Microsoft

General Data Protection Regulation (GDPR) with Azure Database for PostgreSQL

Mark Bolz

Principal Program Manager
Azure Data
Microsoft

mark.bolz@microsoft.com

Disclaimer

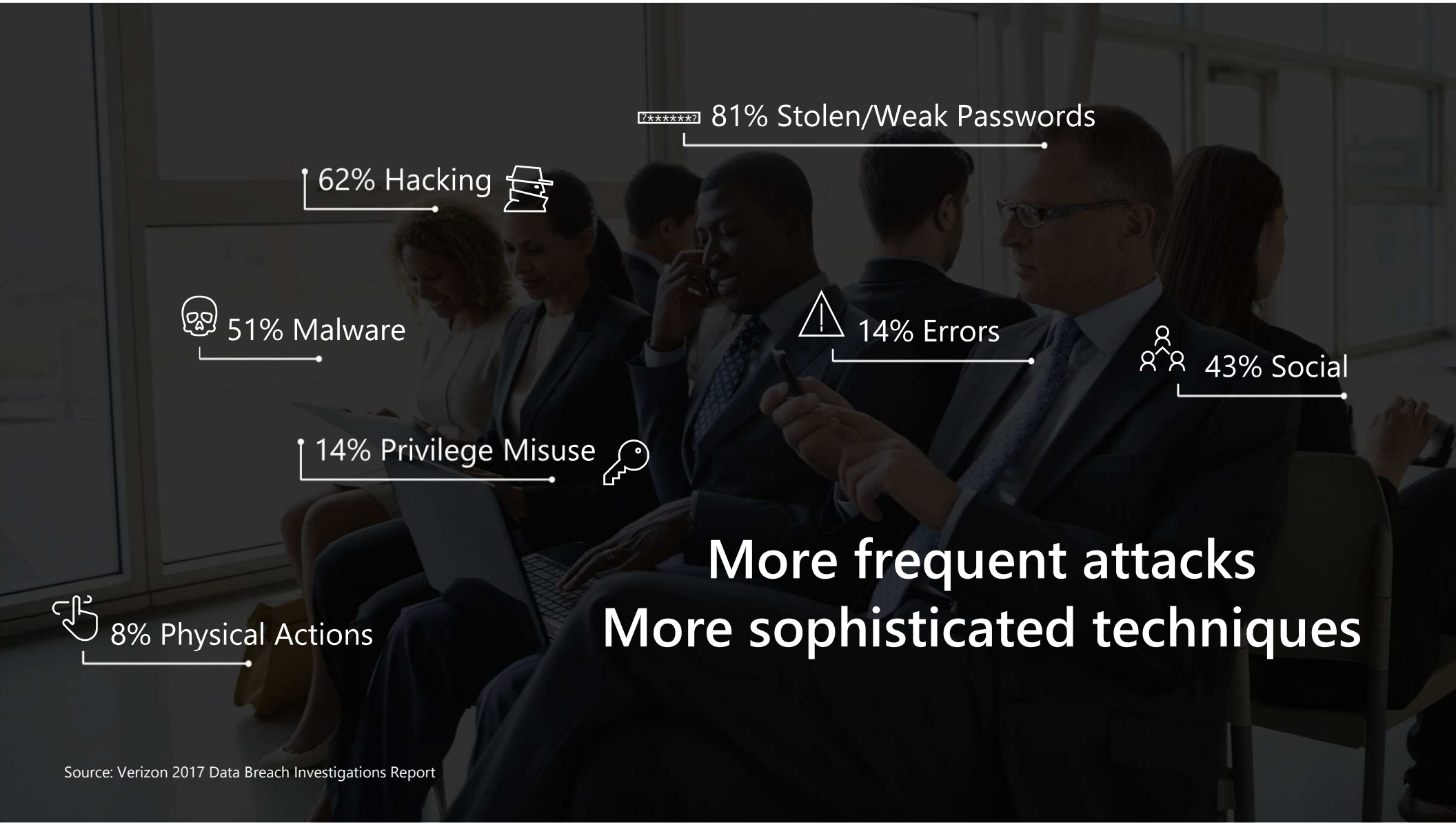
This presentation is a commentary on the GDPR, as Microsoft interprets it, as of the date of publication. We've spent a lot of time with GDPR and like to think we've been thoughtful about its intent and meaning. But the application of GDPR is highly fact-specific, and not all aspects and interpretations of GDPR are well-settled.

