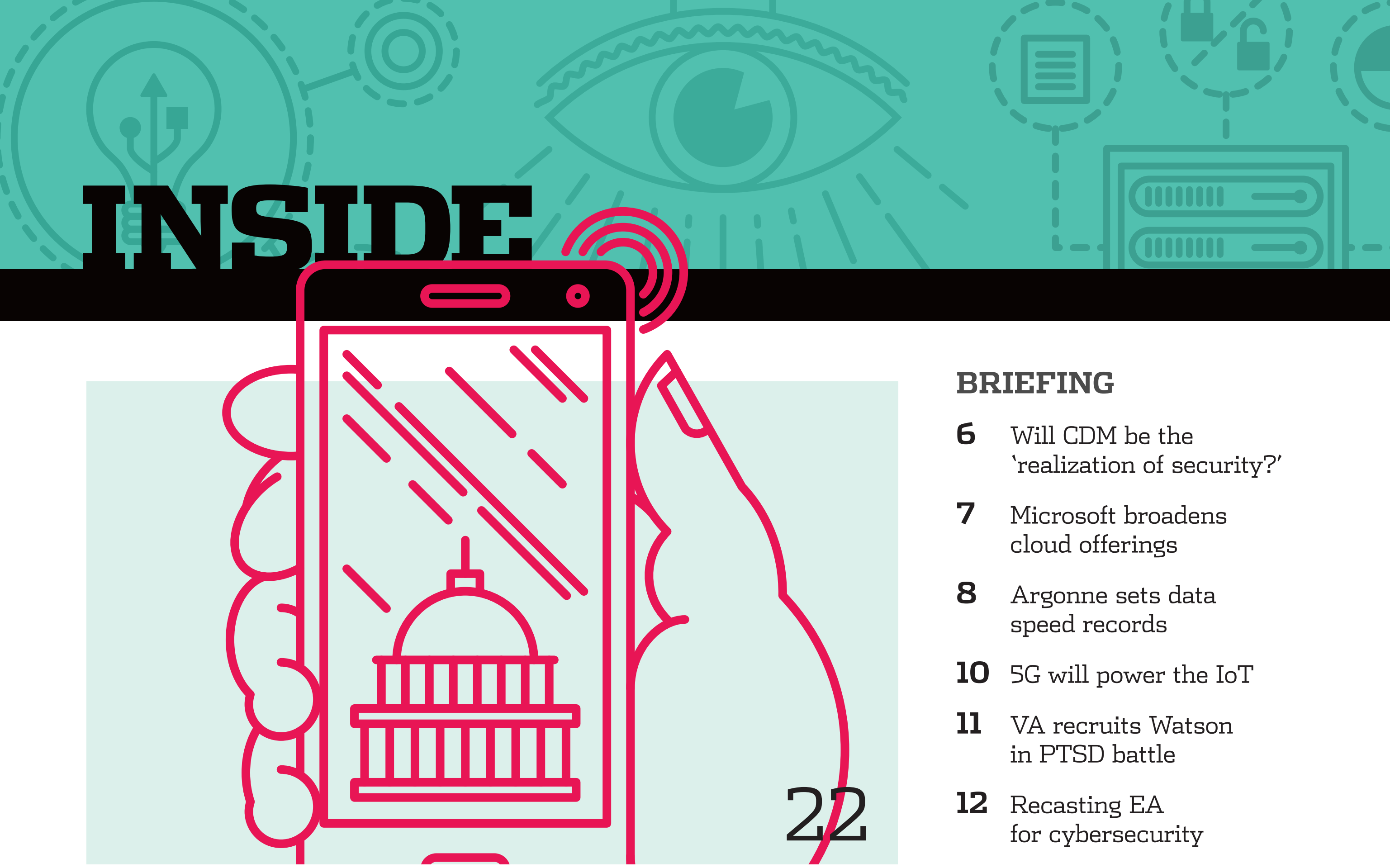
Senior Vice President & Chief Financial Officer
Richard Vitale

Executive Vice President
Michael J. Valenti

Vice President, Information Technology & Application Development
Erik A. Lindgren

Chairman of the Board
Jeffrey S. Klein

INSIDE



GCN (ISSN 0738-4300) is published 11 times a year, monthly except Dec by 1105 Media, Inc., 9201 Oakdale Avenue, Ste. 101, Chatsworth, CA 91311. Periodicals postage paid at Chatsworth, CA 91311-9998, and at additional mailing offices. Complimentary subscriptions are sent to qualifying subscribers. Annual subscription rates payable in U.S. funds for non-qualified subscribers are: U.S. $125.00, International $165.00. **Subscription inquiries, back issue requests, and address changes:** Mail to: *GCN*, P.O. Box 2166, Skokie, IL 60076-7866, call (866) 293-3194, outside U.S. (847) 763-9560; fax (847) 763-9564 or email GCNmag@1105service.com. **POSTMASTER:** Send address changes to *GCN*, P.O. Box 2166, Skokie, IL 60076-7866. Canada Publications Mail Agreement No: 40612608. Return Undeliverable Canadian Addresses to Circulation Dept. or XPO Returns: P.O. Box 201, Richmond Hill, ON L4B 4R5, Canada.

Will CDM be ‘the realization of IT security’?

BY WILLIAM JACKSON

For more than a decade, the federal government has been moving from a periodic, compliance-based approach to IT security to real-time awareness based on the continuous monitoring of IT systems and networks.

While progress has been spotty so far, some security watchers say Phase 2 of the Homeland Security Department’s Continuous Diagnostics and Mitigation program, expected to be implemented in 2015, could be a major step forward.

Jeff Wagner, director of security operations for the Office of Personnel Management, said Phase 2 could be “the realization of IT security.”

“I’m happy with the CDM program, Wagner said. “It’s moving us away from the old generation of defense in depth to a new generation of seeing attacks as they occur.”

The next phase of CDM, called Least Privilege and Infrastructure Integrity, focuses on managing identity and access to resources and puts a premium on being able to see and control what is going on in a system. This can enable effective real-time response.

“This phase could be transformative, rather than evolutionary,” said Ken Ammon, chief strategy officer of Xceedium, which provides access control technology.

Phase 1 of the CDM program, which focused on endpoint security, went into effect in 2013. The next phase reflects the new reality of IT security in which perimeter defenses have been recognized as inadequate and breaches as inevitable. This puts a premium on monitoring and controlling behavior inside systems and networks.

Phase 2 of CDM will require a standardized approach that will enable automated functions and improve communication among siloed systems.

The CDM program is a part of the implementation of the Federal Information Security Management Act, which has for years been mired in regulatory compliance.

> “The CDM program is moving us away from the old generation of defense in depth to a new generation of seeing attacks as they occur.”
>
> – JEFF WAGNER, OPM

CDM is enabling the government’s orderly but critical move to continuous monitoring and better real-time visibility.

The program specifies 15 monitoring capabilities, which can be performed by agency sensors or provided as a service. Sensors will feed data into local agency dashboards, allowing managers to prioritize risks based on standardized and weighted scores and to document and track actions. Summary information is fed into enterprise-level dashboards and eventually to a DHS dashboard.

A blanket purchase agreement was awarded in August 2013 to 17 companies, each with multiple partners, to cover endpoint management in the first phase of CDM.

A request for information was sent in April to CDM suppliers to identify products for Phase 2, and products now are being evaluated for inclusion in the BPA, which is expected to be updated this year to make approved products and services available.

Because products in the CDM program are off-the-shelf, Phase 2 will not involve any radical new capabilities. It is intended to deliver a standard set of tools and services to provide better understanding and control of who is accessing resources and what they are doing.

Although perimeter defenses are not being abandoned, years of successful breaches have made it clear that they are not adequate defenses. The new reality in IT security is that breaches are inevitable, and the ability to monitor and control behavior through improved identity management and access control will allow intrusions to be more quickly identified and more effectively addressed.

OPM’s Wagner calls CDM Phase 2 “a sign that the federal government finally is taking FISMA seriously.”

Attaining better security is not about developing new technology, he said. “The PIV card is a perfect example.” It has been around for 10 years to provide interoperable, strong multi-factor authentication, but is not being widely used. Requiring the use of a suite of proven, off-the-shelf tools available at affordable prices will ensure that the technology is put to use, not on a shelf. •

Microsoft broadens government cloud offerings

BY CAROLYN DUFFY MARSAN

Microsoft has expanded its cloud services for public sector customers with an announcement that Azure Government and Dynamic CRM Online Government are now available.

Michael Donlan, vice president of state and local government at Microsoft, said the company's end-to-end integrated cloud now offers the broadest array of government-ready cloud capabilities on the market, including CRM and Office 365 services.

"It spans all the offerings that can be in the cloud: productivity, infrastructure-as-a-service, software-as-a-service, business process-as-a-service, identity management and mobility," Donlan said.

"It is one government cloud that meets U.S. regulations for federal and state and also has the ability to integrate in hybrid public/private environments."

Microsoft also claims it supports the broadest array of security and privacy standards, including: Health Insurance Portability and Accountability Act (HIPAA), Criminal Justice Information Services (CJIS), the IRS 1075 encryption standard, Federal Information Security Management Act of 2002 (FISMA) and Federal Risk and Authorization program (FedRAMP) standards.

Early adopters of Microsoft's integrated cloud offerings include the states of Texas and Alabama. Texas has 110,000 Office 365 seats and is rolling out Azure Government for law enforcement applications because of its support for CJIS standards.

Alabama is deploying Office 365 to 23,000 employees and is developing Medicaid applications on Azure Government in a hybrid environment that uses a private data center.

Azure Government and Dynamics CRM Online Government are designed to save agencies money by eliminating the need for dedicated IT resources for bursty applications such as video storage while also speeding up deployment of new applications in such areas as citizen engagement.

"In some cases, government will move existing workloads to the cloud to run at greater efficiency and reduced cost. Another scenario is developing completely new solutions such as big data analytics with Hadoop or machine learning or scenarios around managing large sets of government multimedia in the cloud," Donlan said.

Microsoft has 3 million federal, state and local government users of Office 365, which provides email and collaboration.

With Azure Government, Microsoft is adding cloud services to the mix, including compute, storage, data networking and identity management via Active Directory. Azure Government is hosted in Microsoft data centers that are located within the United States and operated by U.S. personnel with security clearances. Using Azure Government, agencies can run workloads in the public cloud, government cloud or in their own data center.

Microsoft Dynamics CRM adds cloud-based business applications such as case management and logistics. This platform also operates in hybrid environments combining public and private cloud and integrates with Azure and Office 365 government community clouds.

Microsoft said Azure Government and Dynamics CRM Online Government will be available through all of its government resellers and on all of its government contracts.

Microsoft said 125 companies have ported their third-party applications to Azure Government for local, state and federal customers. One of these partners is Vievu, which markets body cameras for police offers. Another is NC4, which offers public safety and security solutions.

The new features will provide customers a broad set of options, said Donlan. "They don't have to move everything to the cloud. They can move some applications to the cloud, and others can run in their data centers. They can manage a hybrid environment, which will be a differentiator for Microsoft," said Donlan. •

MICROSOFT AZURE AT A GLANCE

- Cloud service offerings include infrastructure-as-a-service, software-as-a-service, business process-as-a-service, identity management.
- Office 365 : 3 million federal, state and local government users for email and collaboration.
- Customers include cities of Chicago, San Jose, New York State and Los Angeles County.
- Early adopters: Texas (110,000 Office 365 seats) and Alabama (23,000 Office 365 employees)
- 125 companies have ported third-party applications to Azure Government for local, state and federal customers.
- Standards compliance: HIPAA, CJIS, FISMA, IRS 1075, FedRAMP.

How SciServer is cutting big data down to size

A group of scientific researchers, who work with datasets in the terabyte range, wants to develop a set of tools for data sharing, analysis and access for data management challenges across the scientific community.

Under the auspices of the National Science Foundation, the group has begun a project called SciServer, whose mission is to, "build a long term, flexible ecosystem" to provide access to datasets generated by astronomy and space science projects.

"By building a common infrastructure, we can create data access and analysis tools useful to all areas of science," Alex Szalay of Johns Hopkins University, the leader of the NSF-funded project told Phys.org.

SciServer grew out of work with the Sloan Digital Sky Survey (SDSS), an ongoing project to map the entire universe. SDSS, begun 15 years ago, now has over 70 terabytes in its database covering 220 million galaxies and 260 million stars.

The SciServer team, which began working on the solutions to the problems in 2013, said they would launch the project in phases over the next four years.

The tactics they will bring to the project include:

Bring the analysis to the data. "This means scientists can search and analyze big data without downloading terabytes of data, resulting in much faster processing times," Szalay said in a statement.

