Why your security best practices don't work?

Nishchay Kothari

PGConf India 2024

Introduction

Nishchay Kothari

Technical Consultant
Fujitsu Enterprise Postgres Global Centre of Excellence
Fujitsu Singapore

nishchay.kothari@fujitsu.com

https://twitter.com/FujitsuPostgres

https://www.postgresql.fastware.com

https://www.linkedin.com/company/fujitsu-australia-software-technology

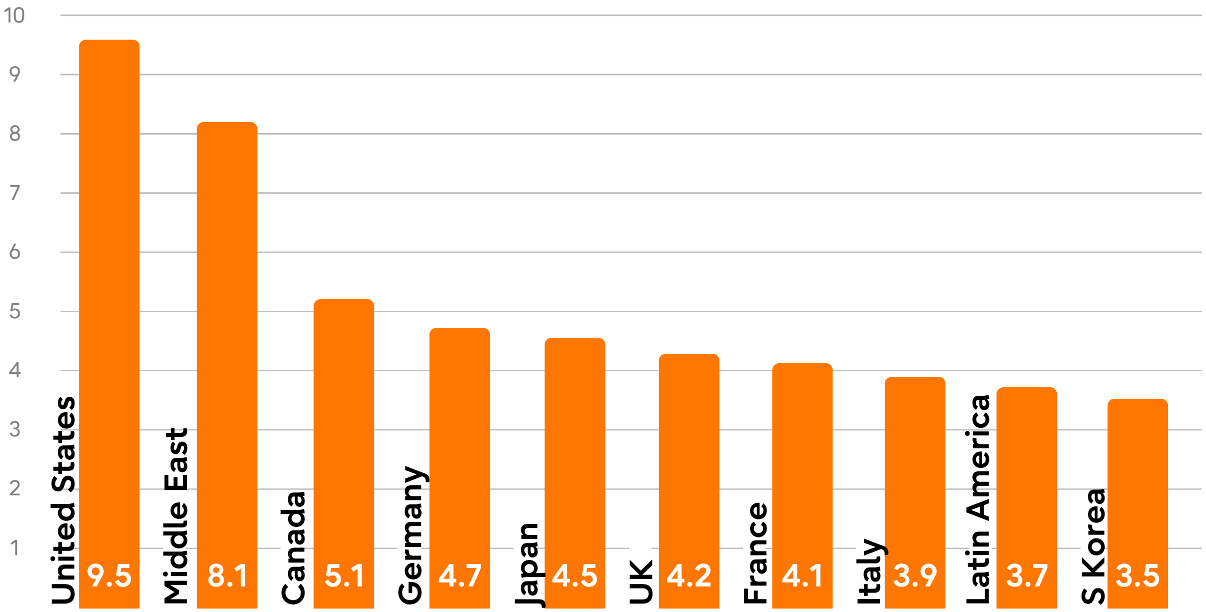
Agenda

- Impacts of data breaches
- Introduction to PostgreSQL security
- Adopting PostgreSQL with security
- When security scans trigger alarms
- Integrating PostgreSQL security management
- Implementing best security practices
- Enhancing communication and patching
- Security policy compliance monitoring
- Q&A

Data breaches

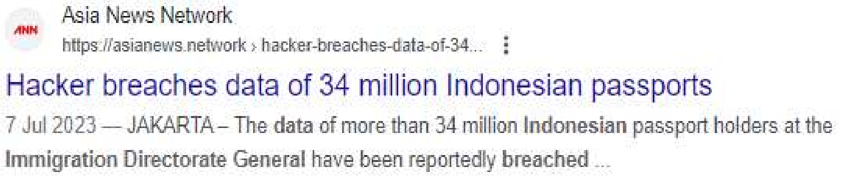
In 2023, the average cost of a data breach has reached a record high of 4.45 million USD, according to the2023 cost of a data breach report by IBM and the Ponemon institute

Cost of a data breach by country or region
(measured in USD millions)



Source: https://www.ibm.com/reports/data-breach

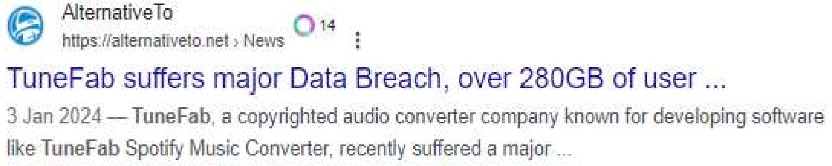
Recent incidents of data breaches



Asia News Network
https://asianews.network › hacker-breaches-data-of-34...

