FEDERAL NEWS NETWORK

INDUSTRY INSIGHTS

IT INNOVATION INSIDER

INSIDE THIS ISSUE:

BROUGHT TO YOU BY:

NUTANIX

FREEDOM
TO
Cloud

TABLE OF CONTENTS

Over the last year, we had some terrific guests and addressed many topics and questions on our show, the *IT Innovation Insider,* with Federal News Network. The inspiration for this project came directly from the challenges and successes we see our federal customers face every day. To name a few:

Cloud computing is proliferating, but the transition and operational state are a lot more complex than anticipated. IT budgeting and procurement guidelines have fostered environments in most agencies where many different clouds – brands, architectures, etc., are being used; the earliest and strongest cloud adopters have found that the best deal for government is not all-in public or private cloud, but a hybrid mix of the two, tightly managed to optimize service levels and cost; and two major cloud selling points are being re-evaluated: Cost savings and whether being in the cloud means that you are really out of the IT business.

Lock-in is real. One of the most memorable moments on the *IT Innovation Insider* was during episode 6, when Nutanix CEO Dheeraj Pandey noted that the phrases 'multi-billion dollar, multi-year contract' were the antithesis of anything that cloud was intended to do. Committing to restrictive multi-year contracts – which look very much like the legacy contracts of old – is relegating federal customers to passenger status on a bus that's being driven by vendors. That equation is out of sequence, yet we see it daily.

IoT and machine learning are becoming much more than the latest buzzwords, but we are still a ways off from being able to harness the power of those capabilities effectively. Although everyone has been talking about big data for a while, it's re-emerging as a critical topic in terms of where it lives, how it's stored and accessed, how to make it actionable in real-time, and more.

IT consumption models are emerging as agencies seek to reduce their role in buying, operating, and managing IT. More than two decades after Y2K, federal IT leaders are not leaving any options off the table, in terms of how to reduce the footprint of administrative/operational IT, and focus more on true mission-oriented IT. Managed services, shared services, subscription-based purchasing, private/public/hybrid cloud, and more are being evaluated.

We thoroughly enjoyed delving into these topics, and sharing our own thoughts and observations on them, and especially those of our guests. I hope you were able to tune in with us over the last year, and if you didn't, this e-book provides a great synopsis of those conversations. Enjoy the read!

Chris Howard
Vice President of Public Sector, Nutanix

Hybrid cloud means understanding predictable, unpredictable apps

BY JASON MILLER

Over the last seven years, two kinds of agencies emerged when it came to cloud computing—the early adopters and the uphill accelerators.

The early adopters were the ones who hoped for savings from moving to the cloud and moved things like email or collaboration to these off-premise service providers.

The uphill accelerators are those who started slowly, unsure of the security of cloud and if the buzz around savings was more than marketing speak, but over time have hastened their move to the cloud.

Chris Howard, the vice president of public sector for Nutanix, said new data shows those federal IT customers in that early adopter group started to pull back from putting everything in the cloud.

The data also showed the uphill accelerators now, seven years after the cloud first mandate from the Office of Management and Budget, are more forward-leaning when it comes to putting data and applications in the cloud.

