SPECIAL REPORT

MODERNIZING THE FEDERAL IT ENTERPRISE

Leveraging Data, Working Smarter and Going Mobile

INSIDE

P2 MAKING SENSE OF THE DATA DELUGE

P3 WORKING TOGETHER THROUGH TECHNOLOGY

P4 THE MANAGED SERVICES CHOICE

P5 MOBILITY — FULL SPEED AHEAD

P6 THE 21ST CENTURY DATA CENTER

PRODUCED BY: FCW

SPONSORED BY: IRONBOW TECHNOLOGIES, DELL EMC, CISCO Gold Partner, intel

MAKING SENSE OF THE DATA DELUGE

Analytics puts agencies ahead of threats, informs decision-making.

That security camera connected to your network? It's a rich source of data. That email log? Another great data source. The same is true of transactions, social media posts, VPN logs, routers and switches, posts, mobile location data, equipment diagnostic records, machine logs, documents and much more.

This torrent of bits and bytes, commonly referred to as big data, is overwhelming federal agencies. But if harnessed and properly analyzed, it can help government to create efficiencies; improve processes; boost productivity; improve cybersecurity; increase citizen and employee engagement; reduce fraud, waste and abuse; enhance supply chain and asset management; and improve financial accountability.

The challenge is finding a way to make sense of the massive data flow that continuously surges into agencies' systems. Without the right processes and technology, big data is unmanageable. According to a recent survey, almost half of federal employees say they struggle to manage big data – analyzing only 12 percent of what's available – and use it to make decisions.

Harnessing the power of data requires the right technology to automate the collection and organization of data; continuously monitor events, conditions, users and important indicators; and provide real-time notification that important events are occurring or are about to occur. The most advanced systems use artificial intelligence and machine learning to detect unusual activity – and predictive analytics to determine potential outcomes based on a set of predetermined indicators.

Cybersecurity is an example of how agencies have taken advantage of these capabilities and adopted tools for specific uses.

What's often missing, says Jim Smid, chief technology officer of Iron Bow Technologies, an IT solution provider specializing in government, is a way to quickly aggregate and correlate security data from multiple sources and stop problems before they escalate. Without these capabilities, it's hard to analyze factors such as the time, location and context of data to determine the details of a cyberattack. Rather than remediating incidents after receiving an alert, agencies can protect systems and data by collecting and analyzing information from firewalls, Web proxies, VPNs, email, intrusion detection systems, host data from workstations and servers, malware scanners, databases, SIEM tools and other sources.

"Every agency wants to be able to compile, analyze and act on threats in real time – not simply to do the forensics after the fact, but that's often what ends up happening," Smid says.

> "Every agency wants to be able to compile, analyze and act on threats in real time
>
> JIM SMID, CTO, IRON BOW TECHNOLOGIES

Gleaning data for insights also is a great way to ensure smooth system operations and to pinpoint potential system issues before they mushroom into bigger problems. With automated collection and monitoring of assets such as weblogs and application logs, agencies can gain the visibility they need to improve system efficiency and ensure compliance.

Data analytics can also make a difference as agencies strive to make public websites more reliable, efficient and user-friendly. Continuously analyzing server logs and user activity, for example, helps agencies to improve citizen satisfaction.

Agencies are striving to get better at managing big data at a time when the challenge is rapidly expanding. Most estimates put worldwide data growth at 44 zettabytes by 2020, driven in part by the proliferation of internet-attached sensors, mobile devices and other types of structured and unstructured data.

The federal government, like other big data users, can prepare now or catch up later.

WORKING TOGETHER THROUGH TECHNOLOGY

Collaboration technologies improve productivity, cost savings.

After weeks of trying to coordinate schedules, the work team finally gathers around a conference table, legal pads in hand. An hour later, the meeting is over, and everybody goes back to their desks, ready to start their next task.

That scenario was common 30 years ago, and it still happens today, causing agencies to lose time, productivity and the opportunity to make timely, effective decisions.

Some agencies are finding better ways to collaborate. Using full-featured collaborative tools, team members can work together via voice, video, messaging or with IP-based tools such as whiteboards. And they can do it in real time, no matter where employees work.

These capabilities are important for today's federal employees, many of whom work remotely. According to a survey from Deloitte, 36 percent of public sector respondents believe face-to-face meetings will decrease, and 66 percent view connected work tools as a positive driver of productivity.

Productivity, in fact, is the main reason agencies are investing in collaboration solutions. According to McKinsey, innovative business collaboration techniques can improve an organization's productivity by up to 30 percent and reduce the time and expense of traveling to meetings.

THE RIGHT MIX OF COLLABORATIVE TOOLS

Most agencies are using some type of technology to collaborate, typically a combination of PBX or IP telephony, videoconferencing, shared storage or older collaboration suites.