Hacker breaches data of 34 million Indonesian passports

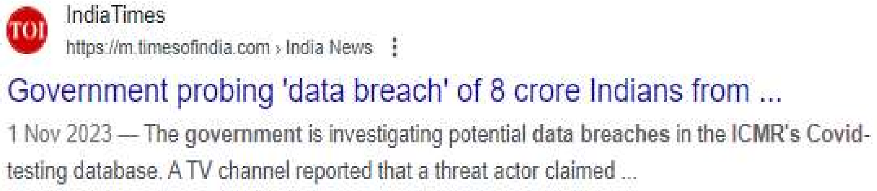
7 Jul 2023 — JAKARTA – The **data** of more than 34 million **Indonesian** passport holders at the **Immigration Directorate General** have been reportedly **breached** ...



AlternativeTo
https://alternativeto.net › News 14

TuneFab suffers major Data Breach, over 280GB of user ...

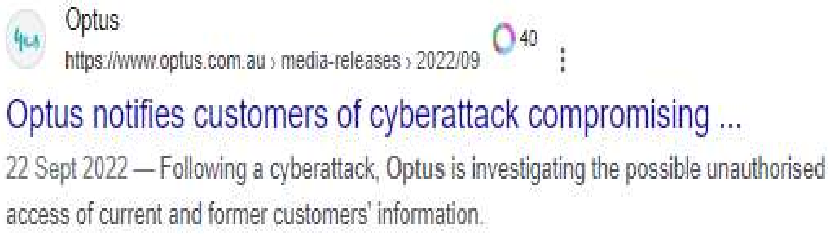
3 Jan 2024 — **TuneFab**, a copyrighted audio converter company known for developing software like **TuneFab** Spotify Music Converter, recently suffered a major ...



IndiaTimes
https://m.timesofindia.com › India News

Government probing 'data breach' of 8 crore Indians from ...

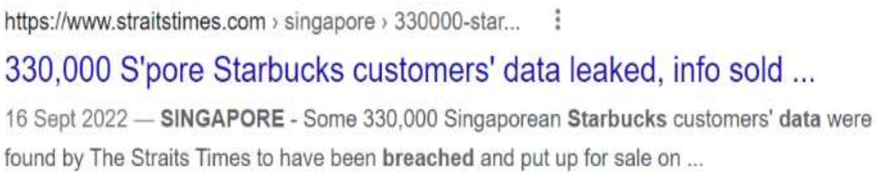
1 Nov 2023 — The **government** is investigating potential **data breaches** in the **ICMR's** Covid-testing database. A TV channel reported that a threat actor claimed ...



Optus
https://www.optus.com.au › media-releases › 2022/09 40

Optus notifies customers of cyberattack compromising ...

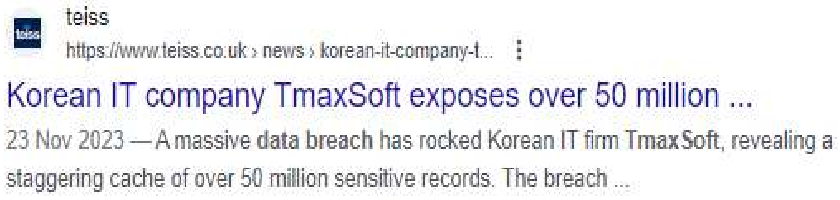
22 Sept 2022 — Following a cyberattack, **Optus** is investigating the possible unauthorised access of current and former customers' information.



https://www.straitstimes.com › singapore › 330000-star...

330,000 S'pore Starbucks customers' data leaked, info sold ...

16 Sept 2022 — **SINGAPORE** - Some 330,000 Singaporean **Starbucks** customers' **data** were found by The Straits Times to have been **breached** and put up for sale on ...



teiss
https://www.teiss.co.uk › news › korean-it-company-t...