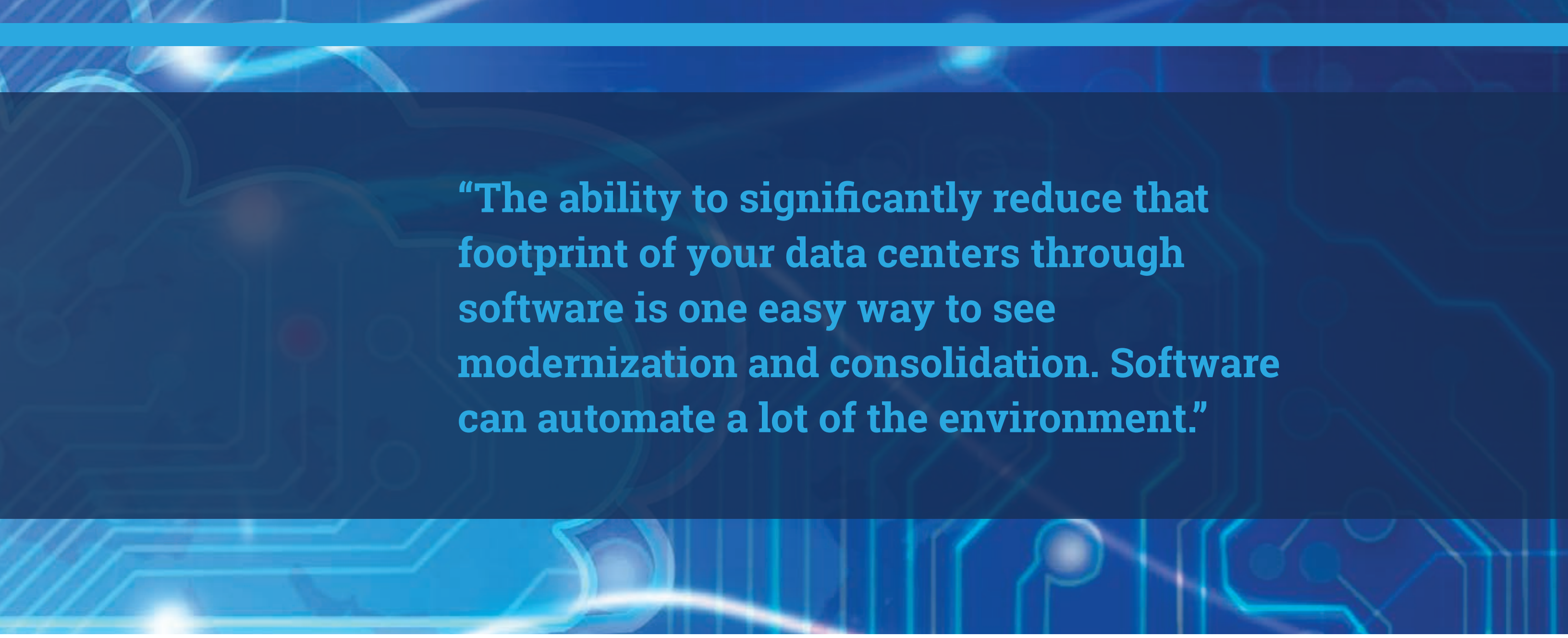
“They are taking a different approach to the early adopters than we’ve seen before,” Howard said on the IT Innovation Insider, sponsored by Nutanix.

As for the early adopters pulling back, Howard said it’s now about understanding what systems or applications are cloud-ready.

“Based on the study, I don’t think you are seeing a wholesale pull back, but when people first got into the cloud, they tried to put everything into the cloud,” he said. “The way we look at the cloud is 25% of your applications are unpredictable or elastic enough to where it makes 100% sense to put them into the cloud. It could be a 30-day big data job or some end of month financial run. It doesn’t make any sense to buy infrastructure and run it. It makes more sense to put it into the cloud, use that cloud for that 30 days or 15 days that you need it, and then pull back that data. Where we see the benefit to the on-premise and where people may be pulling back is when they put predictable workloads in the cloud, workloads where you know what you are getting and you are running full-time for three or five years.”

Howard said if those predictable workloads are done in the agency’s data center or in the agency’s private cloud, and done efficiently, then those activities will cost less or at least be equal in cost, and maybe more secure and have better governance.

“… if those predictable workloads are done in the agency’s data center or in the agency’s private cloud, and done efficiently, then those activities will cost less or at least be equal in cost, and maybe more secure and have better governance…”



“The ability to significantly reduce that footprint of your data centers through software is one easy way to see modernization and consolidation. Software can automate a lot of the environment.”

All of this movement around cloud is leading agencies to manage a dual environment with on-premise and off-premise cloud instances.

The General Services Administration says in its ***2017 Hybrid Cloud Almanac*** that a recent Gartner survey of federal IT managers found 75% indicated plans to implement a hybrid cloud solution by the end of 2017. The biggest challenges to managing a hybrid cloud include a lack of resources and the expertise in the workforce. GSA says agencies should consider several factors as they implement hybrid cloud, including integration of different clouds using application programming interfaces (APIs), cloud management and orchestration frameworks, and the organizational impact of hybrid cloud, which is another way to say agencies need to have the right people resources because hybrid cloud is not a typical IT project.

“Any customer out there wants choice and they don’t want to be reliant on one specific technology. It’s the same with cloud. They want to be able to put data into all the big cloud providers out there,” Howard said. “The challenge with that is now you have siloes of cloud. So that’s where multi-cloud management is really coming into play. It’s a hard problem to solve.”

He said the federal data center consolidation and optimization effort as well as the initiatives around IT modernization all area leading the agencies to managing their assorted clouds in a new way.

Howard said two other related trends Nutanix is seeing from its agency customers: The adoption of a software-driven IT environment, which is leading to using automation to move away from “low-value” work; and the impact of the Internet of Things devices to give agencies new insights into both data and applications.

“The ability to significantly reduce that footprint of your data centers through software is one easy way to see modernization and consolidation,” he said. “Software can automate a lot of the environment. The automation is good because it requires less human interaction and therefore your people are modernizing themselves. They are no longer worried so much about the infrastructure and the hardware piece and they are focusing more on the application, the service level agreements to the customers and uptime for the agency.”