Though better than nothing, these tools don't provide the functionality and ease of use available with newer collaboration suites that combine IP telephony with video, audio, presence, conferencing, and messaging. Modern collaboration suites also enable desktop sharing, task and workflow management and discussion boards.

These tools can make a marked difference in efficiency, cost savings and productivity due to metrics like reduced travel costs, faster problem resolution, and quicker completion. A study from SCORE found that collaboration tools can reduce the cost of international calls by 90 percent and the amount of travel by 30 percent. The study also found that the typical employee saves 43 minutes per day due to more efficient message management.

Introducing full-featured collaboration tools into an environment can be complicated, especially for groups using collaborative technology that they want to keep. For example, it can be challenging to find ways to integrate existing collaborative technology, such as video or IT telephony, with new collaborative technologies.

"Often, agencies have different types of tools being used by different groups, and they can't share information with each other. Just integrating existing collaboration tools is complicated, and has to be approached strategically," says Jim Smid, chief technology officer of Iron Bow, an IT solution provider. "The same is true at an even more advanced level when agencies want to incorporate newer collaboration suites while keeping some of their legacy tools. It can be done, but it's got to be done strategically."

Smid suggests that agencies consider moving to an on-demand, cloud-based, hosted collaboration solution. This type of service should provide everything an agency needs for teams to collaborate effectively: IP telephony services like unified messaging and voicemail; video; instant messaging and presence; and the ability to use the service from any device.

Regardless of the technology, Smid cautions agencies to not overlook security. Make sure all systems and tools meet federal standards, including FedRAMP and, if applicable, federal cloud mandates, he says.

THE MANAGED SERVICES CHOICE

Agencies look to outsource temporary needs, fill gaps.

To beef up authentication of network users, a Defense Department agency recently hired a managed services company to oversee its identity access management program. The vendor authenticated users, managed digital identities, authorized access to resources and fully integrated all identity services and dashboards. The company also updates, secures, monitors and manages those assets, continuously.

The arrangement is hardly rare in the federal sector, where agencies increasingly are turning to managed services firms to bridge resource gaps and perform critical functions. Yet security-related services are just one type of managed service agencies are using. They're also getting help moving cloud, managing enterprise mobility, upgrading and managing networking and infrastructure on site, and managing communications platforms.

A recent report by CompTIA, an IT industry trade association, found that 64 percent of organizations use some form of managed services, a number projected to grow over the next several years. Those organizations are choosing managed services to gain better security and uptime, cost savings over in-house IT, peace of mind and time for internal staff to perform more strategic work.

FILLING THE GAPS

Like most federal agencies and departments, the Defense agency that contracted with a managed services firm couldn't easily monitor and manage its system on a continual basis. The IT skills shortage – especially in the cyber arena – is a contributing factor. The Office of Management and Budget acknowledged in a recent report that the skills shortage could hinder agencies' attempts to combat cyber threats.

"We're never – certainly in government and also in industry – going to be able to get the workforce we need … to defend all of these different systems," said acting Federal CIO Grant Schneider at a cybersecurity conference in December.

Dedicating federal employees to specific services also doesn't always make good economic sense. Sometimes, employees simply don't have the time to take on extra responsibilities, and the cost of training can be prohibitive.

"While most agencies require the expertise, they usually don't require it 100 percent of the time," says Jim Smid, chief technology officer of Iron Bow Technologies, an IT company. "If they only need 15 or 20 percent of an employee's time, it often makes more sense to outsource the work to a specialist rather than training an employee who already has full-time responsibilities in something they don't know."

Customization and expertise are two more reasons why more agencies are turning to managed services. Through this model, agencies can be sure they are getting IT professionals trained and experienced in their specific technology requirements. A good managed services provider also can customize any solution to meet an agency's needs, such as integration with legacy systems.

It often makes sense for agencies to turn to managed services for temporary needs, such as migrating software or infrastructure to the cloud, that require developing strategy, migrating workloads and optimizing operations. Some agencies choose to retain the managed services approach for cloud services over time, leveraging experts for support, monitoring and maintenance.

"It's important to keep track of the analytics … to determine what workloads should run in certain clouds," Smid says. "It can make a big difference in terms of efficiency and cost."

MOBILITY: FULL SPEED AHEAD

Legacy apps and potential data loss must be considered.

Eager to deliver faster, higher-quality healthcare to nine million military veterans, the Department of Veterans Affairs in recent years acquired a sophisticated telemedicine system that is growing and evolving. VA has also redesigned its mobile apps to work with a variety of mobile devices. As a result, the system's healthcare professionals are using mobile devices to access critical health information and communicate with colleagues and patients almost anywhere in the world.

Federal agencies, keen to meet demand for ubiquitous mobility, consider it a pillar of IT modernization. According to a Dell EMC survey, 93 percent of federal IT executives reported that mobility is one of the most important attributes of a "future-ready" agency, for federal employees and citizens.