Specify real-world use cases. The SciServer team is collaborating to ensure the system will be most helpful to working scientists.

Develop new tools. To help ease the burden on researchers, the team developed "SciDrive," a cloud data storage system that allows scientists to upload and share data using a Dropbox-like interface.

Adapt existing working tools. The strategy of building systems by adapting existing, successful tools is a key factor in ensuring the success of the project.

"The tools we build will create a fully-functional, user-driven system from the beginning, making SciServer an indispensable tool for doing science in the 21st century," Szalay said.

As SciServer becomes more mature, the team will expand to other areas of science including genomics and connectomics, which explores cellular connections across the structure of the brain, according to the researchers.•

Argonne sets new marks for high-speed data transfer

Researchers from the Argonne National Laboratory, working with DataDirect Networks (DDN), transferred 65 terabytes of data in under 100 minutes between storage systems, a digital accomplishment that would have taken two days with a 10 gigabit/sec connection.

The demonstration took place over a 100 Gbps wide-area network connection between storage centers in Ottawa Canada and New Orleans, La., in November at SC14, a conference for high-performance computing.

The team, with support from networking firms Ciena and Brocade and Internet research group ICAIR, reached data transfer rates above 85 Gbps—with peaks at over 90 Gbps, according to a report from the Argonne lab.

Achieving the record speeds involved combining file and virtual machine features of the DDN storage controller, the wide-area data transfer capabilities of the Globus GridFTP server and an advanced 100 G wide-area network.

DDN offers massively scalable storage systems for big data and data intensive applications, such as supercomputing, seismic processing and genomics. The open source Globus GridFTP server uses an extension of the standard File Transfer Protocol for high-speed, secure data transfers.

"Embedding the GridFTP servers in virtual machines on DDN's storage controller eliminates the need for external data transfer nodes and network adapters," said Raj Kettimuthu, principal software development specialist at Argonne.

Kettimuthu pointed out that networking experts often say storage is the bottleneck in end-to-end transfers on high-speed networks, while storage experts claim that the network is the stumbling block.

Achieving more than 90 Gbps for memory-to-memory transfers using a tool like iperf, a benchmarking tool for network performance measurement, is straightforward and has been demonstrated several times in the past, he added.

However, achieving similar rates for disk-to-disk transfers presents a number of challenges, according to Kettimuthu, including choosing the appropriate block size that works well for both disk I/O and network I/O and picking parallel storage I/O threads and TCP streams for end-to-end performance.

"The demonstration was aimed at bringing together experts and the latest developments in all aspects of disk-to-disk WAN data movement, including network, storage and data movement tools," said Kettimuthu. •

5G will power the Internet of Things – and governments

BY BRIAN ROBINSON

It's by no means complete yet, but the transition to a mobile IT environment in government is well established. Parallel with that, however, is the expectation that mobile communications will be able to deliver all that society expects in the way of seamless audio, video streaming and fast transfer of multi-megabyte data files.

Third-generation (3G) wireless technology, which many people are still using on their cell phones, is clearly not up to the task. 4G service is the current version, and it offers much broader capability. However, with the inevitable increase in bandwidth demand, eventually even that won't be enough.

Enter 5G, still some ways over the horizon, but something government will have to grapple with – and incorporate into its networks—sooner than later.

For the United States, according to the Congressional Research Service (CRS), it may be a competitive necessity. Already a leader in the deployment of 4G LTE (Long Term Evolution) wireless, the most widely adopted standard, the country could maintain its edge by moving to 5G by 2025. If it doesn't, CRS warned, development of 5G technologies already demonstrated by other countries could erode that lead.

For most agencies, however, 5G probably isn't on the horizon because 4G seems like it will deliver what they need to cover their current concerns.

Today, 4G is certainly becoming a necessity for agencies, said Warren Suss, president of Suss Consulting. "But with so many near-term issues, I don't think many of them have put a lot of thought yet into 5G. Most of their focus right now is on things like the cloud, and how to provide access for their users to the data that's contained in the cloud," he said.

Starting in the early 2000s, 3G mobile delivered a minimum of 200 kilobit/sec, bumping that up over the years to several megabit/sec. That was a decent speed for mid-decade services – which comprised mainly voice, email and web browsing – but pokey even by the time the early 4G networks started to appear in 2008.

4G mobile service has now been adopted widely throughout North America and Europe, and by much of South America. Based mainly on the LTE specifications first proposed in 2006, it offers current smartphone users average download speeds of between 15 and 30 megabit/sec, with peak speeds up to 300 megabit/sec. So-called Advanced LTE could provide speeds of up to 1gigabit/sec.

Already a leader in 4G LTE (Long Term Evolution) wireless, the most widely adopted standard, the United States could maintain its edge by moving to 5G by 2025.

Newer mobile devices support 4G by default, though so far it's not just a matter of agencies ordering the service from carriers. Government requirements such as strong security and mobile device management aren't usually included with 4G service, so agencies still have to buy those tools separately and manage them internally.

So far, service is also mostly limited to urban areas. City governments, therefore, seem likely to be the ones to benefit the most from early deployments of 4G, using the technology to collect data from parking meters and lights, and to connect that to city wide area networks.

The small cell infrastructure that's often used for 4G in cities, with a range of up to two miles for each low-powered network node, is ideal for city environments but not for the much greater distances rural users operate in. For that reason, in February 2012 the federal government created the First Responder Network Authority (FirstNet), whose primary goal is to build out a 4G mobile network for public safety organizations throughout the United States.

The 4G technology FirstNet uses operates in the 700 MHz spectrum, which is lower than what urban 4G networks use, but which gives better signal penetration that can carry for greater distances. A year before the law creating FirstNet was signed, President Obama outlined a plan to get as much as 98 percent of the U.S. population access to 4G.

However, the eventual limitations of 4G are becoming evident. Because of the heavy demands by some users, carriers are already "throttling" bandwidth use at times. As the kinds of content that government and others users seek to provide through mobile services increases, that problem will only become more acute.

5G technology is still at a nascent stage of development. Specifications and standards haven't been agreed upon, but there's a broad understanding that it could offer speeds up to at least 100 times that of current 4G LTE. In October, Samsung said it had recorded a speed of 7.5 gigabit/sec over its 25 GHz test network. Earlier, Swedish vendor Ericsson said it had posted 5 gigabit/sec on its network.

5G will also have the capacity to simultaneously connect the billions of sensors and other devices that will be linked in the emerging Internet of Things. •

Improving ROI with a Holistic Approach to Software-Defined Solutions

Over the past several years, federal IT departments have worked hard to reduce costs and increase efficiency in response to tight budgets, increased oversight and other pressures. Despite progress, technology continues to change and customers are asking for a host of new services that require more capacity or innovation than current technology infrastructures can provide. Add to that the need to comply with mandates such as the Federal Data Center Consolidation Initiative (FDDCI) and the Digital Government Strategy, and it's clear that agencies need to continue pushing to increase efficiencies and innovation while reducing costs.

For many agencies, the first step has been to virtualize various parts of the infrastructure, starting with desktops and servers and, more recently, storage and networking services. Agencies have realized many benefits due to virtualization, including cost reduction and ease of management, faster deployment, and greater levels of automation.

While virtualization is an excellent first step that provides exceptional returns, agencies face continuing challenges, from quickly growing data stores and mobile traffic to a demand for new services that require modern infrastructures. This is in addition to the continued struggle of maintaining aging infrastructures and succumbing to budget pressures. A recent MeriTalk survey found that agency personnel spent more than 73 percent of their time performing routine tasks such as provisioning equipment and services, load balancing, back-ups and monitoring, or waiting for technology and service deployments. The survey found that taken together, these tasks cost nearly $5 billion each year in productivity. As agencies continue to drive virtualization across their infrastructure to further increase efficiency and control costs, they must also consider opportunities to optimize the operational aspects of that infrastructure.

The next logical step in the evolution of agency technology infrastructure is adoption of the software-defined enterprise (SDE). The SDE takes virtualization to a new level by extending the benefits of virtualization to all infrastructure in the data center—networking, storage, servers, etc.—and delivering everything as a service through a set of common management principals. In many cases, the software-defined enterprise extends beyond the data center and across the campus LAN, WAN, and even public cloud services. Control in the SDE is entirely governed and automated by software. This increases availability, scalability, agility and manageability, and requires fewer people to operate. One immediate result is the reduction of capital expenditure as high-cost hardware is replaced with commodity infrastructure.

A recent VMware survey found that enterprises that adopt a software-defined strategy find immediate returns; many organizations are able to save on both operations and development staff time while increasing revenues by delivering modern applications and IT services. In addition, there are often additional funds available to invest in the innovative technologies necessary to satisfy user demand. And more than one-third of software-defined enterprises are more responsive to IT requests than their less mature counterparts after moving to a highly-automated software-defined infrastructure.

The key to success, says Jad El-Zein, principal engineer for VMware's public sector division, is to take a holistic approach to the software-defined enterprise. That means looking at the enterprise as an ecosystem of hardware and software providers with one vendor as the centerpoint. If, for example, VMware is that centerpoint, VMware is responsible for ensuring that all applications and devices in the enterprise are integrated and automated. Integration is another key to success; point solutions drive up the management, overhead and complexity of the environment, reducing the potential for positive ROI. By delivering solutions that are integrated and leverage each other's technology, positive ROI is much easier to achieve.

"Our approach is to integrate first, then automate, and then augment… where possible," El-Zein explains. "Augmenting means inserting VMware's networking and storage technologies when it makes sense, usually during refresh cycles, to gradually move the enterprise toward a true software-defined enterprise."

Federal agencies are beginning to understand the importance of the software-defined enterprise, and are taking steps towards implementing it. According to MeriTalk, 66 percent of federal agencies are working toward a software-defined data center, while 55 percent are moving in the direction of software-defined networking and 59 percent towards a software-defined storage strategy.

Software-Defined Enterprise ROI

While virtualization has brought agencies an exceptional return on investment over the past decade, there is much more to be gained by moving to a software-defined enterprise. The integration of the entire ecosystem, fueled by higher levels of automation, and a holistic management approach largely accounts for the higher ROI. For example, replacing daily, repetitive or complex

Key Components of the Software-Defined Enterprise

The software-defined enterprise consists of three major parts: network, storage and data center.

Software-defined networking

SDN controls network resources, including switches and routers, with open protocols, enabling agencies to maintain tighter control of network resources. It also automates many network-related processes, such as provisioning and load balancing, while allowing agencies to scale network resources up and down as demand requires. This is particularly useful for seasonal spikes, which many agencies experience. For example, a natural disaster or tax season can temporarily increase the need for more resources, which go back to lower levels after the spike.

The federal government is on board with the concept of software-defined networking. A recent study found that 61 percent of federal IT management executives and IT professionals expect SDN to play a role in network purchase decisions.

Software-defined storage

Data storage is a major pain point for government agencies, mainly due to the continued fast growth of government data. According to a study from the 1105 Public Sector Media Group, government data is expected to increase at a rate of about 30 percent each year. The need for more and more storage is one reason why federal agencies are moving forward with software-defined storage solutions, either as an add-on to physical storage or for new data centers. With software-defined storage, a virtualized storage controller manages storage provisioning, as well as communication between storage devices and networks and servers. Other features are high availability, the ability to support hardware from multiple vendors, enablement of policy-driven provisioning of storage volumes and centralized management. All of this means that when an agency needs to provision storage for a particular application, service or workload, it doesn't have to buy a new storage array.

Software-defined storage lowers operational expenses by automating complex or frequent storage operations. It also simplifies the management of different classes of storage using storage virtualization technology and integrated management tools. SDS contributes to lower capital expenditures by reducing the number of physical storage devices required.

Software-defined data center

The goal of SDDC is to free the application layer from the hardware layer through virtualization, automation, orchestration and the use of cloud computing. Everything is controlled and managed centrally, via software, and is fully aligned with application and service requirements. SDDC works seamlessly across heterogeneous IT infrastructure, and provides repeatable configurations of software and infrastructure for workload deployment, along with capacity management, cloud management and configuration management. Over time, SDDC helps enterprises transform the way it delivers IT at lower cost, with more flexibility, automation and efficiency.

tasks with software that automates those tasks requires less human intervention, lowering operational costs. In addition, an automated infrastructure can provision resources much more quickly, giving users faster access to critical applications and services. This is especially true for repeatable tasks, which are the majority of all data center service requests. Other sources of reduced operational costs include less required physical space, along with lower heating and cooling expenditures. This area of ROI, related to employee productivity, is the unsung hero of the ROI equation, says Clifford Grossner, a directing analyst at Infonetics Research.