Howard said these and other trends are leading the way for agencies to get off legacy systems and provide better services.

“A lot of agencies are at the point where they know they have to make a change and just need to know they can manage all of this change through a single management plane,” he said. “Everyone wants to get rid of siloes. The agencies who are willing to take a leap, even just for a workload or a certain use case, will see the benefits and will expand more quickly into the software world.”

How to free agencies from vendor lock-in with the cloud

BY JASON MILLER

The move to the cloud was supposed to end many of the age-old concerns with on-premise data centers. Changing hardware, updating software and, maybe most importantly, ensuring agencies didn't get caught in the dreaded "vendor lock-in" were part of the great promise of the cloud.

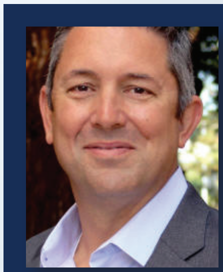
While the first two concerns seem to be taken care of, the threat of agencies becoming beholden to one cloud vendor remains a real challenge.

"We see this concept of vendor lock-in in requests for proposals with restrictive language," said Chris Howard, vice president of public sector for Nutanix, on the *IT Innovation Insider* program. "The most noticeable was the Department of Defense's initial path with its JEDI acquisition where it wanted to go to a single cloud. That alone would be pretty significant lock-in."

Howard said agencies don't just need to move off legacy technology, but move away from a legacy mindset about how they buy and manage technology.

To help facilitate that change in mindset, Nutanix is promoting a concept called "Freedom."

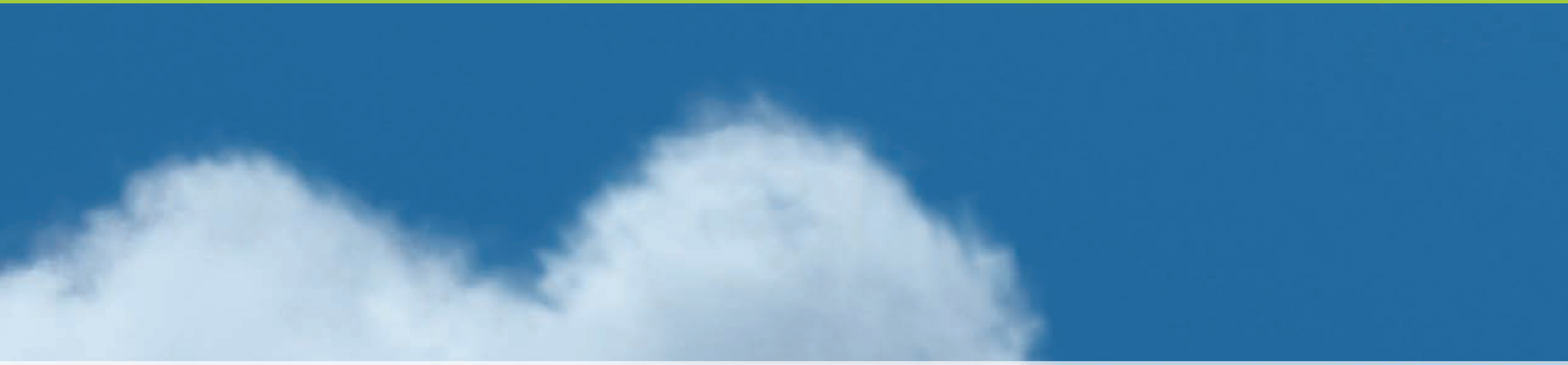
"At the heart of this campaign is 'How do we give our customers the freedom to build and modernize the data centers they always wanted to build or the freedom to run the workloads that they want to run where they want to run them, whether it's on their own private cloud or the public cloud?" said Ben Gibson, the chief marketing officer for Nutanix. "It's about the freedom to make those decisions, freed up with simplicity and with the knowledge in terms of what's the most cost-effective cloud platform to run different applications on."



Ben Gibson
Chief Marketing Officer, Nutanix

"The 'Freedom' initiative is really about the commoditization or electrification of cloud services—no matter what service or application an organization has, it can be plugged in and played on any cloud."

Gibson said the "Freedom" initiative is really about the commoditization or electrification of cloud services—no matter what service or application an organization has, it can be plugged in and played on any cloud.



And this concept becomes even more important as agencies continue to implement a hybrid cloud approach.

“We like to talk about ‘one-click.’ With one click, you can manage applications and application mobility across different cloud environments,” Gibson said. “Also, it’s about making informed choices. Every work load has cost implications dependent on which cloud it runs on. The more we can provide that visibility into that kind of information, the smarter our customers become, the more informed decisions they make, and ultimately [the more] they can impact both top and bottom line for their organization’s operations.”