The leadership at VA and other federal agencies understand that customers want to interact with government on their own terms, including the option of accessing digital services and communicating with agencies on mobile devices. Federal employees expect much the same – especially younger workers accustomed to constant connection. They typically expect to use mobile devices in their personal and work lives.

Indeed, growing demand for mobile-friendly access to applications, via the web, informs the Connected Government Act, passed by Congress in January. The law stipulates that federal agency websites used by the public should be mobile-friendly to the greatest extent possible. The Act also requires retrofitting legacy applications for the mobile era.

Agencies will continue to improve mobile apps, expand access to them and strengthen connectivity. Soldiers in the field rely on wearable mobile devices to communicate with other soldiers and access critical information. In the civilian world, agencies are developing more citizen-facing mobile apps, and a record number of federal employees use mobile devices to do their jobs.

Redeveloping existing applications for use by mobile devices, however, can be tricky. Interfaces must look good on different types of mobile devices and screen sizes – and work well on a variety of platforms.

To achieve their mobility goals, agencies typically look for a vendor that understands an agency's mission and legacy applications. A good partner can determine how best to optimize applications, whether to modernize legacy apps or completely rewrite them, and how best to mitigate the risk of data loss.

"Mobile security is so important today that it should never be a do-it-yourself situation," says Jim Smid, chief technology officer at Iron Bow. "It's too important, and the options are too overwhelming. If you do nothing else, find an experienced third party to evaluate your requirements and vulnerabilities and come up with the right set of security solutions."

DON'T TAKE CHANCES WITH MOBILE SECURITY

Securing mobile devices includes the applications that run on them. If not written to be secure, apps can be vulnerable to bad actors.

Agencies should insist on:

- multi-factor authentication
- separation of personal and work data and applications
- the ability to remotely wipe and lock devices that are lost or stolen
- malware and virus protection, firewalls and other security protections

THE 21ST CENTURY DATA CENTER

To find the future, consider hopping on a cloud.

One of the best ways an agency can move toward modernizing its data centers is to start with a private cloud. Functioning as the nerve center of an agency's data center requirements, a private cloud is a natural hub from which to grow a multi-cloud data center solution.

When done well, this model expands agencies' agility, flexibility, scalability and cost optimization, while allowing agencies to keep legacy applications and systems operational as long as they're needed. According to a Meritalk survey released this year, 64 percent of federal IT managers say their agency's data center acquisitions are beginning to shift toward utility-based or pay-as-you-go models.

An agency's private cloud should be efficient, agile, secure and automated, whether hosted in a different facility or on premise, whether self-managed or managed by a third party.

The private cloud that serves as the hub of a multi-cloud solution should run management/orchestration software that controls all other clouds. This is also the place to implement automated software that provisions resources on demand from whatever cloud resource is most appropriate. If Microsoft Azure is the most economical approach for specific requirements requested by a user, for example, the automated tool should automatically provision those resources.

The private cloud also should provide full visibility into resources and dependencies across clouds, measure service integrity, enforce security policies and ensure compliance. In the case of Defense agencies, it should also house and oversee the continuous monitoring required by the Risk Management Framework.

It's also a place where agencies can safely and securely test cloud applications before moving them to a public cloud.

"The key to an effective, multi-cloud data center strategy is making sure your private cloud infrastructure has the automation necessary to move workloads, the ability to provision resources, and the analytics that allows you to determine whether or not you are putting your workloads in the right places," says Jim Smid, chief technology officer of Iron Bow Technologies. Analytics also are critical to maintaining peak availability and security of applications and proactively preventing problems.

With a private cloud hub in place, the next step is choosing the right mix of public clouds – a mix that will provide the best agility, performance, security, compliance and cost. This requires understanding the cost structure and capabilities of all cloud computing platforms under consideration. With the right mix of clouds, agencies will have the capacity to adopt new technologies and manage vast amounts of data.

> "It's about developing a custom recipe that works best for an agency."
>
> JASON LAMB, INTEL

Choosing the right mix of public cloud technology isn't an easy task for agencies constrained by specific requirements and limited financial resources. Jason Lamb, a cloud solution architect at Intel, says experts familiar with many different cloud vendors and tools are indispensable when developing cloud solutions.

"It's about developing a custom recipe that works best for an agency," he says. "It's got to fit the environment, allow agencies to continue using legacy applications, as necessary, and enable the agency to move forward at their own pace."

IRONBOW® TECHNOLOGIES

In partnership with: cisco DELL EMC intel

Accelerate Your Path to IT Modernization

Leverage data-driven, customer-focused strategies to modernize legacy systems, consolidate common agency service, adopt new shared service models and embrace secure cloud solutions.

Create **Efficiencies.** Remove **Barriers.**
Increase **Security.** Gain **Flexibility.**

Explore:

Ironbow.com/Modernize