Sponsored Content

FCW

The New Look of Cyberdefense: Converged Infrastructure

Data protection and cybersecurity intersect within converged infrastructure.

These are interesting times when it comes to technology. Outside of security, both industry and government have come to realize that traditional infrastructures can no longer cope with the data traffic, which rapidly continues to grow. Market analyst IDC believes worldwide that it could reach 180 zettabytes—or 180 billion terabytes—in 2025, up from just 4.4 zettabytes in 2013. How to cost-effectively upgrade and scale their IT infrastructures to handle this explosion of data is a primary focus for government agencies.

This in turn increases the attack vectors for cybersecurity threats. As agencies look to improve their infrastructure to handle larger volumes of data, they are also looking to better safeguard that data—and more importantly, which technology partnerships to engage.

"Where that data resides, how it's used, and what happens to it has become extremely important," says David Rubal, Vice President of Oracle's North America Public Sector Cloud and Infrastructure Solutions Engineering organization. "It's important that the infrastructure can help support processing data in a secure fashion, and to be able to support a defense-in-depth cybersecurity strategy."

David Rubal, CISSP—
Vice President, Public Sector
North America Cloud
and Infrastructure
Oracle Corporation

The types of attacks and the people behind them, both external and internal, are not new to the government realm. They've been around for years. Traditionally, the security put in place to defend against those attacks focused on protecting the weakest links in those technology swim lanes. Current infrastructure and processes can be challenged to protect different varieties of data moving much faster throughout the entire technology stack.

Several highly public breaches at a number of large government agencies have recently driven that lesson home. This includes the breach at the US Office of Personnel Management (OPM) made public in 2015. This breach compromised millions of government employee records and helped focus the government's attention on the intrinsic value of all data. "It's obvious that data protection is now one of the top priorities," says Rubal.

ARISE OF CONVERGENCE

The next generation architectures will be defined by converged infrastructure, a tight integration of hardware and software end-to-end across the entire IT stack. This environment encompasses all infrastructure elements—compute, virtual machines, operating systems, database, applications, cloud, security, networking and storage. These have all traditionally been built component by component, using different pieces from different vendors.

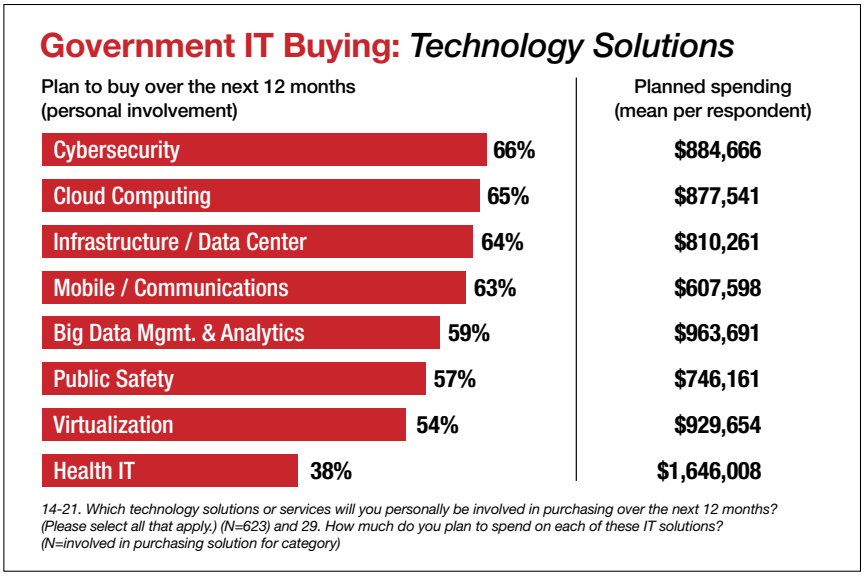
While the concept of a converged infrastructure strategy has a long history, dating back to the minicomputer days of the 1980s, its development has been hampered by that "swim lane" approach. In government, this has sometimes resulted in different IT silos within agencies going their own way with systems

and software. Integrating these disparate technologies into a coherent agency-wide infrastructure has proven difficult, to say the least.

While Oracle is renowned for its database solutions that are ubiquitous in government and industry, over the past few years, the company has been successfully extending that influence into the hardware space through its version of converged infrastructure. Oracle believes that its solution—comprised of co-engineered hardware and software with a single source of support—can help agencies address their cybersecurity operational needs.

"Security doesn't stop at the network," says Rubal. "From our view, security needs to be considered everywhere data resides—from the network, storage and compute levels to the operating system, middleware and applications. This is consistent on-premises, or in a public or private cloud."

Oracle's approach facilitates that extension, he says. The benefits to government agencies come from wrapping a cloud services approach around the company's converged infrastructure. "In that type of infrastructure, Oracle offers important security features for data processing, compute, and data storage; supporting the security of data at all levels."



Government spending on cybersecurity continues to rank highly, indicating this is clearly a top priority.

Defense in Depth under NIST

The intersection of converged infrastructure with cybersecurity fits well with the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which the Obama Administration first proposed in 2013 as a way to reduce cyber risks on US critical infrastructure. That framework recommends a defense-in-depth strategy to protect data through five core security functions: identify, protect, detect, respond and recover.

