

Cyber Attacks: How to Protect Your Data



Your hosts:

Nectar Daloglou

Mike Furgal

George Kiorpelidis





U.S. intelligence chief warns Congress of rise in cyberattacks - *May 2024*

UnitedHealth CEO tells lawmakers the company paid hackers a \$22 million ransom - *May 2024*

Microsoft needs to prioritize security over feature development: Former CISA Director Chris Krebs - *April 2024*

U.S. warns newly discovered malware could sabotage energy plants - *April 2024*



About Nectar Daloglou



President of OmegaServe and Senior DBA

Working with Progress for over 25 years.

Three-time winner of the DBA Challenge at the Progress User Group Conference

Performed specialized services at more than 100+ Progress customer sites

nd@omegaserve.com | omegaserve.com



About OmegaServe



Managed DBA Services

- 24/7 Monitoring & Support
- Migrations
- Health Checks
- Business Continuity planning and implementations
- Pro2 Implementation & Monitoring

Specialized in Progress

Our goal: The end of downtime!

Official ProTop Reseller

Cyber Attacks: What Can Be Done?

- **Bad Actors look for weak points in the infrastructure**

- Email and Phishing
- Port Scanning for known exposed software
- Immature Authentication
- Many more

- **This session will cover OpenEdge specific items**

- Authentication
- Encrypting data in motion
- Encrypting data at rest
- Recovery if/when a breach occurs