Because the software-defined enterprise provisions networking, servers, storage and applications only when they are required, less infrastructure is required, lowering capital costs as well.

In the traditional data center, the compute, storage and network are physical, inflexible resources that can't be easily shared, so an agency might have an entire bank of storage devices with all of them only partially used. It's the same for networks; an agency could deploy a significant amount of network and security infrastructure along its perimeter but if it's provisioned in a very static way, there may be portions of the network that are underutilized while others are stressed or unknowingly insecure. Dynamically provisioning networks, through software, per application can drastically reduce these pain points while providing a significantly increased security posture.

"With a software-defined paradigm, there is a flexible pool of resources that are dynamically used on the fly by the application that needs it," Grossner explains. "So right away once you get to that point there is much better use of resources so you need fewer resources to deliver your applications to the end users."

Here is just one example: An agency with mission-critical applications but unpredictable use of those applications is spending $50 million per year on physical network and storage technology to ensure that its users will always have the infrastructure and access they need. Under the old paradigm, the agency would have to keep investing millions of dollars in the infrastructure each year. If the agency invested that same $50 million in a software-defined enterprise, after absorbing the initial capital costs, ongoing costs will decrease significantly, while the intelligence and responsiveness of the technology increases dramatically.

Calculating the ROI

One of the best metrics to measure the ROI of the software-defined enterprise is the cost per application or service. That involves understanding the true cost of running the application—the people, labor, licensing, energy, real estate and infrastructure. Comparing those costs before implementing a software-defined enterprise and afterwards is a valuable metric. If the application in a traditional data center costs $100 per day for operations and management, it might cost $20 per day in a software-defined data center, for example.

There are other important metrics that can be measured as well. One is the investment in orchestration software versus the time freed up in an employee's day that used to be filled with tasks such as manual network configuration and storage provisioning. Others include measuring the time it takes to get an application up and running under the old and new infrastructure, downtime, reclaimed free space, percentage of applications that meet SLAs, average time to provision a node or deploy an application, average delivery time of new products or services, and percentage of managed nodes. The specific metrics you measure will depend on your specific infrastructure and agency priorities.

There are many tools available to measure these metrics. In addition to project management tools already in use by many IT departments, there are standalone tools such as VMware vRealize Business. Systems integrators and consultants often have their own tools as well.

What's the Difference Between Virtualization and Software-Defined?

At first glance, it might seem like the software-defined network, storage or data center is just virtualization by another name. In some ways that's true—both aim to more efficiently, directly, consolidate or segment resources—but there are important differences. Network virtualization, for example, reproduces isolated versions of the physical network that can be created, operated and removed without disturbing physical assets. SDN uses switches that can be programmed through an SDN controller using an industry standard control protocol such as OpenFlow. It changes the network architecture by separating the control plane from the data plane.

There are also differences between software-defined storage and storage virtualization. Storage virtualization is a process that pools data from multiple storage devices in a way that functions as a single device managed from a central console. Software-defined storage allows storage services to be dynamically created and delivered per virtual machine and controlled by policy. This allows storage services to be fully aligned with application requirements.

VA recruits Watson analytics, cloud to fight PTSD

The Department of Veterans Affairs launched a pilot project to test the ability of IBM's Watson analytics technology to help VA doctors rapidly sift electronic medical records for treatment and research data that could support clinical decisions in the care of veterans.

The VA will also assess how Watson technology, which became famous by competing against Jeopardy! quiz show winners, might help speed data-driven clinical decisions, including those involving post traumatic stress disorder cases.

"Physicians can save valuable time finding the right information needed to care for their patients with this sophisticated and advanced technology," said Interim Under Secretary for Health Dr. Carolyn M. Clancy in announcing the project.

"A tool that can help clinicians quickly collect, combine and present information will allow them to spend more time listening and interacting with the veteran. This directly supports the patient-centric medicine VA is committed to delivering every day," she added.

The VA-Watson project leaders also want to study the potential of the technology for producing relevant medical data at the point of care as well as to reduce the number of systems and tools physicians have to juggle in clinical settings.

According to IBM, analyzing a single EMR is on a par with scanning up to 100M of structured and unstructured data, much of it in the form of plain text, across a patient's lifetime of clinical notes, labs and treatments.

Using Watson, Veterans Health Administration physicians, "can now interact with the data in natural language, process vast amounts of big data to uncover patterns and insights and learn from each interaction," said Anne Altman, IBM general manager for U.S. federal in a blog post.

During the pilot, clinical decisions will not be made on actual patient encounters, but instead will use realistic simulations.

The project will also use IBM Watson Discovery Advisor, a new tool that uses visualization techniques to help uncover patterns in data. The cloud-based service can help accelerate research from months to days and hours, IBM said.

The VA project isn't the first time Watson has been enlisted to support healthcare or veterans programs.

The company announced in October it was partnering with the Cleveland Clinic to use Watson Genomics to study cancer treatment options based on a patient's genome. The Memorial Sloan Kettering Cancer Center in New York and the Anderson Cancer Center in Houston, Tex., both use Watson-based tools in analyzing cancer treatments. •

NSA releases open source tool for high-volume data

The National Security Agency released an open source software product that automates data flows among multiple computer networks, even when data formats and protocols differ.

As the volume and rate of data grows and as the number of systems, protocols, and formats increase, so too does the complexity and need for greater data management insight and agility.

Niagarafiles (Nifi) is a dataflow system based on the concepts of flow-based programming and was designed to manage dataflow in massive distributed computing systems operated by numerous teams and organizations.

Joseph L. Witt, the lead developer of Nifi, said it "provides a way to prioritize data flows more effectively and get rid of artificial delays in identifying and transmitting critical information."

Over the past several years, Nifi has developed a strong community of both developers and operators within the U.S. government, according to the Nifi proposal on the Apache Incubator Wiki. In open sourcing Nifi, the NSA lets private sector programmers examine the code, and potentially improve it through additional enhancements and applications. At the same time, the government can gain from their related research advances.

The tool could benefit the U.S. private sector in various ways. For example, commercial enterprises could use it to quickly control, manage, and analyze the flow of information from geographically dispersed sites – creating comprehensive situational awareness, the NSA said in its announcement.

The Nifi code is available to the public through the Apache Software Foundation. It is the first in a series of releases of in-house software products by NSA's Technology Transfer Program.

"NSA's innovators work on some of the most challenging national security problems imaginable," said Linda L. Burger, director of NSA's tech transfer program. "Their research breakthroughs often have broad, commercial applications, too. We use open source releases to move technology from the lab to the marketplace, making state-of-the-art technology more widely available and aiming to accelerate U.S. economic growth."

In 2011 the NSA's code for the agency's Accumulo project was also released through the Apache Software Foundation. •

Energy Dept. recasts enterprise architecture for cybyersecurity

BY JOHN MOORE

Dismissed as little more than "shelfware" over the years, enterprise architecture is now getting a fresh look as an approach for addressing specific IT problems, including enhancing agency cybersecurity defenses.

Enterprise architecture, or EA, emerged in the government sector in the 1990s after the Clinger-Cohen Act tasked agency chief information officers with establishing IT architectures in order to improve the alignment between an agency's IT plans and business practices.

Since then, EA has to compete for management attention with other trends for instituting enterprise efficiency, most recently DevOps and agile development practices that stress collaboration between software and IT development. EA has also had to accommodate an increasingly dynamic IT environment in which cloud-based computing resources can be summoned on the fly.

Against this backdrop, however, some agencies are taking EA in novel directions.

The Department of Energy's CIO office, for example, has built a tool that enlists EA in the agency's cybersecurity cause. The Enterprise Architecture Roadmap Solution (EARS) aims to help identify IT assets nearing end-of-life so aging servers and unsupported software don't become vulnerabilities. An IT security incident in 2013 helped solidify that particular use case.

"We had a cybersecurity breach last year and one of the weak points was ... out-of-date software," noted Rick Lauderdale, chief enterprise architect of the Department of Energy.

An old copy of ColdFusion had become the point-of-entry for an attack, a discovery that inspired Energy to develop a better record of information it was collecting on its IT assets, he added.

Tools like EARS represent a shift in thinking among agencies, according to government IT watchers.

Brian Fogg, chief technology officer at NCI Inc., an IT services provider, said agencies are cleansing and enriching asset data so they can make better enterprise IT decisions, part of an effort to frame EA within a broader agency asset data discussion.

"Our clients in DOD tend to use it that way and are driving decisions around security and vulnerability management and threat identification," Fogg said.

> "We had a cybersecurity breach last year and one of the weak points was out-of-date software."
>
> – RICK LAUDERDALE, DOE

EARS IN THE MAKING

To create the EARS tool, Energy integrated software it already had in place with additional off-the-shelf technology. The department had been using BigFix, which scours Energy's network to collect data on hardware and software assets, as an asset discovery tool. Energy was also using Troux Technologies' EA management tool.

The agency began using the applications to explore data on its IT assets. Lauderdale said 30 percent of that data was analyzed to get an estimate of how much of Energy's hardware and software inventory was hitting end-of-life status.

In doing so, the department discovered problems with its inventory information. For example, merger and acquisition activity among IT companies meant that the same hardware and software products would sometimes appear under different names.

To enhance its asset identification, Energy added products from BDNA to the mix, including BDNA's Technopedia and Normalize products. Technopedia offers a categorized repository of hardware and software, which gave Energy an enterprisewide standard for IT asset terminology. BDNA Normalize then takes the data from BigFix and normalizes it against the Technopedia standards.

BDNA works with IT vendors to prevent data describing EA from becoming stale. That approach improves the reliability of information on end-of-life assets. "They keep up with the life cycle information … every day, and they update the data structure," Lauderdale said.

In the next step, the Troux Platform pulls the fully normalized asset information from BDNA, combines it with other contextual business/IT information and provides analytics and visualizations that help identify areas of excessive risk and cost, according to Ted Reynolds, Troux's vice president of public sector.

Troux generates reports that highlight IT assets with a color-coded lifecycle status – red for assets that are in trouble and ripe for removal, and yellow for assets that are heading for end-of-life, he said.

Agencies looking to apply EA to problems such as IT security need to focus first on preventing their IT asset data from becoming stale. "It begins there," Fogg said, noting the necessity for a strong commitment to keep the data around the EA up to date.

"The less it is current, the less it is applicable to the enterprise," he said.

Agencies also need tools to make EA more responsive to IT management challenges. Lauderdale said BDNA and Troux provide a foundation for an EA solution, noting that an agency could include BigFix or another IT asset information products as part of the overall package. •

the Viewpoint
business

The Enterprise Security Shift

Q **What are the major threats to mobile security today? How will those change?**

Sam Phillips, Vice President of Global Enterprise Services (GES), Security Solutions, Samsung

A Unlike the desktop and stationary environments of the past, the biggest threat today is having end points that are moving around outside the physical boundaries of the organization and without close control. The challenge is to make sure government information and data are protected with devices that match up with specific agency security policies and requirements. Some agencies already have a solid set of defined requirements and a sound understanding of the issues, but others still need strong support from device providers.

Q **Is there such a thing as a totally secure mobile device?**

A Security is a relative goal. First, you have to understand the capabilities of the devices, and then, the associated services and products that come with them. After that, you can better judge the risk/reward and tradeoffs when selecting a product. Samsung's platform incorporates both hardware- and software-based security components, rather than software alone, and that's already shown dividends. Samsung Galaxy devices, supported by the Samsung Knox platform, have passed rigorous government testing and are now included on the Commercial Solutions for Classified (CSfC) list.

Q **The focus for enterprise security is shifting. Where does mobile device security fit?**

A You're right, in that the paradigm for security is shifting and BYOD continues to drive the need for more control of data on the device and better device policy management. For example, there's an accelerating trend to move certain types of employees off of laptops and PCs and onto tablets and smartphones. Agencies want more operational effectiveness, so the future of mobile technology needs to meet or exceed the requirements for fixed base assets while being mobile. That said, mobile security first has to be integrated into existing security paradigms. Once those baseline needs are met, then you can move beyond those requirements.

Q **How different are the mobile security needs of individual programs? How do you meet them?**

A Again, you must have a good understanding of an agency's baseline needs, then you can make educated decisions on how and when to increase security requirements. For example, think about the option to move into the biometric space to improve multi-factor authentication. You should leverage the technology that's already there in mobile devices, then add additional resources and capabilities as required. Existing technologies like fingerprint readers, camera quality which promotes iris and retina recognition are some examples of adapting existing technologies. From the Samsung perspective, that starts with executing things such as encryption and key management in hardware and then, moving forward, adding things like secure boot and trusted boot, as well as the trusted integrity management architecture and application framework as a solid baseline to build on.