Korean IT company TmaxSoft exposes over 50 million ...

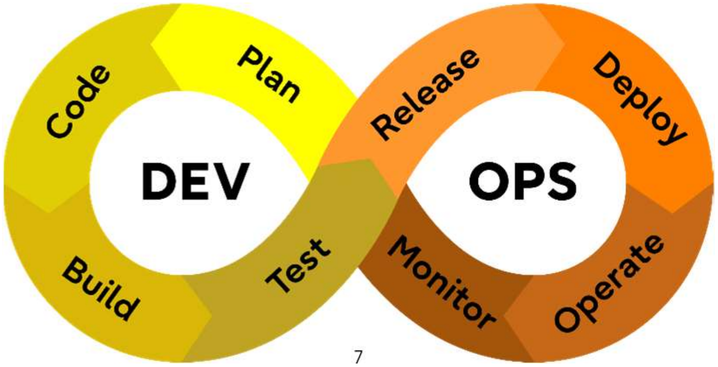
23 Nov 2023 — A massive **data breach** has rocked Korean IT firm **TmaxSoft**, revealing a staggering cache of over 50 million sensitive records. The breach ...

What is DevSecOps

> “DevSecOps is a collaboration framework that expands DevOps by adding security principles into the software development life cycle.”

Introduction to PostgreSQL security

- **The need for security in CI/CD**
  - Software development trend
    - Speed
    - Security
  - Tug-of-war
  - Rapid application and data deployment with CI/CD
  - Importance of integrating security in DevSecOps
  - Special considerations for PostgreSQL in Micro-Services and Cloud



Adopting PostgreSQL with security

- **Why security matters**
  - Data is valuable treasure
- **Initial steps to secure PostgreSQL**
  - Choose a secure lock
    - Don't settle for a rusty padlock! Opt for a PostgreSQL solution with built-in security.
      - Strong authentication: Secure logins with passwords, certificates, or MFA
      - Data encryption: Scramble your data at rest and in transit to keep it safe from hackers
      - Access control: Define who can access what data.
  - Learn from the security masters
    - No need for a cybersecurity degree! Use **Security Best Practices Guide**
      - Configure settings: Set up your database like a pro with optimal security settings.
      - Master built-in features: Unleash the power of built-in security tools like user roles and permissions.

When security scans trigger alarms

FUJITSU

- **Beyond the blaring: understanding security alarms for a healthy digital defense**
  - Scans as checkups
    - Think of security scans as your tech doctor, monitoring your systems' health.
  - Red alerts, no need to panic
    - Alarms highlight the potential issues, not guaranteed breaches. Investigate calmly.
  - Bridging the gap
    - Review scan reports regularly, analyze triggers, & patch vulnerabilities.
  - Friends, not enemies
    - Scan helps strengthen defenses, not shame on mistakes.

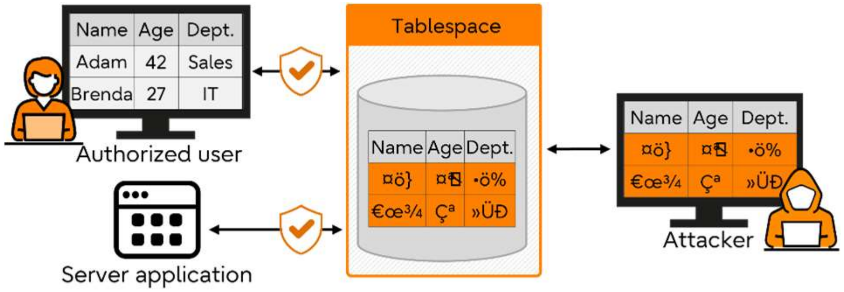
Integrating PostgreSQL security management 1/7

- **Transparent Data Encryption**
  - Encrypting data at rest to prevent unauthorized access
- **Data Masking**
  - Hiding sensitive information from non- privileged users
- **Dedicated Audit Logging**
  - Tracking and recording database activities for security audits

