How SQL 2016 Helps the Modern Enterprise Combat Cyber Security Threats

Not all databases are created equal. Kate Bevan looks at what sets SQL Server 2016 apart from the crowd.

With data thefts happening almost every day, and many of those hitting the headlines, the risk that a database could be hacked should be at the forefront of every CIO’s mind. The words “Panama Papers” alone should be enough to make anyone tasked with database security break out in a cold sweat. As Christopher Wilder, senior analyst at US firm Moor Insights says, “Nobody wants to be on the front page of the Wall Street Journal.”

What we know about the Panama Papers theft was that it was a database containing 11.5m files from the world’s largest offshore law firm, Mossack Fonseca. Those files revealed the tax affairs of a number of high-profile individuals, from the iconic film director Stanley Kubrick to the Duchess of York.

More recently, according to Gemalto’s breach database, 5 million records from the US Office of Child Support Enforcement were stolen in May, while Fling, an adult dating website, suffered the loss of 40 million records at the beginning of June.

Altogether, more than 700 organisations around the world have suffered data breaches so far this year, mostly the result of hacks by malicious outsiders.

Meanwhile, the final signing-off of GDPR, the EU’s new data protection framework, means that even without the healthy fear any CIO should feel when looking at breach statistics, the C-suite should be considering their current security set-up, not least because fines for a breach under GDPR could be as high as 4% of global turnover.

This is where all eyes turn to the software and services being used by enterprise, and particularly to database, client applications and most importantly, how data is stored, transferred and accessed.
Harnessing the power of the cloud

Microsoft’s SQL Server 2016 is making some major strides towards solving some of those problems, with new features that address many of those issues.

That the new features in SQL Server 2016 specifically harness the power of the cloud shouldn’t come as a surprise – moving enterprise customers away from on-premises systems and boxed software into its Azure services has been a key plank of Microsoft’s strategy for some time.

There were a lot of challenges about how you manage data in motion, and Microsoft has done a very good job of turning that around.”

Christopher Wilder

One important new feature is AlwaysEncrypted, which performs the encryption and unencryption of data in the client application, which means that the data in the server application is not visible. While this applies both to the on-premise SQL Server 2016 as well as to Azure SQL Database, this is clearly a big part of Microsoft’s strategy to move customers to the cloud.

Moving to the cloud has always been fraught with dangers for chief technology officers, as it means handing over control of your data to a third-party provider – with all the risks that entails. While due diligence should ensure that a cloud provider is as safe as it can be, in practice it’s almost impossible to ensure that your data is totally secure.

Previous versions of SQL Server could handle the encryption requirements, but all three parts of that -
column-level encryption, encryption at rest and encryption in transit – had to be configured separately, which of course left plenty of room for errors that hackers could later exploit.

AlwaysEncrypted adds a reassuring extra layer of security to the data you have stored in the cloud: even if the cloud provider is breached, hackers won’t be able to decrypt the records held there as the encryption key is held in the client application – it’s never passed to the database. That alone should slow down hackers looking to exploit an insecure database.

“That’s a pretty significant layer on top of the basic encryption piece,” notes Wilder, adding: “There were a lot of challenges about how you manage data in motion, and Microsoft has done a very good job of turning that around.” He adds: “IBM’s DB2 has always been pretty good at that, but Oracle is still suspect from a security perspective.”

This is where the next new piece of SQL Server 2016 comes into play – Stretch Database. This allows you to move data between the cloud and local databases, and to be accessed by client applications both locally and in the cloud, with the data encrypted as it moves between database and application and cloud and local storage.

This should help enterprises manage the difference between “hot” and “cold” data better – it’s generally thought that only about 10% of an organisation’s data is “hot”, ie active. The usual practice is to stash “cold” data in offsite storage, where costs are reduced, and keep active data onsite, with all the attendant costs of infrastructure, maintenance and support.

For enterprises that need to access both types of data, it can be easier, but more expensive, to keep it all onsite. Stretch Database means that you can differentiate between your active and “cold” data to manage your IT costs better while still being able to access the inactive data when you need it, say for analytics purposes.

The downside of this new approach, however, is costs: while it’s not particularly expensive to stash data in the cloud, Azure starts to look more costly if you end up processing the offsite data you access via Stretch Database.

“Nobody wants to be on the front page of the Wall Street Journal.”

Christopher Wilder
New in SQL Server 2016 is Row-Level Security, which provides granular access to any row in the database, with the security manager able to define in advance who can see what. Wilder says this new feature “is a really neat thing – it allows you to be more flexible with analytics and how you manage large databases, particularly with IOT [Internet of Things] security”.

