Microsoft

Azure SQL

Crystal Tenn
Crystal.Tenn@microsoft.com

MICROSOFT CONFIDENTIAL

The Basics

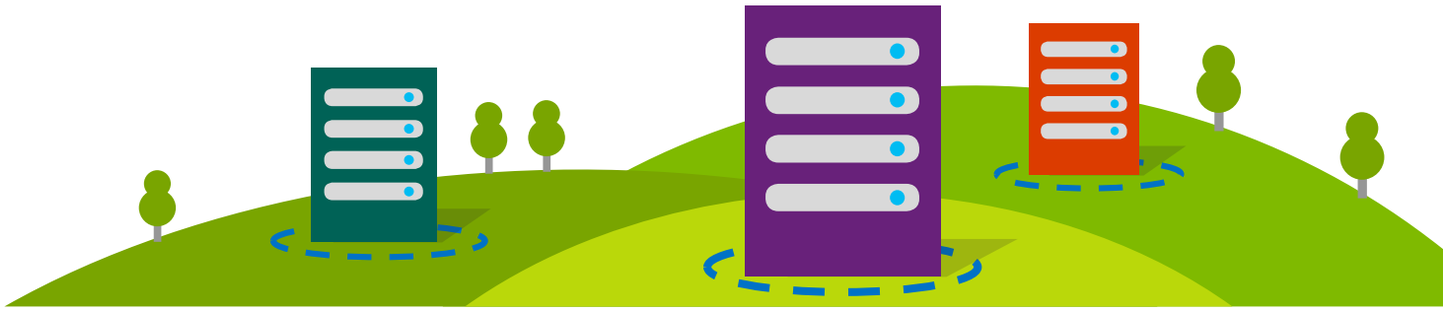
- PaaS
  - SQL Database technology as a service
  - Fully managed
  - Enterprise-ready with automatic support for High Availability
  - Designed to scale-out elastically with demand
  - Ideal for simple and complex applications
  - Three copies of the database for the cost of one database - always in sync

MICROSOFT CONFIDENTIAL – INTERNAL ONLY

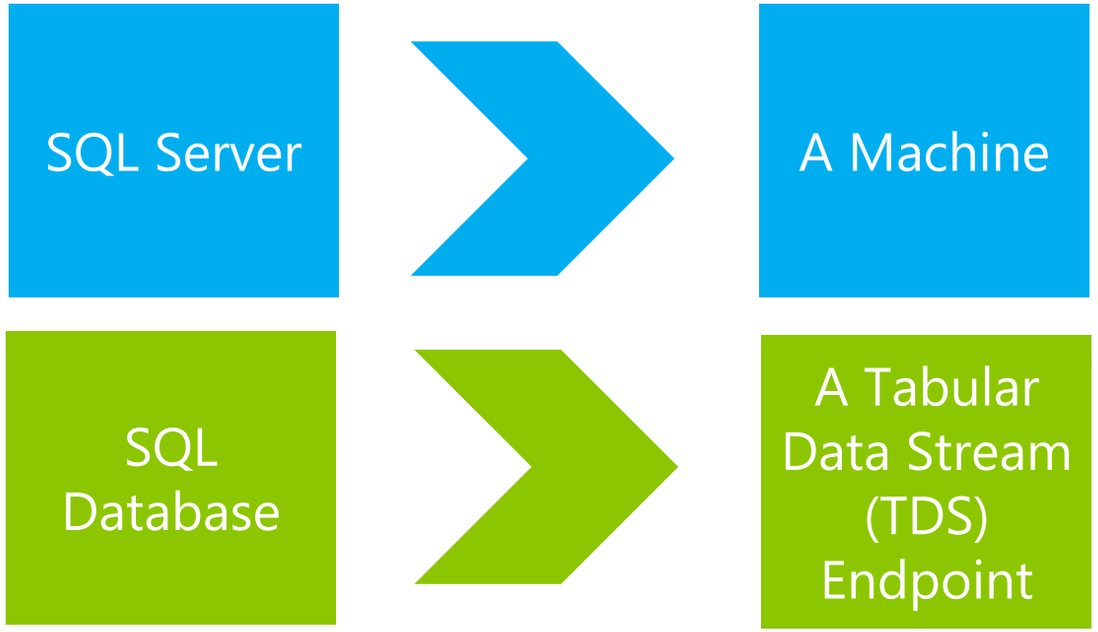
SQL Database Service

- A relational **database as a service**, fully managed by Microsoft
- For cloud-designed apps when **near-zero administration** and **enterprise-grade** capabilities are key
- Perfect for cloud **architects and developers** looking for programmatic DBA-like functionality

Elastic Scale and performance	Business continuity and data protection	Familiar and self-managed
Predictable performance levels	Self-service restore	Familiar & compatible
Programmatic scale-out	Disaster recovery	Programmatic
Dashboard views of database metrics	Compliance-enabled	Self-managed



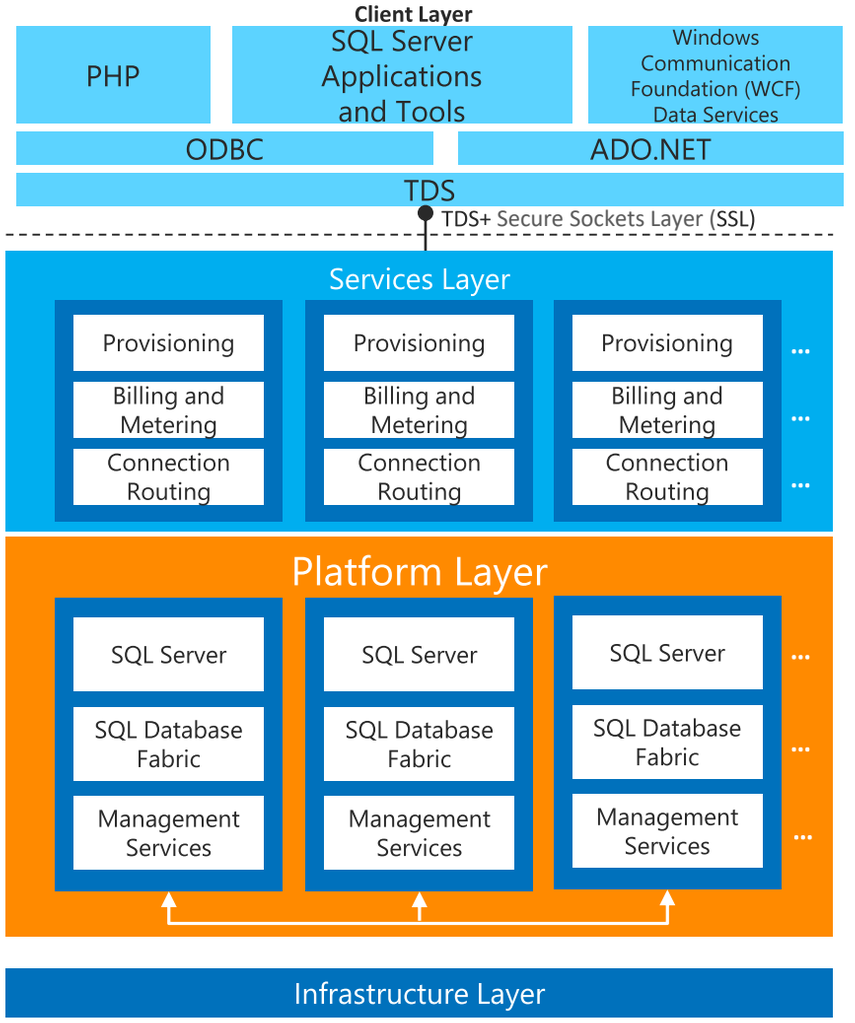
An *Azure SQL Server (SQL Database)* Is Not a Machine



Microsoft Confidential

How It Works

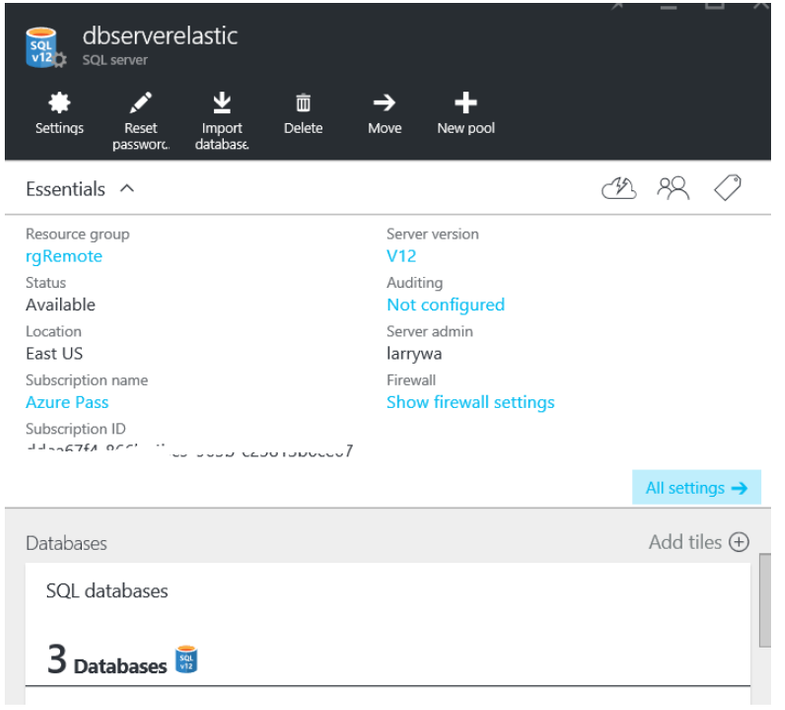
- Architecture
  - Client layer—used by application to communicate directly with SQL Database
  - Services layer—gateway between the client layer and the platform layer
  - Platform layer—includes physical servicers and services that support the services layer
  - Infrastructure layer—IT administration of the physical hardware and operating system