Integrating PostgreSQL security management

2/7

- **Transparent Data Encryption**
  - AES 128 and 256-bit encryption
  - Compliant with PCI DSS standard
  - Encrypts the physical files of database
  - No modification required for existing business application
  - Encryption key can be changed without re-encrypting data
  - Specially used to protect data at rest



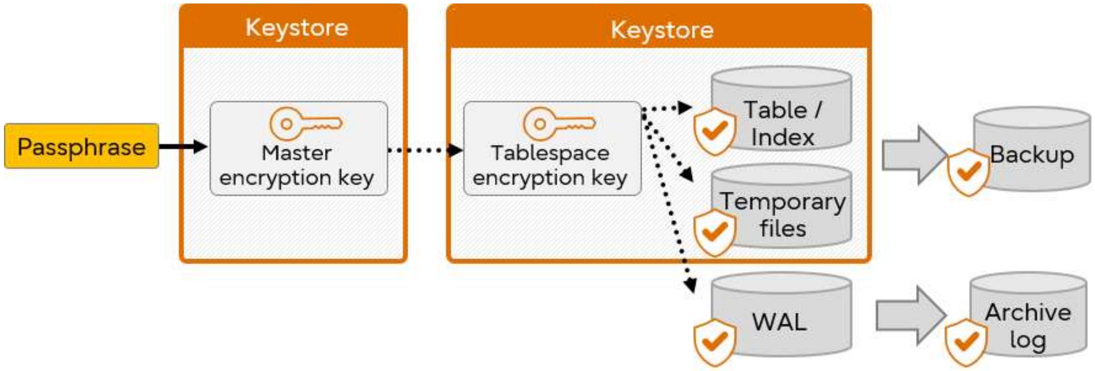
Name	Age	Dept.
Adam	42	Sales
Brenda	27	IT

Name	Age	Dept.
¤ö}	¤[illegible]	•ö%
€œ¾	Çª	»ÜĐ

Name	Age	Dept.
¤ö}	¤[illegible]	•ö%
€œ¾	Çª	»ÜĐ

Integrating PostgreSQL security management

- **Transparent Data Encryption scope**
  - Tablespace (table, indexes, temporary tables, temporary indexes)
  - Backup
  - Temporary files
  - WAL

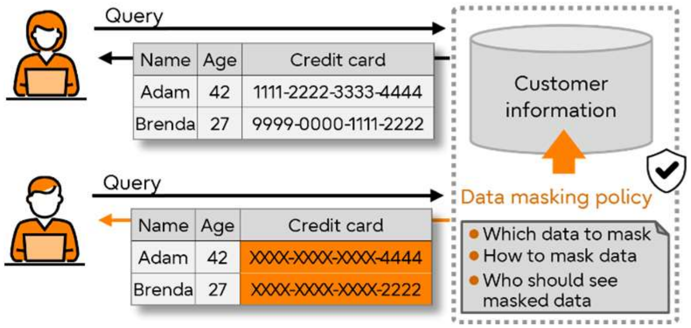


Integrating PostgreSQL security management

4/7

- **Data Masking**
  - Provides the ability to obfuscate specific columns or part of a column, while still maintaining the usability of the data
  - Example: Encrypting — Replacing — Randomizing
  - PCI DSS standard
  - Protects both online & offline data