As a result, this presentation is provided for informational purposes only and should not be relied upon as legal advice or to determine how GDPR might apply to you and your organization. We encourage you to work with a legally qualified professional to discuss GDPR, how it applies specifically to your organization, and how best to ensure compliance.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION. This presentation is provided "as-is". Information and views expressed in this document, including URL and other Internet website references, may change without notice.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this white paper for your internal, reference purposes only.

Published May 2017
Version 1.0



Source: Verizon 2017 Data Breach Investigations Report

What is GDPR?

What are the key changes being introduced?

What does this mean for my business?

What is Microsoft's unique value proposition and how do I prepare?

How is Azure Database for PostgreSQL built to help customers with GDPR compliance?

What resource are available for me?

Microsoft

What is GDPR?
What are the key changes being introduced?

Microsoft

A NEW MANDATE TO PROTECT PERSONAL DATA

The **General Data Protection Regulation** provides European Union citizens, wherever they reside, and lawful residents greater control of their data by requiring organizations to maintain appropriate security of personal data.

GDPR includes

- Enhanced personal privacy rights
- Increased duty for protecting data
- Mandatory breach reporting
- Significant penalties for non-compliance

What does this mean for my business?

Microsoft

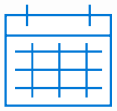
THE IMPACT OF GDPR ON BUSINESSES

Fines for noncompliance

Companies can be fined up to €20m or 4% of annual global turnover, whichever is greater, for failure to meet certain GDPR requirements

An impact beyond Europe

Organizations outside the EU who process data for goods and services offered to EU citizens, wherever they reside, and lawful residents must also comply



Upcoming implementation

GDPR enforcement begins May 25, 2018

What is Microsoft's unique value proposition and how do I prepare?

Microsoft

"Make no mistake, the GDPR sets a new and higher bar for privacy rights, for security, and for compliance.

And while your journey to GDPR may seem challenging, Microsoft is here to help all of our customers around the world."

Brad Smith
President & Chief Legal Officer
Microsoft Corporation


Threat Intelligence
Data Loss Prevention
Intune
Active Directory
Security Center
Office
eDiscovery
EMS
Data Log
Audit Logs
Cloud App Security
Microsoft Azure
Key Vault
SOLUTIONS TO HELP YOU
PREPARE FOR THE GDPR
Data Classification
Threat Detection (preview Q2 2018)
Dynamics
Data models
Advanced Threat Protection
Windows Server
Azure Database for PostgreSQL
Windows
Information Protection
Analytics
Windows Hello
Network Data Encryption
Always Encrypted Azure Storage

PREPARING FOR THE GDPR

Simplify your privacy journey

Elevate your privacy practices with our cloud

Uncover risk & take action

Use our solutions to expose areas of risk and respond with agility and confidence

Leverage guidance from experts

Use our partner network to help you meet your privacy, security, and compliance goals

THE JOURNEY TO GDPR COMPLIANCE

GDPR compliance requires a comprehensive program supported by a modern data platform

Compliance program

GDPR compliance framework

Privacy program for business processes and IT systems

Cloud strategy

Decision making policy and optimization model for the cloud

Data strategy

Data governance and stewardship throughout the organization

Application migration

App layer updates to ensure customer privacy

Modern data platform

Technology solutions which enable the following steps to data protection

1. **Data discovery**
2. **Data management**
3. **Data protection**
4. **Data reporting**

Let's discuss how modern data platform technologies support GDPR compliance

THE STEPS TO ENHANCED DATA PROTECTION

1. Discover
where personal data is located

→ Identify what personal data you have and where it resides

2. Manage
access to personal data

→ Govern how personal data is used and accessed

3. Protect
personal data against threats

→ Establish security controls to prevent, detect, and respond to vulnerabilities & data breaches

4. Report
activities regarding personal data

→ Keep required documentation, manage data requests and breach notifications

How is Azure Database for PostgreSQL built to help customers with GDPR compliance?

Microsoft

DATA PROTECTION WITH AZURE DATABASE BASED TECH

The Azure Database for PostgreSQL service ensures secure processing and storage of personal data

Discover

Identify and track personal data

Discover and classify specific data

Tag data with sensitivity labels

Track personal data access across resources

Manage

Control access

Help securely authenticate access to your database and apply granular authorization

Restrict access to users with easy-to-use tools

Protect

Safeguard data Respond to breaches

Help secure data whether at rest, in transit or in client applications

Track unusual or suspicious activity to identify threats

Report

Keep records

Track and report on all database activities

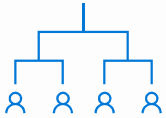
Maintain an updated assessment of data security posture

AZURE DATABASE FOR POSTGRESQL-BASED TECHNOLOGIES SUPPORT GDPR SECURITY NEEDS

Track personal data

Easily query databases to uncover personal data

Tag data with sensitivity labels



Separation of duties

Securely authenticate to your database Restrict access to users using

Separate network duties from DBA and developer duties

Encryption everywhere

Encrypt data whether at rest, in transit or in client applications

Audit capabilities

Track and report on all database activities with granularly configurable auditing

Use continuously learning algorithms to identify unusual or suspicious activity

Identity and Access Management

Control who can access data.