Authentication in your application

- **Password Management**

- Password Expiration
- Password Requirements

- **Single Sign-on**

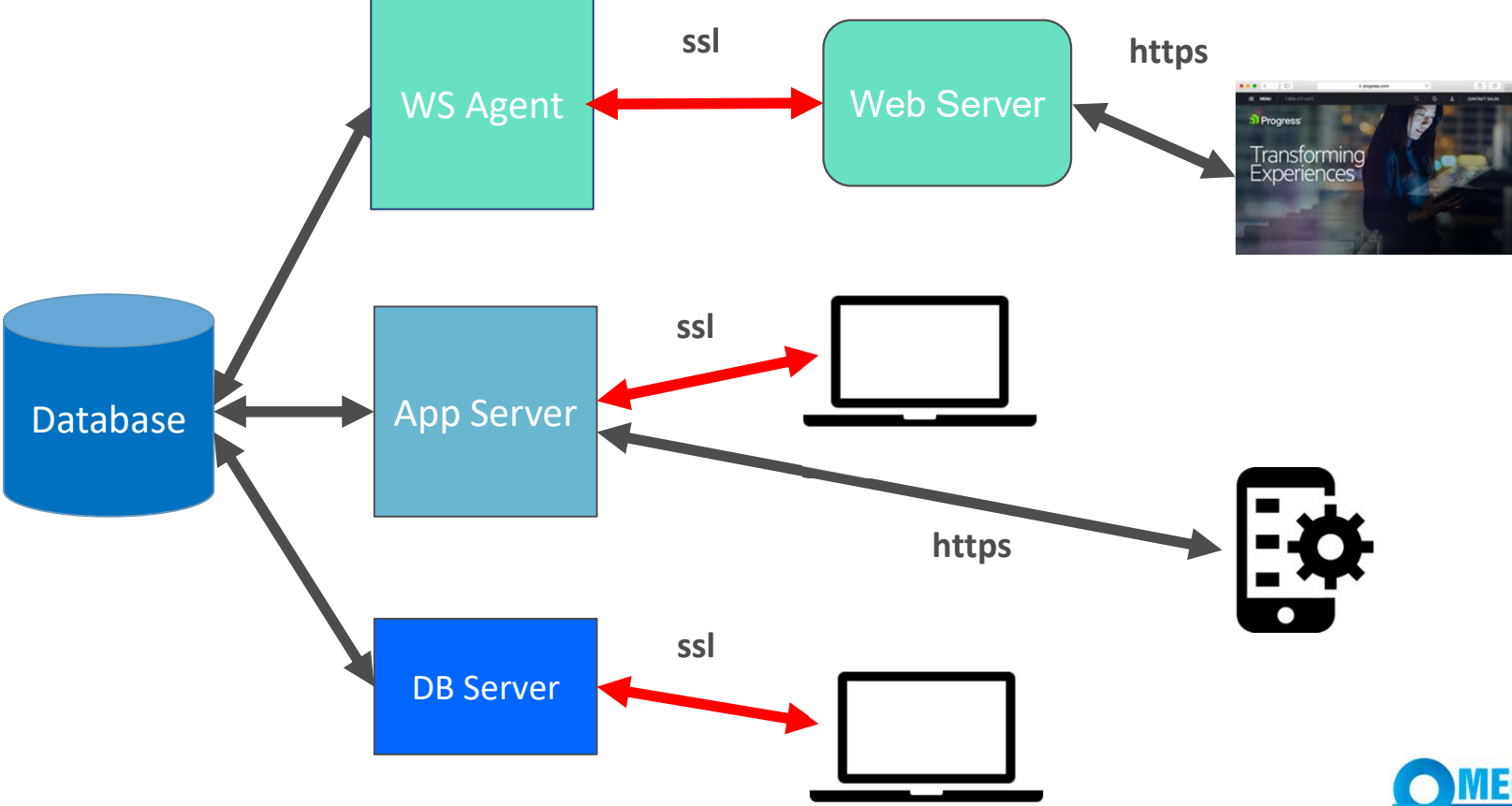


Encrypting Data in Motion

- When on the wire encryption is needed
 - When access is outside a VPN
- OpenEdge has Secure Sockets Layer (SSL) for all wire transmissions
 - Easy to implement
 - Has considerable performance penalty



Securing Data In Motion – Implementation



Securing Data In Motion – Implementation

Configuration Change

- Add the `-ssl` command line switch to the database server and the clients
- Use of HTTPS in Tomcat (for .NET UI)
- All network messages are encrypted when sent and decrypted when received

Significant performance penalty due to the number of times `encrypt()/decrypt()` is called



Securing Data In Motion – Performance



Data Entry requires 7 SSL operations

Updates a record across the network:

1. Client ask for a record in a message (encrypt)
2. Server provides the single record in a message (decrypt)
3. Client responds that it received the record in a message (encrypt)
4. Client asks to lock the record in a message (encrypt)
5. Server responds that it is locked in a message (decrypt)
6. Client sends updated record to the server in a message (encrypt)
7. Server responds that the record has been updated in a message (decrypt)

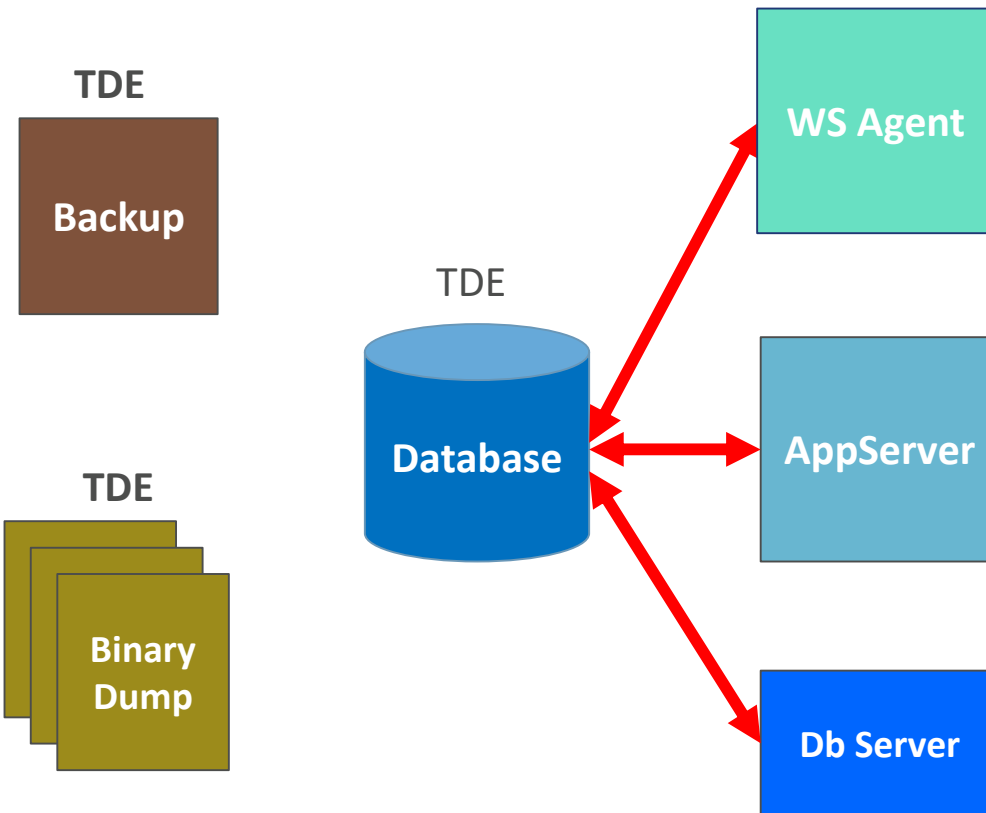


Reporting requires 2 SSL operations

Fetching 50 records across the network:

1. Client asks for 50 records, bundled up a single message (encrypt)
2. Server provides 50 records in one message (decrypt)

Securing Data At Rest



Transparent Data Encryption

- Encrypt/Decrypt at the Database I/O level
 - Encrypt() at write()
 - Decrypt() at read()
- Pick Tables or Areas to Encrypt
- Seamless to the Application

Securing Data At Rest– Implementation

- **Add Encryption Policy Storage Area**
 - e "Encryption Policy Area" :100,32;8 .
- **Enable the Database for Encryption**
 - proutil mfgprod –C enableencryption –Autostart admin
 - Passphrase must have 8+ characters, 1+ capital, 1+ numeric, 1+ special
- **Create a Policy to Encrypt a Storage Area**
 - proutil mfgprod –C epolicy manage area encrypt “Area Name”
- **Create a Policy to Encrypt a Specific Table**
 - proutil mfgprod –C epolicy manage table encrypt "pub.tr_hist”



Securing Data At Rest– Implementation

- **Encrypt legacy data**

- proutil mfgprod –C epolicy manage table update "pub.tr_hist"
- proutil mfgprod –C epolicy manage area update "Area Name"

- **Warning! This can take long on large areas/tables**

- Run off hours
- Benchmark in Test

- **Do not lose the mfgprod.ks (keystore file)**

- Make copies of this, email it to yourself (securely)
- DO NOT STORE WITH BACKUPS!
- If lost, DB is gone, no tool to gain access to database!!!



Securing Data At Rest – Performance

Data Entry

- Updates a record across the network
 - Client ask for a record
 - Database Server reads a database block that contains 100 records (decrypt)
 - Client updates the record
 - Database Server writes a database block (eventually) (encrypt)

Reporting

- Client asks for 50 records
 - Database Server reads a database block that contains 100 records (decrypt)

No detectible performance penalty.

