

DELL EMC ENHANCES CLOUD SERVICE PROVIDER PARTNER PROGRAM TRACK

DUBAI: Dell EMC announced an enhanced focus and investment in the varied service provider industry that includes communications service providers, cable multiple system operators, hosting/co-location providers, public cloud providers, vertical market cloud specialists, and consumer webtech providers. The effort includes an expanded service provider track in the Dell EMC Partner Program and a new solutions engineering practice. As traditional enterprises shift investments to enable their Digital Transformation and cloud delivery models, they increasingly rely on modernized, flexible and agile service providers.

Adapting to this shift, service providers increasingly turn to common infrastructure building blocks of compute, storage and networking for multi-cloud services to increase their operational agility, speed time-to-service delivery, raise customer satisfaction and build differentiation into how they manage and operate cloud services. These building blocks - whether from Systems Integrators, Network Equipment Providers or infrastructure providers - must meet the industry's rigorous requirements and specifications.

Enhanced Cloud Service Provider Program Track
The Cloud Service Provider track in the 2017 Dell

EMC Partner Program features an expanded go-to-market engine, anticipating significant scaling of the Dell EMC partner ecosystem. Participating partners can leverage the program to create differentiated cloud services, shorten time-to-market and accelerate time-to-revenue. Key investments demonstrating the renewed Dell EMC commitment include:

Strengthened partner compensation benefits including predictable revenue-based rebates and access to both earned-and proposal-based business development funds. Enhanced rewards for cloud resale partnering between participants in the Dell EMC Partner Program Cloud Service Provider and Solution Provider tracks. Increased Dell EMC sales and marketing investments that expand the available sell-with and sell-out resources on behalf of service provider partners globally and regionally.

To complement the partner program, Dell EMC is also investing in a global solutions engineering practice to produce a wide range of tested and validated systems for various service provider use cases. The practice leverages Dell EMC's industry-leading compute, storage and open networking solutions, providing industry-standard building blocks for deployment at any scale from the customer edge to hyper scale data centers. Customers

can take advantage of Dell EMC Extreme Scale Infrastructure for tailored offerings, cloud-native architectural expertise and modular data centre designs.

The solutions integrate state-of-the-art, software-defined storage (SDS) and software-defined networking (SDN) from Dell EMC including ScaleIO and OS10 respectively, as well as SDS and SDN capabilities with partners. Dell EMC OEM customization capabilities and extensive partner ecosystem provide additional sourcing options to speed time to market. This flexible infrastructure base is combined with virtualization, automation and orchestration software from various ecosystem partners and the Dell EMC Service Assurance Suite, yielding highly scalable and extensible cloud infrastructure.

Service providers and their partners can leverage this infrastructure to host a wide range of workloads to modernize service delivery or support new service creation. The service provider solutions engineering practice will focus initially on network functions virtualization (NFV) solutions principally for communications service providers. For mobile operators, Dell EMC plans to introduce validated systems for virtual evolved packet core (vEPC) with Affirmed Networks and virtual IP multimedia subsystem (vIMS) with MetaSwitch Networks.



EEMNES: Prime Minister and VVD-leader Mark Rutte, 3rd right, attends the tv show *Koffietijd* with Loretta Schrijver, 2nd right, and Pernille La Lau, 1st right, in Eemnes, yesterday. —AFP

DITCH COMPUTERS TO SAVE DEMOCRACY DUTCH ELECTION'S RETURN TO PAPER AND PEN

UTRECHT, Netherlands: In an age of superfast computers and interconnected everything, the only sure way to protect the integrity of election results is to return to paper and pen. That is the view of Sijmen Ruwhof, an ethical or "white hat" hacker, who last month revealed that the Dutch election's commission computer software was riddled with vulnerabilities. In a shock announcement just weeks before the March 15 elections - seen as a bellwether of the rise of far-right and populist parties across Europe - Dutch officials announced they were abandoning the computer system in use since 2009 to return to counting ballots by hand.

