Cybersecurity and Resiliency for z/TPF

2022 TPF Users Group Conference
March 27-30, Dallas, TX

Main Tent

—

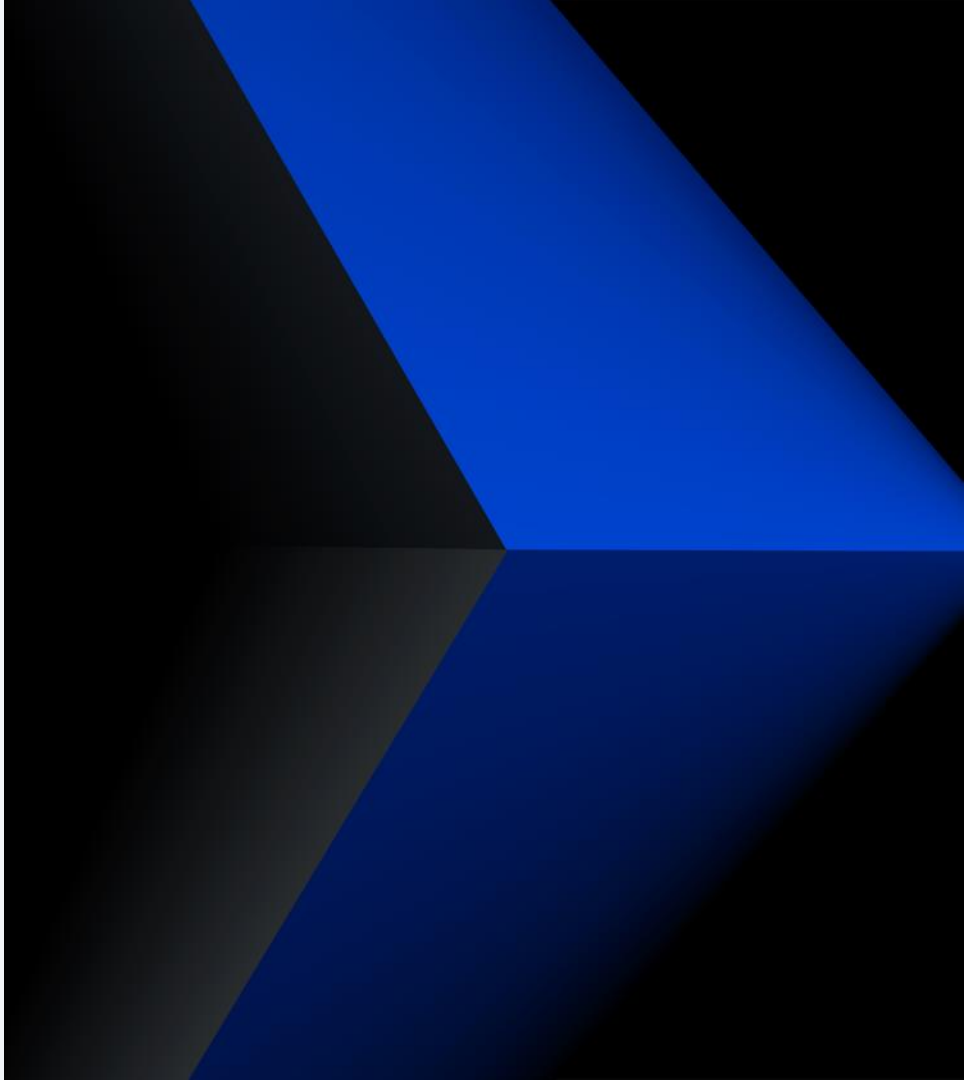
Mark Gambino, IBM z/TPF Chief Architect

IBM Z

IBM

Disclaimer

Any reference to future plans are for planning purposes only. IBM reserves the right to change those plans at its discretion. Any reliance on such a disclosure is solely at your own risk. IBM makes no commitment to provide additional information in the future.



X = Business Continuity

- Continue mission critical functions at all times during any type of disruption

Y = Information Security

- NIST definition: “Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide Availability, which means ensuring timely and reliable access to and use of information.”
- Protect data in any form from any threat

X + most of Y = Cybersecurity (Cyber Security)

- NIST definition: “The ability to protect or defend the use of cyberspace from cyber attacks.”
- Ability to continuously deliver the intended outcome, despite adverse cyber events
- Specific to the protection of **data** that originates in a **digital** form
- Focus on protecting network, servers, end user devices, and databases

Business Resilience is Baked into the z/TPF Architecture

Application Bug

- Process Isolation
- Key protected memory
- Restricted use macros

Only that one message is impacted

Application/service remains active

Hardware Device Failure

- Multiple network (OSA) cards
  - Virtual IP address (VIPAs)
- Duplicate DASD
- Multiple channel paths
- Multiple tape grids
- Primary/fallback consoles
- Redundant memory (RAIM)
- Spare CPU cores

Transparent to transactions

Logical Server (z/TPF image) Failure

Physical Server (IBM Z box) Failure

- Multiple z/TPF images (loosely-coupled)
- N+1, N+2 architecture
- Very fast reboot (re-IPL)

Remaining z/TPF images handle workload

Workload Spikes

- Partition Manager (PR/SM) shared CPUs
- Dynamic CPU support

Add CPU capacity on demand

Primary Data Center Failure

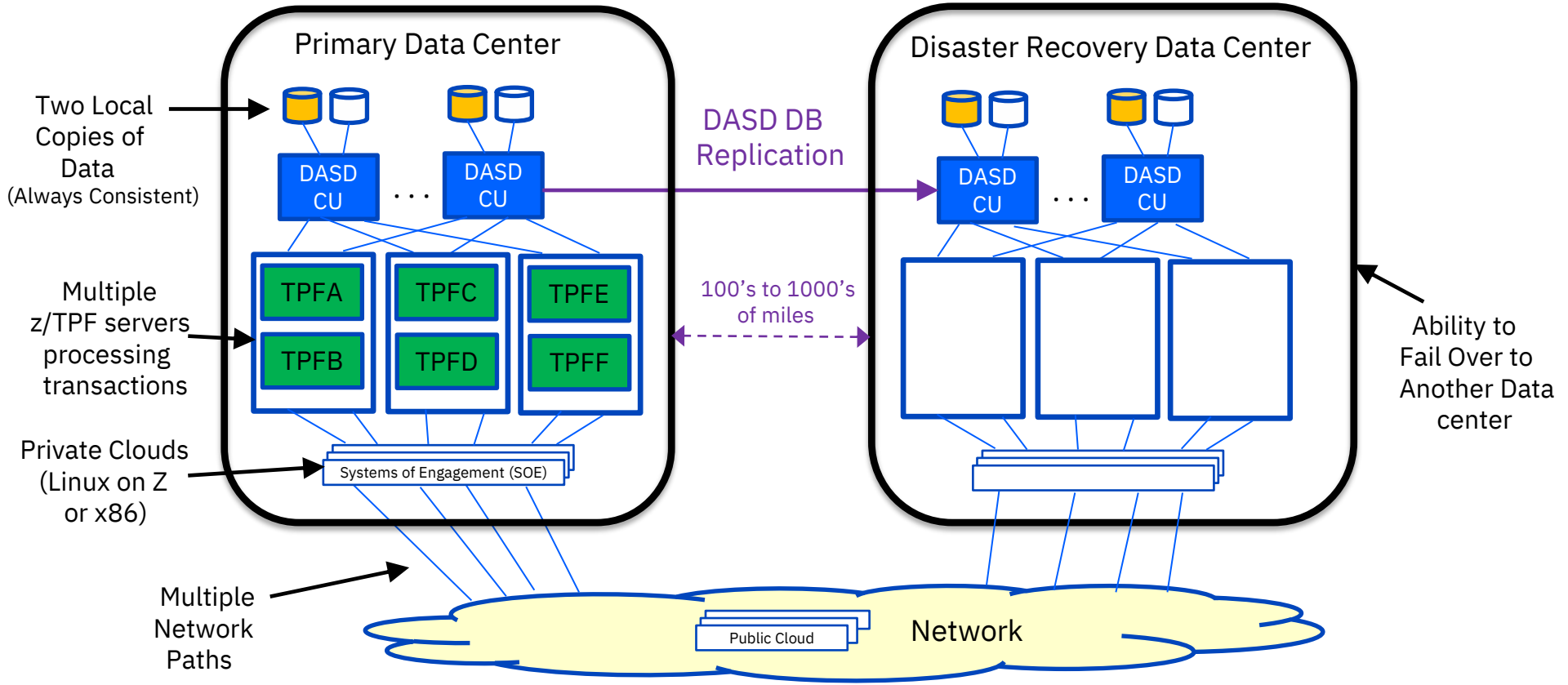
- Disaster Recovery (D/R) site(s)
- At least one D/R site geographically distant