Key features

Array columns for Tagging

Virtual Network Service Endpoints (in private preview)

Azure portal built-in and custom RBAC roles

Always On and Encrypted Azure Storage – AES 256 bit

Transport-Layer Security

Built-in Activity Monitoring

Support for pgaudit extension (Q2 2018)

Support for Threat Detection (Q2 2018)

Native firewall and authentication

LAYERED SECURITY STARTS AT THE EDGE…

EDGE AND IDENTITY PROTECTION

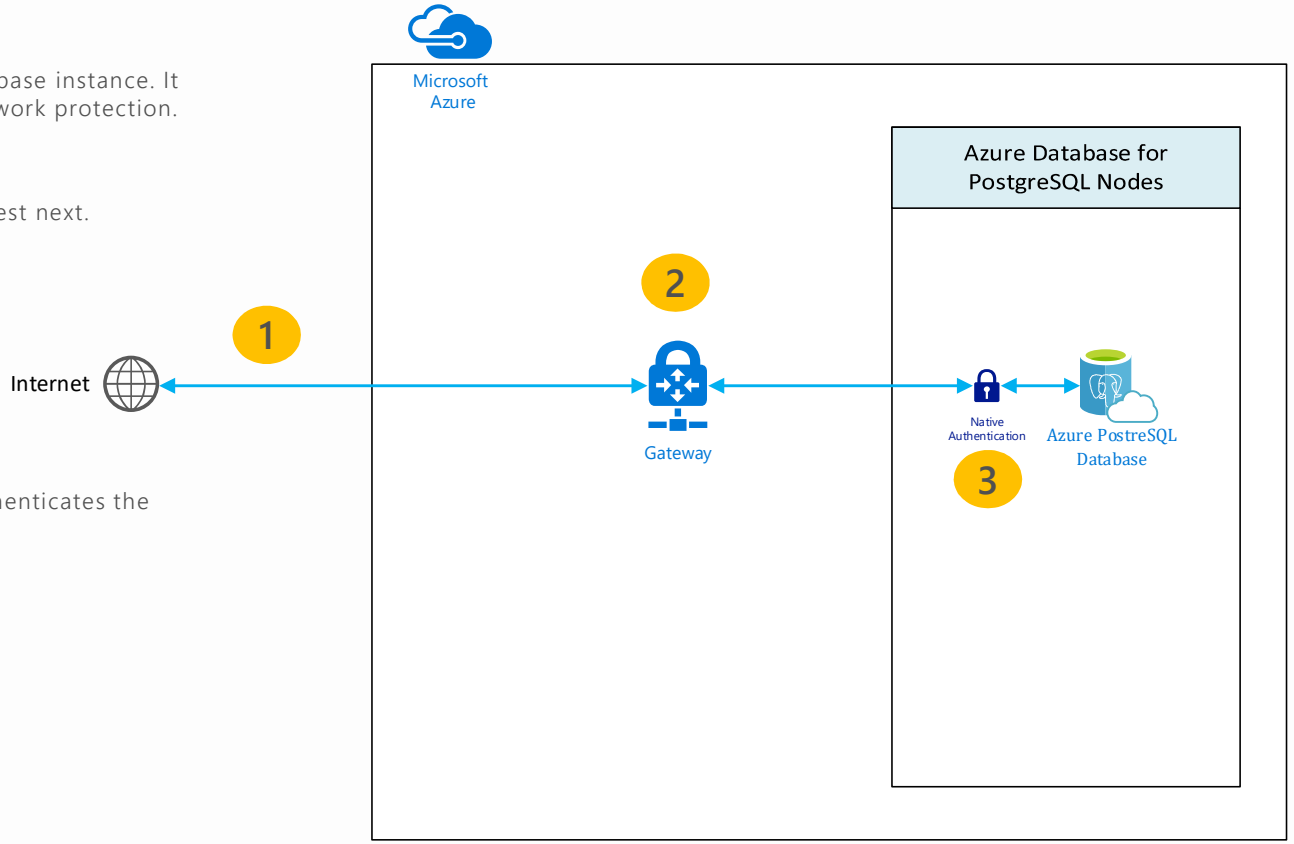
AZURE EDGE PROTECTION

NATIVE AUTHENTICATION

1. A connection is never directly to a database instance. It must first pass through Azure edge network protection.

2. A gateway services the connection request next.