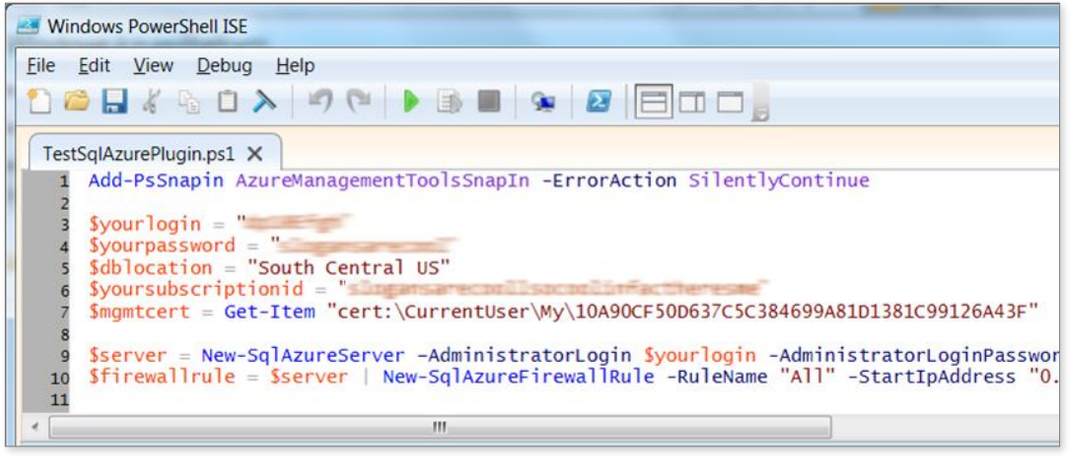


Microsoft Confidential

Server Provisioning

- Server defined
  - Service head that contains databases
  - Connect via automatically generated fully qualified domain name (FQDN) (xxx.database.windows.net)
  - Initially, contains only a master database
- Provision servers interactively
  - Log on to Microsoft Azure Management Portal
  - Create a SQL Database
  - Specify admin login credentials
  - Add firewall rules and enable service access
- Automate server provisioning
  - Use Microsoft Azure module for Windows PowerShell cmdlets (or use Representational State Transfer (REST) API directly)
  - https://www.windowsazure.com/en-us/downloads/?fb=en-us





Microsoft Confidential

Point-in-time restore

Automatic backup

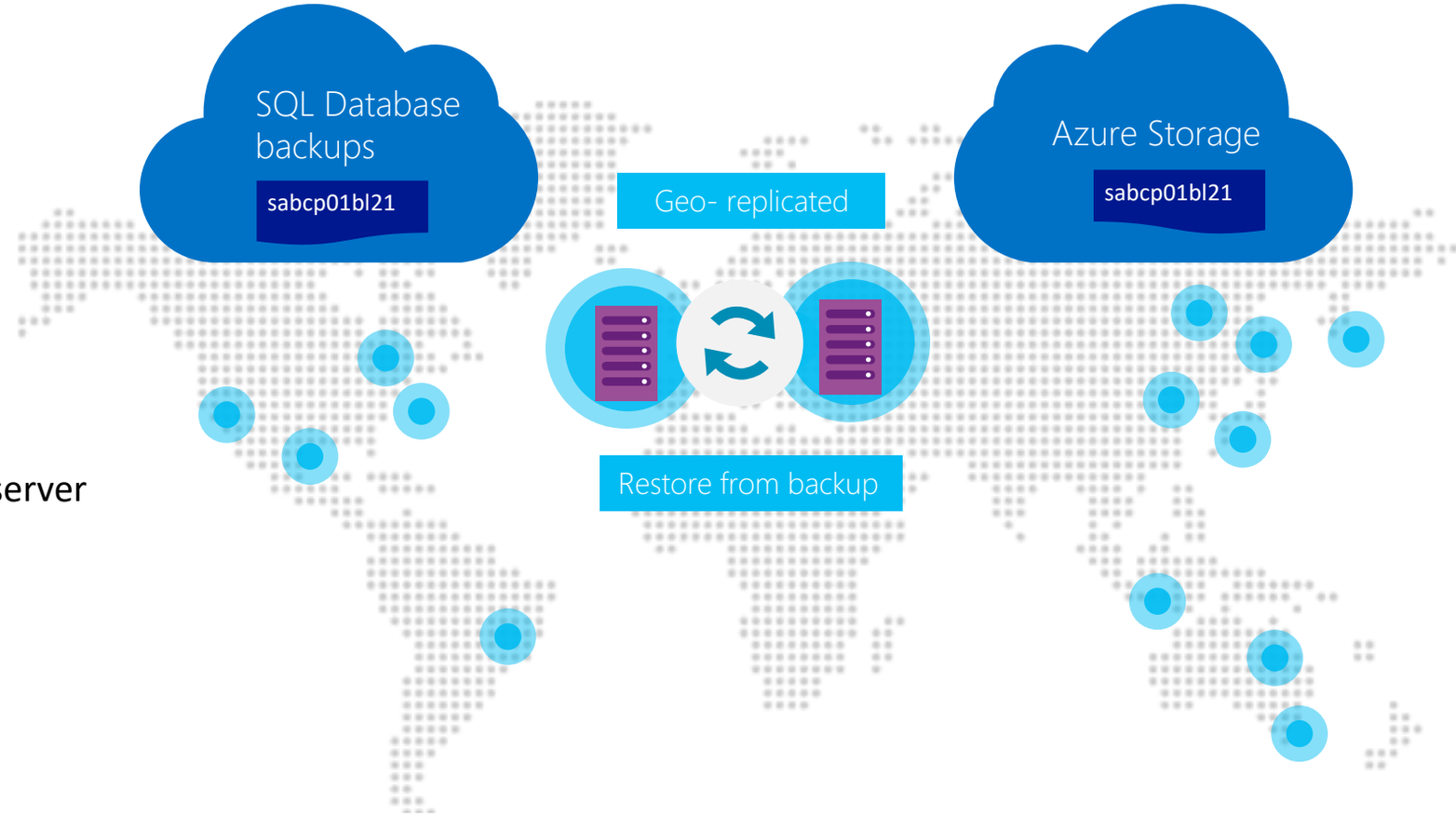
- Full backups weekly, different backup daily, log backups every 5 minutes
- Daily and weekly backups automatically uploaded to geo-redundant Azure Storage

Self-service restore

- Point-in-time up to a second granularity
- REST API, PowerShell, or Portal
- Creates a new database in the same logical server

Tiered retention policy

- Basic - 7 days
  Standard - 35 days
  Premium - 35 days
- No additional cost to retain backups