Workload moves to a D/R site

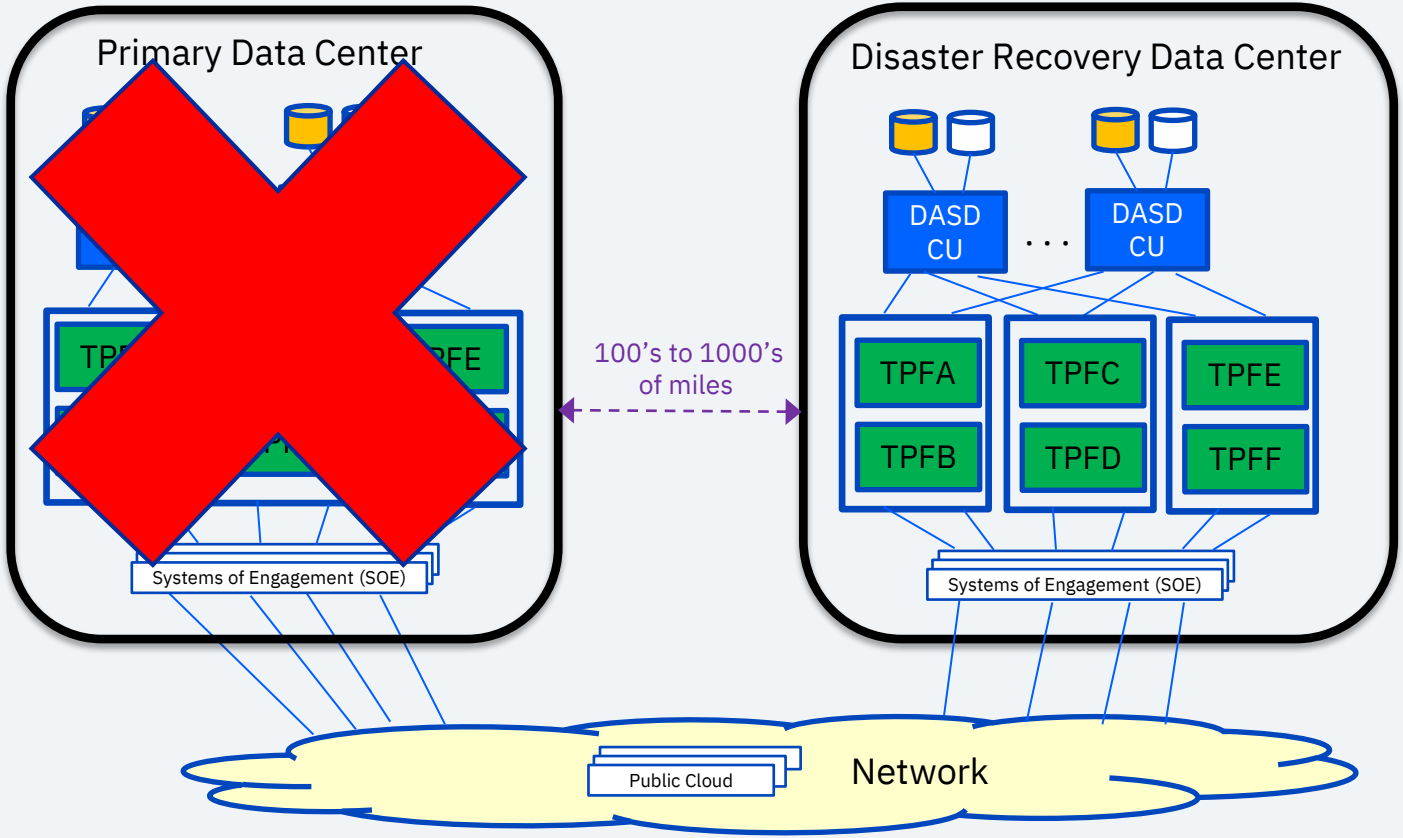
Geographic D/R is More Important Than Ever – Just Look at 2021

Historic Flooding
Massive Wildfires
Frozen Electrical Infrastructure
Hurricane/Tornado Damage
Oh yeah, the Pandemic

z/TPF Active-Active Reference Architecture



z/TPF Active-Active Reference Architecture – During a D/R Event



Primary Data Center is Lost

Workload Now Runs in D/R Site

I Have Some Good News and Some Bad News

You Have a Strong Foundation to Protect Against:

- Software Failures
- Hardware Failures
- Multiple Electrical Failures
- Mother Nature

... but nowadays there are bigger threats than that

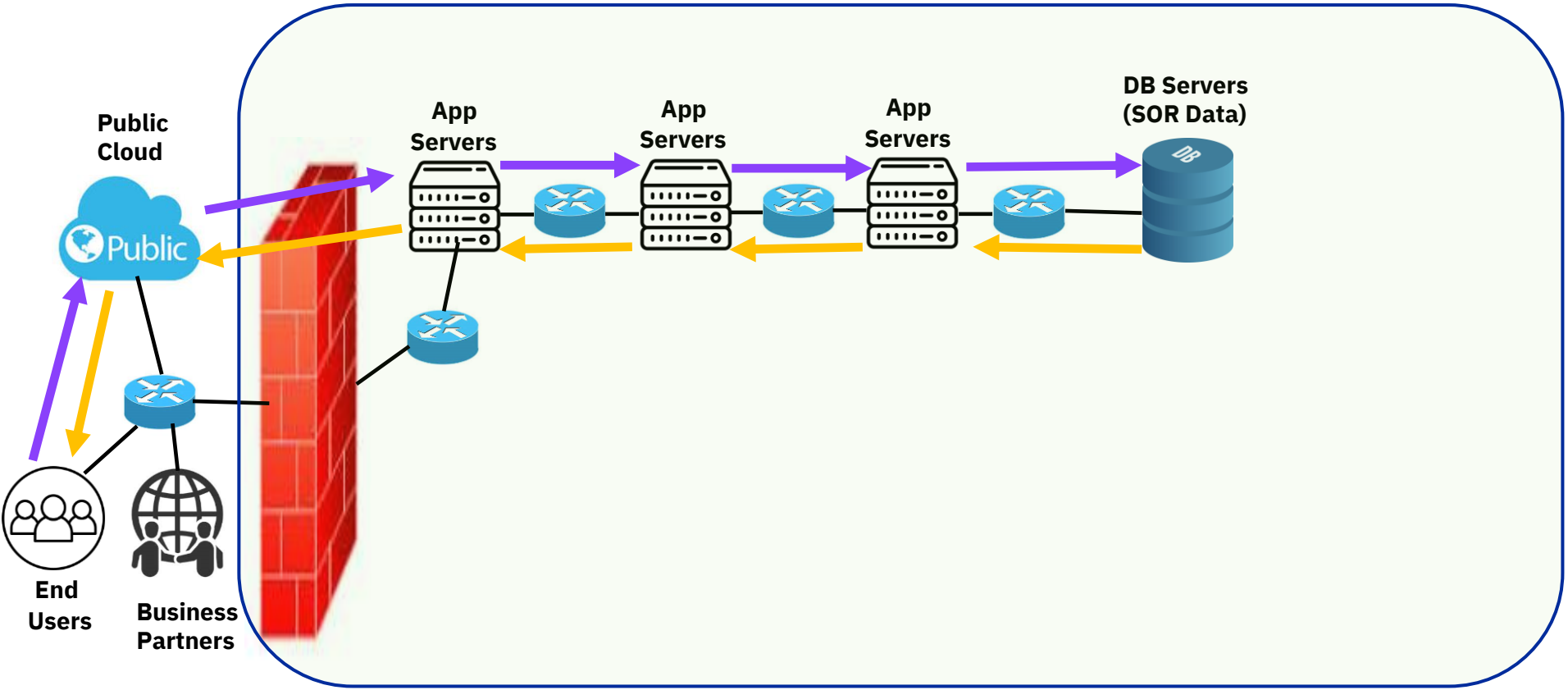
Now Let’s Look at Cyber Attacks

- What are they?
- How do they work?
- Who do they go after?
- Who does these?
- Why do they do them?
- How do I prevent them?
- How do I recover from them?