Online data masking

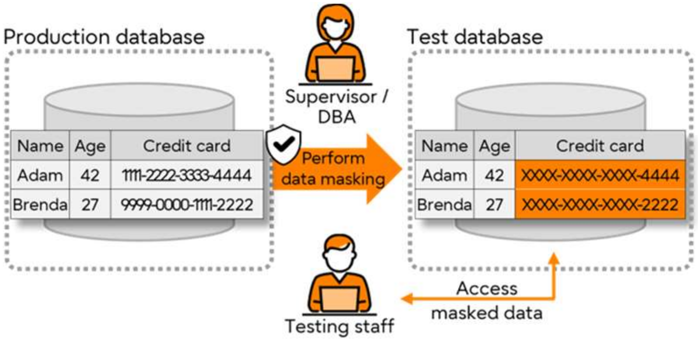


Name	Age	Credit card
Adam	42	1111-2222-3333-4444
Brenda	27	9999-0000-1111-2222

Name	Age	Credit card
Adam	42	XXXX-XXXX-XXXX-4444
Brenda	27	XXXX-XXXX-XXXX-2222

- Which data to mask
- How to mask data
- Who should see masked data

Offline data masking



Name	Age	Credit card
Adam	42	1111-2222-3333-4444
Brenda	27	9999-0000-1111-2222

Name	Age	Credit card
Adam	42	XXXX-XXXX-XXXX-4444
Brenda	27	XXXX-XXXX-XXXX-2222

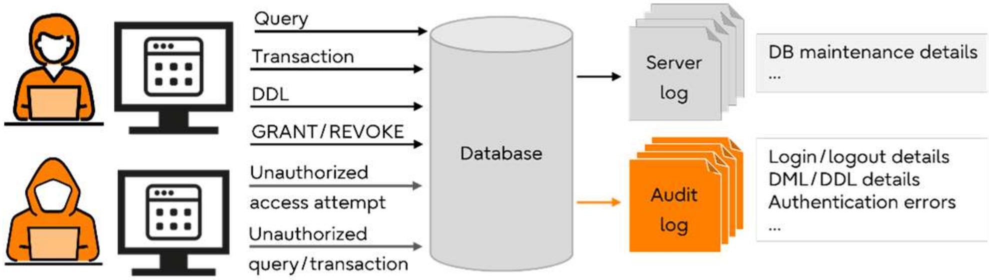
Integrating PostgreSQL security management

5/7

- **Data Masking Types**
  - Full masking
    - All data in the masked column is modified.
    - Modified values are dependent on the column data type.
  - Partial masking
    - Only a portion of the data is masked as specified.
  - Regular expression masking
    - Data is modified according to a regular expression.
    - Allows data, such as an address, to be modified to not show the street number.

Integrating PostgreSQL security management 6/7

- **Auditing**
  - Audit logging enables organizations to trace and audit the usage of sensitive data and connection attempts of the database
  - Provides a clear picture of data access by logging
    - What data is accessed
    - When the data is accessed
    - Who accessed the data
    - How the data is accessed
  - Logs can also be stored in dedicated audit log files that are separate from the server log for easy access
  - There are two types of audit logging:
    - Session audit logging
    - Object audit logging



Integrating PostgreSQL security management 7/7

- **Auditing - Classes**
  - Provides the ability to produce logs that comply with government and financial standards like PCI DSS or ISO certifications

Class name	Statements that will be logged
READ	SELECT, COPY FROM
WRITE	INSERT, UPDATE, DELETE, TRUNCATE, COPY TO, etc.
FUNCTION	DO
ROLE	GRANT, REVOKE, CREATE/ALTER/DROP ROLE, etc.
DDL	CREATE, ALTER, DROP, REINDEX, SELECT INTO, etc.
MISC	DISCARD, FETCH, CHECKPOINT, VACUUM, ANALYZE, BEGIN, COMMIT, ROLLBACK, SET, LOCK, etc.
ALL	All of the above

Implementing best security practices 1/5

- **GDPR compliance**
  - Adhering to data protection regulations
- **Centralized management**
  - Centralized user access control, and key management
- **Automated security in CI/CD**
  - Incorporating database security processes in continuous deployment

Implementing best security practices 2/5

- **GDPR Compliance**
  - Data protection for all
    - The General Data Protection Regulation (GDPR) empowers individuals with control over their personal data
- **Guidelines**
  - Transparency
    - Clearly communicate how you collect, use, and protect user data
  - Consent
    - Obtain freely given, informed, and unambiguous consent before processing personal data
  - Rights at your fingertips
    - Respect data subjects' rights to access, rectify, erase, restrict, and port their data
  - Security
    - Implement robust technical and organizational measures to safeguard data against unauthorized access, loss, or breach
  - Event of Breaches
    - Be prepared to notify authorities and individuals promptly in case of data breaches

Implementing best security practices 3/5

- **Centralized user access control**
  - Centralized access control permits a user to access multiple applications using just one set of login credentials
  - Often referred to as Single Sign-On (SSO), authentication is simplified and performed using one tool, enabling access to a number of services without having to repeatedly log in/out of each
  - Centralized Access controls can be integrated into CI/CD by using the appropriate LDAP plugins
  - Centralized Access has two main advantages:
    - More efficient to manage
    - Easier to enforce policies
    - More scalable