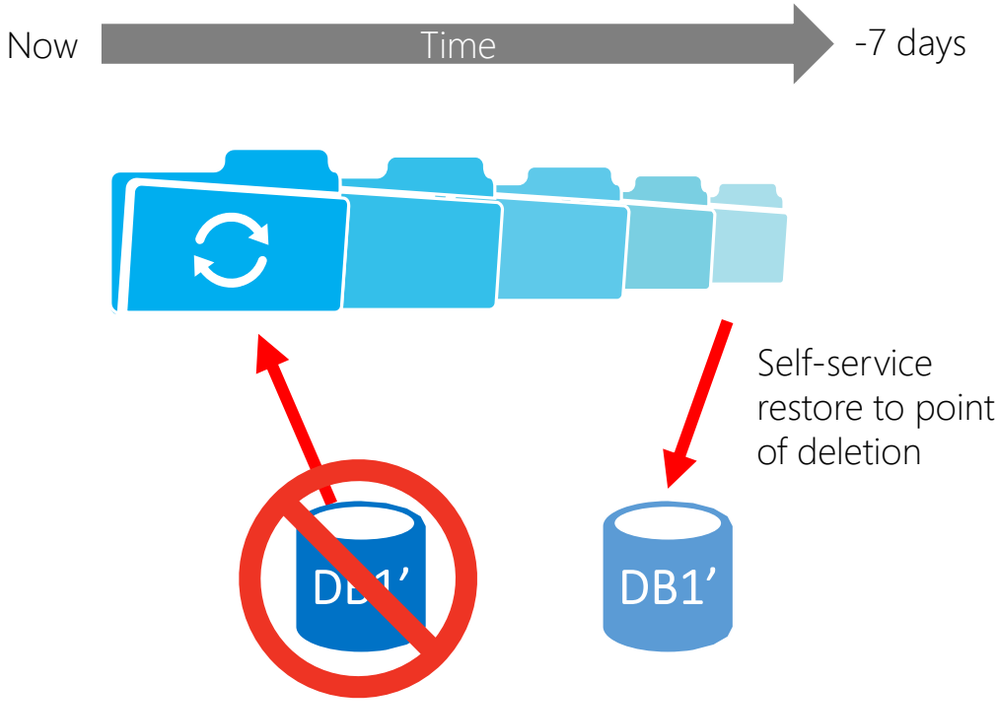


Restore deleted database

Recovery after accidental database deletion

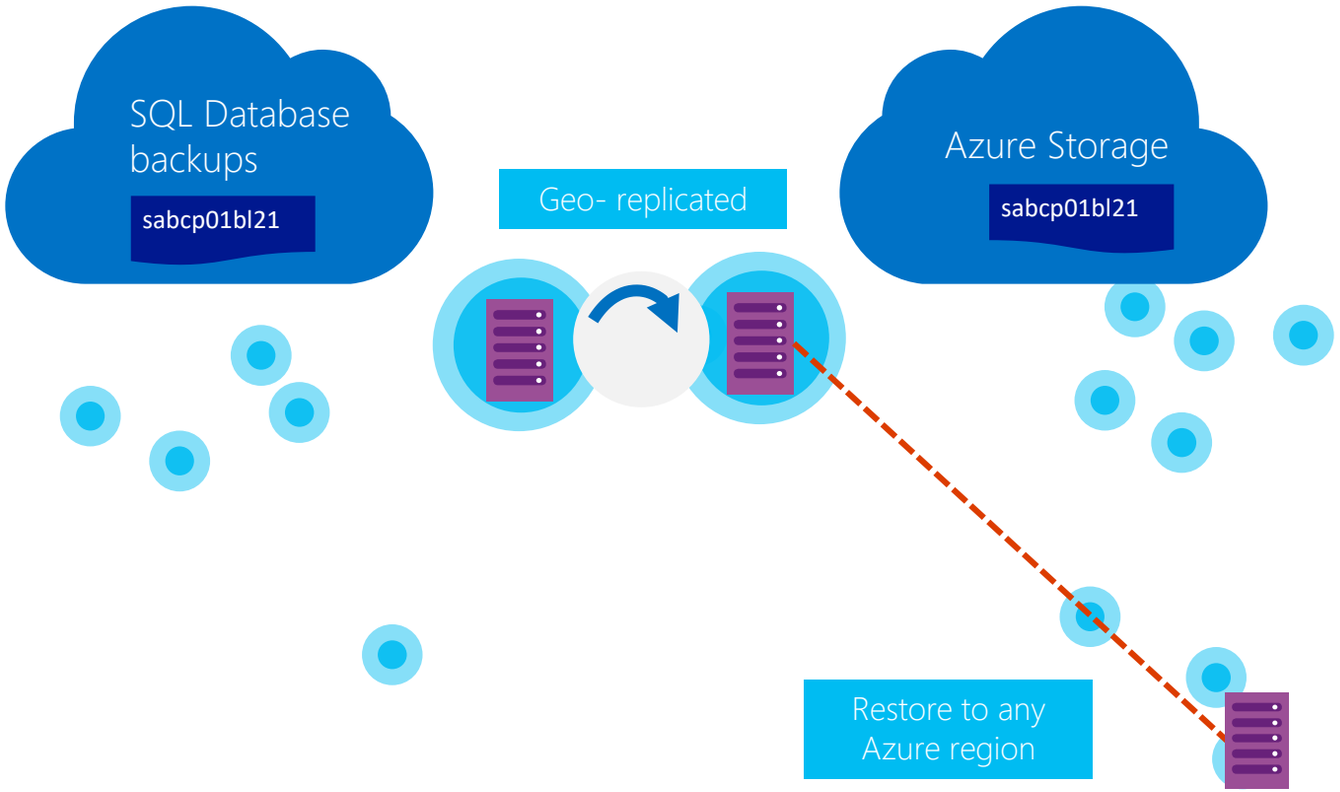
- Restores the database to the point of deletion
(earlier backups are deleted)
- Creates a new database on the server used by the original database
- You can choose to failover to the restored database or use scripts to recover data

Backups retained for 7/14/35 days



Geo-restore

- Self-service restore API
- Restores last daily backup
- No extra cost
- ERT >= 12h, RPO=1h
- Database URL will change after restore
- You will need to change your connection string to point to geo-replicated database



Database Transaction Unit – DTU

Bounding box

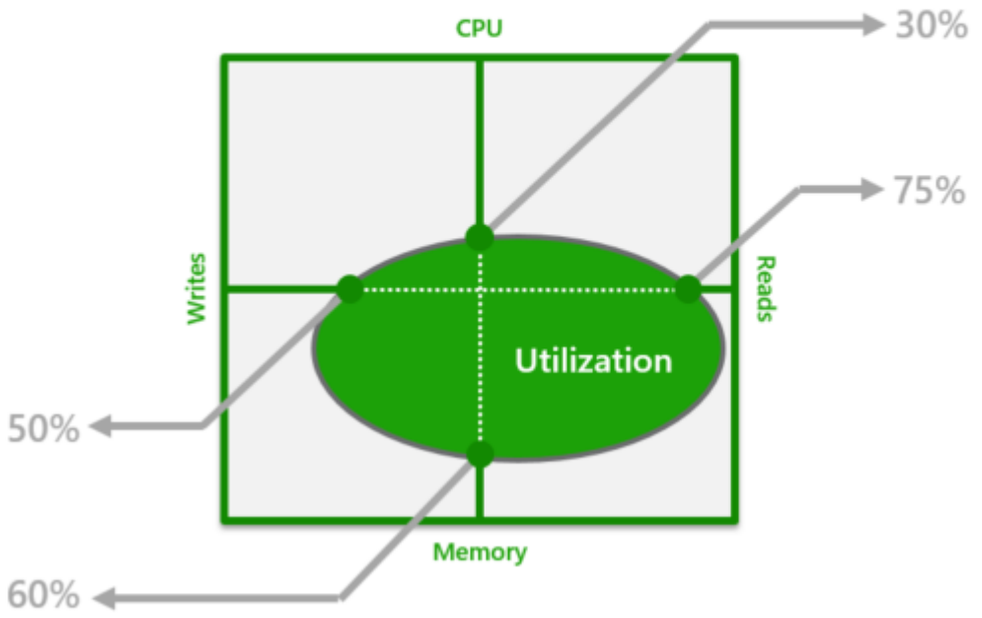
Monitoring database workload utilization within bounding box

Represents the relative power (resources) assigned to the database

Blended measure of CPU, memory, and read-write rates

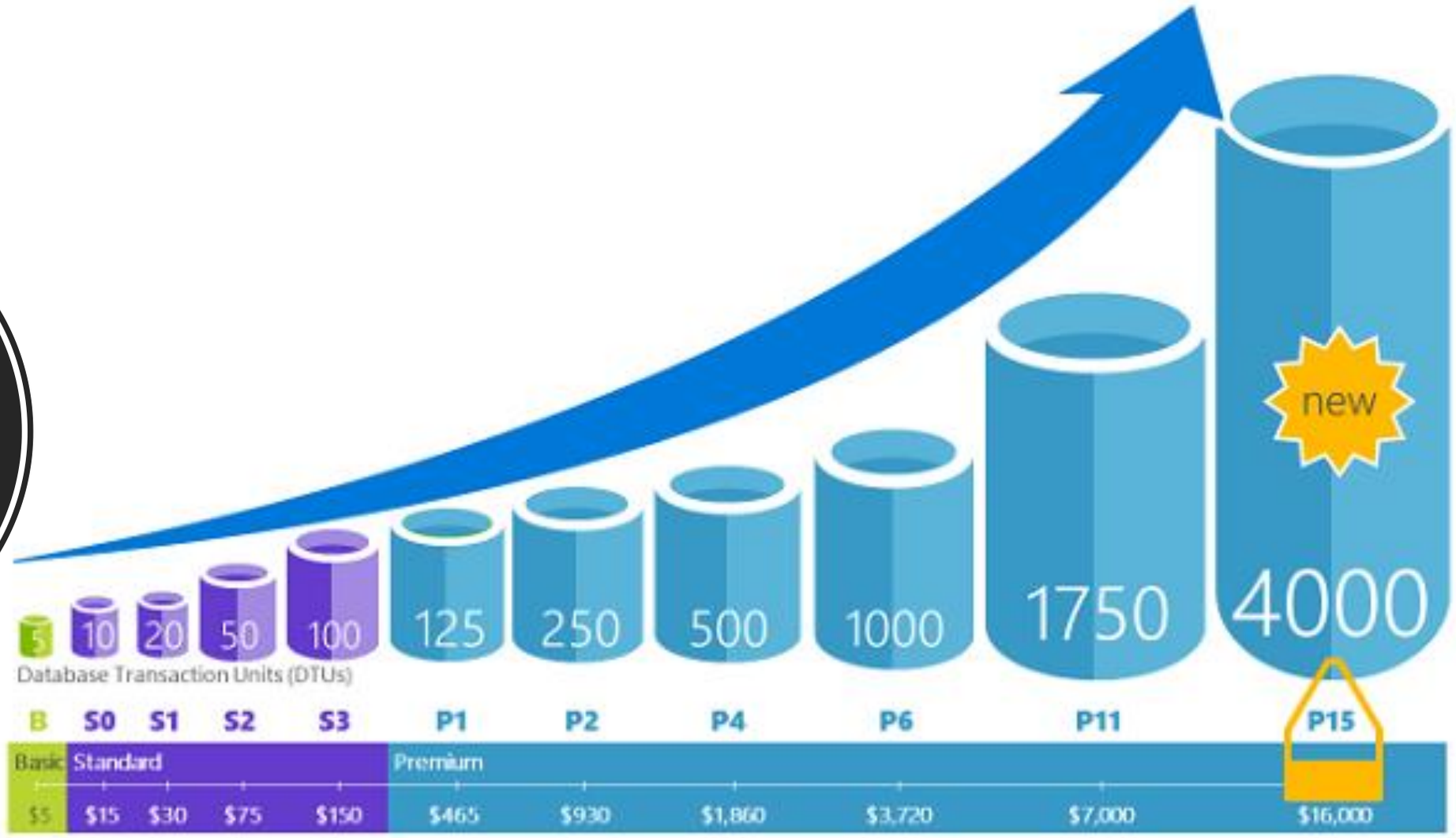
Compare the power across performance levels