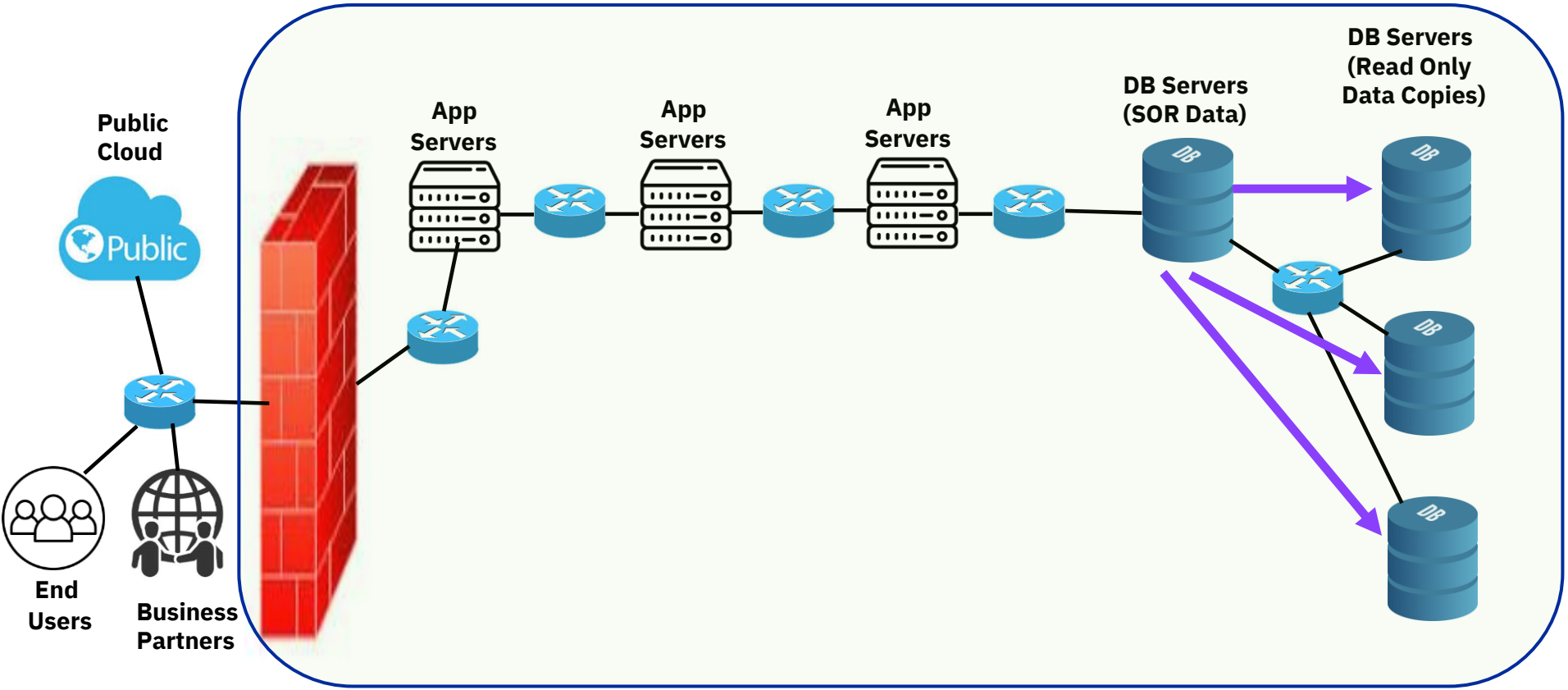
Common Types of Cyber Attacks

- **Malware** - virus, worm, trojan, ransomware, spyware
- **Phishing -** mass emails attacker makes it appear as if it's from a legitimate source hoping you will do what the email asks
- **Man-in-the-Middle (MitM)** – imbeds itself in between two legitimate parties
- **Denial-of-Service (DoS)** - flood system with requests preventing it from processing legitimate requests. Distributed Dos (DDoS) as well
- **SQL Injection** - attacker injects malicious code via SQL commands
- **Zero-Day Exploit** - after a vulnerability is disclosed, attackers exploit it before a fix/patch is released and installed
- **Password Attacks -** hack into password DB, find passwords flowing on unsecure networks, dictionary attacks, and so on
- **Cross-Site Scripting (XSS)** - typically malicious JavaScript code executed on victim's browser