There are five key concepts around the “Freedom”:

- **Freedom to build**—Modernizing your data center environment to simplify your architecture environment and reduce costs and other resources.
- **Freedom to run the applications where you chose**—This means having application mobility across different environments.
- **Freedom to cloud**—Almost have a brokering environment where you can make decisions based on cost and performance requirements.
- **Freedom to invent**—Gives IT professionals more time to think of new applications or innovate rather than maintain legacy systems.
- **Freedom to play**—“Part of the promise we’d like to see with our customers’ experience is that they have some better work-life balance. They are not being called in on weekends with some kind of availability issue. Instead, because of radically simplifying their private cloud and moving into hybrid cloud environments, they have time to have fun,” Gibson said.

Gibson said the reason cloud lock-in remains a challenge for agencies is every public cloud has its own set of application programming interfaces (APIs) and its own set of security implementations and other features that may be hard to break free from.

“We think this is an opportunity for an IT organization to reclaim some strategic control over what, in many cases, has become a bit of an uncontrollable environment: A lot of different organizations firing up a new workloads in a new public cloud platform at any given time,” he said.

Howard said the “Freedom” concept also will help agencies as they continue to push toward technology modernization.

“We want you to be able to run your application in any cloud you want - with the freedom to move it anytime you want - based on security, based on cost, based on governance or for whatever reason,” he said. “You need to have the freedom to move and be flexible.”

> “We want you to be able to run your application in any cloud you want - with the freedom to move it anytime you want - based on security, based on cost, based on governance...”

Hybrid cloud is changing the one-size fits all mindset

BY JASON MILLER

If one thing is true, agencies are excited about hybrid cloud.

Research firm Gartner said in 2017 that 75% of all IT managers are using hybrid cloud to meet their needs. And adoption of hybrid cloud has increased by 13% year-to-year while overall cloud adoption overall has increased by 2% across the government.

This means there is a huge appetite for a multi-cloud approach and it's only getting bigger.

A new survey from Nutanix of federal agencies found 20% of all respondents are using a multi-cloud approach, and of them, 75% say it's working well or very well.

> "**20%** of all respondents are using a multi-cloud approach, and of them, **75%** say it's working well or very well."

Chris Howard, the vice president of public sector for Nutanix, said the results, once again, reinforce the fact that one-size doesn't fit all when it comes to cloud services.

"There has to be different approaches. Everyone has different uses cases. There is an openness to evaluate the best place to run applications and data sets," Howard said on the *IT Innovation Insider* program. "As technology has evolved, customers have become more open. I've definitely seen a shift. But that doesn't mean there isn't a legacy mindset in some agencies, and that there isn't one-size-fits all mindset and hopefully the government, as time progresses, continues to expand their use of the public cloud, on-premise and hybrid cloud technologies."

Howard said agencies also have evolved how they write solicitations, asking less for specific vendors and more highlighting the need for the flexibility and agility of the cloud.

It was no surprise that security remains the top concern about cloud computing, but 44% recognized that using multiple clouds makes them more secure.

Howard said agency security requirements around compliance, data sovereignty and sensitivity levels also are driving the decision to move a multi-cloud approach.

"The workload itself was driving whether they ran it at one cloud or another or kept it on-premise," he said. "Security drove a lot of the on-premise specific workloads, but now people are looking at security and evaluating a multi-cloud approach. The security requirements that the application has are actually dictating which cloud they go with now. That's a big change from 2016 when it was 'go to the cloud.' You could check a box by putting an application in the cloud, but there was less thought around security and the multi-cloud approach."

Another big driver of the multi-cloud approach is an agency's desire to better understand and control its costs.

Howard said, initially, cost wasn't a main driving factor. But five years later, agencies want to optimize costs when putting applications in the cloud.

"You should be able to move - whether that's on a weekly or monthly basis - based on where the cost is going to be most beneficial," he said. "That's where the multi-cloud approach is really winning out because it enhances competition [and] innovation and gives us a better measurement of cost. Because now we have true competition among these cloud vendors."

Howard said in the 2017 survey 50% of respondents said cost savings would be greater if it would be easier to control and manage costs with the public cloud, while 45% of the respondents expressed concern that it was easy for costs to escalate quickly when using a public cloud.

By 2018, Howard said 49% of respondents said cloud costs what they thought it would, while 25% said the cloud costs more than they expected it would.

At the same time, 72% of the respondents are in the process of creating better management and optimization of their costs in the cloud.

"We feel 25% of your applications are best suited for the cloud because they are unpredictable workloads, they scale up real quick and have to scale down," Howard said. "But 75% of your applications are better suited for on-premise - assuming you have an efficient infrastructure. This panacea that the cloud was going to be cheaper than expected? Most people realize the cloud is not a cost-saver. There are so many more reasons to use the cloud. It's really [about] how you optimize it."