Simplifies talking about performance, think IOPS vs. %



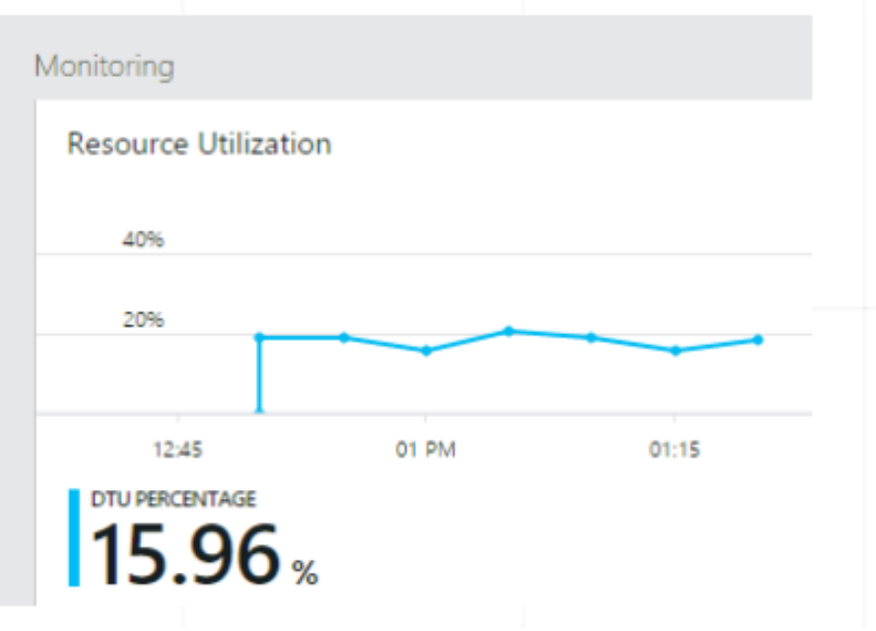
- DTUs provide a way to describe the relative capacity of a performance level of Basic, Standard, and Premium databases. DTUs are based on a blended measure of CPU, memory, reads, and writes.
- As DTUs increase, the power offered by the performance level increases.
- For example, a performance level with 5 DTUs has five times more power than a performance level with 1 DTU.

DTU Cost per month



Resource Monitoring

- Percentages relative to performance level
- master.sys.resource_stats
  - **Averages over 5 minutes**
  - All editions
- userdb.sys.dm_db_resource_stats
  - **Averages over 15 seconds**
  - Only Basic/Standard/Premium
- Accessible though Azure Portal
  - Allows to configure alerting!



What is scaling…

- Vertical scaling – easy, cost management, can be automated, not very “cloudy” – give me a larger machine
- Horizontal scaling – more “cloudistic”, also can be automated, multi-tenet databases, has tool support
- The ability to elastically scale databases and share resources
- Yellow pages sharding
- Multi-shard queries / multi-shard connections

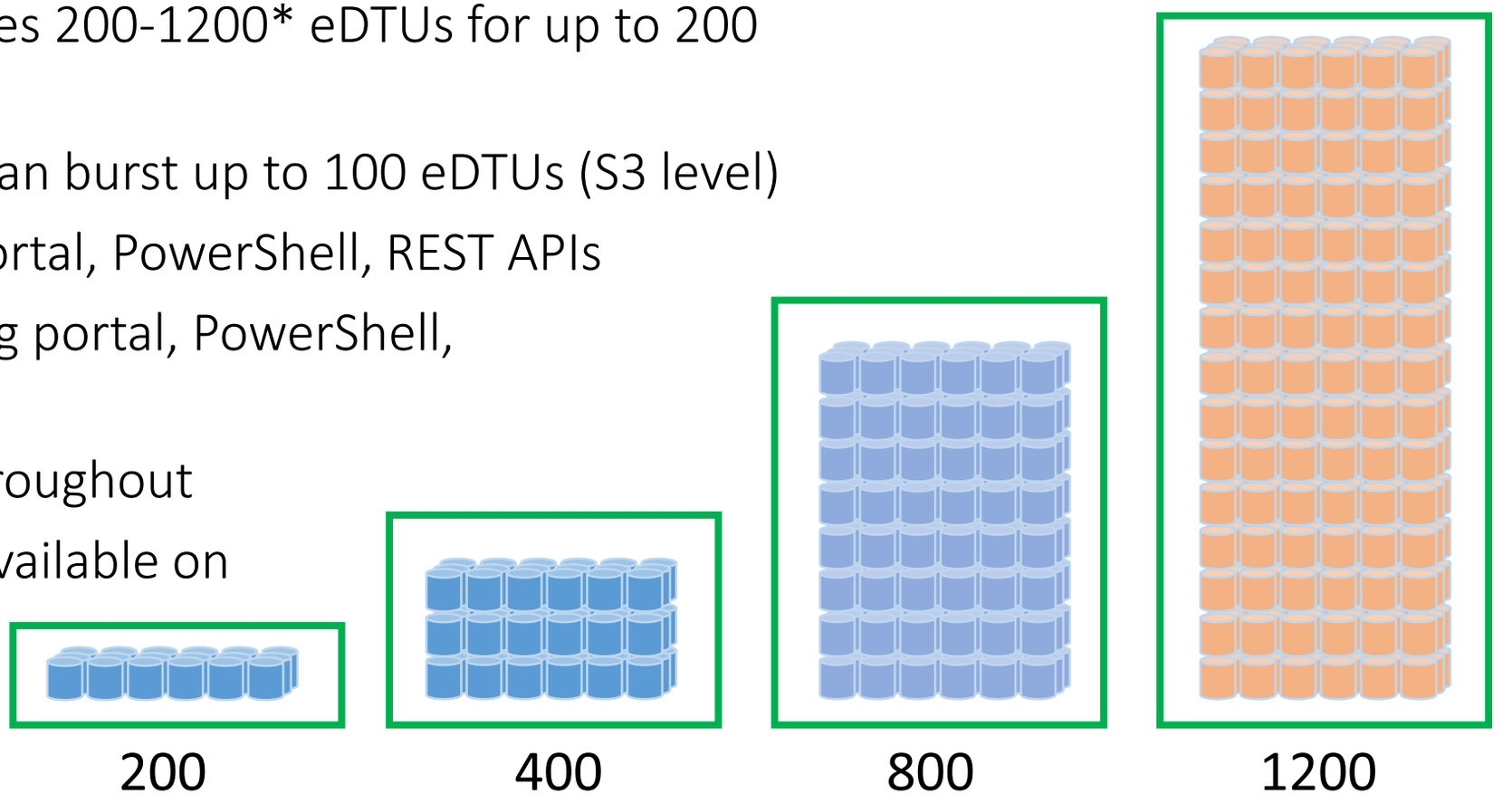
Microsoft Confidential

When is Elastic Scale the right consideration?

- Application workload can be partitioned across a number of scale units, and workload directed to each partition can fit into the biggest scale unit available
- Application workload doesn't contain large scans or aggregations that need to touch the entire data set
- Total capacity demands (CPU, IO, memory, storage) of the application exceed the hard limits of a single Azure SQL Database scale unit
- Application requires on-demand or automatic policy-driven scale out or scale in
- Caveat: Typical data warehousing does not easily fit the patterns for Elastic Scale

Elastic Database Pools

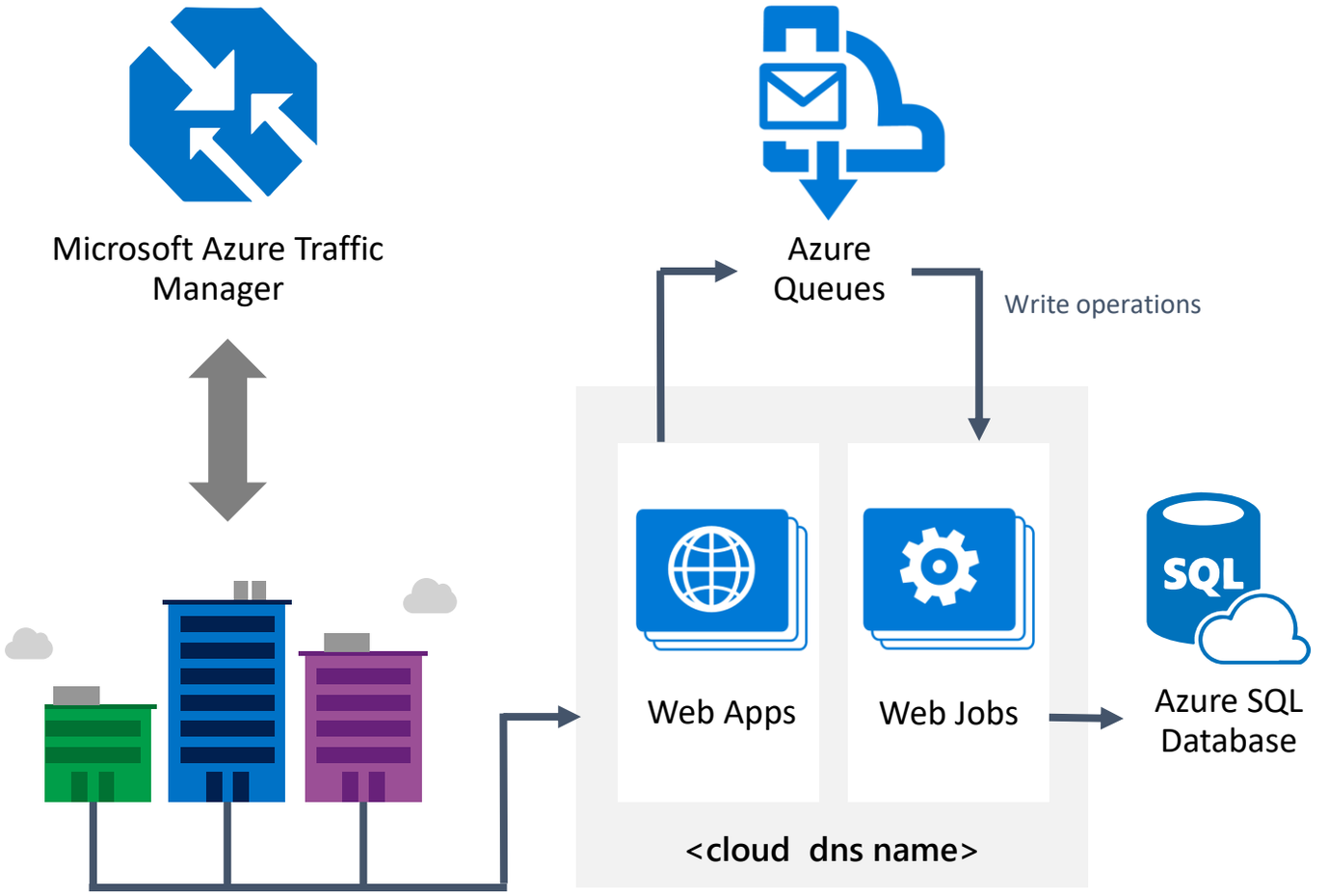
- Elastic databases, Elastic database pools
- Pooled resources leveraged by many databases
- **Standard** elastic pool provides 200-1200* eDTUs for up to 200 databases
- **Elastic Standard** databases can burst up to 100 eDTUs (S3 level)
- Create/configure pool via portal, PowerShell, REST APIs
- Move databases in/out using portal, PowerShell, REST APIs, T-SQL
- Databases remain online throughout
- Monitoring and alerting is available on both pool and databases