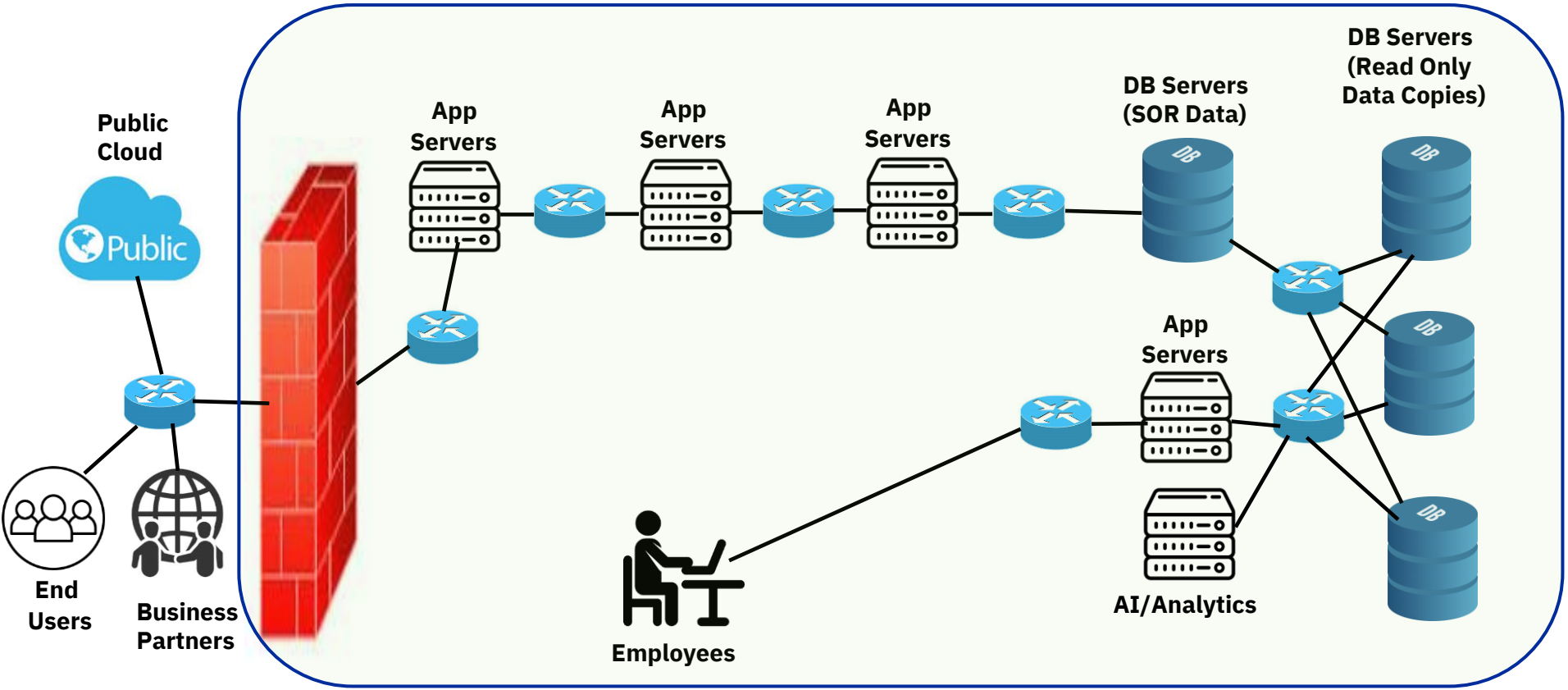
Sample Transaction Request/Reply Flow



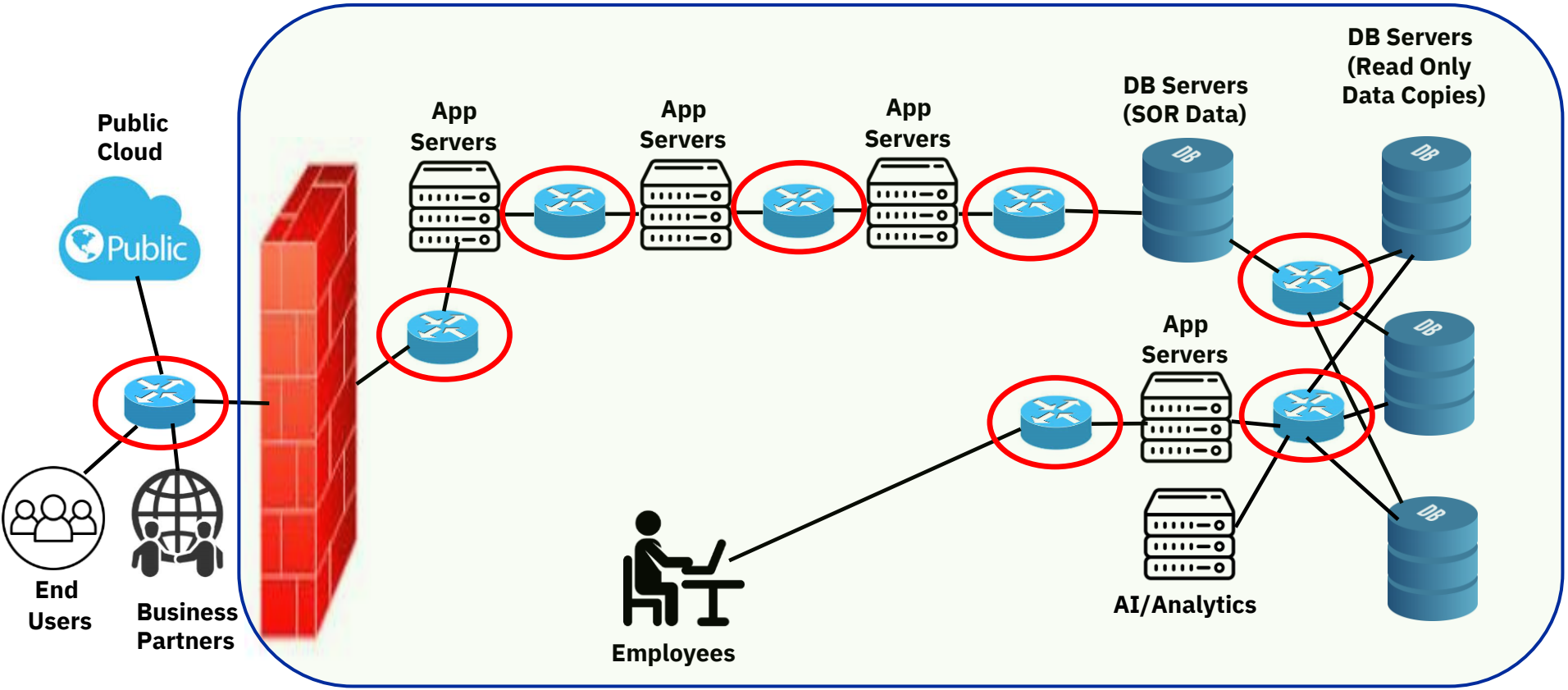
Post Transaction - Some DB Updates Propagated to other DBs



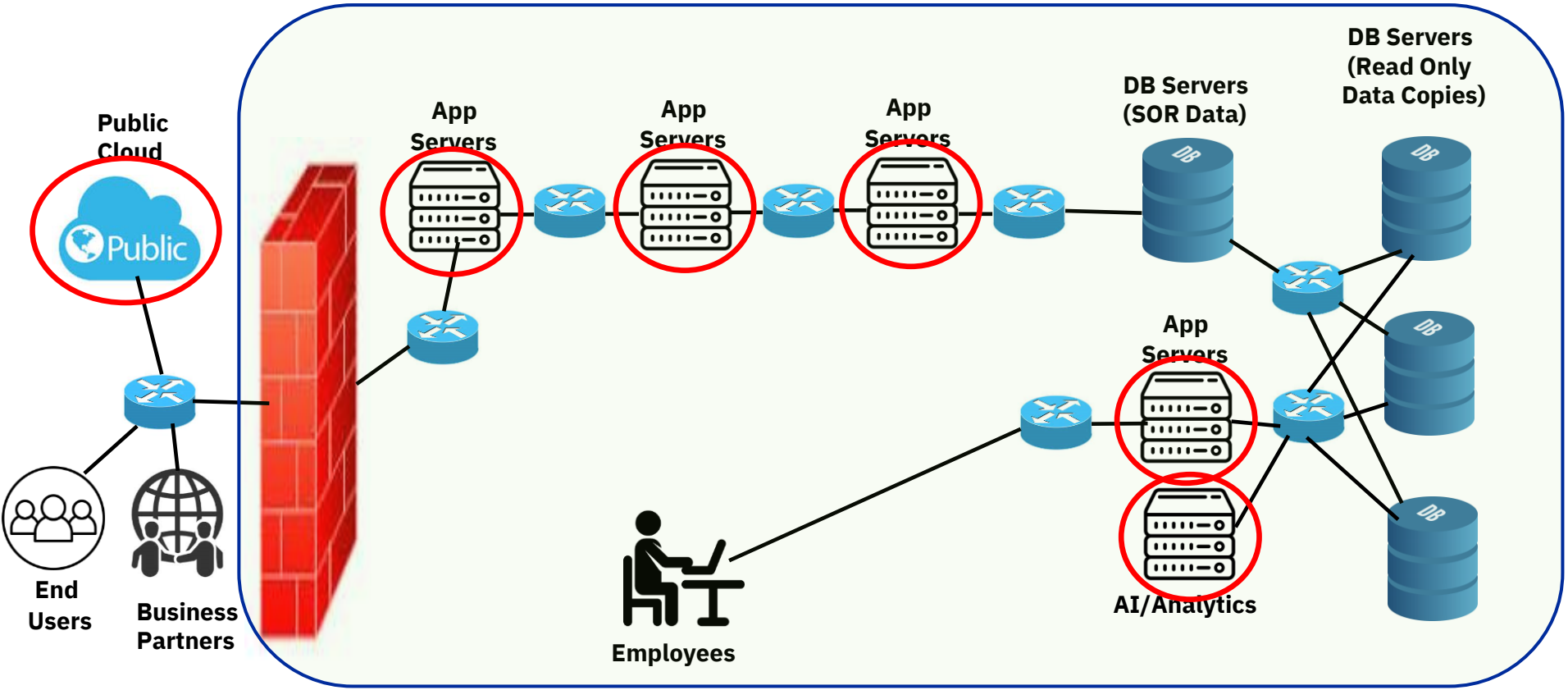
Other Parts of Your Business Work Against Read-only Copies of that Data