FREEDOM
TO
Invent

Cybersecurity as a shared responsibility

BY JASON MILLER

October ushers in Cybersecurity Awareness Month, so agencies and industry must remember the challenges they face are among the most common for organizational and personal security.

The separation between work-life and personal-life are increasingly less distinct, and with more digital natives in the workforce than ever before, cybersecurity is emerging as a fully-shared responsibility. This means there are important roles and obligations for everyone, not just the cyber team.

With so much at stake, organizations can't afford to assume someone else is handling cyber defense. Instead, they need to remember they are only as secure as their weakest link.

Dan Fallon, the senior director of engineering for Nutanix's public sector, said this idea of shared responsibility becomes even more important as agencies move more applications and data to the cloud, especially a hybrid cloud.

"We are looking at what [agencies] are doing around data security and data encryption, and what are they doing to automate what clouds they are looking at," Fallon said on the *IT Innovation Insider*, sponsored by Nutanix. "We are focusing on the basics there. What are their compliance standards? There are a lot of different standards that are ever-changing. We are showing them how we can check the box with a product that takes security that is more of a built-in than bolted-on approach."

David Reber, the director of cybersecurity for Nutanix Xi Frame, said because agencies will be operating in a private data center and public cloud for the foreseeable future, they need to have automated security checks and a way to provide visibility to make rapid response decisions when there is a problem.

> "... because agencies will be operating in a private data center and public cloud for the foreseeable future, they need to have automated security checks and a way to provide visibility to make rapid response decisions when there is a problem."

"How you get an enterprise cloud view across both ecosystems in a unified manner tends to be one of the biggest challenges for end users," he said. "How do we automate security checks while the developers are rolling code or capabilities out to the workforce? This way you get real-time feedback."

"… email remains the biggest attack vector for bad actors and most employees don't do enough to protect themselves in their personal lives."

Reber said the dev/sec/ops model lets agencies balance security and compliance with agility and speed.

The sharing of responsibility means agencies and vendors alike have to start with a consistent baseline that includes a predictable infrastructure. Then the automated rules can kick in to alert chief information officers or chief information security officers if a device or application has fallen out of compliance.

As work and personal lives continue to merge, Reber said the need to have a shared responsibility perspective becomes even greater. He said email remains the biggest attack vector for bad actors and most employees don't do enough to protect themselves in their personal lives.

Reber said agencies need to understand where the line in the sand is drawn between cloud or on-premise vendor security and a department's responsibility to protect their data and systems.

"The real truth is 'Can your vendor outline specifically what they do for you?' Here is how they help and here is where you take control and ownership. You need to define that and make sure you educate your users in that personal responsibility area as well," he said. "If you are using bring-your-own devices, you need to make sure there is good education for everybody, specifically at the top of your organization. They tend to be the busiest. They tend not to take the training or, if they do, it tends to be ad hoc. But they are targeted the most. Their names are a Google search away from being targeted. They and their families are at risk."

Reber said executives have to realize that cybersecurity is a constant effort around training, people, process and technology, and it starts with them.

Fallon added as agencies continue to shift their security model toward continuous monitoring and automation of security, standards will further get human errors out of the discussion about how to deal with known and unknown vulnerabilities.

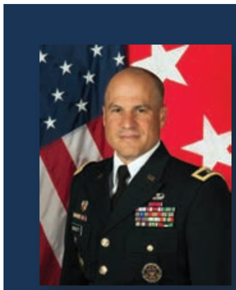
"If you are using bring-your-own devices, you need to make sure there is good education for everybody, specifically at the top of your organization. They tend to be the busiest. They tend not to take the training or, if they do, it tends to be ad hoc. But they are targeted the most. Their names are a Google search away from being targeted. They and their families are at risk."

DoD’s drive toward better tactical capabilities begins with simplicity, capacity

BY JASON MILLER

Recently, the Defense Department participated in the Enhanced Logistics Base or ELB demonstration in Norway. The goal of this exercise, called Trident Juncture 2018, was to test, refine and further develop existing or new capabilities while coordinating and integrating with NATO and other partners.

The exercise demonstrated future capabilities of autonomous and automatized systems within military logistics. The integrated Enhanced Logistic Base will cover all aspects of future logistics in a military-civilian demonstration to include a fully-integrated autonomous and automatic logistics stream.



Maj. Gen. David Bassett Program Executive Officer; Command, Control and Communications – Tactical, U.S. Army

“We want to learn from immediate soldier feedback so we can … get equipment quickly in the hands of soldiers, be able to leverage what technology can deliver and make much quicker decisions about what we can field across the force.”