Microsoft Confidential

Canonical cloud app architecture

- Classic 3-tier enterprise architecture
- Required to scale to 10,000s of users and process terabytes of relational data
- Scaling out (and in, elastically) web and worker tiers is relatively easy



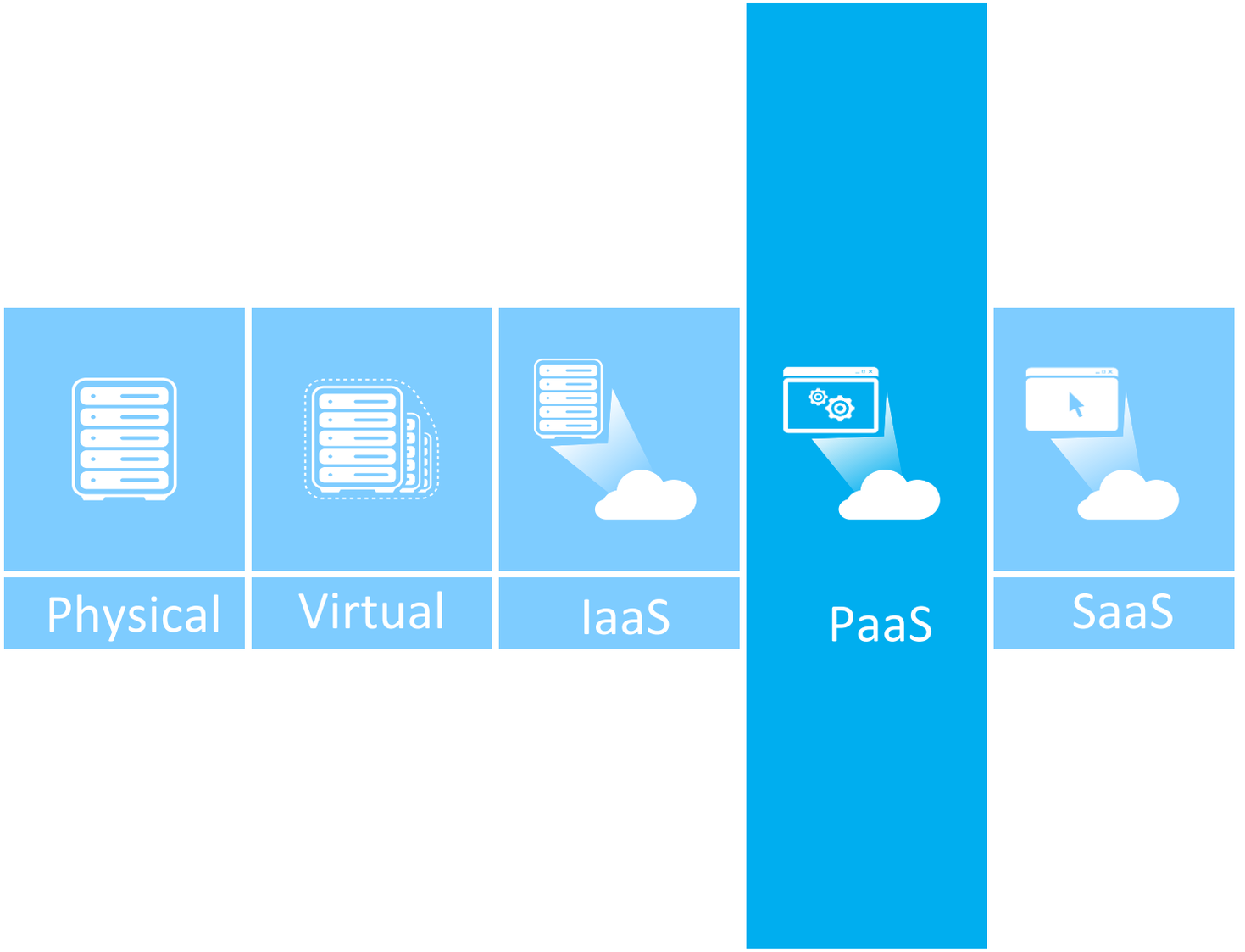
Microsoft

Azure SQL vs. SQL Server on VM

Crystal Tenn
Crystal.Tenn@microsoft.com

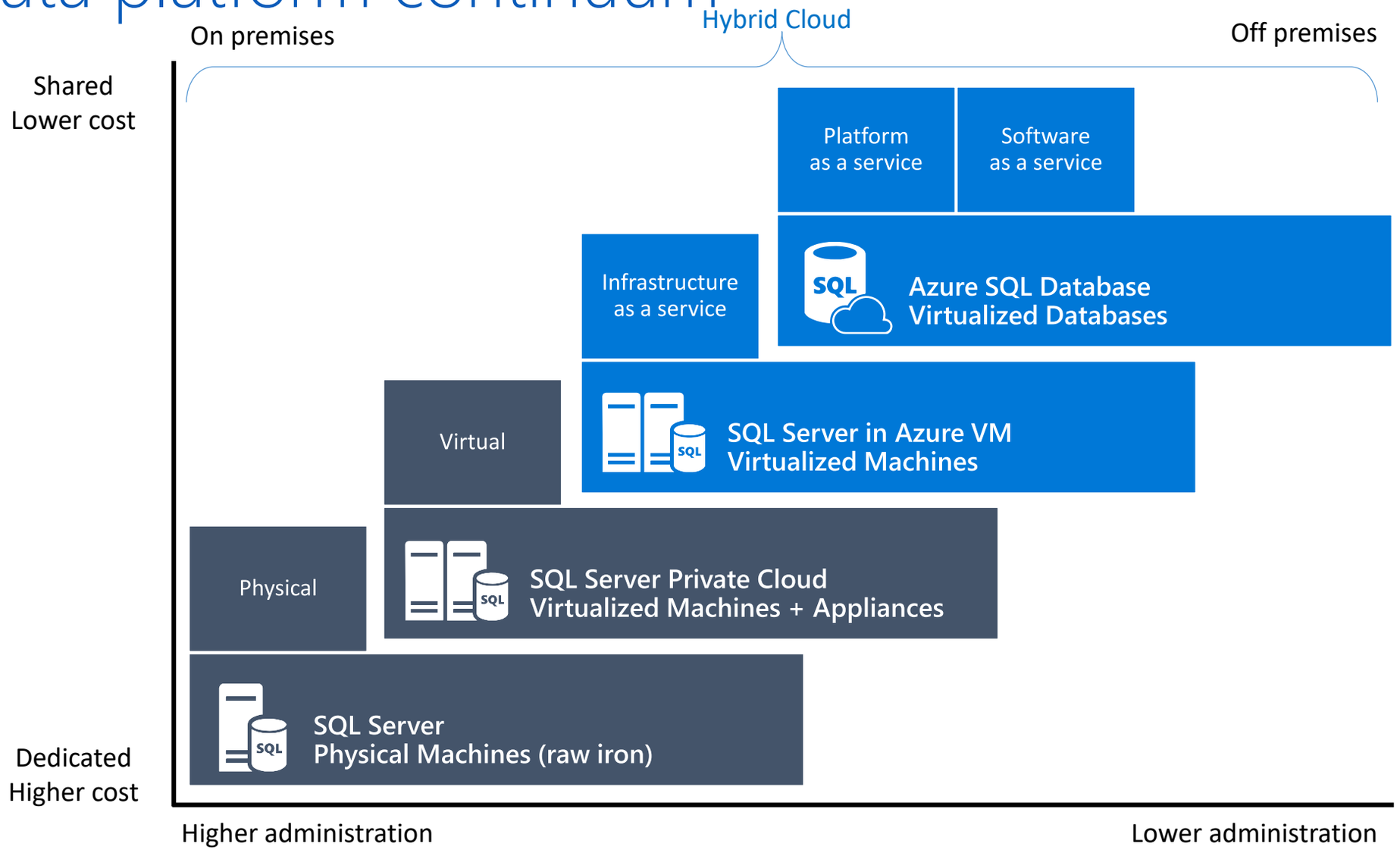
MICROSOFT CONFIDENTIAL

A Continuous Offering From Private to Public Cloud



Microsoft Confidential

Data platform continuum



How is it different from virtual machines?