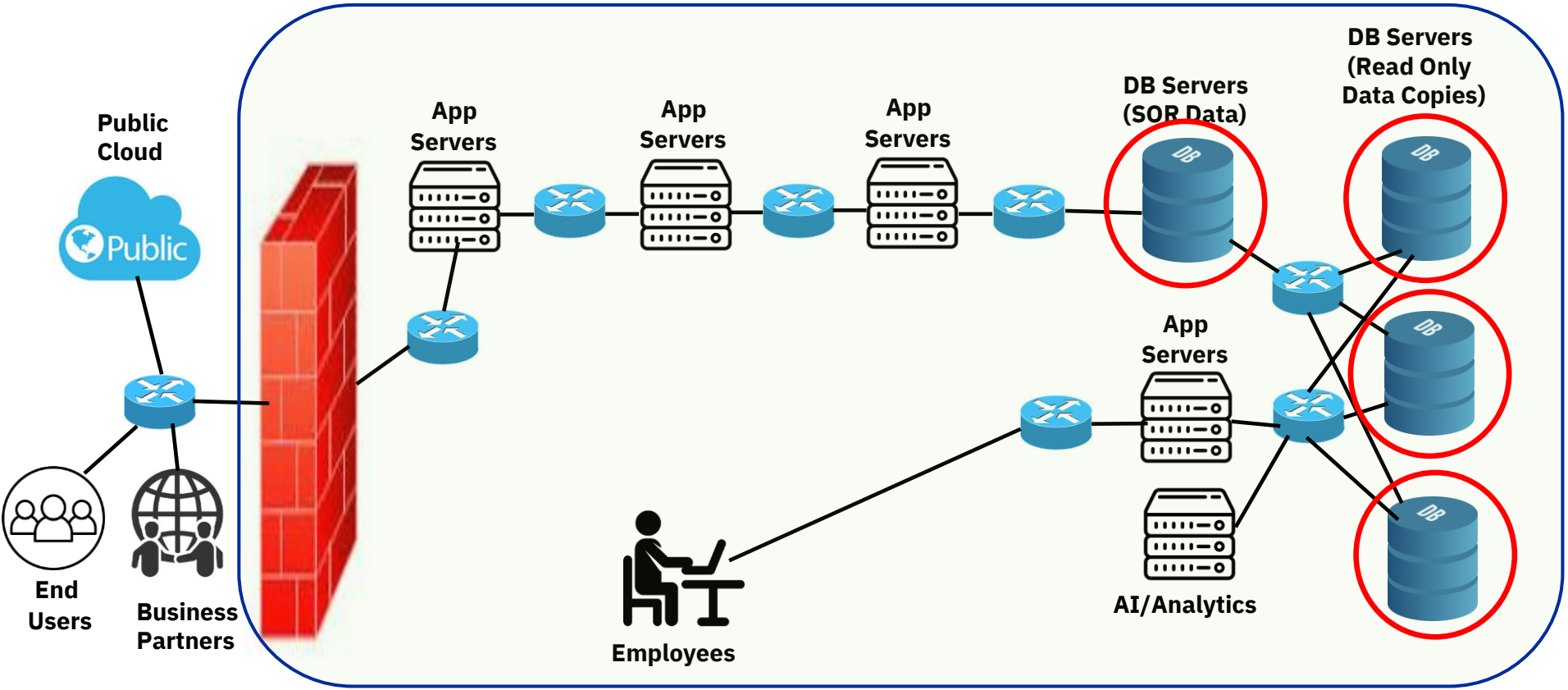
Threat Target – Network Routers



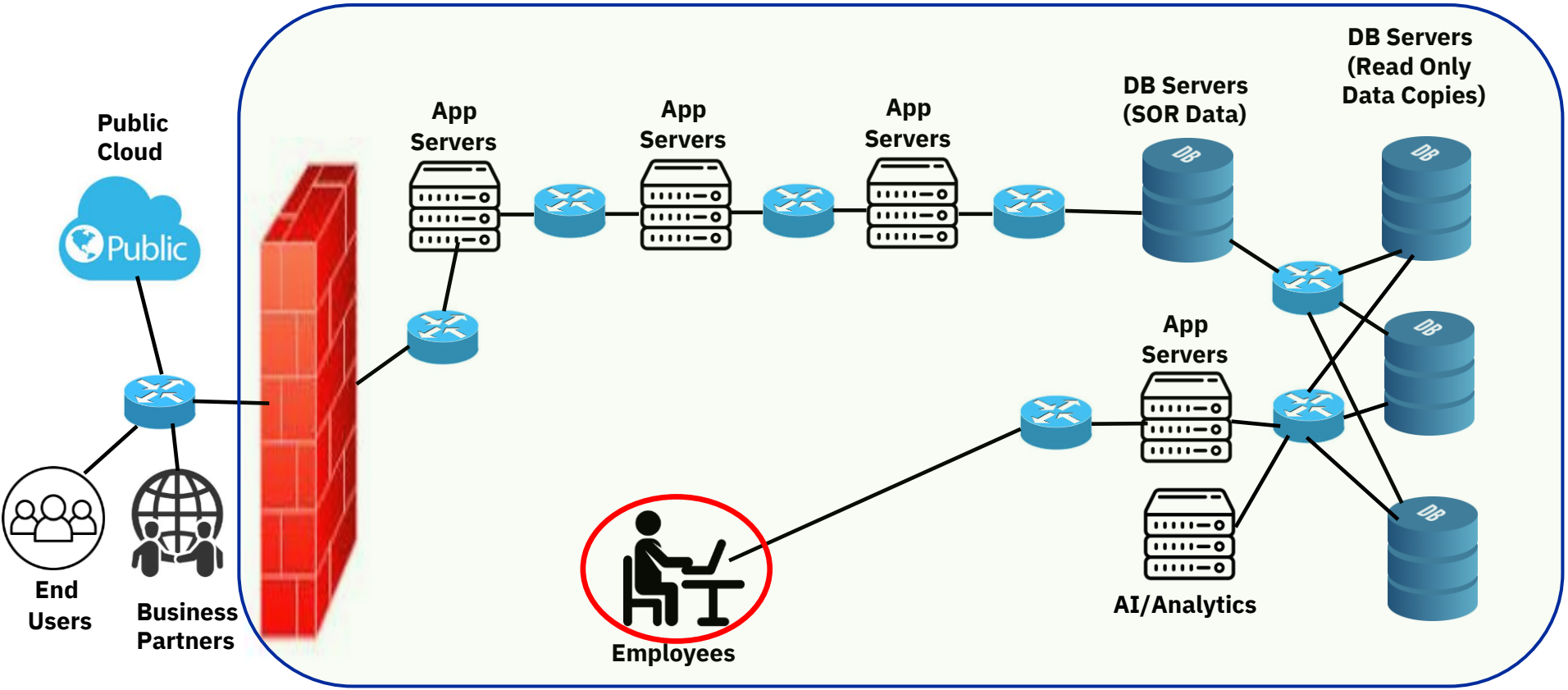
Threat Target – Application Servers



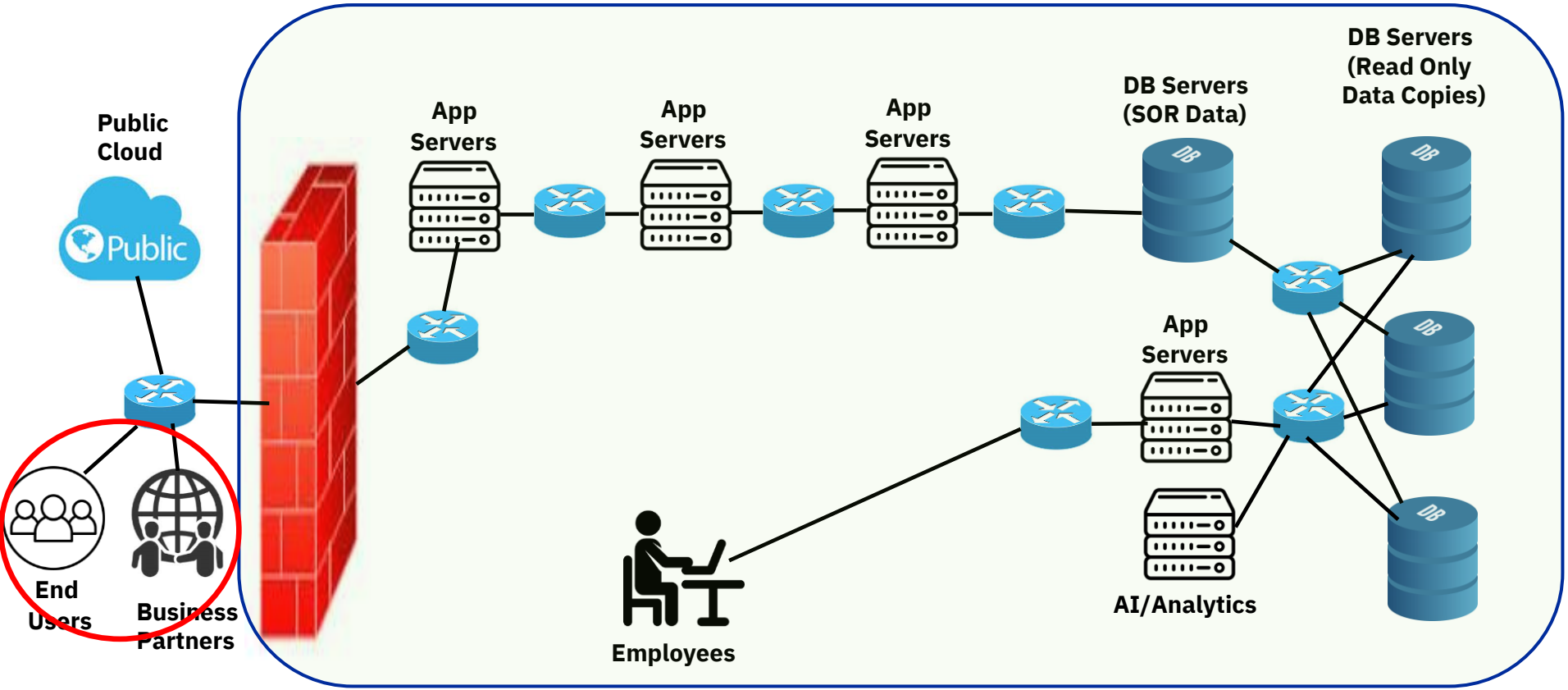
Threat Target – Database Servers



Threat Target – Your Employees



Threat Target – Your Clients



Summary of Some Things Bad Guys Can Do if They Infiltrate…

Network Routers
- View data on unsecure connections
- Record all traffic
- Multiple types of MitM attacks
- Reroute traffic to hijacker's servers

Application Servers
- Infect with malicious code
- Monitor all transactions
- Drive harmful transactions

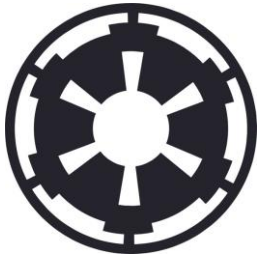
Database Servers
- Steal some/all of your data
- Corrupt some/all of your data
- Hold your data/business hostage

Your Employees
- Impersonate the employee to gain access
- Hijack the employee's account
- Grant access to other hijackers
- Infect their workstation/laptop
  - To access other parts of your business
  - To mount future attacks
  - To launch DoS attacks

Your Clients
- Impersonate the client to access/steal data
- Drive fraudulent transactions

Attacks Can Come From Anywhere...

International Terror Organizations



Interstellar Terror Groups

Bored Teenagers

Insider Threats

Cybersecurity Principles

- **Govern**
  - Identify and manage security risks
- **Protect**
  - Implement security controls to reduce security risks
  - Make compromising and disrupting your business difficult to do
- **Detect**
  - Detecting and understanding possible cyber security events
  - Leverage monitoring and analysis (AI/ML)
- **Respond**
  - Respond to and recover from cyber security incidents
  - Minimize the damage and outage time

Cybersecurity Principles – Govern (Enterprise Wide)

- **BEFORE** designing your architecture (and continuously thereafter):
  - Identify the confidentiality, integrity and availability requirements for systems, applications and data
  - Understand and adhere to industry and government regulations
  - Do threat modelling
