Nominee: Databarracks

Nomination title: Cyber-DRaaS

By combining its experience of over 13 years in the DRaaS business with its knowledge of security and cyber attacks, Databarracks has bought a new, innovative, exciting and unique cloud security service to market with Cyber Disaster Recovery as a Service (Cyber-DRaaS).

Cyber-DRaaS combines Databarracks' DRaaS solution, underpinned by Zerto, with Trend Micro's Deep Security Platform to offer the fastest, secure recovery from ransomware. The recovery window is extended and frequent automated recovery and malware scanning is performed. Customers have access to a portal where they can view their last 'clean' snapshot to recover to. In the event of a new malware signature being identified after the first scan, Databarracks runs recursive checking to quickly find the most recent snapshot that has not been infected. This means that not only does the solution provide the fastest recovery time, it can also find the most recent clean recovery point, minimising both downtime and data loss.

Cyber-DRaaS provides the rapid Recovery Time Objectives (RTO) delivered by its award winning DRaaS solution, with the added protection from ransomware attacks. Traditional DR is not optimised for cyber threats and ransomware is currently the most prevalent threat to cyber security. Cyber-DRaaS identifies issues in a customer environment and helps identify the last 'clean point' to roll back to and spin up and operate on a clean version of the customer's servers in the Databarracks' DR environment.

Cyber-DRaaS from Databarracks provides a unique RTO for its customers. With many of its clients being in strictly governed industries, where compliance and security can be overwhelming, one of the biggest fears is the threat of ransomware. By creating a managed service specifically to mitigate this fear is the key innovation behind Cyber-DRaaS from Databarracks. Until now, successful recovery from ransomware could only be achieved through restoration of backups rather than the much faster recovery from replicated snapshots. The problem with ransomware, like any malware or technical issues like a database corruption, is that the issue is copied from the live production system to the replica. Cyber-DRaaS allows recovery from replicated snapshots that have been scanned and proven to be clean – therefore significantly reducing the time for a recovery and the amount of data lost.

The launch of this service has also secured Databarracks' inclusion, again, in the Gartner DRaaS magic quadrant published June 2016. And as a further measure of success, following Databarracks' briefing with industry analysts, Gartner has included in its "10 Strategic Questions to ask potential DRaaS Providers" guidance to listen for "…responses that not only address immediate proactive-related needs such as typical two-factor authentication, DRaaS internal and external password policies, and malware testing on the replicated data — but also those areas where the provider expects to add value toward integrating hybrid cloud management and minimising impact of data breaches and ransomware, such as CryptoLocker or CryptoWall." From Gartner Research Note GU00302860 written by Ron Blair and John P. Morency 23rd March, 2016.

One customer in particular, Magrath LLP, protects their global infrastructure with Databarracks Cyber-DRaaS. Magrath LLP is a leading practitioner of immigration and employment services specialising in assisting corporations and private clients to relocate high-value individuals around the world. It has established itself as the legal brand of choice amongst its prestigious roster of clients. With high-value clients across a number of different time zones – many of whom keep incredibly busy schedules – Magrath need to be ready to provide time-sensitive services whenever they're required. Their IT systems must fundamentally enable a reliable, speedy response and as they continue to globally expand, they need to strategically choose partnerships and services that will support that growth. As their head of IT and facilities stated, "The problem we have is that although we can put in preventative measures to stop ransomware at the perimeter, some will get through and, at that point, we are always subject to the human error of users." Historically, Magrath were using an on-site appliance to take snapshots of their environment for DR, and off-site storage for their tape-based backups. The issue with ransomware attacks is the issue is transferred from production systems to the replica, thus the only way to recover from them is backups. To recover their entire environment from backups would take far too long.

Cyber-DRaaS was a no-brainer for us. As we all know with cyber threats, there is no certainty and no way to guarantee we are 100% protected, so we have to take all necessary steps to prepare and protect ourselves."

From a technical standpoint, Cyber-DRaaS means having 2 different scanning engines, and as Magrath are scanning offline, they can do so far more aggressively than in their own production systems. "To recover from a ransomware attack without Cyber-DRaaS from Databarracks would take an uncomfortable length of time, so by using the service I know we're protecting ourselves in the best possible way."

Databarracks' support staff is 100% located in the UK, providing a free 24x7x365 service with freephone lines staffed by trained engineers. The engineers are all trained in the ITIL service lifecycle, which, alongside IS09001 and ISO27001, ensures consistently high quality IT service management.

As Databarracks' customer Magrath LLP commented, "Operationally, you're only ever as strong as your weakest link and using a supplier necessarily means broadening that risk, particularly for DR. Fortunately for us, Databarracks has been nothing but reliable. Their support team in particular is exceptional. I've called them in the past with technical issues well outside their stated remit, but they're always happy to assist and talk me through a resolution."

Another customer, previously affected by the CryptoLocker virus stated:

"We initially considered paying the ransom. The threat wasn't exactlyambiguous, in bold on the monitor "THE SERVER WILL DESTROY THE KEY AFTER THE TIME SPECIFIED IN THIS WINDOW. AFTER THAT NOBODY CAN, AND NEVER WILL, BE ABLE TO RESTORE FILES." We decided to contact Databarracks before making any decisions. From the minute he answered the phone, our engineer, Tom, knew exactly what to do. He was unequivocal: 'don't pay the ransom, we can get your data back for you.' Tom ended up giving us our get out of jail free card. He sent us our files back immediately so we could access them locally and then stopped the daily scheduled backups from running to prevent the encrypted files from overwriting our existing backups."

Why nominee should win

- Databarracks has bought a new cloud security innovation to market with Cyber-DRaaS. The vendors we've used to create this product have cited our use of their technology as innovative and unique, as no-one else is doing this. Also, we were asked by Gartner's continuity team to brief their security team as the intersection of continuity and security is of interest to them and also stated no-one else is doing this.

- Databarracks' DRaaS offering has been recognised by Gartner in their April 2015 and June 2016 DRaaS magic quadrant for its ability to execute and completeness of vision. Being included alongside global brands such as VMware and Verizon, is a testament to Databarracks' service offering, no other UK-only company was included.