Sounds like a fascinating effort that can show the potential of technologies like remote machine guns, cubed storage and a field-made 3D printer.

But none of these great technologies will work to their full capacity without data and connectivity.

It’s imperative for DoD to ensure warfighters can access data from anywhere, at any time.

One way that’s starting to happen is in the increased use of cloud computing services, which many see as critical to maintaining the nation’s military advantage.

Today and tomorrow, cloud services can help transform the warfighter’s ability to meet their mission in a safe and secure manner.

Add to that emerging capabilities like artificial intelligence and machine learning, the potential to make warfighters better and faster is huge.

Maj. Gen. David Bassett, the Army’s program executive officer for command, control and communications–tactical (PEO-C3T), said one way to do that is to follow a halt, fix and pivot strategy.

“We will halt efforts which we know will not get us to our end state. We will make changes, fix some programmatic efforts in some new capabilities that we know we can bring to the field quickly. Then we will pivot to a new process for experimenting and delivering technology, as well as a new set of capabilities that will get us to the network that we know we need in the future,” Bassett said on the *IT Innovation Insider* show. "It will not happen overnight, but we've been on that path and have begun experimentation."

The Army is doing this across four lines of effort:

- Unified transport, which is about putting the communication infrastructure in place to get data from point A to point B, both in the tactical space and back to enterprise systems.
- Mission command systems and moving to a common operating environment where the Army doesn't have systems that are stovepipes, but can leverage software to give soldiers a common operating picture that works across the battlefield applications and reduces the amount of servers and infrastructure needed in the field.
- Interoperability across services and with allied partners.
- Making command posts more deployable, more survivable and more capable.

"Across all four of those lines of effort we have efforts underway both programmatic and experimentation," Bassett said. "We want to learn from immediate soldier feedback so we can move toward a model where we don't necessarily start with a set of requirements that were written in a school house somewhere, but rather get equipment quickly in the hands of soldiers, be able to leverage what technology can deliver and make much quicker decisions about what we can field across the force."

Retired Lt. Gen. Stephen Boutelle, the former Army CIO and now a visiting fellow at MITRE, said the tactical edge means so many different things to each of the services - there isn't a generic approach that will work for all the services.

Lt. Gen. Steven Boutelle (Ret.)
Senior Visiting Fellow, MITRE

Scot Susi
Director of DoD, Nutanix

"It's really important to define the environment," he said. "As we look at it, we have to look at the lowest level of the tactical edge all the way up to the enterprise."

Scot Susi, the senior director of DoD for Nutanix, said the military, and for that matter any organization that works in an austere environment, must get away from cobbling systems together that are difficult to maintain and complex to use.

"We need to give the folks in the field a simple interface … like the iPhone or iPad that make it as simple as possible and reduce the number of moving parts," he said. "That way there are fewer things to break, and when they do break, they are easier to fix in the field without having to send a highly-trained, highly-paid service engineer to completely rebuild an entire application stack."

Bassett added the Army would layer on functionality after functionality, which added to that complexity. Now, the Army's changing its current process to make simplicity and usability to the forefront.

"Some of that can be helped along the way by systems that employ artificial intelligence to help abstract away some of that complexity and help commanders turn all that battlefield data into actionable intelligence," he said. "Some of it is about managing those functions and making sure the things we deliver work together well. We are figuring out how we can leverage commercial capability but not utterly rely on it so we can operate in that congested and contested environment. It's absolutely at the heart of where we are trying to go with this network modernization."

Why a mindset change is needed to deal with the IT rebellion

BY JASON MILLER

Disruption is a word that is used commonly when it comes to technology, especially over the last decade.

The ever-growing challenge around cybersecurity has been and continues to be that it is a disruptor.

The cloud, many said, was the ultimate disruptor. Until it wasn't.

In the federal market, there are companies that are supposed to be disruptors, changing how agencies buy and use technology.

For Nutanix CEO Dheeraj Pandey, disruption isn't a technology or a company, rather it's a mindset.

"At the core of this is the velocity and agility requirements of our customers. People want to move fast because everything around them - their customers, their consumers and even their adversaries, like the hackers around the world – is moving very fast," Pandey said on the IT Innovation Insider.

"And then you have such a high-velocity environment, people want to look for ways to consume technology and infrastructure as fast as they can. That also means they don't have time for specialists. They cannot go to too many teams of people, one doing storage, one doing networking, one doing compute, one doing virtualization and yet another one doing servers and applications," Pandey said."

Instead, the need for velocity and agility is forcing agencies to move from what Pandey called a "highly-fragmented infrastructure" to one that is hyper-converged, where services and people are centered around a multi-cloud environment.