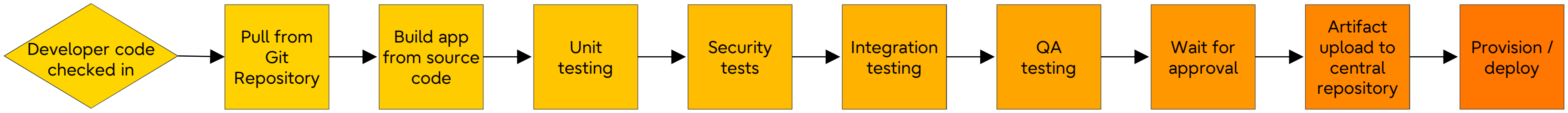
Implementing best security practices 4/5

FUJITSU

- **PostgreSQL key management**
  - Enterprise data encryption/decryption helps protect data against security breaches.
  - Encryption in the cloud is very common, but there are added risks of unauthorized data access.
  - PostgreSQL can use all the main 3rd party key store & secrets solutions on the market.
    - Keystore list includes HashiCorp Vault, NitroKey, and YubiHSM
  - PostgreSQL supports storing keys both locally and on an external key store
  - External key stores provide increased security and simplify key lifecycle management
  - Key management, regardless of whether local or external key store, is another candidate for CI/CD integration.

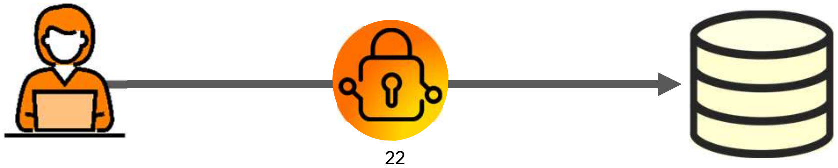
Implementing best security practices 5/5

- **Automation of security processes for PostgreSQL in CI/CD**
  - PostgreSQL security control summary baselines and security control templates can be treated like any other code changes, and checks can be checked into the code repository and into CI/CD pipeline for unit testing
  - Writing security scripts is shared among all members of DevSecOps team
  - Using CI/CD for provisioning and for deploying security hardening and compliance monitoring ensures consistency and validation earlier in the SDLC cycle
  - An automated healthy security compliance report, which covers the contents of the security baseline at the end of a test phase, could be used as security team sign-off. Agreement on security checks at the start of a project saves on meeting/action time and delays later on in the project



Enhancing communication and patching 1/2

- **Enable SSL/TLS – data in transit encryption**
  - SSL (Secure Sockets Layer) is built into PostgreSQL.
  - TLS – Transport Layer Security
    - Public key encryption
    - Symmetric encryption
  - Encrypts client/server communications for enhanced security.
  - Required OpenSSL installed on both client & server.
  - Encrypts data across network SSL.
  - Supports self-signed & 3rd-party CA certificates.
  - Server key & certificate required to enable TLS for PostgreSQL.