3. Native PostgreSQL authentication authenticates the connection request.



ACCESS CONTROLS PROVIDE ADDITIONAL SECURITY

ACCESS CONTROL

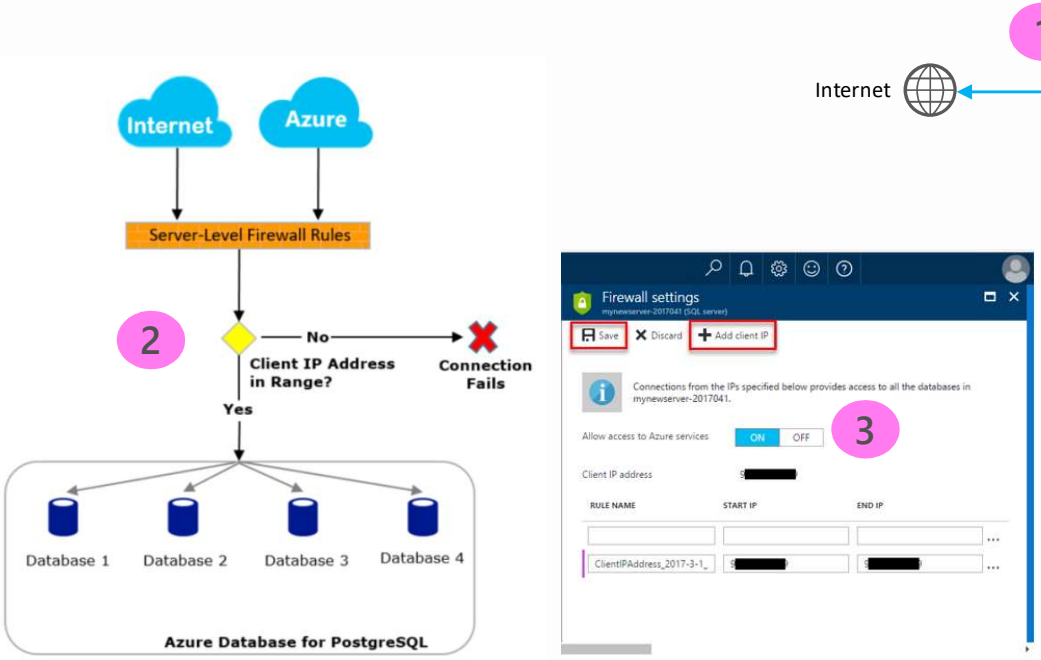
SECURE SSL CONNECTIVITY

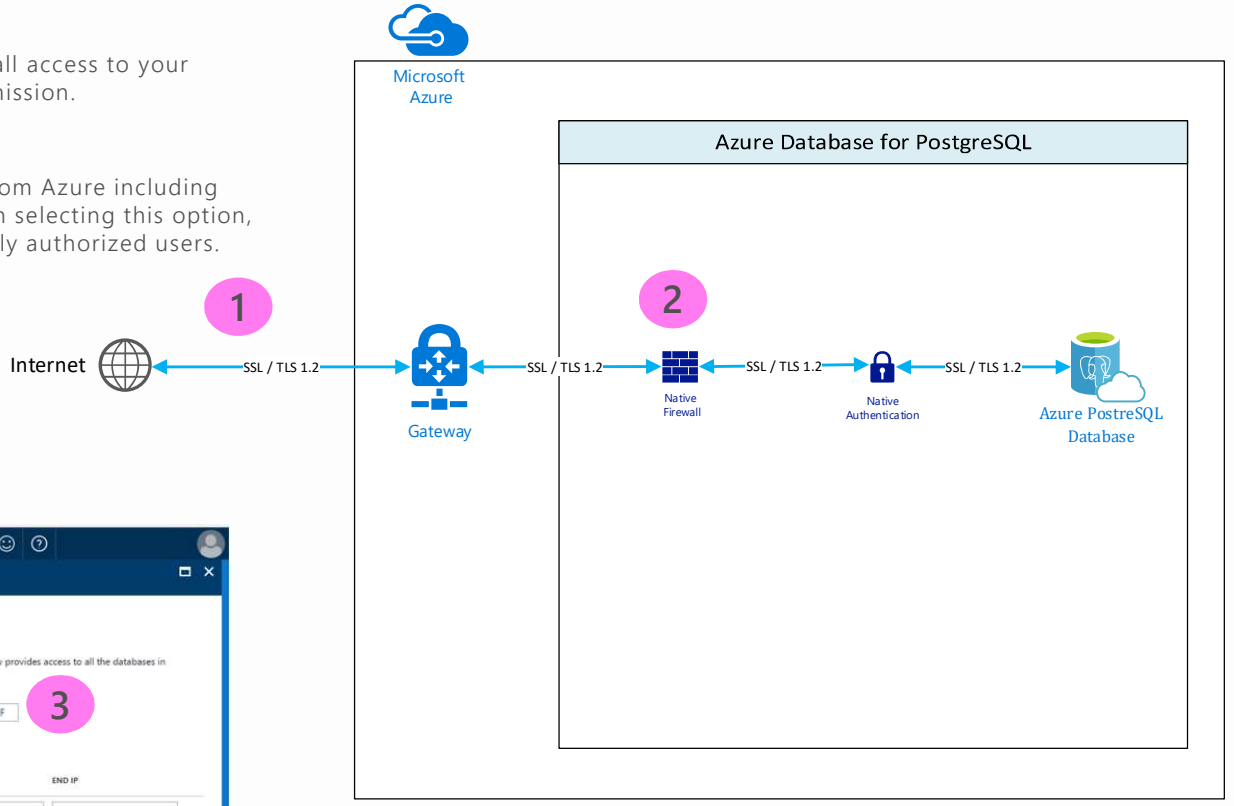
SERVER FIREWALL RULES

1. SSL / TLS 1.2 is enforced.

2. Azure Database for PostgreSQL and server firewall prevents all access to your database server until you specify which computers have permission.

3. This option configures the firewall to allow all connections from Azure including connections from the subscriptions of other customers. When selecting this option, make sure your login and user permissions limit access to only authorized users.