"We believe that this framework is the best approach for agencies to take to be able to provide data protection at all levels," says Oracle's David Rubal. "While it specifically addresses risk, we feel that Oracle's focus on data protection at the infrastructure level supports the objectives of the framework."

When an agency implements the NIST framework throughout all stages of the data lifecycle and aligns that with a converged infrastructure, he says, it will be able to inspect and analyze data as it's processing that data and check for unnecessary risk. The framework calls for a range of near real-time, interactive services from an agency's IT infrastructure to implement its core functions. And the converged infrastructure is well-positioned to provide those services.

Naturally, says Rubal, agencies could accomplish that with Oracle. They would waste no time in having to build the infrastructure themselves.

Oracle operating as a hardware and infrastructure company may come as a surprise, but it's no accident—the company has invested some $10 billion in R&D over the past five years, following its purchase of Sun Microsystems in 2010. The goal has been to build a converged infrastructure framework designed to help derive the maximum possible value from any organization's use of Oracle's database software.

Oracle Cloud Infrastructure includes hardware-based "Silicon-Secured Memory," which is intended to protect against such things as malware and other cyberthreats. It also provides onboard and accelerated encryption at the chip level. The available end-to-end security features that Oracle offers is what the company calls the "table stakes," which everyone should now expect from a true converged infrastructure solution. And this is essential for any agency looking to protect its data.

OPTIMIZED INFRASTRUCTURE

The company argues "nothing runs Oracle software better than Oracle infrastructure." Oracle can go into an

agency with its Cloud Infrastructure and upgrade its IT environment to make Oracle's database and middleware run at optimized levels, which the agency won't get on any other hardware platform, not to mention a significant decrease in deployment time.

The services approach to converged infrastructure can be likened to how IT delivered services to users before the cloud, such as separate network services, connectivity and mobility services, storage services and the like. This was mostly a manual effort. The various services were configured and delivered directly from the organization's datacenter.

Converged infrastructure services are focused on what's needed to effectively modernize an IT environment, such as compute capacity, storage, data processing and analytics. "You don't rely on purpose-built aspects of an environment anymore," says Rubal. "Now you have to build enterprise environments that are able to serve up a wide set of services and capabilities."

DEALING WITH DATA

The data analytics component is increasingly important when dealing with cybersecurity. Oracle's converged infrastructure approach provides the types of services needed to handle both structured and unstructured data. That is important for any Big Data examination of security events, along with streaming data, and other different types of data services needed for comprehensive and holistic cybersecurity.

It's more important now than ever before to catch something like a malware event or security breach when the event actually happens. Oracle's goals is to create an IT environment where event data is served up as close to real-time as possible. That's something where converged infrastructure—which operates across the full width of that IT environment—has the advantage.

"It's where converged infrastructure provides a set of high performance, optimized capabilities that you can't get elsewhere, and intersects with the cybersecurity operations," says Rubal. "We see this as something that a converged infrastructure solution can work together with cybersecurity operations in an agency to meet its security objectives."

Government agencies produce and collect massive amounts of data. Now the goal is to generate as much value and learn from that data as much as possible. Those data repositories represent significant value, which changes the requirements of databases themselves. Now they need to link into business intelligence and other analytical systems to help agencies solve problems more efficiently and enhance their mission outcomes. And all that data needs to be secured; otherwise they'll continue to be at risk from cyberattacks reminiscent of the OPM breach.

In that sense, cybersecurity and data protection represent another workload for converged infrastructure. However, given the increasing priority and requirements for data protection, they are also the most important.

An Understanding of Infrastructure's Impact on Cybersecurity

How long will it take for government to effectively use converged infrastructure to help with their data security? The first part is an understanding of the importance of infrastructure overall to data security. "I don't think agencies fully do," says Oracle's David Rubal. "At least not to the point where they understand the data management aspects of security, and how that relates to the kind of defense-in-depth that NIST advocates."

According to the recently released "The State of Cybersecurity from the Federal Cyber Executive Perspective" report by KPMG and the International Information Systems Security Certification Consortium, 59 percent of federal workers say their agencies struggle to understand how cyberattackers could potentially breach their systems, while 40 percent even revealed they were unaware where their key assets were located. Surprisingly, about 65 percent said the federal government as a whole can't detect ongoing cyberattacks. Clearly, further education is required.

"Deploying the NIST Cybersecurity Framework creates on a heavy dependency around data security within the IT infrastructure", he says. That means there is also a much higher level of reliance on the services an infrastructure can provide to achieve cybersecurity operational objectives.

That won't necessarily be intuitive for most agency IT and security executives, he feels. "I don't think they understand all of the dependencies involved," he says. "A cyber event as it is happening is both a data-driven and an analytical services event."

There may be a lack of recognition on the need to keep building the infrastructure to attain better reach and visibility into what's happening. The data-driven converged infrastructure will provide that information on a real-time basis. "Agencies may have a grasp that an approach like this is needed, but I don't think they understand what the key components fully entail," he says.