	SQL Server in a virtual machine	Azure SQL Database
Best for…	Migrating existing applications with no modifications, or very minor changes	Applications that need elastic scale and/or reduced infrastructure management overhead
Resources	IT has adequate resources and bandwidth for support and maintenance	Customer does not want to add additional IT resources for support and maintenance
TCO benefits	Removing CAPEX (capital expenditure)	Avoiding CAPEX and OPEX (operating expense)
Scalability	Scale up to 20,000 IOPS*	Scale out to thousands of databases, process terabytes of OLTP (Online Transaction Processing) data

Feature Comparison

	PaaS	IaaS
Features	Less features than box	Full box product features
Performances	Max 1750 DTU in Premium Tier	Depends on VM SKU/Storage
DB Size	Max 1TB in Premium Tier (P11)	64TB on G-SERIES
Workload	Sizing by average usage	Sizing based on peaks
High-Availability	Built-in by platform	Manual configuration by AlwaysOn AG
Fault-Handling	Necessary fault-handling & retry	Recommended fault-handling & retry
Locality	No co-location with application	Co-located by VMs and VNETs
Segregation	Internet exposed endpoint	Internal private endpoint
Versioning	No control on upgrades	Full control over DB upgrade
TCO	Very low, almost self-managed	High (as on-premises)

MICROSOFT CONFIDENTIAL – INTERNAL ONLY

Feature Comparison

	PaaS	IaaS
Administration	No full-time DBA required	Full staffed DBA required
Management	Easy to manage many DBs	Complex to manage many DBs/VMs
Scale-Out	Tools & Frameworks available	No easy scale-out
Configuration	No setup customization	Full access to OS and SQL
Authentication	Only SQL standard authentication *	SQL standard and integrated
Security	No Fixed IP, fixed 1433 port	Fixed IP possible, port can be changed
Backup	Backup files not accessible, 35 days PITR	Full control of backup files, unlimited PITR
Hybrid	No AlwaysOn AG support	Can join on-premises AlwaysOn AG topology
Cross-DB Access	NO: DTC, Linked Srv, USE, 4-parts names	YES: DTC, Linked Srv, USE, 4-parts names

MICROSOFT CONFIDENTIAL – INTERNAL ONLY

Azure SQL vs VM SQL Server

Depends on what the customer needs.

- VM is traditional box product of SQL so you can do SSAS / SSRS / SSIS in additional to the DB engine and SQL Agent. You're responsible for the OS and HA/DR setup.
- Azure SQL, on the other hand, has HA baked in but not SSIS or SSRS. There's an SSAS but it's a different PaaS product.
- Azure SQL doesn't support every data type and has limits on DB size based on service tier.
- Azure SQL is a public IP secured by a firewall. IaaS SQL can have private IPs.
- Both support SQL and AD Auth.

https://docs.microsoft.com/en-us/azure/sql-database/sql-database-paas-vs-sql-server-iaas

MICROSOFT CONFIDENTIAL

Best For

IaaS	PaaS
Existing applications that require fast migration to the cloud with minimal changes. Rapid development and test scenarios when you do not want to buy on-premises non-production SQL Server hardware.	New cloud-designed applications that have time constraints in development and marketing.
Existing applications that require fast migration to the cloud with minimal changes. Rapid development and test scenarios when you do not want to buy on-premises non-production SQL Server hardware.	Applications that need built-in high availability, disaster recovery, and upgrade mechanisms.
If you need a customized IT environment with full administrative rights.	Teams that do not want to manage the underlying operating system and configuration settings.
Databases that are bigger than 1 TB in size that cannot be horizontally or vertically partitioned.	Databases of up to 1 TB in size, or larger databases that can be horizontally or vertically partitioned using a scale-out pattern.
Building hybrid applications	Building Software-as-a-Service (SaaS) applications

MICROSOFT CONFIDENTIAL – INTERNAL ONLY

Additional Considerations

- Azure SQL Database is cheaper in the long run, and easier to manage and maintain, but has **less features and performance capabilities** than a SQL Server running on Premium VMs.
- The Premium Virtual machines will have better CPU and IO throughput than what the highest Azure SQL Database service tier (P11) can offer, but they are also more expensive.