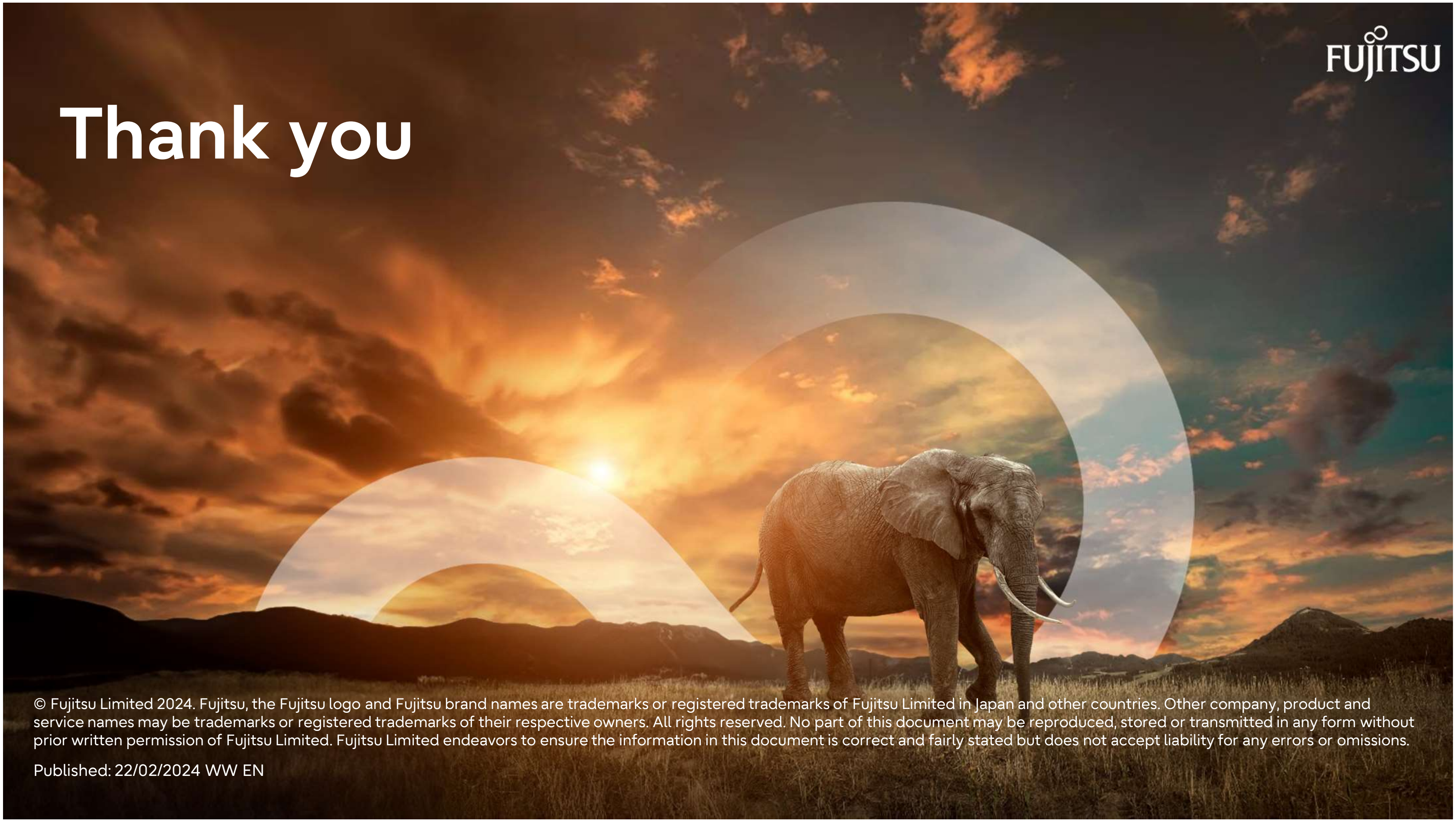
Enhancing communication and patching 2/2

- **Security patching**
  - Keep DB s/w up to date - OS security patches usually published every quarter
    - Patching should start with dev, and then to the next environment
    - OS security patching is usually managed outside application SDLC
  - Database vendors may also publish quarterly security patches via a new minor number
  - General patching schedule
    - OS: Quarterly
    - Database: Quarterly, Half-Yearly or Yearly
  - DB patching should follow your SDLC environments and included as part of CI/CD work stream
    - Complexity
    - Urgency
    - Frequency
  - Apply security patches programmatically

Security policy compliance monitoring

- **CI/CD Security controls can be used to provision and deploy the security monitoring checks**
- **How to improve?**
  - Automate the process
    - Use right CI/CD tools for security checks and integrate it from the beginning of SDLC.
  - Create a security baseline
    - Like a checklist of all security controls
  - Treat security controls like test cases
    - Test our security controls as like our application code to check the effectiveness
  - Schedule regular checks
    - Configure automated security check and it's report generation
  - Keep a security logbook
    - Record the security checks results inside the database to maintain the history
  - Fix problems promptly
    - Just like any other change, treat the security failure on priority and fix it ASAP

Q&A



Thank you

Published: 22/02/2024 WW EN