Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 9, Issue 6

Conquering the Logical in Next-Generation Data Centers

By Tim McElligot

The greatest logical thinker of our time said, “Logic is the beginning of wisdom, not the end.” That the words were uttered by a fictional character known the sci-fi world over as Mr. Spock should not diminish their significance; after all, they were written by a human, perhaps even Leonard Nimoy himself.

But here in the 21st century, on earth, in a world of evolving computing technology, logic is often the beginning of something else: stifling complexity. Humans think of themselves as logical beings, but they are still proving to be much more adept at the physical.

The logical and the physical are two aspects of the modern data center. We appear to have a good handle on the physical aspects of designing, building, securing, maintaining, and operating ones that are increasingly more powerful and efficient data centers. However, many IT departments are experiencing a loss of control over the logical aspects of their data centers, which, in a word, are becoming too complex; advances primarily due to virtualization are generating angst over security, compliance and manageability, and are causing them to start tapping the brakes on deploying next-generation data centers.

According to a report last month from Symantec (“State of the Data Center Survey: Global Results”), complexity is being driven by virtualization, cloud computing and the proliferation of mobile devices. Unless IT executives learn to better cope with this complexity, “their investments in virtualization software, blade servers and other technologies designed to modernize the data center might be in vain,” the report said.

These drivers, however, are more accurately described as enablers, because it is the number of business-critical applications that virtualization enables, as well as the volumes of data that mobile devices generate and the uncertainties of the cloud and cloud security, that are the true drivers. The Symantec survey showed that 65 percent of company IT departments felt that the increasing number of apps was the top driver of complexity, followed by the growth of data (51 percent), mobile computing (44 percent) and virtualization (43 percent).

While most companies surveyed agreed that virtualization saved money, it led to costs in other areas, and 47 percent said increased costs were the biggest side effect of data-center complexity. In fact, they listed a range of side effects ranging from longer lead times for storage migration (39 percent), reduced agility (39 percent), security breaches (35 percent), and compliance incidents (34 percent).

And while these concerns can all be addressed to some degree, companies are first putting their efforts into governance: 90 percent of companies surveyed are actively discussing governance or implementing solutions. Security is the most important driver for these initiatives. Companies also hope to make it easier to actually find the data they have stored when they need it, reduce the cost of information management and reduce the legal and compliance risks associated with their data.

One way to mitigate data-center complexity, which flies in the face of the whole distributed architecture of the cloud, is to consolidate, a move confirmed by most Tier 1 service providers across the globe, according to

Mike Sapien, principal analyst for enterprise telecoms at Ovum, in his report "Global Telco Data Center Strategies."

However, that doesn't mean companies aren't modernizing or expanding into new markets. They are — just more strategically and in a more centralized fashion, Sapien said. In a word, they are consolidating locally so they can expand globally.

Not your mama's data center

With physical security being a fairly settled art except for increased use of remote monitoring and management and some environmental management advancements, data-center operators are concentrating on buttoning down the logical hatches.

the data center is no longer being used as a showcase for customers. For one thing, there is little for them to see or comprehend from a tour that they either didn't already know or couldn't glean from a center's certification. "Once you have a premium data center, people know what they look like. Mostly, they look the same, sound the same and have the same physical security features," Sapien said.

Secondly, operators have had to implement much stronger controls over who has access to facilities and data because of HIPPA and other compliance restrictions. "HIPPA compliance and some financial services require you to know who went into a cabinet, who had access to the server or the database, and all that needs to be tracked," said Sapien, adding, incidentally, that all this recording and tracking is one of the drivers for big data.

"Anyone touching a server that has sensitive healthcare data has to be tracked and recorded, so you have a whole new level of data and access to keep track of," he said. "New compliance and governance solutions that can help find that info that's been tracked when you need it is an important new market."

Sapien also said that because of these requirements, industries such as financial services and healthcare may have to stay with a private cloud model and may never be able to fully leverage a shared cloud platform.

Security scares people

When it comes to accepting the promises and performance claims of security providers, data-center companies, including service providers, have more than a healthy share of skepticism. According to a survey last year by Crossbeam, 60 percent of companies surveyed distrusted the claims of security vendors, while 94 percent felt the claims were misleading. Mobile operators were the most distrustful.

"HIPPA compliance and some financial services require you to know who went into a cabinet, who had access to the server or the database, and all that needs to be tracked"

An updated survey from which results were released in March shows that security is still a major concern for data-center operators and is delaying the deployment of next-generation data centers. Ninety-four percent of survey respondents said security was the top reason for NGDC deployments being stalled, and 41 percent said network security was the biggest obstacle to success for those being installed.