MICROSOFT CONFIDENTIAL – INTERNAL ONLY

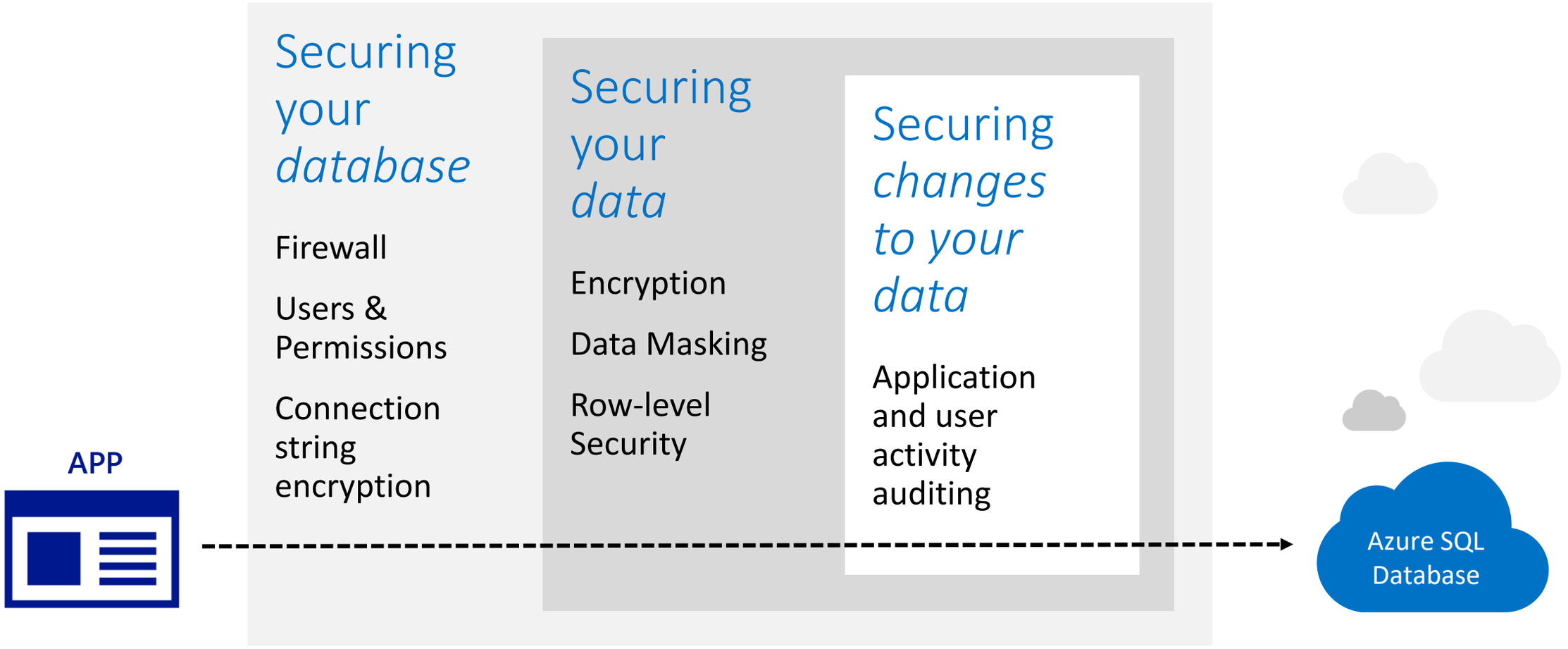
Microsoft

Azure SQL Database

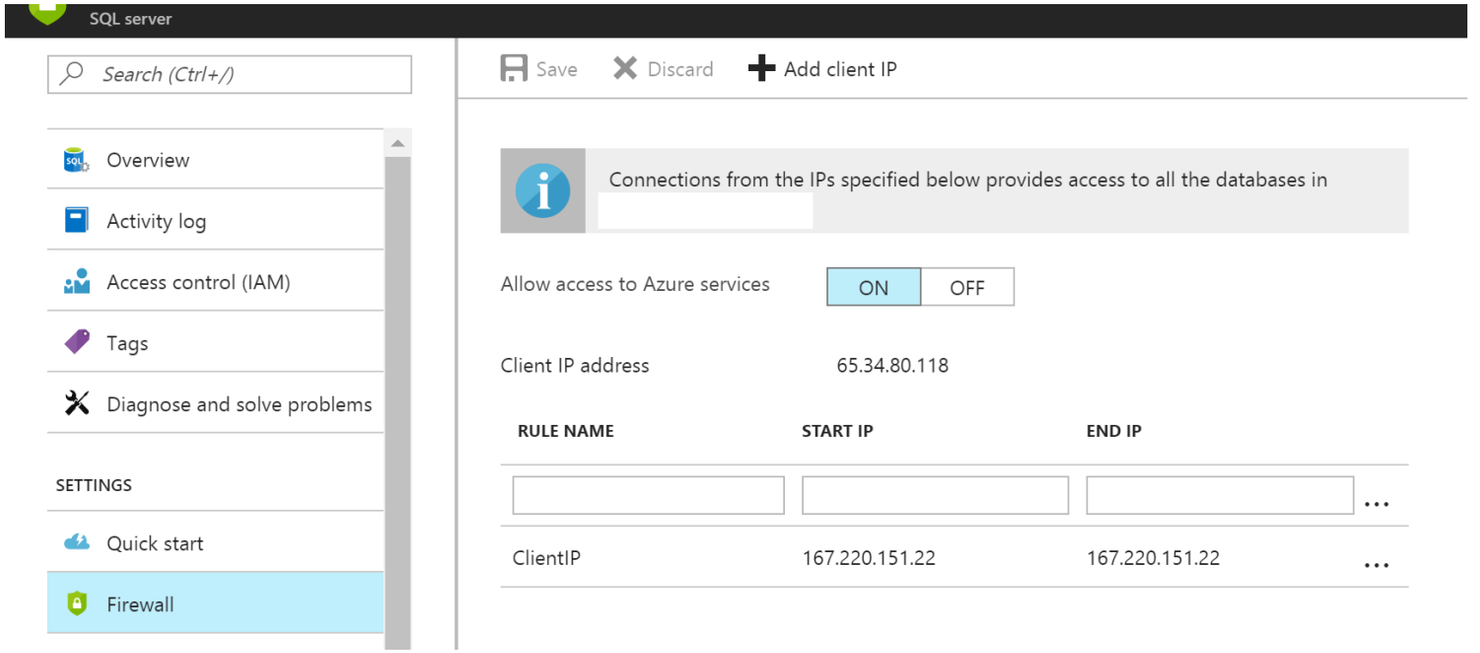
Securing your Database

Microsoft Services

Layered Approach to Security



Firewall configuration using portals



By default, Azure blocks all external connections to port 1433

Enabled in the following ways:

Azure portal

- Classic portal: Server level – **configure** page
- New portal: Server **settings** – **firewall** – **firewall settings** blade

Overview SQL Database Security Administration

Point of Difference	On-premises SQL Server	Microsoft Azure SQL Database
Where you manage server-level security	The **Security** folder in SQL Server Management Studio's **Object Explorer**	The **master** database
Server-level security role for creating logins	`securityadmin` fixed server role For more information, see Server-Level Roles	`loginmanager` database role in the master database

Commands for managing logins	`CREATE LOGIN`
	`ALTER LOGIN`
	`DROP LOGIN`
		`CREATE LOGIN`
		`ALTER LOGIN`
		`DROP LOGIN`
		(There are some parameter limitations and you must be connected to the **master** database)

View that shows all logins	`sys.syslogins` (`sys.sql_logins` for SQL Server authentication logins)	`sys.sql_logins` (You must be connected to the **master** database)
Server-level role for creating databases	`dbcreator` fixed database role For more information, see Server-Level Roles	`dbmanager` database role in the master database
Command for creating a database	`CREATE DATABASE`	`CREATE DATABASE` (There are some parameter limitations and you must be connected to the **master** database)
Dropping databases	`DROP DATABASE`	`DROP DATABASE` If a user is in the **dbmanager** role, they have permission to DROP any database, regardless of which user originally created it.
View that lists all databases	`sys.databases` (view)	`sys.databases` (You must be connected to the **master** database)

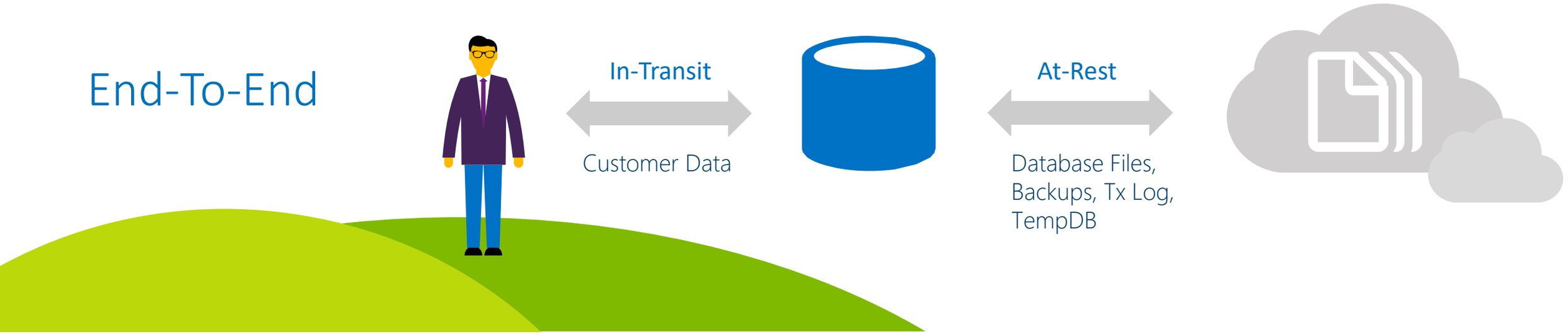
Azure AD Authentication

- Applies to SQL V12 only
- Alternative to SQL Server authentication
- Similar paradigm to Windows Authentication
- Helps stop the proliferation of user identities across database servers.
- Allows password rotation in a single place
- Customers can manage database permissions using external (AAD) groups.
- It can eliminate storing passwords by enabling integrated Windows authentication and other forms of authentication supported by Azure Active Directory.
- Azure Active Directory authentication uses contained database users to authenticate identities at the database level.
- Azure Active Directory supports token-based authentication for applications connecting to SQL Database.
- Azure Active Directory authentication supports ADFS (domain federation) or native user/password authentication for a local Azure Active Directory without domain synchronization.

Microsoft Confidential

Encryption Overview

Encryption Type	Type	Customer Value
Encryption-In-Transit	TLS from Client to Server TLS = Transport Layer Security	Protects data between client and server against snooping & man-in-the-middle attacks. SQL DB is phasing out SSL 3.0 and TLS 1.0 in favor of TLS 1.2.
Encryption-At-Rest	TDE for SQL DB TDE = Transparent Data Encryption	Protects data on disk. Key management done by Azure. **Makes it easier to obtain compliance.**
Encryption-End-To-End	Client-side column encryption for SQL DB (library available for download)	Data protected end-to-end but application is aware of encrypted columns. **Used in the absence of data masking and TDE for compliance related scenarios.**



Transparent Data Encryption

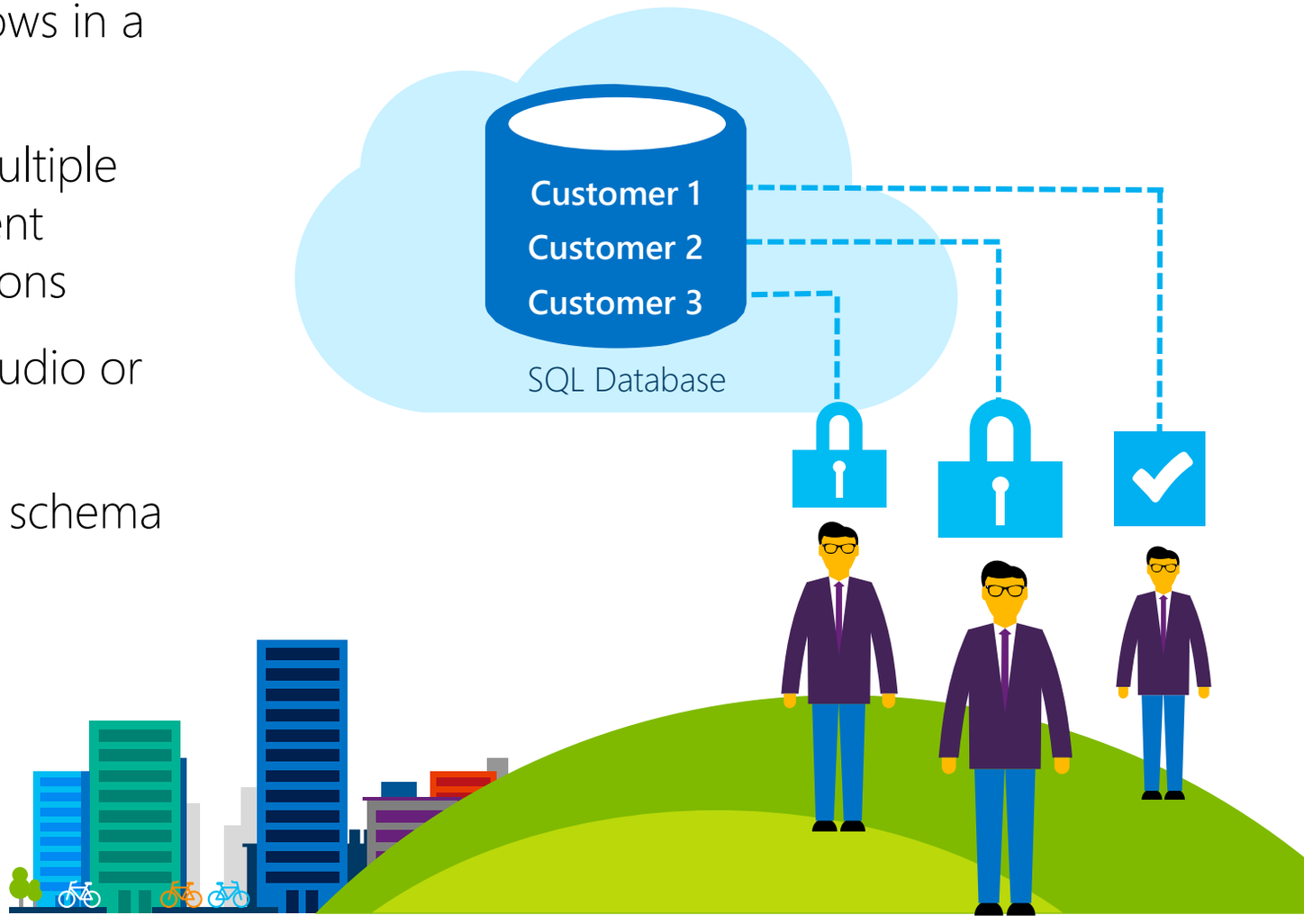
Protect sensitive data stored in a SQL database from unauthorized access