- More and more regulations keep coming around data
  - Where must data at rest reside?
  - How am I allowed to use (and not use) the data?
  - What are the penalties for misused or stolen data?
- Embed security risk management processes into whatever risk management framework you choose
  - Such as IBM's Security and Privacy by Design (SPbD) which is an agile set of focused security and privacy practices, including threat models, privacy assessments, security testing, and vulnerability management
- Identify, document, and accept security risks before systems and applications are authorized for use

These apply to all your systems, including z/TPF

z/TPF Allows You to Control What Data Goes Where

Billing System

z/TPF Local DB
(SOR – System of Record)

PNR

PNR

PNR

Customer Support

PNR Subset

z/TPF

Data Events
(Filtering)

mongoDB.

PNR

z/TPFDF Remote Subfile Support

mongoDB.

PNR

Analytics

PNR Subset + transaction metadata

Cybersecurity Principles – Govern (Reduce the Risks)

- Limit data replication and number of copies of your data
  - Historically when there have been data breaches, it has been against these copies of the data, not the data on IBM Z

- Rather than full replication, filter data to just send what the target needs for business reasons
  - z/TPF data events allows you to filter data for each destination

- Leverage Linux on Z (LoZ) for security
  - Data flowing between z/TPF and LoZ never leaves the IBM Z box (no external networks)
  - Secure Service Container (SSC) architecture is a highly secure, trusted execution environment
  - Pervasive encryption for data volumes provides efficient end-to-end protection for data at rest
  - In addition to security benefits, for higher volume transactional workloads or heavy-weight analytical workloads LoZ has better price performance, scales higher, lower latency, is easier to manage, uses less electricity, and requires less floor space compared to thousands of x86 servers

Would You Rather Have Door Number 1...

