SMB Solutions
CLOUD SERVICES

Security, Backups and Redundancy:

A Detailed View

Hi, my name's Richard Duffy and I'm the CEO of SMB Solutions Cloud Services.

One of the things we get a lot is people want us to explain a number of the different aspects of our cloud. We do have got a frequently asked questions page on our website, but what I thought I would do is a brief explanation so that way you get to hear it straight from the horse's mouth.

SMB Solutions
CLOUD SERVICES

Security

The first thing that people are concerned about is security, and they ask how you secure your cloud environment.

So, security is a bit like Fight Club – the first rule in Fight Club is you don't talk about Fight Club.
The first rule of security is don't talk too much about how you do it, but I will give you as much information as I can without giving too much away.

We actually utilise an integrated platform from Sophos and Sophos have a brand name for it called Sophos Synchronised Security.
So, what that does is that means that all traffic that comes in or out of our network passes through a Sophos XG Firewall.
Then, every single server inside our environment also runs Sophos InterceptX Endpoint Protection so that means that the firewalls and the servers are constantly talking to one another.

The Sophos components are monitoring all the traffic that occurs on those servers, checking for malicious behaviour, checking for malware, checking for viruses – not looking at your personal information, of course, but just keeping an eye to make sure there is none of that malicious activity happening, while it's constantly talking to the firewall.

So, let's say, for example, somehow somebody manages to get something inside our network, and it tries to infect a particular server. What immediately happens is the InterceptX shuts down the server, shuts down all the network connectivity because it's talking constantly to the firewall and the firewall says something's not right here, I haven't got the right security heartbeat, I'm going to shut down the connection.

So that happens instantaneously.

SMB Solutions
CLOUD SERVICES

Managed Detection and Response 24x7x365 from 4 Security Operations Centres around the world

Now, the other thing that we also do is we have a security operations centre that is part of what we use from Sophos, and it is called Sophos Managed Detection & Response, or MDR. I think the last count the guys told me there's about 160 security engineers working in locations all around the world, so there's 24/7 coverage.

So, what those guys do as well as us managing and monitoring our own systems, they are also monitoring our systems for security incidents and security breaches, anything that looks out of the ordinary and abnormal, and they swing into action if they detect something immediately.

They can either call us and we can work on it together, or let's say they can't get hold of someone from our team, they're actually able to go ahead and make the necessary corrective actions to respond to the breach.

So, it's a very well-architectured, well-engineered security infrastructure, and of course, we follow all the standard processes you would expect.

We keep our servers and operating systems patched and up to date – of course we have cybersecurity insurance and one of the things we need to do to keep that cybersecurity insurance is make sure all our machines are patched within a week of those patches becoming available, so we are constantly doing that.

SMB Solutions
CLOUD SERVICES

Multi-Factor Authentication

The other thing that we also do is we utilise multi-factor authentication. Those of you reading this that are already on our cloud will be familiar with the Cisco Duo multi-factor authentication platform that we use.

So anytime anybody signs on whether that's you as a customer or one of our people inside our organisation, they have to prove that they are who they say they are by using that multi-factor authentication.

So, no one signs on to any servers in our environment without that MFA. We believe it's a great combination of those different aspects, and of course, all our servers are kept in a state-of-the-art data centres; in Sydney, Australia we use Equinix SY4 and SY3. In Munich, Germany we use Equinix MU4. In Los Angeles, USA we use Equinix LA3.

There's a video tour of the SY4 environment so you can see what happens from a security perspective there and I would encourage you to take a look at that because nobody can get physical access to our servers except myself and my team.

So again, you have all those different levels of control in place.

SMB Solutions
CLOUD SERVICES

Data Backups

Let’s talk for a second about backups.
So, we have in excess of about 250TB of storage available in our environments. We have storage in our main data centres, and then we have storage offsite.

So, what happens is that every day your databases are backed up, those backups are then also copied to another offsite backup location and then they’re copied to another backup location using what’s called immutable storage.