Q **Does it really matter what mobile device technologies are used when it comes to security?**

A Absolutely. If you don't have a common, solid core of security that you're building on top of, then the mobile device technologies you're deploying aren't truly secure and potentially won't meet the needs of the business. Nearly every smartphone, for example, comes with both a front and a back camera. Building security capabilities into those devices allows for the management of policies around the camera, mitigating the risk of an information leak. We built our Samsung Knox framework on our devices by starting from the hardware up. When you add a feature or capability to a device, you can take a look at the core security structure and make a determination about the potential use, or potential abuse, of the new technology and adapt according to the need.

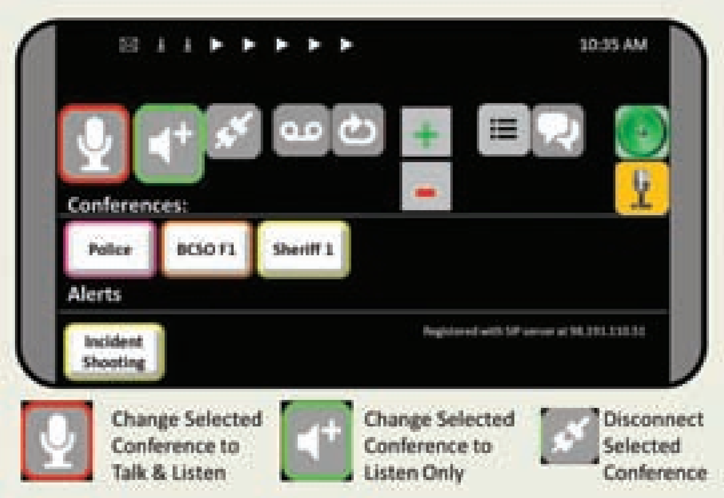
SAMSUNG

To learn more go to:
www.samsung.com/us/enterprise

Turtle Mike speeds emergency response

BY KATHLEEN HICKEY

The Department of Homeland Security has developed a bridging technology that enables multiple public safety and law enforcement response teams to unite land mobile radio (LMR) and broadband to help coordinate rescue and speed the care of emergency victims.


10:35 AM
Conferences:
Police
BCSO F1
Sheriff 1
Alerts
Incident Shooting
Change Selected Conference to Talk & Listen
Change Selected Conference to Listen Only
Disconnect Selected Conference

Turtle Mike app creates a teleconference accessible by radio and broadband.

The Hybrid Public Safety Microphone, dubbed Turtle Mike, merges LMR and broadband systems to form a teleconference platform that can be accessed by both systems.

DHS's Science and Technology Directorate's (S&T) recently completed successful two-week field tests of the technology in Nebraska. Turtle Mike was funded by S&T's First Responders Group (FRG) at the request of DHS's U.S. Customs and Border Protection.

The ultimate benefit of Turtle Mike is that it enhances coordination with responders who may not have access to LMR radios. Furthermore, Turtle Mike does not require costly replacement of existing communications equipment and infrastructure.

Broadband and LMR systems currently operate independently of one another. First responders, medical teams and other supporting elements use standard LMR radios, which have limited frequencies and bands, and augment them with smart devices using cellular broadband networks.

"If you have an incident, there are many different people who have to communicate at the same time on the same system. Turtle Mike allows direct contact easily between police, medical and fire responders and the hospital using different communications equipment; this is vital," said FRG telecommunications specialist Tom Chirhart.

The cellular networks allow for greater coverage. "Some radio bands don't have the signal penetration in buildings that others do," Chirhart added. "The signals bounce off or are absorbed by the structure. Because broadband frequencies are higher, they have better signal penetration in densely constructed buildings."

Broadband offers better capacities to carry or exchange content such as images and video, according to an S&T description of the technology.

Even so, first responders will likely continue to use LMR, at least for the foreseeable future, as commercial broadband networks do not have the same capabilities of an LMR system, such as push-to-talk and radio-to-radio capabilities. Turtle Mike, a hardware platform and app, creates a "teleconference platform" accessible by both systems. Users can communicate via LMR or broadband and set up broadband conferences on their cellular networks.

"The Turtle Mike takes the conversation off the frequencies and bridges them together," Chirhart said. "You can talk radio-to-radio or broadband-to-broadband or radio-to-broadband. It connects everyone together."

Turtle Mike is also compatible with any existing LMR system and the app can be downloaded to any smart device. Once installed, the app allows first responders to access LMR channels from their smart phones and other devices. Users can then set up an unlimited number of separate broadband conferences that can be tailored to the incident.

Phase one laboratory testing is now concluding at the Public Safety Communications Research Program in Boulder, Colo. If the Turtle Mike solution is approved, phase two testing with actual DHS users will take place in 2015.

During phase two, S&T will update the preliminary prototype, correct shortfalls and add advanced features. The prototype will then undergo additional field tests to evaluate the technology and verify that responder requirements were met. Turtle Mike is also expected to be commercially available this year.

S&T is already moving forward with new applications of the technology. Last year, Vanessa Burnett, program manager of FRG's Office for Interoperability and Compatibility, S&T, described using Turtle Mike technology for school safety measures.

"Turtle Alerts" would be used to provide "managed, direct communication between school staff and first responders in emergency situations," Burnett noted in her presentation. •

Privacy wearables for the secure – and stylish

There are no shortage of devices and technologies to keep government information and communications secure. From the use of strong, frequently changed passwords and two-factor authentication to biometrics, agencies have a suite of options to protect their users' data.

And with the wakeup call from the Sony hack, people inside and outside of government are taking a harder look at extra protection for their personal information from the devices they carry to the clothes on their backs.

To answer the demand, vendors are ready with security solutions ranging from stylish privacy accessories to secure wearables and communications ecosystems.

In a collection at Macy's, Royce Leather is offering a selection of accessories that integrates fingerprint technology, RFID blocking and GPS into its handbags, briefcases and wallets "to protect users most private possessions, said CEO Andrew Royce Bauer.

The Freedom Briefcase, which features "a slim, sleek silhouette, hand-milled hardware and Italian Saffiano leather," uses what Royce calls "DNA-based fingerprint technology" to allow only a single user to access the bag.

The bag also uses RFID-blocking technology to thwart electronic identity theft, as do the company's wallets, money clips and passport jackets. Privacy is further enhanced by blocking scanning devices that can read and store personal information from common contactless smart cards.

A conductive layer provides a secure barrier that limits the flow of RF energy between the reader and the smart card or other RFID device.

Royce also offers GPS tracking for those who can never find their wallets. A slim tracker inside the wallet uses a Bluetooth connection to iOS and Android devices within 100 feet of the wallet. "The greatest gift the Royce Leather Freedom Wallet offers is the security of not losing what you already have," Bauer said.

Wait there's more: the iWallet not the iOS app, but a metal wallet case that protects an owner's cash and credit cards with "space-age materials and biometric security." •

N.C.'s iCenter leads multistate technology testing lab

BY STEPHANIE KANOWITZ

While many states and federal agencies have innovation offices to help transform the way government delivers services, North Carolina's Innovation Center (iCenter) operates a working laboratory where state agencies, educational institutions, private industry and citizens can perform technical evaluations, conference room pilots, prototype testing and proofs-of-concept.

The "try before you buy" working lab has tested more than $6 million worth of technology at no cost to the state, allowing agencies to make better-informed decisions about how to invest their technology dollars. The iCenter has also led to savings of approximately $1.4 million a year in storage costs and $7 million in renegotiated IT contracts.

Launched in October 2013, iCenter is now collaborating with states nationwide, North Carolina Gov. Pat McCrory recently announced. About 25 states are part of the effort and they will meet monthly to share best practices and challenges, said Erik Ross, the state's chief digital officer and director of iCenter.

"We look forward to sharing our experiences and learning from other states as we all work to improve the service we offer our citizens," McCrory said in a statement.

Before iCenter began reaching out to other states, it spent about a year perfecting its operations, including how to do testing, how to work with vendors and university students and how to engage with citizens.

The center was borne from state Chief Information Officer Chris Estes' assessment of the state's existing technology and a need to update much of it.

A state auditor's report that 84 projects prior to 2013 were 389 days behind schedule and $356 million over budget also spurred iCenter's creation.

The center works like this: CIOs from North Carolina's cabinet-level agencies meet weekly to discuss pain points and areas of opportunity – operating essentially as a board for the center. They also identify and prioritize areas they want to leapfrog old technology to get up-to-date, after which the center helps coordinate the appropriate state, vendor and university partners, Ross said.

Among the technologies tested are social media listening tools, interactive kiosks, Office 365, mobile field applications and computing devices (smartphones, tablets, thin and zero clients and laptop computers), beacon technology and virtualized desktops.

"One theory that that group came up with is around cloud and virtual technology, so we did a pilot with hosted virtual desktop and virtual applications," Ross said.

"We worked with a number of vendor partners to put together a pilot that lasted roughly six months. Through that process we learned a lot about what the requirements are, we learned a lot about our own technology, we learned a lot about how that technology would work internally and we also had a number of different agencies that were involved in that test."

Part of the evaluation included analyses of what users would need and mapping the results to a virtual technology to see how a new technology could meet those needs. Advantages of virtual include the ability to access the desktop and applications on any device from anywhere as long as there's an Internet connection.

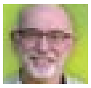
"That's a big focus for the governor as far as empowering the next-generation workforce as well as all of the cabinet agencies," Ross said, which is why that evaluation was a top priority.

The duration of the tests ranges from a few weeks to a few months, depending on the technology. So far, iCenter has tested about 20 products and has four more in the queue, he said.

iCenter has no budget; partners cover evaluation costs, Ross added. Because the center is part of Estes' office, most of what's tested is for enterprise use, although it has studied a specific product for one or two agencies.

"The idea is that a particular test could be emulated and used across multiple agencies because we're trying to gain efficiencies," he said. "Most of the agencies, at least in North Carolina, have been operating as independent entities, so there's a good bit of duplication of infrastructure and services. We're trying to enable, by bringing all these folks together, a way to leverage the scale and skills we need to work together as a team."

In the private sector, the innovation function is often integrated with the production process so there's a market-forcing element, but in government it's more about service and cost effectiveness, said Dan Chenok, executive director of the IBM Center for the Business of Government. •



CYBEREYE

BY BRIAN ROBINSON

Cyberattack ‘platforms’ call for defense in depth – and breadth

IT’S GETTING A LOT HARDER to be impressed by the latest piece of malware or cyber threat that hits the streets, given the already formidable arsenal that has been created for hackers to choose from. The every day distributed denial of service (DDoS) threat now seems almost quaint. Then along comes Regin.

To be more precise, along comes Backdoor.Regin, recently discovered and described in detail by Symantec. What astounds about this Trojan is not just its complexity, but the time it’s taken for it to mature into its current state.

Symantec has traced attacks back to at least 2008, and some reports suggest components of Regin go as far back as 2003.

What astounds about the Regin Trojan is not just its complexity, but the time it’s taken to mature; some reports suggest components of Regin go as far back as 2003.

That takes the definition of Advanced Persistent Threat (APT) to a new level. And it may go even further since Symantec warns that analysis of it will probably reveal much more.

“Threats of this nature are rare and only comparable to the Stuxnet/Duqu family of malware,” it said. “Many components of Regin remain undiscovered, and additional functionality and versions may exist.”

The company describes Backdoor.Regin as a multi-staged threat, with all but the first stage hidden and encrypted. It also uses a modular approach and can be tailored with custom features for specific targets. Based on what’s been discovered so far, it has dozens of potential payloads.

In its own analysis, security researcher Kaspersky Labs said malware is not an accurate description of Regin. It should instead be seen as a cyberattack platform, which attackers deploy to gain total remote control of networks at all levels. According to Kaspersky, Regin is one of the most sophisticated it has analyzed.

“The ability of this [Regin] group to penetrate and monitor [Global System for Mobile] networks is perhaps the most unusual and interesting aspect of these operations,” the company said. “Although GSM networks have mechanisms embedded that allow entities such as law enforcement to track suspects, there are other parties which can gain this ability and then abuse it to launch other types of attacks against mobile users.”

GSM is the most widespread mobile standard, and has over a 90 percent share of the world’s mobile market. Other than the United States, which primarily uses the Code Division Multiple Access (CDMA) standard, most countries that have mobile networks use GSM.