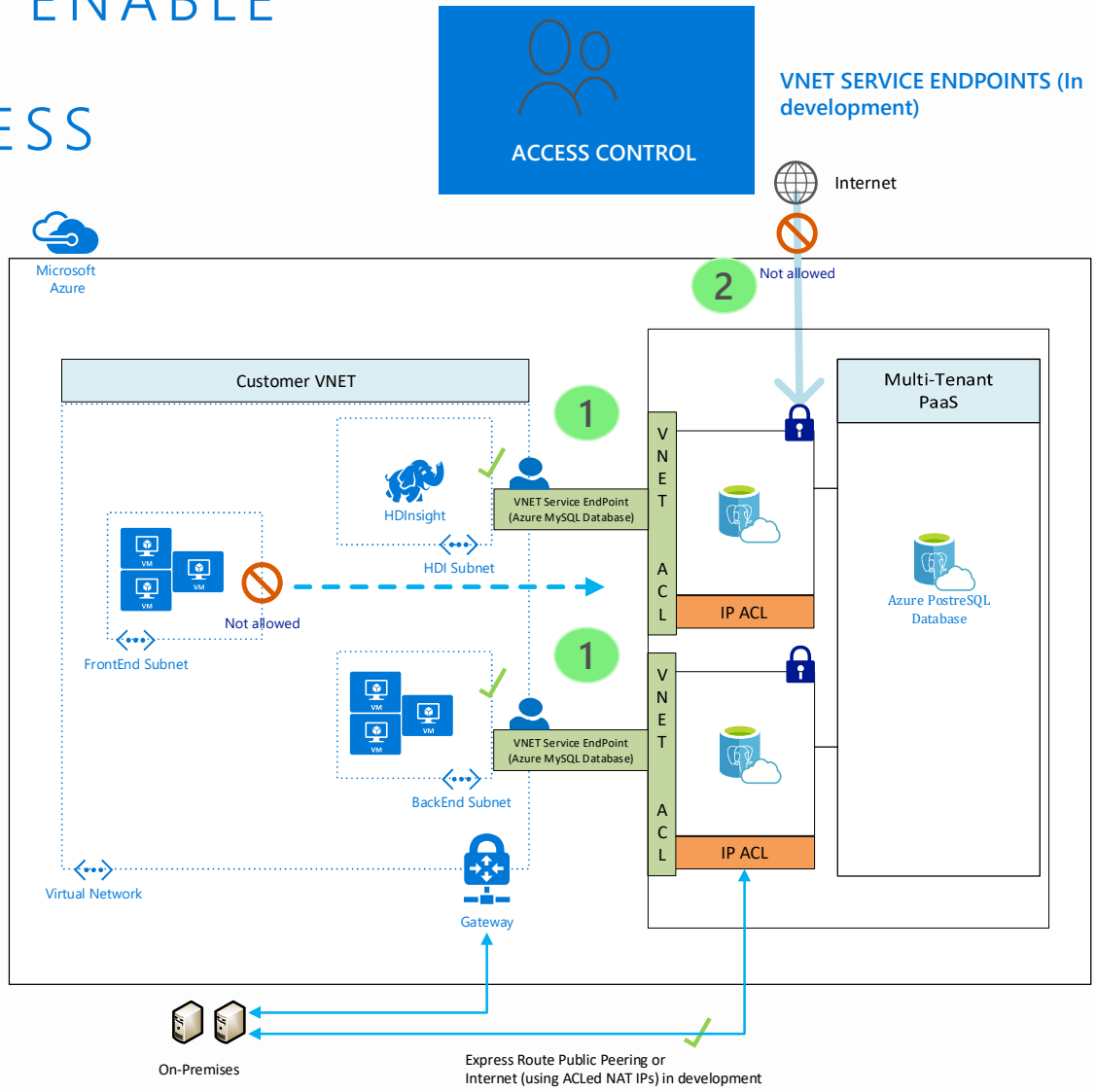




VNET SERVICE ENDPOINTS ENABLE PRIVATE, FINED GRAINED ACCESS

1. Virtual network rules are one firewall security feature that controls whether your Azure PostgreSQL Database server accepts communications that are sent from particular subnets in virtual networks.

2. VNET enables 'private access' to tagged Microsoft.SQL services. These service includes Azure SQL Database, Azure SQL Database Warehouse and Azure Database for PostgreSQ.



DATA ENCRYPTION AND LOGGING ENSURES PROTECTION

PROTECT DATA

BUILT-IN ENCRYPTION FOR DATA AND BACKUPS WITH AES 256 BIT.

ACTIVITY LOGS ENABLE ROBUST SECURIITY MONITORING

1. Encryption of data at rest is AES 256 bit, system managed and always on.

2. Built in activity logging facilitates security monitoring. Native OMS integration is in development. Exporting logs manually to OMS is possible.

Firewall example:

Query returned 2 items. Click here to download all the items as csv.

OPERATION NAME	STATUS	TIME	TIME STAMP	SUBSCRIPTION	EVENT INITIATED BY
Write FirewallRules	Started	4 wk ago	Fri Oct 06 20...	[redacted]	[redacted]@microsoft.com
Write Servers	Succeeded	1 mo ago	Tue Oct 03 2...	[redacted]	[redacted]@microsoft.com