"I think there is this rebellion happening right now in the IT industry where we have too many people doing too many specialist niche things. We need to step back and [ask] 'Do we simplify technology and have more people use technology to meet their needs?" he said. "What's happening to personal computing is the same thing that happened to enterprise computing. If you go back in time 10 years, before the introduction of smartphones, we used to have 50 devices that we'd interact with, not the least of which were music players, cameras, video cameras, GPS devices, flashlights, etc. Then they all converged as pure applications running on a common operating system, whether Android or IOS, and that's exactly what is happening in enterprise computing as well."

The combination of velocity and agility as disruptors, the convergence of services, usually in the cloud, and the growing use of artificial intelligence, machine learning and automation is forcing agencies and industry alike to shift their thinking about how they serve customers or meet their mission.

Pandey said hyper-convergence around a multi-cloud approach helps push data and compute power to the edge, whether it's through mobile devices or how services are consumed by an organization's customers.

"The network is the enemy because of the amount of data we are producing is just enormous. Data has immense gravity," he said. "You really want the applications to move to the data rather than the data to move to a large cloud data center itself. That is what is causing this demand for dispersing computing to where people are, to where machines are and to where the operations are."

"The network is the enemy because of the amount of data we are producing is just enormous. Data has immense gravity …"

"I think there is this rebellion happening right now in the IT industry where we have too many people doing too many specialist niche things."

The end goal, in many ways, is to make infrastructure invisible to the user and consumer in such a way that it doesn't matter if the agency owns or rents the servers and cloud instance. Pandey said hyper-convergence makes that happen.

"Many organizations like the Navy, for example, have this view that they need to have a cloud at the edge in these battleships. They need to have extremely space-efficient, power-efficient and skillset-efficient infrastructure that can be used by application folks," he said. "Then they have to remove offices, branch offices and then they have core, large data centers. And finally, they also are now scratching the surface of renting it from a secure public cloud service."

Pandey said hyper-convergence and cloud give the users more power, and the thus the agility and velocity to meet customer needs.

"At the core of all of this is how to democratize technology and democratize computing and bring it to anyone at the click of a button," he said. "That is what hyper-convergence aims to do. Bring all this computing power at the click of a button to folks who really run applications because that's where the business logic runs. These are the people who have deadlines and budgets and heads will roll if applications are not available, not reliable or not fast enough."

As IoT devices and AI grow, are agencies ready to benefit from computing at the edge?

BY JASON MILLER

The Internet of Things or connected devices and artificial intelligence are quickly emerging in the federal sector. These emerging—if we can even call them emerging anymore–technologies are impacting the federal market in a big way.

Over the last few years, the use of connected devices has grown from sensors on networks to sensors in the field to measure agriculture output. It's all about bringing computing to the edge.

At the same time, there are security concerns that come with it. The National Institute of Standards and Technology will be releasing updated guidance to adopting IoT and addressing security concerns in the coming months.

Agencies have to understand how to harness these opportunities, address the challenges that come with them and, maybe most importantly, take advantage of the power of the technology evolution to bring services, compute power and data to the tactical edge.

Jason Langone, the vice president and general manager for service providers at Nutanix, said the agencies are recognizing more and more that much of the data it uses is generated in the field where its employees are meeting their mission. The old approach of sending that information back to a centralized processing center isn't working.

"... agencies are recognizing more and more that much of the data it uses is generated in the field where its employees are meeting their mission."

"The way developers have been developing applications have moved from legacy middleware apps to containerized applications that are much easier to move out to the edge. And everything is IP connected and has the ability to send data now," Langone said on the *IT Innovation Insider*. "We are collecting this data, what can we now do with it and how can we make smart correlations to take intelligent actions?"

Greg O'Connell, a senior director for Nutanix, said while devices have generated data at the edge for years, the difference is the

"… while devices have generated data at the edge for years, the difference is the underlying infrastructure, such as cloud services, can move or process that data quickly, letting users make decisions in near-real time."

underlying infrastructure, such as cloud services, can move or process that data quickly, letting users make decisions in near-real time.

O'Connell said research finds that devices and applications at the edge will generate 40 times more data by 2020 than what's currently being generated.

"With all of this data comes the requirement to manage and process the data," he said. "There is a broad range of examples that span organizations and agencies within government that are absolutely flat-footed yet need to adopt edge-based capabilities. There is an Air Force program office that is responsible for flight suits and helmets for pilots. We gather terabytes of information on military jets by the minute, yet to date, we gather zero physiological information on the pilots themselves. This is a classic example of IoT and edge computing where if we could better collect information with the sensors and process it in real time … we could take advantage of that to protect the pilots."