At first glance, one would think that makes the United States safe from Regin attacks. Looking at the list of infections so far, big countries such as Russia and Germany are among the victims, along with some smaller ones. The United States is notably absent.

But as it turns out, that shouldn’t necessarily offer any comfort. As recent column here indicated, many of the most sophisticated attacks now come through the exploitation of privileged network accounts. That means that while government organizations may not be direct victims of an attack, if attackers get into the network of a trusted partner, they can eventually get to government data.

With the kind of global reach that government agencies now have to have to do business – even at the state and local level – no one should presume they are safe from bad guys getting into their networks and systems and stealing data.

And even if they haven’t been directly attacked, that doesn’t mean their partners have not been, nor the trusted partners of those partners and so on down the line.

Defense-in-depth has become the solution du jour for protecting data from malware and Trojans such as Regin that organizations now have to assume will penetrate their networks. Perhaps that should now be extended to a “defense-in-breadth” in order to cover vulnerabilities posed by threats outside the organization.

Modern organizations, including government agencies, have to do business with those lateral partners, so it should make sense to have such protections in place. •

INTERNAUT

BY SHAWN McCARTHY

5 trends that will drive IT management in 2015

2015 IS SHAPING UP as a year when data analytics, ubiquitous video, and cyber forensics will force government IT managers to make decisions about how they deploy their resources. The following five technology trends will drive those decisions.

1. Big data analytics will expand in a multiple directions.

Many government agencies are starting to realize they must not only deal with a coming big data deluge, they also need to make sense of that data – in multiple ways and through many aspects of government information and services delivery.

This includes “entity analytics” to look for common elements related to terrorism and fraud analytics related to taxes, unemployment compensation, health payments and more.

Leveraging data collected from the Internet of Things as well as smart city applications ranging from traffic analysis to perimeter security monitors, are also on the near horizon for local public safety agencies.

Each of these efforts involves analyzing different types of data that are held in different collections. Thus the world of analytics will start to have highly specialized focus areas, even as databases themselves are merged and shared. What’s more, metadata will play a larger role in tracking these data types, and agencies will need to expand their efforts to build reliable metadata structures.

In many cases, data ownership has taken top billing in the data logistics debate.

2. The rise of ubiquitous video.

Here are some of the drivers: Police are under pressure to wear body cameras. Many types of vehicles, not just police cars but even snow plows and other maintenance vehicles are being equipped with dashboard cams. Likewise there is a growing number of cameras in hallways, stairwells and common spaces of government offices. Some workers even choose to leave their webcams on as a way of keeping watch on their work spaces.

All of this not only creates more data, it begs for new sets of rules. Who has access to these video feeds? How can they be used? How long should the files be stored? Consequently, new rules may need to be set for when police cameras are turned off and on, who has access to the full range of video, and whether the files can be released immediately or if longer delays are necessary.

3. The logistics of data collection raises more than just ownership issues.

In many cases, data ownership has taken top billing in the data logistics debate. Under pressure to share data, agencies often lose control of how it is updated, what their metadata covers and how the data should be used once it leaves their hands.

However, other sets of issues arise as high-end computers need specific rules about the locations of their data stores. In converged infrastructures, processing is faster if data is stored in high-speed network attached systems. “Hyperconverged” systems further ramp up performance by moving storage closer to the compute element – even resident in memory – while also streamlining the management of those resources.

These trends mean data logistics will become an important part of future government data collection and the decision making process about where it is stored.

4. Cyber investigations become more complex.

The Sony studio hacking has ramped up the need for better cyber forensics.

Everything from improved egress filtering to data visualization for attack patterns and high-end tracing tools for packet traffic is on the table. The problem is that most of these tools already exist, but most agencies don’t use all of them because of management costs and processing overhead. Thus, to use the best possible security tools, investments must also be made in infrastructure.

5. Predictive analytics and maintenance is on the rise.

Predictive analytics can be tied to many activities. Security experts are building applications that monitor external penetration efforts while predicting the next steps that hackers will take. At the same time behavioral profiling – collecting, analyzing and interpreting information to identify risks and predict threats – is on the rise.

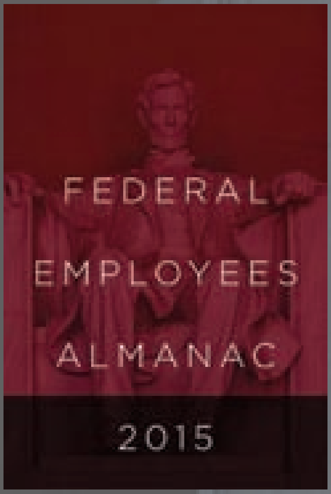
Meanwhile physical asset-intensive government departments will invest in predictive maintenance solutions enabled by the intersection of big data, IoT, mobile and cloud computing.

New applications can send messages and calendar tickler files when maintenance is anticipated. In the long term, this can cut maintenance costs and allow maintenance to be scheduled rather than treated as an emergency. •

— Shawn McCarthy is research director for IDC Government Insights.

SHIPPING FEBRUARY 2015

2015 FEDERAL EMPLOYEES ALMANAC

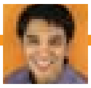


The *Almanac* is your one-stop resource on federal policy information — used annually by thousands of federal employees to reference the latest 2015 rules, regulations, and procedures.

ORDER TODAY!

Single copies start as low as $23.95
Federal Soup subscribers save an additional 10%!

FederalSoup.com/FedStore • 800-989-3363



BY CHRIS LaPOINT

It's time to restock and upgrade your disaster recovery toolkit

IT'S WINTER, and you know what that means: snow and ice storms, power outages and the need for IT emergency preparedness. It also means this is a great time to make sure your disaster toolbox is well stocked – before a major calamity strikes.

That doesn't have to come from Mother Nature, either. As a federal IT manager, you always have to be prepared for the unnatural disaster, too. While cyber attacks really ramp up in the business sector around the holidays, government agencies have to worry about them 365 days a year (and let's not forget, the 2016 presidential election – a prime time for cyber terrorism – is not that far away).

Before the weather gets worse – increasing the chances that you may experience significant system downtime – make sure you have a plan in place.

The scary thing is that even the idea of creating a disaster preparedness and response plan has been put on the back-burner at many government agencies. In fact, according to a federal IT survey by my company, Solar Winds, over 20 percent of respondents said they did not have a disaster preparedness and response plan in place.

So, before the weather gets worse – increasing the chances that you may experience significant system downtime – make sure you have a plan in place, and follow these best practices:

Continuously monitor the network. Here's a phrase to remember: "collect once, report to many." This means installing software that automatically and continuously monitors IT operations and security domains, making it easier for federal IT managers to pinpoint – or even proactively prevent – problems related to network outages and system downtime.

Continuous monitoring can give IT professionals critical data pertaining to network performance, availability and security. This information can help managers detect abnormal behavior much faster than manual processes. Abnormalities can range from rogue devices accessing the network – which could signify an impending attack – to UPS network devices shutting down as a result of a power outage. Continuous monitoring can help federal managers react to these challenges quickly and reduce the potential for extended downtime.

Monitor devices, not just the infrastructure. You can't just monitor your network and call it a day; you need to keep track of all of the devices that impact it, including desktops, laptops, smartphones and tablets. Heck, these days, even the holiday ham probably had a Wi-Fi port.

For this, consider implementing tools that can track individual devices. First, devise a whitelist of devices acceptable for network access. Then, set up automated alerts that notify you of non-whitelisted devices tapping into the network or any unusual activity. Most of the time, these alerts can be tied directly to specific users. This tactic can be especially helpful in preventing those non-weather-related threats I referred to earlier.

Plan for remote network management. There's never an opportune time for a disaster, but some occasions are just, well, disastrous. For example, when a blizzard knocks out electricity in your data center and you're stuck at home looking at two feet of snow thinking, "Yeah, right." In such cases, you'll want to make sure you have software that allows you to remotely manage and fix anything that might adversely impact your network. Select software that will allow you to safely power down systems to prevent against data loss or to ensure that systems remain online throughout the emergency.

Remote management technology typically falls into two categories: in-band and out-of-band remote management. Both get the job done for their particular circumstances. In-band allows federal IT managers to connect to a system using a primary interface, whereas out-of-band uses private connections, such as Ethernet. The former requires a primary network to be online, while the latter is used when an individual server is not operational.

Alas, there are some instances where remote management is insufficient. It's perfectly adequate when your site loses power, or your network goes offline, but in the face of a major catastrophe – massive floods caused by a hurricane, for example – you'll need onsite management. In many cases, however, remote management tools will be more than enough to get you through some rough spots without you having to get through that snow.

Each of these best practices, and the technologies associated with them, are like backup generators. You may never need to use them, but when and if you do, you'll be glad you have them at your disposal this winter – or any time of the year. •

— Chris LaPoint is vice president of product management at IT management software provider SolarWinds, based in Austin, Texas.

BY (ISC)2 GOVERNMENT ADVISORY BOARD EXECUTIVE WRITERS BUREAU

8 ways to reduce unauthorized software

ATTACKERS LOOKING to gain access to government systems and networks are constantly scanning targets for vulnerable software and initiating campaigns to trick users into downloading and executing malicious files.

Unauthorized software increases the attack surface for adversaries, because any software that is not authorized is likely unmanaged, without proper patching, updates and configurations. Moreover, IT managers with incomplete knowledge of their agency's software cannot fully secure their assets. Unfortunately, preventing and identifying unauthorized software in large government networks is often a formidable challenge.

Following are eight key guidelines and recommendations that can make tackling the issue of unauthorized software much more manageable:

1. Nip it at the source. While a robust application whitelisting capability should be the goal, a first step is to prevent unauthorized software from even entering the government environment in the first place. Agencies should have clearly defined groups or individuals who are responsible for obtaining, testing, approving, deploying and maintaining software so that end users cannot obtain software directly from external sources.

Primary sources for unauthorized software are email, web and removable media. Security teams with strong perimeter security controls can block files with extensions of known executables (.exe, .msi, .bin) along with mime types such as binary/octet-stream, application/octet-stream and application/x-msdownload via existing email and web gateway technologies (including inside compressed files). Host-based controls can similarly block known extensions and file types or block removable media entirely if not authorized in the environment.

This practice may eliminate some of the obvious targets and force attackers to give up or develop more expensive techniques.

2. Don't forget active content and browser extensions. Application whitelisting at the client level can be very effective to prevent stand-alone malicious programs from executing on the host. However, many whitelisting tools cannot effectively prevent the execution of active content or capabilities of browser extensions or add-ons.

For example, a whitelisted browser still provides a rich environment for potential attacks and execution of malicious mobile content via ActiveX controls, java and browser extensions. Active content is also often executed when simply browsing the Internet and can be installed without knowledge of the end user. Active content and extensions can be limited by enforcing local browser/client settings or blocking associated network requests for such content at perimeter security gateways.

3. Minimize administrative privileges. End users on government workstations should never be operating with administrative privileges by default and should not even have an option to elevate themselves to administrators unless required and properly audited. Without administrative privileges, users can be prevented from running software installation packages or executing other binary content requiring registry modifications or other privileged actions.

4. Use audit/monitor mode. Depending on the size of an agency, it could take months or even years to get to a complete, current and manageable whitelist of approved software. However, most application whitelisting tools offer "audit" or "monitor" modes to provide logging and visibility of what software is being executed throughout the organization. The audit/monitor mode can be used to determine which applications should and should not be permitted.

5. Draw a line in the sand. As noted above, achieving effective application whitelisting across a large agency is neither trivial nor quick. Instead, consider drawing a line in the sand with the current footprint of executable software. Essentially serving as a "temporary whitelist," this baseline can be used to ensure no additional software is permitted into the enterprise.

6. Confirm senior leadership support. Full support from senior leadership is critical to make sure efforts to address unauthorized software continue while also forcing non-compliant business unit applications and processes to take appropriate remedial actions.

7. Engage stakeholders early. Because of the potential for stopping certain business processes from functioning, it is critical to identify all stakeholders and engage them early and often. A robust communications plan will help ensure stakeholders understand and support the efforts and are not surprised by any results.

8. Prepare for emergency requests. Although the team responsible for maintaining an application whitelist should generally be engaged, resource constraints may limit this option. As an alternative, emergency firecall accounts and processes could be established to allow help desk or other personnel to provide temporary support of emergency requests if the risk to the agency is acceptable.

Following these recommendations should help agencies gain control of unauthorized software and realize the substantial benefits of an environment where malicious or unauthorized binaries are no longer able to wreak havoc. •

— Members of the (ISC)2 U.S. Government Advisory Board Executive Writers Bureau include federal IT security experts from government and industry.