He adds: “That’s one of the challenges that a lot of the public cloud – Google, Amazon and Microsoft – have had to fix, which is how do you take all this information and not just blast it back to the datacentre, but also secure the data and move it around. This is where Microsoft has a good opportunity to be a leader.”

Also new is Dynamic Data Masking, which means you can make sure data is protected in the client application. So for example, you might store credit card numbers in full but not want to make the full number available to help-desk staff, instead showing them, say, only the final four digits. Dynamic Data Masking means you can set rules to manage that masking, protecting sensitive customer details while at the same time enabling staff to support them.

The Internet of Things is just one area creating an explosion of data to be mined for insights: social media, store cards, memberships, what your browser reveals about you, who you call, where Uber takes you, where you shop and what you shop for are all datapoints that can help businesses. “All the database products are about the same, but everyone is moving towards doing more sophisticated analytics,” says Wilder. He adds: “This is where Microsoft may be able to take the lead a bit ahead of everyone else.”

“The weakness of database products is that they can be difficult to use,” adds Wilder. “Microsoft is starting to address that with the Polybase connectors – they’ve made it a bit better and a bit more straightforward.”

Polybase, which is now part of SQL Server 2016, means not only do you not have to
buy the connectors to analytics engines such as Hadoop or SQL Azure blob storage, you can pull the data natively and then query it on the fly.

Analytics clearly isn’t new with databases, but Wilder says while “everyone is about the same, moving towards doing more sophisticated analytics, this is where Microsoft can take the lead ahead everyone else. It’s what you do with that data and how you manage it and push it into applications that will separate them” – and having native tools rather than third-party additions will also help make databases and the way the data is handled more secure.

As well as contributing an explosion of data to be managed, stored and queried for insights, the Internet of Things has also created a whole new raft of security issues. Independent security consultant Graham Cluley observes: “The foundation of the Internet of Things should be to start by making devices secure, and then making them useful. I worry that these devices will be made cheaply, and not with the future in mind.”

One area of particular concern with IoT devices is those devices that generate data from sensors which is sent to the cloud for processing – machine-to-machine, or M2M data. This data isn’t subject to the same detailed protections as personally identifiable data, and so the temptation for manufacturers is to take less scrupulous care. Wilder is particularly concerned about this:

“The number of attacks isn’t going to go down, they’re just going to be moved to different points, and IoT creates a lot of problems.”

Wilder also has concerns about the public cloud and how providers of consumer services deliver on security. “They talk the game of security but in practice they’re not walking the talk. A lot of enterprises won’t go near the public cloud.”

So it’s very much in the interests of enterprise to consider moving to SQL Server 2016 – not only will it make it easier to secure data, access it and run analytics on it, moving to SQL Server 2016 could be a key differentiator when it comes to marketing services, too, both to other businesses and to consumers.
Opening up to open source

One final thing to note is that SQL Server is also coming to Linux, so organisations that have gone down the open-source route rather than sticking with proprietary operating systems will also be able to benefit. Wilder is excited about this, pointing out that the open-source community brings further expertise to the table.

With the problems of IoT, he says, “I think the open-source community will help fix this. There’s a lot of group thinking to solve specific problems that you can’t do with proprietary stuff. They already have the mindset; they know what methods the bad guys are using and they’re already starting to put out security patches.”

With any significant upgrade to a big product, take-up is bound to be slow, but Wilder reckons the growth area for Microsoft – and one that will benefit businesses not yet using SQL Server – will be from Oracle users who take up the offer of free licences if they switch to SQL Server 2016. Judson Althoff of Microsoft said back in March: “For every instance of Oracle you have, free SQL Server licences.”

There is of course a catch: “All you have to do is have a Software Assurance agreement with Microsoft. If you take this journey with us before the end of June, we’ll actually help and invest in the migration costs, put engineers on the ground to help you migrate from Oracle.”

With that introductory period nearly finished, it remains to be seen how many Oracle users will have made the leap. If it has been successful, those businesses will be in the first wave of organisations seeing the dawn of better and easier to manage security built in to SQL Server 2016.

Kate Bevan is a technology writer and broadcaster with more than 25 years of experience of working for, among others, the FT, the Guardian, the Daily Telegraph, the BBC, ITN, Channel 5 News, Sky News and Al Jazeera. She is interested in all things technological including data protection, IoT and social media.