Langone said agencies and developers must keep in mind the challenges of deploying apps to the edge, given in some cases there is low bandwidth or connectivity. He also said an additional challenge is the number of devices that employees use in the field could number in the hundreds of thousands, which adds more complexity to the effort.

"There are a couple of things to think about. One is the sensor data, where does that live at the edge and how is that encrypted as well as the machine learning logic that is delivering the value?" Langone said. "If that edge device were to grow legs and walk away or to be stolen, how do we ensure that we've lost nothing?"

This is why Langone and O'Connell recommend agencies apply IoT devices and AI only after they know what problem they are trying to solve. The technologies and devices have to be a part of a larger business solution.

"One of the working relationships I've seen is when the chief data officer is fielding requirements from the business or mission. They typically understand they have a problem with something. And the CDO is often responsible for developing that strategy and ultimately deploying the solution to solve that problem," Langone said. "When that is not a connection that is functioning in an agency, those things are in a void and it's difficult to come up with something specific to solve."

O'Connell said agencies need to address these challenges today because the growth of IoT, AI and machine learning will contribute trillions of dollars to the U.S. economy over the next 10 years and create tens of millions of new jobs.

Moving to the cloud requires agencies to use a consumption model

BY JASON MILLER

Since 2010 when the Obama administration launched its cloud-first policy, the momentum of applications and systems moved to public, private or hybrid cloud services has been growing.

Eight years after the cloud-first policy, agency spending on cloud computing services surged to $4.1 billion, according to analysis from Bloomberg Government. BGov says cloud spending grew by 9% among civilian agencies and by almost 30% among defense agencies from fiscal years 2017 to 2018.

The growth curve is expected to continue on the upward climb as the Trump administration finalizes its cloud smart strategy as well as new contracts for common back-office cloud services and shared services.

At the same time, there are a host of challenges to consuming cloud services in a way that is accessible and immediate.

Chris Howard, the vice president of public sector for Nutanix, said as agencies continue to move the cloud, the way they use and pay for these services needs to be front and center.

"We are trying to bring the characteristics of the cloud to where the customer is going to deploy those IT assets, whether it's in their own data center, a contractor-owned data center or a public cloud company. It's the consumption model that is important," Howard said on the *IT Innovation Insider* show. "One of the benefits of the cloud we've realized is when you want an application or workload spun up in the cloud, it's very easy and it's fast to market. The agility and the speed to bring those applications so the users can access them is one of those characteristics. Another characteristic is how you consume it and how you pay for it. You pay for what you use and that's [all]."

Howard said there are certain applications - ones that have spikes and troughs - that make sense to take advantage of the cloud and the consumption model that comes with it. At the same time, some applications may make sense just to modernize but keep on premise.

Dan Fallon, the senior director of engineering for Nutanix's public sector, said this is why application rationalization is so important, and is a growing trend across government.

"Part of what agencies can do is get the small wins and move the apps that are easy, the external facing things like web servers. Email is a classic one. But then when you get into the apps that are on servers, still physical or even still on main frames, this could be a huge undertaking and a lot of budget dollars may be required. These are the ones you leave for last," Fallon said. "There is a growing trend of moving to containers when doing the cloud migration, but that does introduce extra complexity."

As agencies move into these more difficult or complex applications, Howard said approaches such as managed services or shared services are starting to gain popularity. The Trump administration recently issued a new strategy for how agencies should move to back-office shared services, naming four agencies to lead human resources, financial management, grants management and cybersecurity.

"The main trend is agencies want out of the hardware business," he said. "There are a couple of different ways to do that, and it doesn't mean just a lift-and-shift to the cloud. Managed services can be accomplished in a lot of different ways. It can be done on-premise at the customer's site. It can be done in a co-location site and it can be done in the cloud. I think it's about how you consume and what color of money makes the most sense for you. A lot of people are more flush with the operations money versus the capital investment money and that's a big driver."

Operational money, known as OpEx, is used mainly to keep legacy systems up and running. Howard said agencies can use that type of funding to pay for managed or shared services more easily.

"No matter what kind of contract you enter into, whether a managed service or shared service, you still want to make sure you have the flexibility to make change. You don't want to be locked into something for five or 10 years that doesn't give you the same level of innovation or cost protection," Howard said. "No matter what you go into, and the consumption model generally allows it, allows you to turn it off and pivot when you have to so that is the key takeaway on what would make a successful contract."

Fallon added there also is a technical side that agencies should consider along with the contracts piece. He said departments should make sure they can easily move their apps and data between clouds or between a cloud and on-premise.

"No matter what kind of contract you enter into, whether a managed service or shared service, you still want to make sure you have the flexibility to make change."

FEDERAL NEWS NETWORK

INDUSTRY INSIGHTS

IT INNOVATION INSIDER