+ Add activity log alert

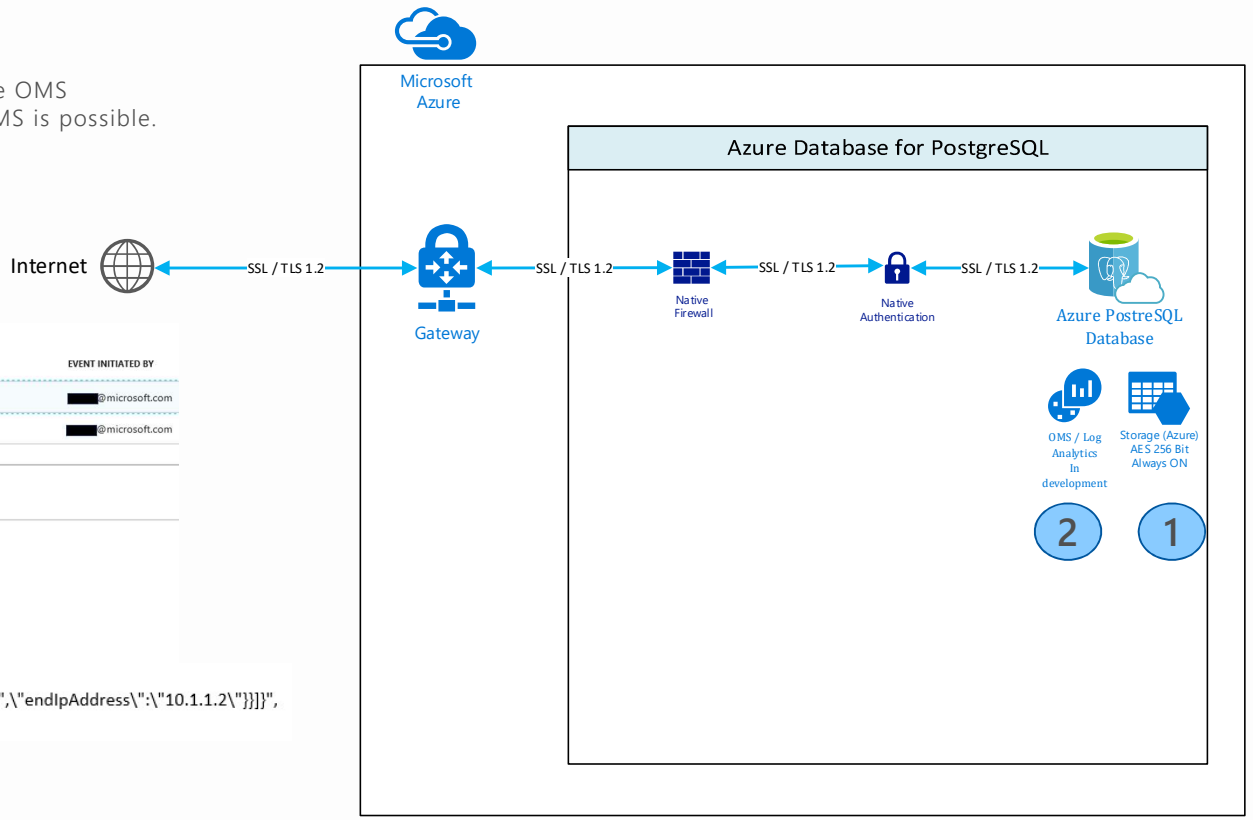
Summary JSON

Operation name
Write FirewallRules

Time stamp
Fri Oct 06 2017 11:48:47 GMT-0700 (Pacific Daylight Time)

Event initiated by
[redacted]@microsoft.com


```
"properties": {
  "requestbody": "{\"value\":[{\"name\":\"Test\",\"properties\":{\"startIpAddress\":\"10.1.1.1\",\"endIpAddress\":\"10.1.1.2\"}}]}",
  "statusCode": "Accepted",
```

THE TRUSTED CLOUD

Azure has the deepest and most comprehensive compliance coverage in the industry for Azure Database for PostgreSQL to leverage