NEW TECH

FOR THE AUTOMATED ENTERPRISE

As cloud deployments gained momentum across government in the last year,

agencies benefitted from increased automation designed to make it easier, cheaper and faster to spin up new IT resources and deploy cutting-edge web applications.

In 2015, those improvements will pick up speed and will include built-in cloud support for security and privacy standards, software to improve data integration between cloud applications and a push toward network virtualization.

The outlook suggests the government's move to the cloud will hit its stride in the coming year, according to analysts, who see faster adoption of enterprise services designed to give agencies more control over their applications and the costs of managing and securing them.

A case in point: Microsoft announced in December that its Azure Cloud for Government supports FedRAMP, FISMA, DOD Enterprise Cloud Service Broker, HIPAA, IRS 1075 and Criminal Justice Information Security standards.

"In the last year, public clouds have emerged that can better support compliance-driven organizations," said Bill Kleyman, national director of strategy and innovation at MTM Technologies, a Stamford, Conn.-based consultancy.

"Cloud providers are now offering solutions that support FedRAMP (and the cloud-first initiative) so agencies can utilize all of this really great infrastructure specifically built for government cloud specifications and use cases," he added.

Cloud auto-services

Microsoft and Amazon Web Services (AWS) also offer automated tools that make it easier for agencies IT administrators to create hybrid systems, where some applications can reside in government-run clouds while others run in public clouds.

Amazon's autoscaling feature, for example, makes it easy for agencies to handle peak usage in the public cloud as needed – at less cost than dedicated IT resources.

"A government organization can go to a private cloud with an application and say that when this reaches an 80 percent threshold, automatically provision 4G of RAM to support it," Kleyman said. "In the past, that application was sitting on a server, and it sent an alert to the administrator that it had just hit a threshold. Now the administrator doesn't have to sit down and do everything manually."

Improved autoscaling is due soon. Amazon is previewing a capability called AWS Lambda, which starts running milliseconds after an event such as a website click and automatically triggers compute resources.

The service is designed as a cost-effective way for a web app to scale from receiving a few requests a day to thousands per second. It could be useful when law enforcement agencies interact with citizens, such as asking for videos after the Boston Marathon bombing.

APPS DRIVE WORKLOADS TO THE CLOUD

Cloud services specialization has reached the point where agencies are migrating individual workloads to government-specific cloud offerings. Initially, agencies used cloud-based services for development/testing, disaster recovery and bursty applications like video storage. Now data analytics and web applications are migrating to the cloud too.

"More government agencies are going to be creating apps because they are the easiest way to get to their end users: the taxpayers," Kleyman said. "All those apps are going to generate more data, and those apps are going to be cloud-hosted because of resource constraints."

These developments point to a wider trend: advances in the use of specialized technologies that cater to public and private stakeholders – including IT administrators, program managers, mobile users and open data consumers – and have the power to manage the government technology agenda.

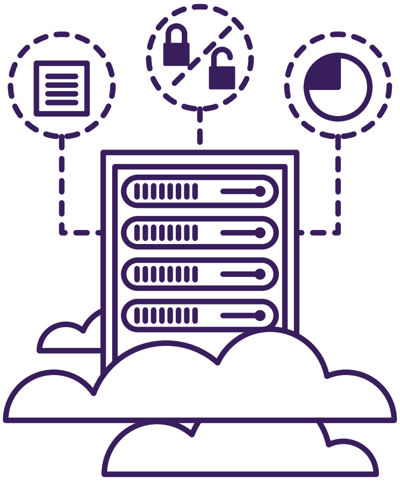
For example, the National Institutes of Health's National Database for Autism Research (NDAR) built a cloud-based collaboration platform using AWS to replace an outmoded system of mailing copies of data stored on hard disks. Researchers now access data through AWS, which automatically stands up a processing environment and provides analytic tools.

"One of the main benefits is that the NIH has more security," said Mark Ryland, chief solutions architect for AWS's worldwide public sector team. "They know who is accessing data now, and they can shut them down if they need to because some of this data is very sensitive."

The cloud-based approach also means more researchers can collaborate on the NDAR database.

"The bottom-line benefit is much faster time-to-science," Ryland said. "There will be more collaborators because it is easier for smaller and medium-sized universities to get involved. They can do this for $20 a day for infrastructure versus creating a physical- or capital-intensive infrastructure."

With cloud-based access to its data, NDAR is leading a culture change within the NIH toward increased data sharing, says Dr. Tom Insel, Director of the Na-



CLOUD & BIG DATA

HYBRID WINS. Questions about the validity of public versus private cloud computing will ease as IT departments gain experience with all forms of cloud, opening the way for hybrid computing to become the norm. (Sand Hill)

DOCKER FINDS ITS WAY. "Docker is not a fad," according to Forrester Research. "It marks a new approach that delivers real benefits." The technology, which automates the deployment of applications inside of software containers and avoids the overhead of virtual machines, has been accepted by big commercial players and is "here to stay." (Forrester)

CLOUD DRIVES COLLABORATION. Facilitated by cloud and big data applications, half of all governments by 2017 will invest in collaborative systems for collective knowledge initiatives. (IDC)

tional Institute of Mental Health.

"Virtually all autism human subjects research data is expected to be deposited in the National Database for Autism Research, which now holds genomic sequences, brain images and clinical data from over 77,000 subjects," Insel said in a recent blog post. "This data provides a platform for discovery through secondary analysis and data sharing specific to a publication."

NEXT: APPLICATION LEVEL INTELLIGENCE

In addition to government-specific cloud offerings from Microsoft and AWS, today's market is packed with cloud management platforms from CSC, RightScale, Cisco, IBM, VMware and others. These tools add an orchestration layer that allows agencies to manage the cost and uses of cloud-based IT assets.

The return on these tools is improved efficiency, said David Linthicum, senior vice president of Cloud Technology Partners, a Boston consultancy. "You have an orchestration or automation layer managing these assets versus a person sitting down at a console spinning up cloud or non-cloud resources," he explained.

Agencies have been using these tools to automate the provisioning of compute, storage and networking, including firewalls and load balancers. But the deployment of application-level intelligence is on the horizon for 2015, Linthicum said. "The first step is provisioning and deprovisioning. Next is adding application-level intelligence into the process," he said.

"Imagine each application is a little silo that does specific things with a static process and data bound to it. A CRM app like Salesforce, a battlefield management app and an HR system are all silos. But what if the apps had the ability to leverage each other's processes, behavior and data? Building a meta app like that is possible with some of the orchestration systems."

Bill Rowan, vice president of federal at VMware Public Sector, said the biggest boon for agencies with these tools is in the automation of network provisioning. Previously, organizations hard-wired compute and storage resources to a particular application through a patch panel. Now these configurations can be changed on the fly through network virtualization.

"The biggest bang in terms of changing the way agencies operate is automating the network process – where the people and process time is spent is on the network," Rowan said. "A year from now, I think we will be surprised at how many customers … have moved to the automation of network provisioning."

– Carolyn Duffy Marsan

How will you manage big (and bigger) data in 2015?

Once agencies determine their requirements for enterprise computing and storage of high-value data sets, they will have to grapple with how to satisfy the appetites of different agency constituencies for data, both open and proprietary.

As the stream of data hitting government agencies grows, the importance of managing it is expanding as well, according to government executives. And it is not just the volume of data that's growing. The variety of data sources are proliferating as video and sensor data from the Internet of Things makes its way into the government data centers and enterprise networks.

"Open data is a nice thing, but most open data is not consumable by people who are not technical or do not have a

GCN

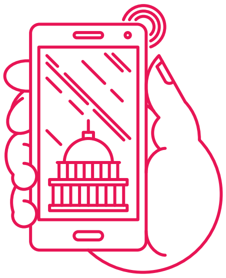
Technology,
Tools and Tactics
for Public Sector IT

Where you need us most.

GCN
Technology, Tools and Tactics for Public Sector IT
GCN Newsletter
Sign up for our newsletter.
Email Address
SECURITY
Agencies must update to newer versions of Transport Layer Security
Build a more robust
DENIAL-OF-SERVICE
DEFENSE

Mobile Tablet Desktop Print

technical infrastructure at their beck and call," said Keith Donley, enterprise data manager at the Virginia Department of Transportation. To meet the needs of this class of users, government IT departments will increasingly turn to data warehouse augmentation tools and tactics in 2015 to help manage their big data challenges.



MOBILE

MOBILE FIRST. Mobile devices become the primary go-to device for all content consumption, with more than 50 percent of users moving to tablet or smartphone first for all online activities. (Gartner)

CABLING OUT, WI-FI IN. By 2018, 40 percent of enterprises will specify Wi-Fi as default connection for nonmobile devices, such as desktops, desk phones, projectors and conference rooms. (Gartner)

RUGGED MOBILE. 2015 is the year mobile computer makers will embrace Android as the operating system of choice for rugged mobile computers. Strong demand emerges for 'maximum screen real estate in the lightest possible form factor. (Hellstrom, Handheld Inc.)

GOVERNMENT END USERS. By 2020, 40 percent of government employees will use multiple form factors on a daily basis, including smartphones, tablets, notebooks/hybrid devices and wearables. (IDC)

SANDBOXES FOR EXPERIMENTATION

A key technique for handling the data surge is to provide a staging area, or sandbox, in which organizations can explore new datasets before deciding whether to add them to a data warehouse.

VDOT uses business analytics software from Tableau Software Inc. to augment the agency's enterprise data warehouse. Tableau provides a sandbox in which VDOT can combine sample data with existing data in the warehouse. This mixing of data from different sources, a process called data blending, lets VDOT determine whether the sample data is valuable enough to warrant adding to its data warehouse, Donley said.

Bill Franks, chief analytics officer of Teradata Corp., said the need to make data available for experimentation is a key force behind the data warehouse augmentation trend. For one thing, data warehouses are typically used for data that is well understood. But the value of the voluminous data generated via temperature and humidity sensors, for example, may not be immediately known.

"There is simply so much more data available, and a lot of that data is of unknown use and quality at the time it may be collected," said Franks.

Another way to augment a data warehouse is to offload the processing of big data to another technology platform such as a Hadoop cluster. However, Taha Kass-Hout, chief health informatics officer at the Food and Drug Administration, suggested that Hadoop may not fit every application.

"As FDA acquires big data in the cloud, appropriate technologies will be deployed," Kass-Hout said. "Hadoop is just one technology option and may not necessarily be appropriate for the particular data or data use."

INCREASING DATA AVAILABILITY

After settling on an approach for data storage, agencies must confront how to make the data available to both internal and public business users.

Traditionally, business users would need to ask the IT shop to generate a report if they wanted to tap a data warehouse. But agencies will be making more data accessible in the cloud, a move that is already underway.

One example is openFDA, which operates in a public cloud environment. The project, which debuted in June 2014, aims to "create easy access to public data," according to the openFDA website. Kass-Hout said openFDA uses new technologies such as Elasticsearch, Luigi, Node.js and the JavaScript Object Notation open standard to manage the data demand.

Those technologies result, "in very fast response times, even when there are very many simultaneous users," according to Kass-Hout, adding that FDA was considering applying these technologies to internal FDA databases next year, "whether or not they are in the cloud."

VDOT, meanwhile, uses Tableau Public, a data visualization software tool, to make data available to both internal personnel and the public. The tool hosts an organization's dashboards, tables, graphs and other visualizations in the cloud.

VDOT's Traffic Engineering division, for instance, uses Tableau Public to publish data on traffic accidents in the state, Donley said. Users can apply a range of filters to analyze the data, including location, year, crash severity and weather conditions.

– John Moore

2015 mobility mantra: manage data instead of devices

The arrival of business intelligence on mobile platforms could also contribute to making data more accessible – and more valuable – to users in the new year. Products are available from vendors such as MicroStrategy, which offers mobile business intelligence products including its Analytics App for iPad. In another example, startup Databox in November unveiled its Databox for Enterprise, a mobile business intelligence platform that the company said is designed for decision makers rather than data mavens.

At FDA and throughout government, agency mobility managers are racing to provide analytics, security and other data-focused features that the devices themselves don't deliver.

That's why 2015 will be when agencies to strengthen their mobility management practices with enterprise approaches that focus on managing data and applications rather than devices themselves, mobile experts say.

"It's harder than people thought it would be," said Bryan Taylor, research director for mobile and wireless at the Gartner consulting group. "Mobility evolves much quicker than your typical enterprise area of technology."

While mobile device management (MDM) platforms have been widely adopted in the private sector, their uptake in the federal arena has been slower. In fact, many agencies are just beginning to set up MDM, even as commercial organizations are moving into more robust solutions like enterprise mobility management (EMM).