This is a technology that means no one, not even me with the root user password, can go and touch those backups for at least 7 days – that’s how we have set it up.

So effectively that means if all of those other systems fail, and somebody gets inside our system and decides they want to run an encrypting malware attack where it tries to go through and encrypt all our information, our backups cannot be touched.
I can’t even go in and delete them as the root user.
You probably know root user is like the God user in a Linux environment.

That’s your databases - so they’re backed up, they’re encrypted, and stored in 3 different locations, including 1 location offsite as immutable storage.

SMB Solutions
CLOUD SERVICES

Veeam Backup and Replication

The next point is that every single one of our servers every night is backed up with a product called Veeam; this is not an advertisement for Veeam, but we have been using it for years, highly recommend it and I swear by it - it has never let us down.

We use Veeam and what it does for every single server, every night it does a bare metal recovery snapshot so that means that at any point in time if one of those servers fails, we can rebuild it in 10 minutes from that bare metal recovery snapshot.

I won't go into the details of how Veeam does it but it's pretty clever, we have very powerful servers that we run all these virtualised environments on, so I can bring that back from the backup and within 10 minutes, that server is back up and running again.

So that's an important aspect, again all those backups stored onsite, then stored offsite and then stored offsite again in that immutable storage.

Hopefully that answers the questions about the backups.

SMB Solutions
CLOUD SERVICES

Data Encryption

Not only do we do that but all of our servers, all of that backup data is encrypted at rest.

Whether it's HANA or SQL Server, all your data is constantly being encrypted – the backups are encrypted and the actual data itself in the data files are encrypted.

So if somebody managed to get hold of one of those data files, they can't just take it and restore it onto another database server together with their sa password and access the data because they're all secured with these encryption keys.
So that's another important point.

SMB Solutions
CLOUD SERVICES

Redundancy

The next thing I wanted to talk about is what we do from a redundancy perspective. I mentioned before we use 3 data centres, SY3 and SY4, and they're connected between the 2 data centres with 60GB of fibre connectivity so that means it's very quick and easy for us to transfer data back and forth between those locations.

We have a complete set of redundant servers in that second data centre. Not only do we have redundancy at the data centre level but all the servers we use are DELL servers and they are enterprise-level servers.

For those of you that know about these things and find them exciting, like I do (which is a sad commentary on my life), they have multiple levels of redundancy – redundant power supplies, redundant hard disks and so on and so forth.

If at any time, any of those components fail, we can immediately move those workloads on that server across to another server and the warranty that we have with DELL is a 4-hour mission critical. - they send a service technician into the data centre with the replacement parts within 4 hours.

But again all of those replacement parts have redundancy so you should see no interruption at all if we do have a hardware failure.

SMB Solutions
CLOUD SERVICES

SLA (Service Level Agreements)

Again, thinking about all those things I've been talking for a while now and covered a lot of different areas but hopefully, you now understand how we address the issues of security, how we address the issue of backups, and what do we do about redundancy.

So we have a service level agreement that specifies what you can expect your uptime and availability to be and of course, at any point in time you can visit our Status Page site
status.smbsolutions.com.au
where you can see the status of all of our services at any point in time and you can see if there have been any incidents.

When we have an incident or an issue, after that we write a postmortem and explain exactly what happened, if it was something we have control over and what have we done to prevent this from happening again.

Transparency about what we do as a cloud provider is very important so that extends out to the use of that Status Page.

Lots of other information you can find on our website –
www.smbsolutions.com.au

SMB Solutions
CLOUD SERVICES

Hopefully, you found this little summary a bit different rather than reading through frequently asked questions, maybe you might be sitting there wishing you had read the webpage instead.

If you have any additional questions, feel free to reach out to us.

My email address is

richard@smbsolutions.com.au

and of course, you can use the contact form on our website if you want to ask any more questions.

Or if this sounds like a great environment and you're thinking I would love to have my SAP Business One hosted in an environment like that, reach out to us – we would be more than happy to talk to you!

Thanks very much for your time and look forward to talking with you again soon.