"While great advancements are being made by companies in software-defined networking, the bottom line is we have made data centers way too complicated," said Peter Doggart, director of product marketing at Crossbeam. "Security remains a problem child for many folks because they are locked into a physical mindset regarding security. In a virtual environment people fear losing control and adding risk."

Despite the complexity introduced by virtualization, the data-center environment is evolving in that direction, and Doggart says the security environment should do the same.

In its report "Security Virtualization Within the Next Generation Data Center," Crossbeam found that 78 percent of IT professionals said their companies were in some phase of planning or implementing an NGDC, but that only 3 percent had been fully implemented. Most survey respondents agreed on the level of virtualization required in a data center and even agreed security should be a part of it. However, most of the current virtualization efforts are going toward application servers (62.4 percent) and storage (44.9 percent), with security at 35.3 percent, followed by switches and routers at 29.6 and 27.2 percent, respectively.

Security virtualization can be achieved in more than one way, but Doggart feels not all security virtualization is created equal. One way to do it is within the server itself, but the problem is that servers running mission-critical applications have stringent performance metrics to meet, and security takes away from that with its processor-intensive nature.

"The more core data a server processes, the more security it has to process, and it can have a compounding effect on performance," Doggart said.

"There are also many more applications running on virtual machines these days, and they operate in different trust zones with different levels of security. How do you make sure you don't get cross-contamination?"

His solution is to run security on its own virtual platform, allowing for physical separation from the servers so they can be tuned for performance. In Crossbeam's survey two-thirds of respondents agreed, saying security should be virtual but separate.

Doggart said the industry is still a long way from realizing the full potential of a fully virtualized data center, and that while strides are being made in virtualizing servers, storage and security, the industry needs to come together to design a roadmap from point A to point B.

The data center as art

In his new book, The Art of the Data Center: A Look Inside the World's Most Innovative and Compelling Computing Environments, as well as his previous works, Build the Best Data Center Facility for Your Business (2005) and Grow a Greener Data Center (2009), Cisco's Douglas Alger explores the history and future of the data center. Then and now there are some constants, such as efforts to be more efficient and reduce costs, and perhaps the biggest driver of change for both is power density.

Starting 10 years ago, as hardware got smaller yet more powerful, power density within the same footprint soared. "The good news for data-center managers [was] you could put a lot more hardware into a cabinet. The bad news was you could put a lot more hardware into a cabinet," Alger said. "On the heels of that you had the goal of making things greener, so a lot of efficiency practices that were exceptions are now the rule."

It would be a mistake to assume, however, that the drive for greener data centers is motivated entirely by a social conscience. Data centers have captured the attention of CEOs, Alger said, because they feel the need to control their costs, most of which are related to energy and resource consumption, the biggest operational cost in a data center. So if their conscience doesn't get them, their CFO will. And if the CFO doesn't, perhaps the operations manager will, because despite the conscientious environmentalism and the cost is another benefit to being efficient. Say you need to take a ride in a car and still aren't convinced by someone else paying the cost of gas: you might be convinced by not having to stop the car so often.

Security virtualization can be achieved in more than one way, but Doggart feels not all security virtualization is created equal.

So even if you pull off the top-layer benefits that people focus on — being green and saving costs — you can increase productivity and optimize resource consumption, and that is the real business value of having a green design, said Alger.

What has changed most — and continues to change — in energy consumption are data-center managers' awareness of the environment within and around the data center and their ability to respond to it. In fact it has changed the way data centers are being planned, according to Alger. Until now engineers' goal was to stay ahead of growth; they would assign a given amount of data-center space to some group that may ultimately only use half of it. That meant the power reserved for that space could not be reused elsewhere. With its data center in Allen, Texas, Cisco stopped planning that way and instead implemented a flexible power scheme that allowed unused energy in one cabinet to be used in another.

Each cabinet in that center, among 750 cabinets, is provided with, on average, 6.5 kilowatts of power, but the room can accommodate up to 20 kilowatts for any cabinet that needs it, "so we consume all the power before having to move to another build," Alger said.

In addition the Allen data center uses outside air for cooling at least half the year, saving $600,000 to $800,000 in local power costs by doing so.

Environmental efficiency is only tangentially related to security, but in the long run it allows companies to choose data-center sites that will not fall victim to changing climates.

Although data centers have come a long way in terms of capacity and efficiency, and despite an interest in pushing the state of the art, there is one thing that ensures a slower embrace of change than the rest of the network, and it isn't the fear and skepticism surrounding security. It is, as Alger said, a base conservatism of folks in the data center that's driven by the embrace of a more important factor: "The ultimate mission is to run and be available, so anything that can be accomplished with new technology is fantastic, but it must get in line behind availability."