It was Ruwhof who discovered the problem. At the request of Dutch broadcaster RTL he spent just one evening examining the OSV software, developed for the Dutch government by a German company, via an online YouTube explanatory video, finding 25 weak points. "It seemed to be completely insecure. I was quite shocked that we run our democracy, our election process based on very vulnerable software," he

said. Within days of the RTL report, the interior ministry announced ballots cast by the 12.9 million eligible voters would now be hand counted.

Then the head of the Dutch secret services (AIVD) made another stunning revelation - in the past six months there had been hundreds of attempted cyber attacks on Dutch companies and government agencies. Most were believed to have been carried out by Russian, Chinese and Iranian hackers. "It's a real challenge to stay ahead of the game," AIVD head Rob Bertholee said.

Weak spots

But these revelations, like the stunning news that Russian hackers appear to have meddled in the US presidential elections, were of little surprise to Ruwhof. As a 12-year-old he became fascinated by computers. Self-taught, he managed to hack into the school computers and informed grateful teachers the system was insecure. That was 19 years and an information technology degree ago. Now 31, Ruwhof makes his living working for banks, government

departments, and major companies hacking at their request into their systems to expose their weaknesses.

"It's very easy," he insisted, without any smugness. But he remains frustrated that for many companies and organizations security is almost an afterthought. "Software systems are so complex nowadays that it's hard for a single IT person to comprehend the whole system. So nobody has the total picture of the system. As a hacker you just go by and you scan for weak spots and you always find something." The world has been lucky so far, because few terror groups like the so-called Islamic State have the capacity yet to unleash "cyber terrorism."

But imagine if from a computer far, far away malfeasants could snap the power grid, change the formula for purifying drinking water, or empty millions at once from bank accounts, undermining the financial system? And that it is not the worst scenario. "If you manage to manipulate election software, you can decide who runs a country, and that's a whole different impact," Ruwhof warned. —AFP

WHEN AMAZON'S CLOUD STORAGE FAILS, LOTS OF PEOPLE GET WET

NEW YORK: Usually people don't notice the "cloud" - unless, that is, it turns into a massive storm. Which was the case Tuesday when Amazon's huge cloud-computing service suffered a major outage. Amazon Web Services, by far the world's largest provider of internet-based computing services, suffered an unspecified breakdown in its eastern US region starting about midday Tuesday. The result: unprecedented and widespread performance problems for thousands of websites and apps.

While few services went down completely, thousands, if not tens of thousands, of companies had trouble with features ranging from file sharing to webfeeds to loading any type of data from Amazon's "simple storage service," known as S3. Amazon services began returning around 4 pm EST, and an hour later the company noted on its service site that S3 was fully recovered and "operating normally."

The concentrated cloud

The breakdown shows the risks of depending heavily on a few big companies for cloud computing. Amazon's service is significantly larger by revenue than any of its nearest rivals - Microsoft's Azure, Google's Cloud Platform and IBM, according to Forrester Research. With so few large providers, any outage can have a disproportionate effect. But some analysts argue that the Amazon outage doesn't prove there's a problem with cloud computing - it just highlights how reliable the cloud normally is.

The outage, said Forrester analyst Dave Bartoletti, shouldn't cause companies to assume "the cloud is dangerous." Amazon's problems began when one S3 region based in Virginia began to experience what the company called "increased error rates." In a statement, Amazon said as of 4 p.m. EST it was still experiencing errors that were "impacting various AWS services." "We are working hard at repairing S3, believe we understand root cause, and are working on implementing what we believe will remediate the issue," the company said.

Why S3 matters

Amazon S3 stores files and data for companies on remote servers. Amazon started offering it in 2006, and it's used for everything from building websites and apps to storing images, customer data and commercial transactions. "Anything you can think about storing in the most cost-effective way possible," is how Rich Mogull, CEO of data security firm Securosis, puts it. Since Amazon hasn't said exactly what is happening yet, it's hard to know just how serious the outage is. "We do know it's bad," Mogull said. "We just don't know how bad."

At S3 customers, the problem affected both "front-end" operations - meaning the websites and apps that users see - and back-end data processing that takes place out of sight. Some smaller online services, such as Trello, Scribd and IFTTT, appeared to be down for a while, although all have since recovered. The corporate message service Slack, by contrast, stayed up, although it reported "degraded service" for some features. —AP