PILLARS OF A NEW MDM

MDM platforms typically allow administrators to remotely configure security and applications on mobile devices, to "kill" devices when they are lost or stolen and to manage operating system updates and applications. MDM platforms are also designed to support mobile devices from multiple manufacturers, enabling employees to use their own devices, or BYOD.

NASA is one agency planning to enhance its mobility strategies in the coming year. The space agency – one of the federal government's most tech savvy – has until now been relying on Microsoft Exchange ActiveSync to manage its fleet of 30,000 laptops and 10,000 cellphones.

Exchange ActiveSync was originally designed to synchronize data on mobile devices, including email and calendaring data. In recent years it has added MDM features, such as the ability to set policies on device and applications usage.

However, the solution lacks more sophisticated capabilities such as application containerization and app wrapping that protects and isolates applications on devices, especially important when employees are using their own devices.

"We are looking at a mobile device management solution to implement right now," said John Sprague, NASA's enterprise applications service executive. "We've got lots of scientists, engineers, researchers, employees and university partners, all wanting to use their personal mobile devices because they are so familiar with them and comfortable with them."

While many federal agencies and departments are just moving to adopt MDM, however, Gartner's Taylor said the shortcomings of the technology as a security solution are already apparent.

"It used to be good enough to put some security controls on the device itself, which is what mobile device management focuses on," said Taylor. "But as applications and content increasingly become important for organizations deploying mobile, they need more. They need mobile application management and mobile content management. If you take those pillars you end up with EMM – enterprise mobility management."

In addition to managing the configuration of mobile devices, as MDM does, EMM focuses on managing applications and data on devices across the enterprise.

SECURING APPS, NOT JUST DEVICES

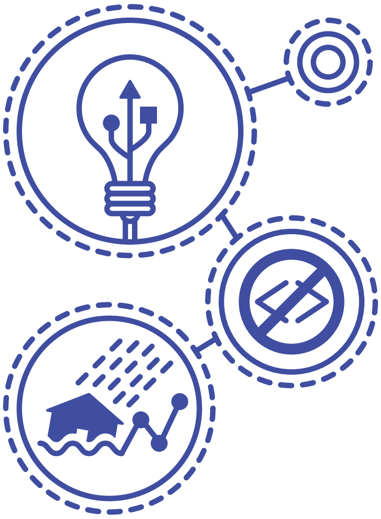
App containerization is a primary tool in that effort, according to government security experts. Isolating and protecting sensitive applications so their data is not accessible from other applications on the device means that administrators

EMERGING TECH

INTERNET OF THINGS. By 2018, local government will drive over 25 percent of government spend to deploy and realize the business value from Internet of Things. (IDC)

PREDICTIVE TECHNOLOGIES. Natural hazards will drive 20 percent of governments involved in emergency response to invest in predictive IT solutions to prevent, manage and mitigate damages. (IDC)

RISE OF DEVOPS. By 2015, 60 percent of CIOs will use DevOps as their primary tool to address speed and sprawl of mobile, cloud and open source applications.(IDC)



GOING CODELESS. The use of codeless tools for rapid development of projects by IT and enterprise business analysts will become an alternative to outsourcing, limiting the use of development partners to more advanced projects. (IDC)

CYBERSECURITY

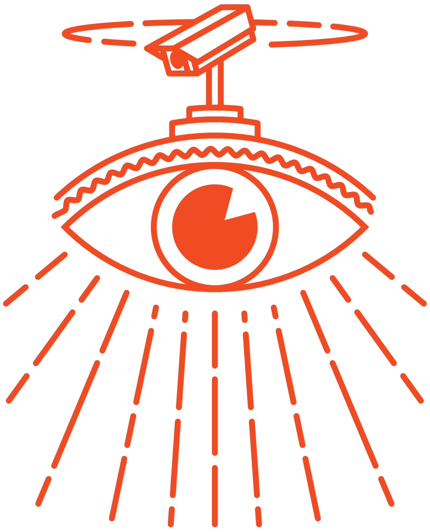
UBER MONITORING: Agencies will adopt some form of continuous monitoring, including threat and identity scanning. (Coalfire)

NEW DETECTION TECH: Crowdsourcing, machine intelligence and advanced analytics emerge as new threat detection tools. (Coalfire)

SHIFT TO OFFENSE: A transition toward offensive tactics, including systems to identify and delay attackers, gathers steam. (Coalfire)

SECURITY TALENT GAP: Rising demand for cybersecurity skill sets means government-commercial partnerships need to be part of the talent mix. (NASCIO-Deloitte)

COMPLIANCE AS A SERVICE: As complexity of cyber threats rise, CISOs will need to respond with more regulation and devote more resources to compliance requirements. (NASCIO-Deloitte)



BUILD AS YOU GO: Greater data center consolidation and cloud projects will provide CISOs creative opportunities for building security into the government enterprise. (NASCIO-Deloitte)

don't have to be as concerned about other applications on an employee's device or just how that device is configured.

"Most organizations these days, both public and private, have gotten away from trying to blacklist or whitelist what you can put on the device," said Taylor. "That's largely because containerization has led them to feel that they can allow more latitude for personally enabling a device while still keeping the apps and content that they are interested in secure."

Fairfax County, Va., which has been using an MDM platform to manage its fleet of mobile devices for some time, is now taking its first steps toward an EMM approach to BYOD. Initially, said Jeffrey Porter, director of the county's Platform Technology Division, support will be limited to iOS and Android devices, to be followed in a few months by support for Windows Phones.

"Now that we're starting to let people touch applications," said Porter, "it presents a problem for us about who we allow to touch what information. We want to make sure we are restrictive." Porter plans to use containerization to help ensure the security of those applications.

LEGACY APPS MANAGEMENT

For many IT managers deploying apps to mobile devices carries special challenges, since many agencies are sill running older legacy apps designed to run on mainframes. These in-place applications are too resource intensive to run on mobile devices.

That, said Michael Valivullah, chief technology officer at the National Agricultural Statistics Service, is the case with some of the applications at the Department of Agriculture. "Based on user needs, we are rewriting those applications," he said, in part to make the applications more appropriate for mobile use.

Data center consolidation is also driving demand for an application-focused approach to device management, according to Valivullah. "We have decreased our data centers from 46 to two, and with the data center consolidation, we have longer distances to go between client devices and the data center," he explained. The result is delays and, eventually, user complaints.

"So we are having to optimize those applications to decrease the I/O," he said. "We're implementing caching so apps don't have to go all the way to the database for every operation."

FOCUS ON THE DATA

Moving forward, said Valivullah, his team will focus more on the data than anything else. "Our mobile strategy is based on the data instead of focusing on devices," said Valivullah. "Our concept is to access anything, anywhere from any technology at any time."

And to protect the data, apps on USDA's mobile devices are configured so that the data is never stored on the device.

"We rolled out a virtual desktop interface that can run on pretty much any device," said Valivullah. All the apps run through the interface, and all the data is stored on USDA's servers or in its cloud storage. "Nothing is resident on the computer," said Valivullah. "We just give them bare-bones devices and they can't save data on it. Even for the couple of minutes that data might be there it is encrypted. We don't see a lot of risk there."

Gartner's Taylor confirms that more government agencies are turning to the cloud for securing mobile data as part of their mobile device repertoire.

"We are seeing a lot more interest in

Visual Studio® LIVE!

EXPERT SOLUTIONS FOR .NET DEVELOPERS

vslive.com/lasvegas

Las Vegas MARCH 16 – 20

BALLY'S HOTEL & CASINO LAS VEGAS, NV

LAS VEGAS

Code Trip

NAVIGATE THE .NET HIGHWAY

Code on the Strip

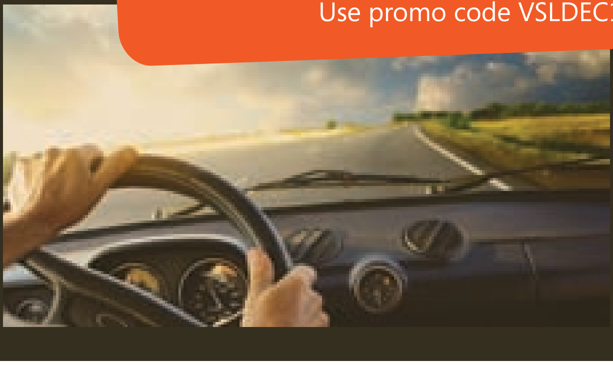
Visual Studio Live!'s first stop on its 2015 Code Trip is Las Vegas, situated fittingly near Historic Route 66. Developers, software architects, engineers, and designers will cruise onto the Strip for five days of unbiased and cutting-edge education on the Microsoft Platform. Navigate the .NET Highway with industry experts and Microsoft insiders in 60+ sessions and fun networking events – all designed to make you better at your job.

TRACKS INCLUDE:

- Visual Studio / .NET
- JavaScript/HTML5
- ASP.NET
- Cross-Platform Mobile Development
- Windows 8.1/WinRT
- Database and Analytics
- Cloud Computing
- Windows Phone

Register NOW and Save $500!

Use promo code VSLDEC1



Scan the QR code to register or for more event details.

SUPPORTED BY

Microsoft Visual Studio msdn magazine Visual Studio MAGAZINE

PRODUCED BY

1105 MEDIA INC

vslive.com/lasvegas

cloud deployments, letting the ISP do the work in maintenance and updates," he said. "And lot of organizations that first went with purchase of on-premise [apps and data] have switched to cloud."

– Patrick Marshall

In 2015, a blending of IT security and operations

Of course, the essential requirement for delivering new cloud, big data and mobile data services will be tougher security technologies and practices. In 2015, two powerful trends will shape the government cybersecurity agenda, say security experts.

First, cybersecurity will increasingly be baked into platforms and software being acquired and developed by agencies. This means that perimeter defenses – already abandoned to the realm of what is necessary but inadequate – will receive less attention as cybersecurity becomes more integrated into the government infrastructure.

Second, cybersecurity will no longer be considered the exclusive domain of the CISO or the CSO. Instead, it will become a professional requirement for everyone responsible for IT services to the agency. "As a security vendor, we are ending up in conversations with the IT shop," rather than just the security shop, said Ken Ammon, chief strategy officer for Xceedium, an identity management company. "Next year will be the year of convergence."

That outlook is backed up by a report by the National Association of State Chief Information Officers and consulting firm Deloitte that found as CISO responsibilities evolve to include risk and compliance, many CISOs are also becoming accountable to a range of other areas. "CIOs and state leaders need to consider creative ways of allocating and managing these expanding responsibilities," said NACIO.

The upshot: The new year will see an increased blending of security and operations in IT.

Meanwhile, the threats facing agencies are becoming more complex and serious, continuing a multiyear trend toward stealthy, long-term attacks that are discovered only long after the damage has been done. The average time to discover a breach is now about 250 days, and most are discovered by a third party rather than by the victim, said Rob Roy, federal CTO for HP Enterprise Security Products.

As these breaches are discovered, it is becoming clear that the human factor in security requires more attention to threats such as spearphishing and other forms of social engineering, which now are common vectors for malware.

This problem is highlighted by the most recent Federal Employee Viewpoint Survey, which shows growing disengagement and dissatisfaction among government employees. The global satisfaction index was flat at a disappointing 59 percent for 2013, and IT specialists scored lowest on employee engagement and satisfaction.

"It shouldn't be a surprise when you see survey results like this," Paul Christman, public sector vice president at Dell Software, said of the growing role of humans in IT breaches. Cybersecurity requires a holistic approach that includes cost-effective training both for IT specialists and for end users.

CLOUD SECURITY

The government's security travails will also have an impact on demand for new tools and agency IT acquisition decisions.

While the adoption of cloud computing will continue to expand in 2015, the benefits of the hybrid cloud model – a combination of secure private cloud for sensitive data and critical functions and a more flexible and economical public cloud for citizen-facing information – could be more attractive as administrators balance flexibility with security.

According to a pair of recent reports on cloud computing, improved security is a primary reason for moving to the cloud, with nearly two thirds of government respondents in a survey commissioned by General Dynamics Information Technology citing secure infrastructure as a top benefit. At a same time, a study by SafeNet found that IT security professionals feel they are losing control of data in the cloud.

These apparently conflicting results show that securing the cloud is possible and practical, but that greater emphasis is needed on governance and establishing policies for using and managing cloud computing. "There is no doubt" that use of everything the cloud has to offer will continue to expand, said SafeNet CSO Tsion Gonen. "That is not surprising."