End Users

100's to 1000's of x86 Servers

System of Record (SOR) Data

Read-Only Copies of Sensitive Data in Multiple Locations

Public

Private Cloud

Data Center

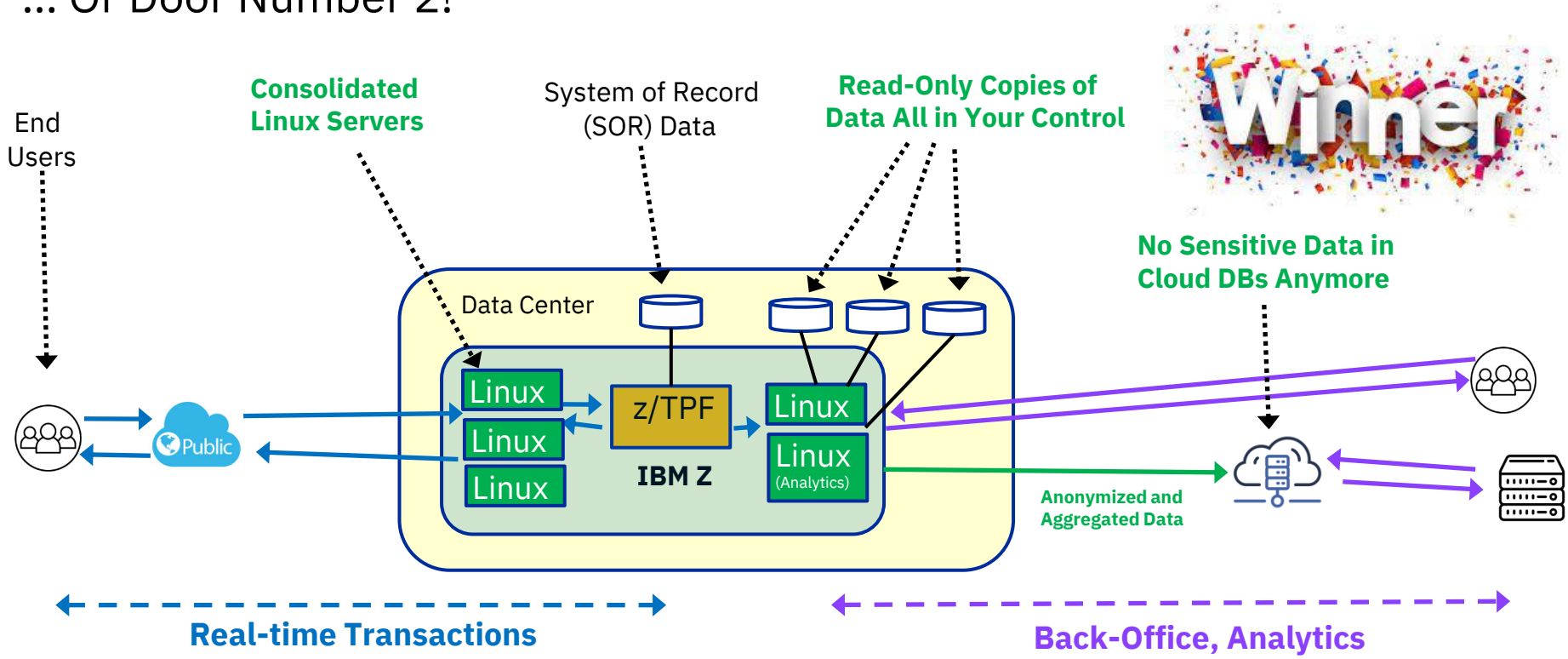
z/TPF

IBM Z

Real-time Transactions

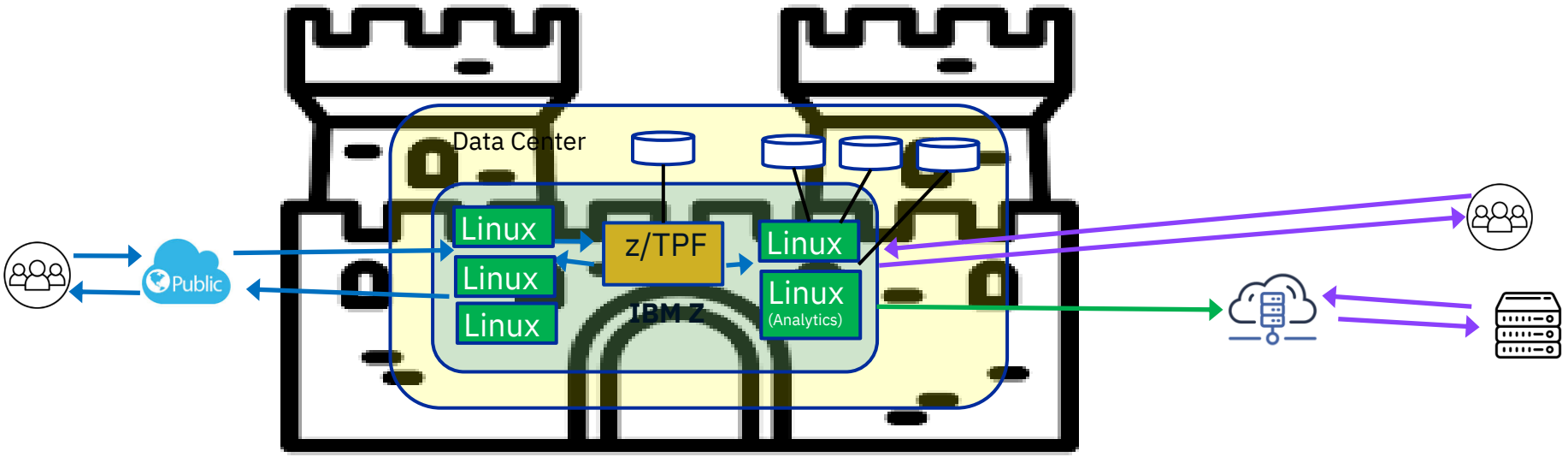
Back-Office, Analytics

… Or Door Number 2!



Better Performance, Latency, Scale, and Security!

Door Number 2 – Keep Your Friends Close and Your **Data** Closer



One Main Fortress

"An ounce of prevention is worth a pound of cure."

Benjamin Franklin

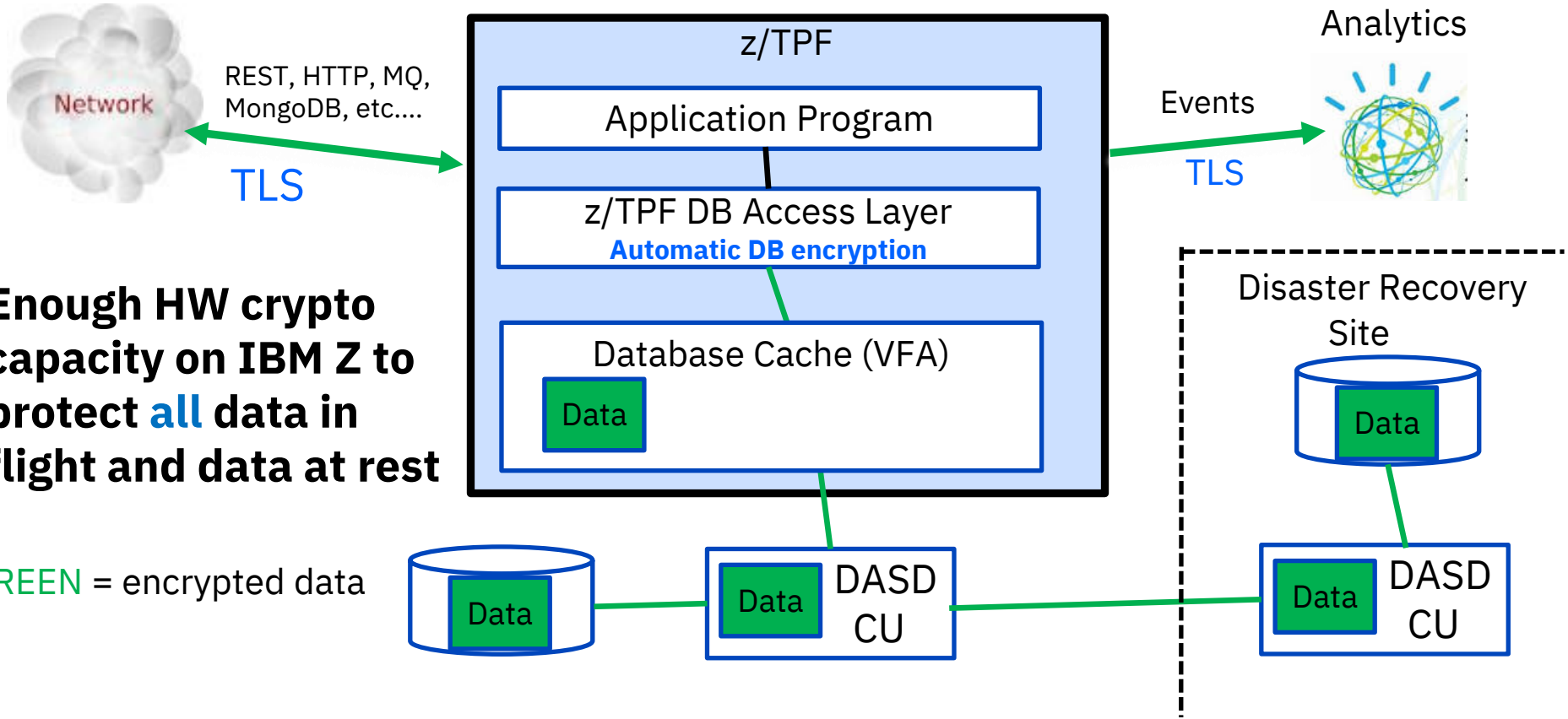
Cybersecurity Principles – Protect (Infrastructure and Systems)