- Encrypted at rest, in flight, and while in use
- SQL Server does not have the keys (nor does it need the keys)
- Keep application changes to a minimum
- Encryption/decryption of data done transparently in TCE-enabled client driver
- Support for equality operations (include joins) on encrypted data
- Azure manages encryption keys
- V12 databases only

Row-level security

Protect data privacy by ensuring the right access across rows

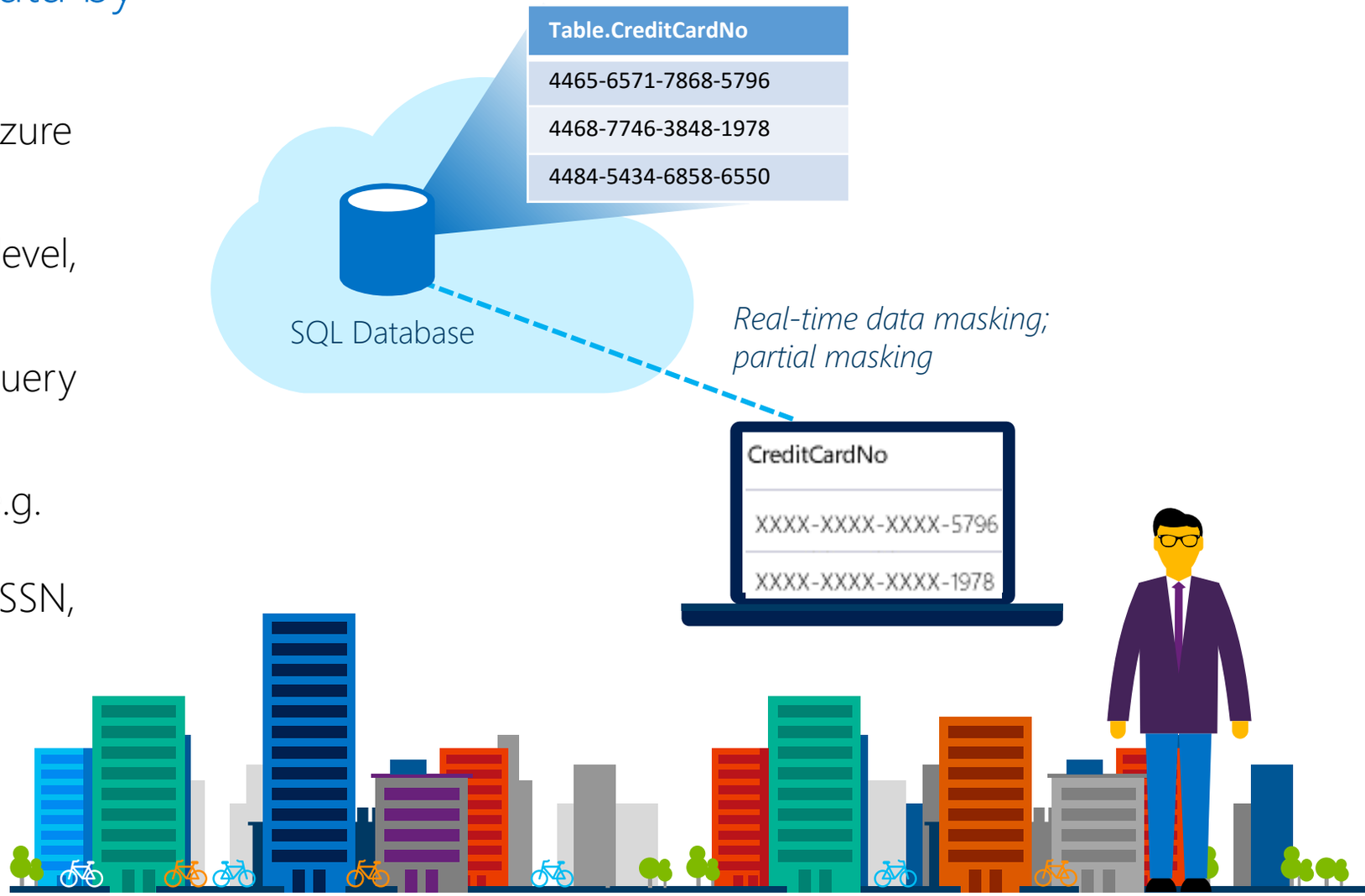
- Fine-grained access control over specific rows in a database table
- Help prevent unauthorized access when multiple users share the same tables, or to implement connection filtering in multitenant applications
- Administer via SQL Server Management Studio or SQL Server Data Tools
- Enforcement logic inside the database and schema bound to the table.



Dynamic Data Masking

Prevent the abuse of sensitive data by hiding it from users

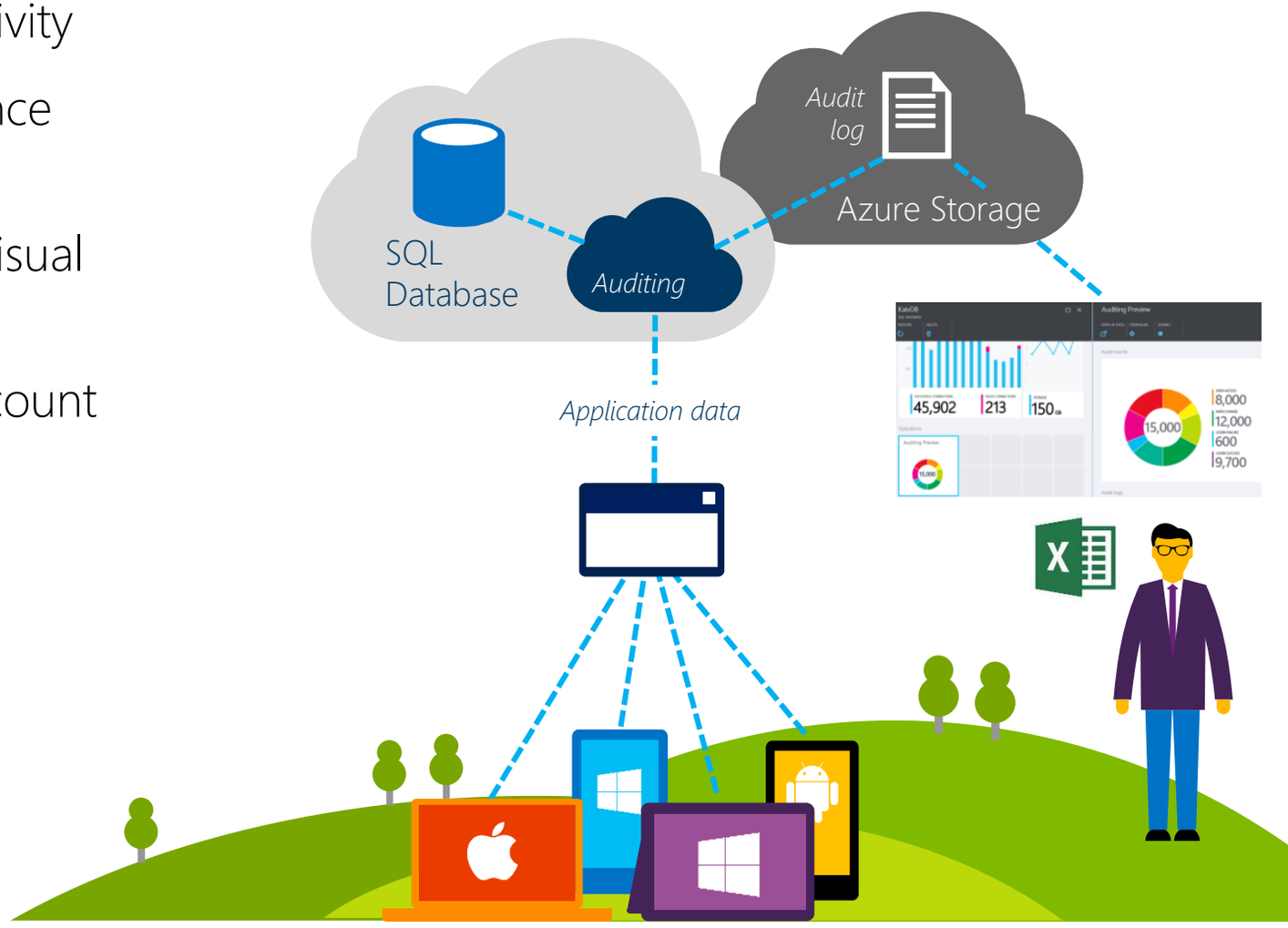
- Configuration made easy in the new Azure portal
- Policy-driven at the table and column level, for a defined set of users
- Data masking applied in real-time to query results based on policy
- Multiple masking functions available (e.g. full, partial) for various sensitive data categories (e.g. Credit Card Numbers, SSN, etc.)



Auditing

Gain insight into database events and streamline compliance-related tasks

- Configurable to track and log database activity
- Dashboard views in the portal for at-a-glance insights
- Pre-defined Power View reports for deep visual analysis on Audit log data
- Audit logs reside in your Azure Storage account
- Available in Basic, Standard, and Premium
- Access via the Azure portal (https://portal.azure.com)



Microsoft

Thank you!

© 2016 Microsoft Corporation. All rights reserved.