GLOBAL


ISO 27001


ISO 27018


ISO 27017


ISO 22301


ISO 9001


SOC 1 Type 2


SOC 2 Type 2


SOC 3


CSA STAR Self-Assessment


CSA STAR Certification


CSA STAR Attestation

US GOV


Moderate JAB P-ATO


High JAB P-ATO


DoD DISA SRG Level 2


DoD DISA SRG Level 4


DoD DISA SRG Level 5


SP 800-171


FIPS 140-2


Section 508 VPAT


ITAR


CJIS


IRS 1075

INDUSTRY


PCI DSS Level 1


CDSA


MPAA


FACT UK


Shared Assessments


FISC Japan


HIPAA / HITECH Act


HITRUST


GxP 21 CFR Part 11


MARS-E


IG Toolkit UK


FERPA


GLBA


FFIEC

REGIONAL


Argentina PDPA


EU Model Clauses


UK G-Cloud


China DJCP

China GB 18030

China TRUCS

Singapore MTCS

Australia IRAP/CCSL

New Zealand GCIO

Japan My Number Act

ENISA IAF

Japan CS Mark Gold

Spain ENS

Spain DPA

India MeitY

Canada Privacy Laws

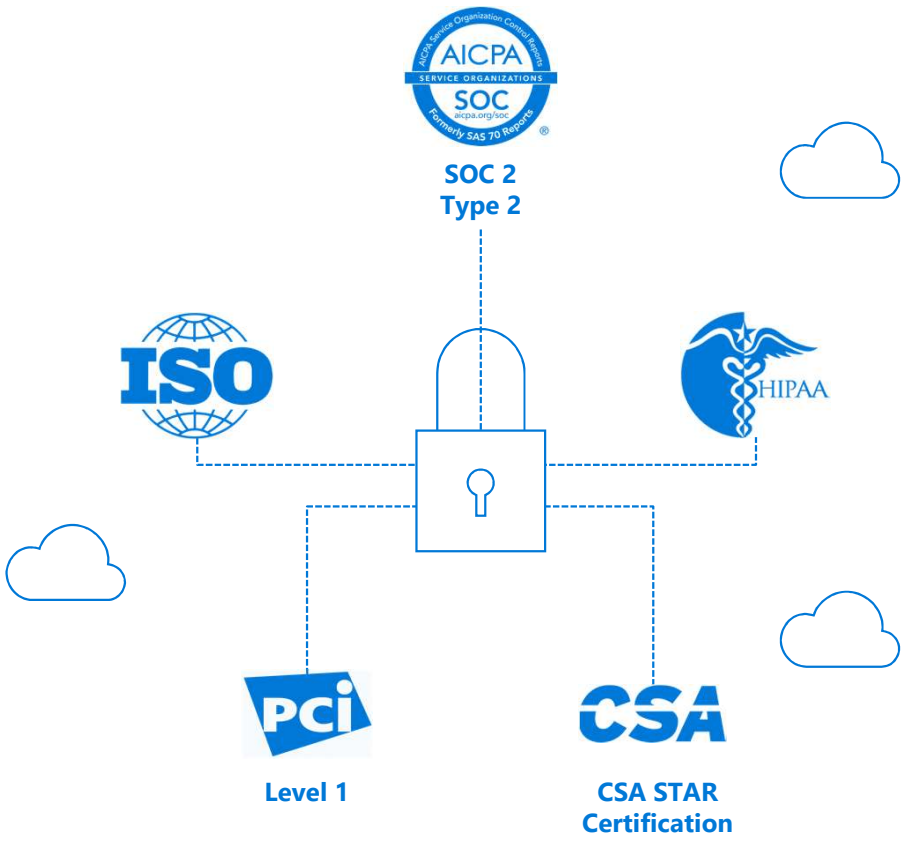
Privacy Shield

Germany IT Grundschutz workbook

AZURE DATABASE FOR POSTGRESQL SECURE AND COMPLIANT

Protect your data with up-to-date security and compliance features with the Azure IP Advantage

- SOC 1 – Compliant
- SOC2 – Compliant
- SOC3 - Compliant
- ISO 27001:2013 - Compliant
- ISO 27018:2014 -Compliant
- CSA STAR Certification - Compliant
- HIPAA / HITECH Act – Compliant
- PCI DSS Level 1 – March 2018
- ISO 27017:2015 – September 2018
- ISO 9001:2015 – September 2018
- ISO 22301:2012 – September 2018
- ISO/IEC 20000-1:2011 – September 2018



What resource are available for me?

Microsoft

ADDITIONAL RESOURCES

Best-in-industry intellectual property protection
Across the globe, the shift to cloud computing is accelerating, impacting every industry and every person. As our customers move to the cloud, business risks are changing. One issue is the increased IP infringement risk associated with delivering software-based products and services in the cloud. To support our customers and to foster a community and business environment that values and protects innovation in the cloud, we created the Microsoft Azure IP Advantage program.

Build confidently with uncapped indemnification
Build on Azure knowing that you have best-in-industry uncapped defense and indemnification coverage that extends to any open source technology that powers Microsoft Azure services, such as Hadoop used for Azure HDInsight. You don't have to do or pay anything extra, just use Azure knowing that our indemnification coverage is available if you ever need it.

Deter and defend lawsuits with patent pick