However, to enable this continued uptake, cloud providers will develop better solutions for separated cloud functions, allowing better segregation of the management of infrastructure and control of data. This will include a separate layer of cryptography managed exclusively by the cloud user to give more complete custody of data. "All cloud providers have or will offer this," Gonen said.

And while some experts see hybrid cloud solutions as a way to provide the necessary level of control necessary to secure these more sophisticated functions, not everyone agrees.

"You hear a lot about hybrid cloud," said Damian Whitham, senior director of cloud computing solutions and General Dynamics IT. But so far there has been little practical implementation of it. Government has focused primarily on the private cloud, with some public cloud use, with only 27 percent of agencies using a hybrid model. "They are trying to crack the code of implementing it," Whitham said.

With much of the low-hanging fruit of cloud computing now gathered, agencies will be paying more attention to how to match business objectives with cloud offerings to achieve their goals of reducing IT costs, becoming more flexible and efficient, reducing their carbon footprints and ensuring the security and privacy of data.

"We need to get more stakeholders involved," Whitham said. "Including the operational side, not just IT."

– William Jackson

Real-time data modeling on your dashboard

Tableau's intelligence tools enable "what if" data visualizations and allow users to share analytics in a collaborative environment

BY BRIAN ROBINSON

Visualization has long been considered a prime tool for data analysis. But as data sets grow bigger and deeper and data management challenges mount, the need to make complex information more accessible is becoming paramount for government decision makers.

However, while current technologies such as Hadoop provide increasingly better ways to store and process data, methods for quickly turning that data into meaningful visual presentations have lagged.

Tableau Software's interactive data visualization products offer an example of the next generation of tools that will allow just about anyone, across a broad range of skill levels, to produce those visualizations. Tableau also takes that further by allowing near-real-time "what if" modeling and letting users share their analyses in a collaborative environment.

THE BOSTON PILOT

The City of Boston, for example, is using Tableau in a pilot program in the mayor's office to set up dashboards for various departments in the city. If it works as envisioned, the mayor will be able to walk into a control center that contains screens showing the dashboards and not only get an idea of what's happening in those departments at any given time, but also ask questions about particular indicators on the dashboards and get answers while standing in front of the screens.

The Department of Interior now uses Tableau to improve its financial analysis, and specifically to find where it is spending its money and root out any discrepancies. The department also has a scorecard that includes "aging reports" that show transactions and payments over a period of time, according to Doug Glenn, deputy chief financial officer and director of the DOI's Office of Financial Management, who added that Tableau helps to raise red flags about transactions that are getting old, "and can tell the who, when and why of those transactions."

"For example, we had an accounts receivable problem where we saw the balance over a 180 day period was going up and we didn't know why," he said. "When we dived into it with Tableau we quickly saw the problem was with Fish and Wild-

"The days of communicating with static spreadsheets or printed statements in reports are over."

– DOUG GLENN, DEPUTY CHIEF FINANCIAL OFFICER AND DIRECTOR OF THE DOI'S OFFICE OF FINANCIAL MANAGEMENT life Services, and that when we talked with them found it was due to Deepwater Horizon and British Petroleum."

After the Deepwater Horizon drilling platform exploded and burned in the Gulf of Mexico in April 2010, eventually leaking nearly 5 million barrels of oil from a ruptured well head, owner British Petroleum agreed to pay billions of dollars to people who claimed they had been damaged by the spill. The Fish and Wildlife oversees that part of the program involved with natural resource damage assessments and reparations.

DEEPWATER HORIZON CASE

However, British Petroleum was holding up some payments out of concern that various agencies were putting questionable costs into reimbursement requests. Once the problem was highlighted with a Tableau analysis, BP got agreement for the requests to be validated before they paid.

While acknowledging that dashboards and visualization tools have been used in the government space for some years, Christine Carmichael, head of marketing, government and education for Tableau Software nonetheless claims Tableau goes further in terms of the intuitive interplay users have with the data.

"If you go back to the Boston example, think of the city having just experienced a nor'easter and now has 196 potholes that need fixing," she said.

"A year ago the mayor would have known he had 196 potholes, but then would have had to go to IT to get to the next level of where they were and how bad, and it could have taken days or weeks to get a response. With Tableau, the mayor can ask questions like that and get a response in real time."

Teri Caswell, a senior associate with Hassett Willis & Company, works with government agencies to help them understand how operational, financial and performance data can influence decision-making. She's currently working with first responder organizations such as the Federal Emergency Management Agency in a proof of concept program to see how rapid analysis of data can help it determine how things are progressing at disaster sites.

There are lots of tools that can do great visualizations and paint great pictures, she said, but there are few that can produce different visualizations with different data as quickly as Tableau can. She said it also allows her to work more closely even with clients who still prefer traditional methods of presenting data, such as spreadsheets and matrixes or text-based reports with visuals inserted in them.

With them, the "pretty Tableau pictures" are a bit of a hook that at least makes clients inclined to look at the visualizations, she admitted, but the real advantage is the ability it gives her to respond quickly and confidently to the iterative questions people ask her.

"Tableau means that, when I give a report and that next question is asked, instead of the usual 'Let me get back to you with that' I can immediately change a parameter or identify something that changes the visualization or numbers on the matrix," she said. "At the least, I can tell them they don't have the data to get the answer, and point them to what data they need."

However, according to DOI's Glenn, the days of traditional methods of analysis and reporting are coming to an end.

"The days of communicating with static spreadsheets or printed statements in reports are over," he said.

"The next phase is where we are dealing with large databases that might contain the answer, and the ability to drill down and sort, sift, analyze and manipulate data that exposes the answer no matter what the question is, is definitely the next step." •

Legs of the tableau

Tableau Software, the company behind the data visualization application, includes four separate products that together form a complete visualization platform.

- Tableau Desktop enables users to interact with Tableau to build their analyses.
- Tableau Server allows users to share and collaborate with the Tableau documents they've created.
- Tableau Online is the cloud hosted version.
- Tableau Public is a free product that lets anyone who has downloaded the desktop environment to publish their data vizualizations to the web.

The last feature is what Christine Carmichael, head of marketing, government and education for Tableau Software, tagged as "the YouTube of data."

The products are based on two technologies developed by the company VizQL, which translates drag and drop actions users perform onscreen into database queries and then converts the response graphically, and a data engine that enables rapid, ad hoc analysis of large volumes data.

Tableau also has over 40 different connectors for most of the data repositories seen in the government and private sectors and integrates with existing systems and security architectures.

ADVERTISER INDEX

Carpathia Hosting, Inc.
www.carpathia.com/Learn/Vmware-Vcloud 1a-1b

Fujitsu Computer Products of America, Inc.
www.ez.com/gcnews 35

GEICO
www.geico.com 9

Federal Employees Almanac 2015
www.FederalSoup.com/FedStore 19

IBM Corporation
www.ibm.com/mission 2

Samsung Electronics America
www.samsung.com/us/enterprise 13

Shure Inc.
www.shure.com/conferencing 5

Verizon Wireless
www.verizonenterprise.com/mobileworkforcemgr. 36

VMWARE Inc.
www.vmware.com/vmwarestory 10a-10d

Visual Studios Live
www.vslive.com/lasvegas 29

This index is provided as an additional service. The publisher does not assume any liability for errors or omissions.

MEDIA CONSULTANTS

Mary Martin
(703) 222-2977
mmartin@1105media.com

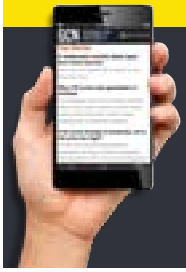
Bill Cooper
(650) 961-1760
bcooper@1105media.com

Matt Lally
(973) 600-2749
mlally@1105media.com

Ted Chase
(703) 876-5019
tchase@1105media.com

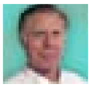
PRODUCTION COORDINATOR

Lee Alexander
(818) 814-5275
lalexander@1105media.com



PUBLIC SECTOR MEDIA GROUP

CORPORATE HEADQUARTERS
9201 Oakdale Ave., Suite 101
Chatsworth, CA 91311
www.1105media.com



EMERGING TECH

BY PATRICK MARSHALL

3D modeling helps preserve Pearl Harbor relics

LAST MONTH MARKED 73 years since Japanese dive bombers launched a surprise attack on Pearl Harbor, sinking four U.S. battleships and damaging a dozen other vessels. Three of the four battleships were later raised and returned to service.

The U.S.S. Arizona was too badly damaged to be salvaged and, in 1962, was designated a national shrine. Lately, the U.S. National Park Service, which manages the underwater site, has become concerned about the effects of 70-plus years of salt water on the structure.

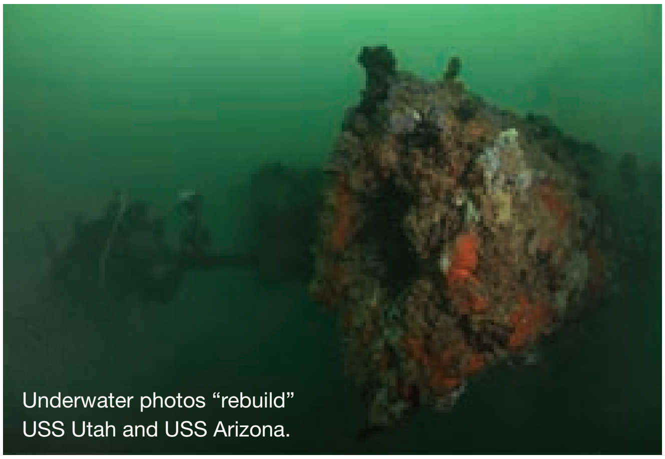
The Park Service's immediate need is to find out what's going on down there, said Pete Kelsey, a strategic projects executive at Autodesk. "It's a steel battleship, mostly under salt water for over for 70 years – you can bet it's not the same ship it was even five years ago."

Kelsey is overseeing a team that is scanning the site above and below water using three 3D technologies, including LiDAR, SONAR and photogrammetry. While LiDAR and SONAR have been in wide use for some time, photogrammetry – the analysis of photographs to create 3D models – is new.

"This is one of the first times that multiple different 3D capture technologies above and below the surface have been used together," said team member Shaan Hurley, a technologist at Autodesk. "Each one has its own unique strengths and weaknesses."

The team is using Autodesk's Recap software for the photogrammetry analysis, which enables 3D models to be rendered from multiple photographs of an object taken from different perspectives.

"We take a series of photos around an object, and the program calculates the camera's position in space by looking at unique little identifiers on the object surface," Hurley said.



Underwater photos "rebuild" USS Utah and USS Arizona.

Having precisely located the images relative to each other, the program uses that information to render the object in three dimensions. "You end up with a textured 3D representation of the object," Hurley said. That representation can either be viewed on a monitor or printed with a 3D printer.

While the principle behind photogrammetry is relatively simple, the computing power it requires is not. "The algorithms require an amazing amount of calculating," Hurley said. As a result, the team chose to implement it as a cloud service using powerful servers and graphics processors on the back end. "The computing power it requires is beyond most laptop or desktop computers," Hurley noted.

Hurley concedes that photogrammetry doesn't offer quite the resolution that LiDAR does. But it offers other advantages.

"The beauty of photogrammetry is you don't have to have a $50,000 laser scanner," he said. "Recently I spoke to a couple of hundred archaeologists and I asked, 'How many of you have a laser scanner here?' One person raised his hand. I asked, 'How many have access to a camera of some sort?' And every hand went up. I've done some of the most amazing models just using my iPhone."

The technology has already been deployed for other purposes. Hurley said he recently learned that the federal Bureau of Land Management was interested in being able to capture Indian ruins in the backcountry.

"It's hard to convey the space, the shape, the size in a photograph," Hurley said. With photogrammetry, he said, "any of those BLM agents in the field can just take a series of, say, 12 photos." Port those photos into Autodesk Recap, and 3D records of the objects can be generated.

Hurley has also used the technology to create 3D models of coral beds in Molokai, an island in the Hawaiian archipelago. "Up until now marine biologists have done it in 2D," Hurley said. "But coral grows in unpredicted patterns, and things happen over time and it's really tough to figure out how it's changed."

"With this they are able to capture beautiful 3D models of coral and at a later day go back and capture the coral again and with superlative accuracy be able to say it is changed so many millimeters in volume. That has caused a lot of excitement among marine biologists."

While the main interest of the Park Service in scanning the Arizona may be change detection, the Autodesk team realized there are other opportunities as well.

"Almost immediately, we knew that a three-dimensional model would provide all kinds of value," Kelsey said, who added that the team is working on developing a model than can be used for virtual tourism of the site. He expects that model to be ready some time in 2015. •

shaping tomorrow with you
FUJITSU
Clear your desk faster