- Systems and applications are delivered and supported by trusted suppliers (like IBM)
- Only trusted and supported operating systems and applications can execute on systems
  - z/TPF systems and application code can **only** be loaded by the z/TPF operator
    - Cannot file transfer (FTP) code into z/TPF and run it, even Java code
    - Cannot plug a USB flash drive into an IBM Z box
- Security vulnerabilities in systems and applications are mitigated in a timely manner
  - z/TPF ships Java refreshes at least quarterly
  - z/TPF publishes Security Bulletins when a fix for a vulnerability is available
    - Suggest you subscribe to receive notification whenever a new Bulletin is published
- Physical access to systems, infrastructure, and facilities is restricted to authorized personnel
  - Higher risk in a public cloud or other shared environment
- Personnel are granted the minimum access level to systems, applications, and data that is required to do their jobs
  - "Zero Trust" model, **but** still need people to be able to diagnose and fix problems during a crisis

Cybersecurity Principles – Protect (Data)

- Data is encrypted at rest and in flight between different systems
  - Use secure (TLS) connections to combat many MitM attacks
  - z/TPF pervasive encryption support
    - Enough HW accelerated strong cryptography capacity to encrypt all data at rest and in flight
    - Automatic z/TPFDF DB encryption support encrypts data at rest **and** cached in memory
      - No application changes required
    - APIs for applications to encrypt/decrypt data directly using secure keys
  - IBM TS1100 Tape Drive encryption protects log data and diagnostic data
- Verify that strong cryptography is used per your company security policy and required regulations
  - z/TPF Keystore displays show what type of secure keys are defined and being used
- Protect data in use (confidential computing)
  - z/TPF architecture provides isolation that prevents one process (ECB processing a transaction) from seeing data in other processes
  - Use non-displayable storage to prevent sensitive data from being displayed by an operator or from being included in system dumps

Use z/TPF Pervasive Encryption Support



Enough HW crypto capacity on IBM Z to protect all data in flight and data at rest

GREEN = encrypted data

Cybersecurity Principles – Protect (Network and Compliance)

- Use firewalls, Intrusion Prevention Systems (IPS), and Virtual Private Networks (VPNs)
- Never use default password for routers or other network equipment
- Secure your wireless access points (WAPs)
- Verify that network connections are secure
  - z/TPF Network Security Compliance support shows which connections use TLS and which do not
- Verify that strong cryptography is used per your company security policy and required regulations
  - z/TPF Network Security Compliance support shows which TLS versions and ciphers each application supports **and** which ones are actually being used
- Start preparing **now** for Quantum Computing impacts to cryptography
  - Upgrade to quantum-safe symmetric key and hash algorithms
    - z/TPF supports AES-256, SHA-256, and SHA-384 (all HW accelerated)
  - New quantum-safe public key algorithms are being developed and standardized
    - Experts predict that by the year 2030 large quantum computers will be able to break existing public key methods like RSA and ECC
    - z/TPF is adding ephemeral ECC support for TLS to use until quantum-safe methods exist for starting TLS sessions

Cybersecurity Principles – Protect (The Front Door and the Repository)

- Use centralized API Management (APIM) for all your servers/services
  - One place for user authentication and service authorization
  - One place to update when users need to be added, removed, or change in their role
- Define fine-grained services to better control access to those services
  - Instead of 1 “PNR” service with options to read and update that everyone is allowed to use, create a “Read PNR” service that everyone can use and an “Update PNR” service that is restricted to a subset of users
- Data, applications and configuration settings are backed up in a secure and proven manner on a regular basis (vaulted data).
  - Use DASD copy services to make back up copies of all z/TPF data (data, application, systems code, config settings, and so on)
  - z/TPF plans for IBM DS8000 Safeguarded Copy are being presented at this conference

Cybersecurity Principles – Protect (Employee Exploits)

- Mandate security education and training
  - Phishing attacks target hundreds of people, but only need one to succeed
  - USB flash drives can contain viruses
  - Do not open attachments from unknown persons
  - Only download/install trusted/approved software
  - … and so on
- Require antivirus software be installed and kept up to date
- Do not use the same password for all sites (work and personal)!
- Require using virtual private networks (VPNs) for remote access
- Use multi-factor authentication (MFA) for access management where appropriate rather than just userid/password
- Manage user privileges in a timely manner, especially revoking privileges no longer needed for business reasons

Cybersecurity Principles – Protect (Built into the z/TPF Architecture)

- Application bug does **not** result in root access
  - Process (ECB) is terminated
- Customer DBs and the hierarchical file system (HFS) are separate
  - Open source and Java can only access data in z/TPF DBs that you make available to them via services
- Systems and application code loads are operator controlled
  - No viruses, worms, trojans, ransomware, spyware
- No SQL injection or XSS attacks

Cybersecurity Principles – Detect (Workload and People)

- Workload overload protection – accidental or denial or service (DoS) attack
  - Traffic limiting in your API Management (APIM) layer for individual services and users
  - z/TPF traffic limiting at the application layer
  - z/TPF input list shutdown
- Identify and stop message exploits that consume too many resources
  - z/TPF ECB Resource Monitor
- "Trust but verify"
  - Feed console logs into artificial intelligence (AI) and machine learning (ML) to identify insider threats and compromised accounts like an operator is displaying 100's of DB records that contain sensitive information or other potentially suspicious activities
  - Investigate access attempt failures
    - Failed logins, attempts to use a service or access data that user is not authorized to use, and so on

Cybersecurity Principles – Detect (What is Not Normal)

- Intrusion detection services (IDS) at the perimeter
- Anomalous activities are detected, collected, correlated and analyzed in a timely manner
  - APIM bad login attempts
  - RTMC higher than normal rates for a given app or business partner, spike in message error rates, and so on
- Feed data from multiple sources/systems into analysis leveraging artificial intelligence (AI) and machine learning (ML)
  - Include z/TPF RTMC data for multi-platform workloads
  - Build history data to have baseline for anomaly detection

Cybersecurity Principles – Respond (Get Me Back to Normal)

- Business continuity and disaster recovery plans are enacted when required
  - You should practice these periodically because you do not want to find out the hard way during a crisis that your plans are out of date
- z/TPF System Recovery Boost (SRB) on z15 provides additional CPU capacity to get you back to steady state faster
- When an incident occurs, have plans/methods in place on how to identify and eliminate the exposure
  - z/TPF supports multiple images for code so if the issues are with application or systems code, use z/TPF loaders (TLDR and OLDR) to fallback to an earlier version of code
- Have a sequence of procedures in place for how you will get back to a "good" database state
  - Might be able to use DASD copy services to go back to a "good" copy of all z/TPF data (data, applications, systems code, config settings, and so on), but might be several days out of date
  - Leverage vaulted data technology to restore a more recent **protected** known good state
    - z/TPF plans for IBM DS8000 Safeguarded Copy are being presented at this conference

Cybersecurity Summary

- Architecture is critical to limit your exposure points and threat vectors
  - z/TPF, IBM Z HW, and Linux on Z all bring a lot to the table here
- You will be attacked - prepare for it
- Protect, protect, protect… and prevent!!
- Identify exposures, remediate, then update your protection schemes
- **If an attack is successful, understand how you will recover**

Thank you