Defend against patent lawsuits targeting your innovation with access to a large patent portfolio. You become eligible for this benefit simply by using Azure on a regular basis. If sued, eligible Azure customers can acquire one of 10,000 patents that Microsoft makes available to help counter assert against an aggressor.

Get broad protection with a springing license
We are pledging to Azure customers that if we transfer patents to non-practicing entities (NPEs), these patents cannot be asserted against them in the future. Non-practicing entities are companies that primarily use patents for revenue generation. While Microsoft doesn't have a general practice of transferring our patents to NPEs, if it were ever to occur, we offer a springing license to all eligible Azure customers.

Azure IP Advantage

Microsoft Trust Center

10 QUESTIONS ASSESSING GDPR READINESS

1. Does your organization have sufficient technical measures and processes in place to secure personal and sensitive data?
2. Are your data collection, data processing, and supporting technologies built to include privacy and protection principles?
3. How much of your personal and sensitive data is currently encrypted both at rest and in transit?

4. I would describe my organization's process for classifying and labeling end user sensitive data as:
a.100% automated
b. Partially automated
c. Manual
d. Don't know

5. Which of the following protection policies do you use to classify and label sensitive data?
a. Encryption
b. Rights restrictions
c. Visual markings (e.g., watermarks)
d. Restricted access
e. End-user notifications
f. None

6. How much control do you have over access to personal and sensitive data (e.g., physical, remote, etc.)?
a. We protect user and admin credentials
b. We deploy conditional or contextual access
c. We have multi-factor authentication
d. We use passwords
e. All of the above

7. For which types of data can you apply your control policies?
a. Email/communications
b. Sales
c. Applications
d. Documents
e. Data warehouse
f. HR
g. Finance

8. If a data breach occurred, how would your organization be able to respond?
a. Process in place to notify data subjects
b. Process in place to notify authorities within 72 hours
c. Don't know/not sure

9. How often does your organization test the effectiveness of technical measures and processes for ensuring security of data processing?
a. In real time
b. Weekly
c. Once or twice a month
d. Two or three times a year
e. Once a year or less

10. How much of your data currently resides in the cloud?
a. All of it
b. More than half of it
c. Less than half of it
d. We are still migrating our data to the cloud