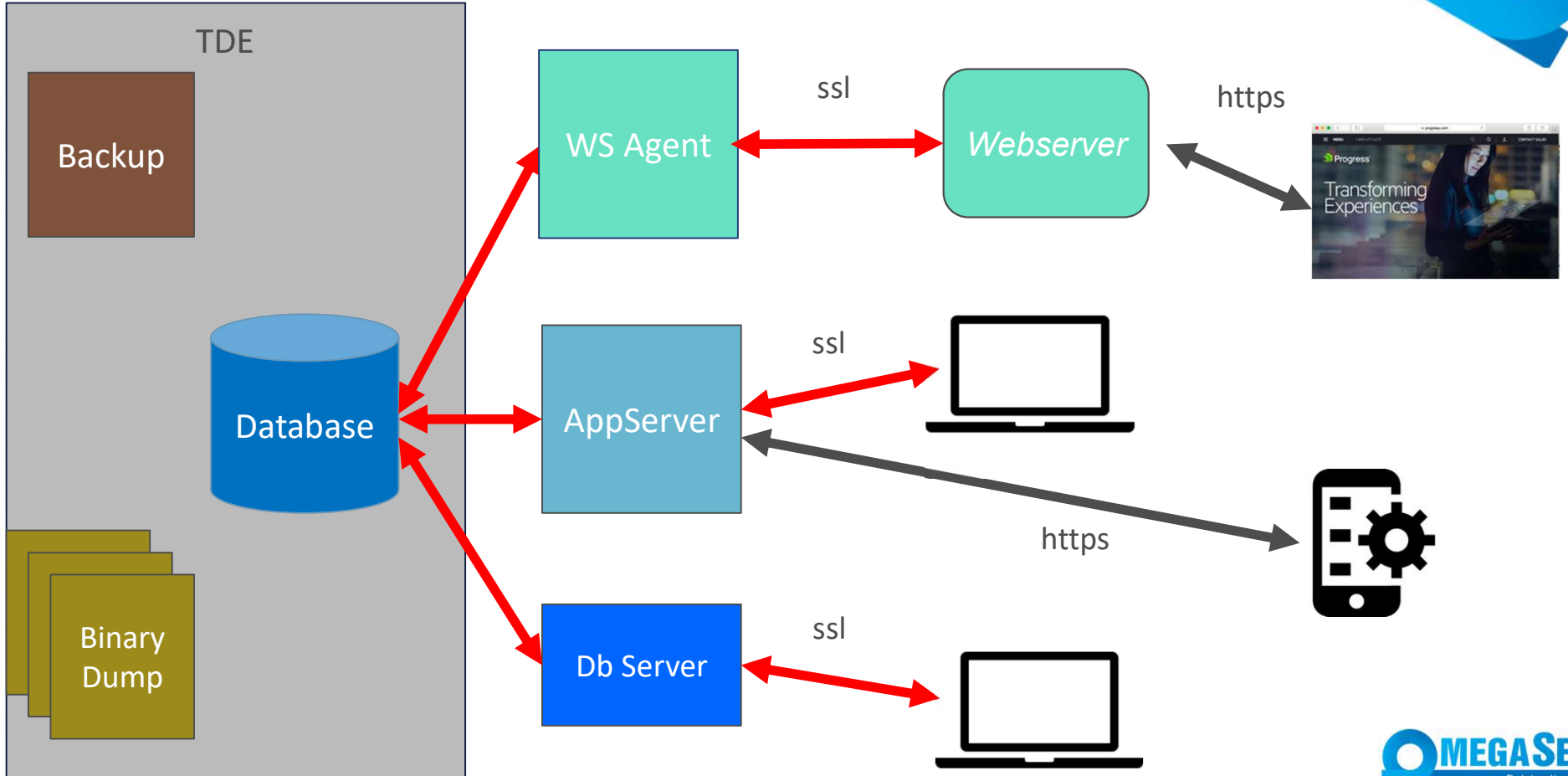


Offsite Storage of Database Backups

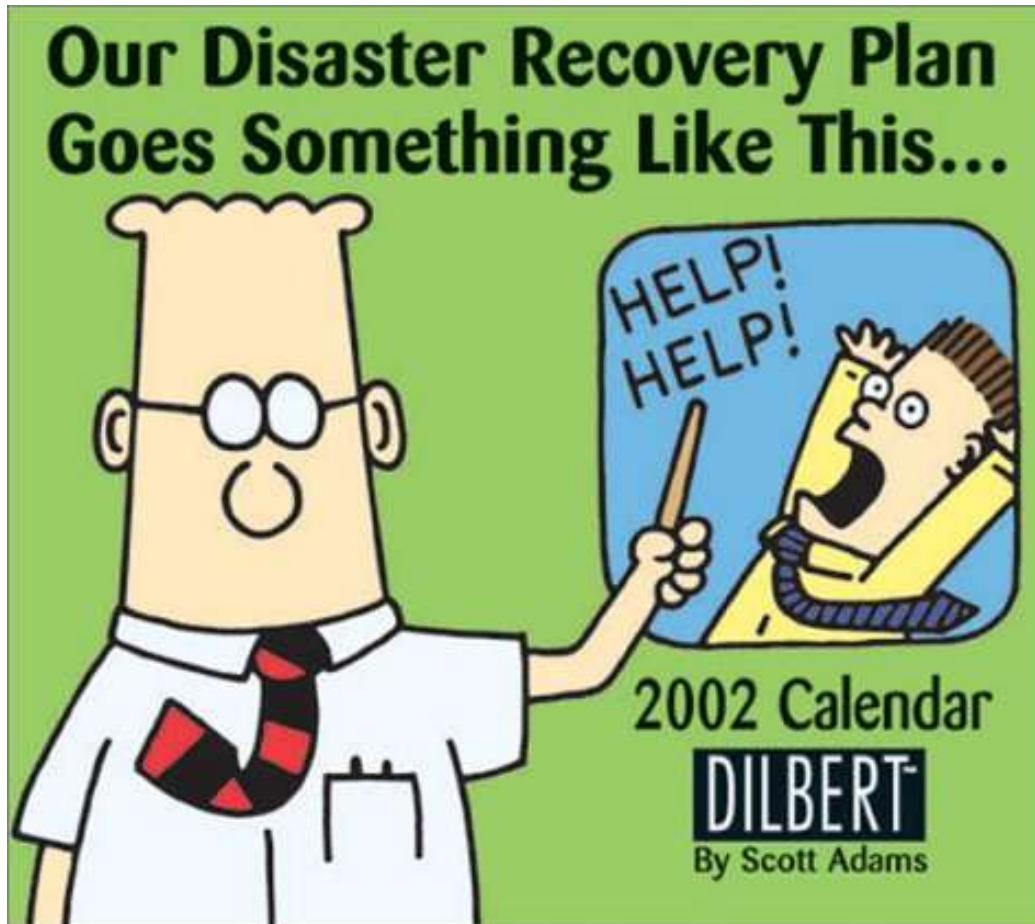
- Database Backups need to be stored on a separate machine that the production machine
- Store the Database Backups in the cloud
- What happens if someone gains access to these backups?
 - Transparent Data Encryption keeps the private data secure provided that the keystore is not with the backup



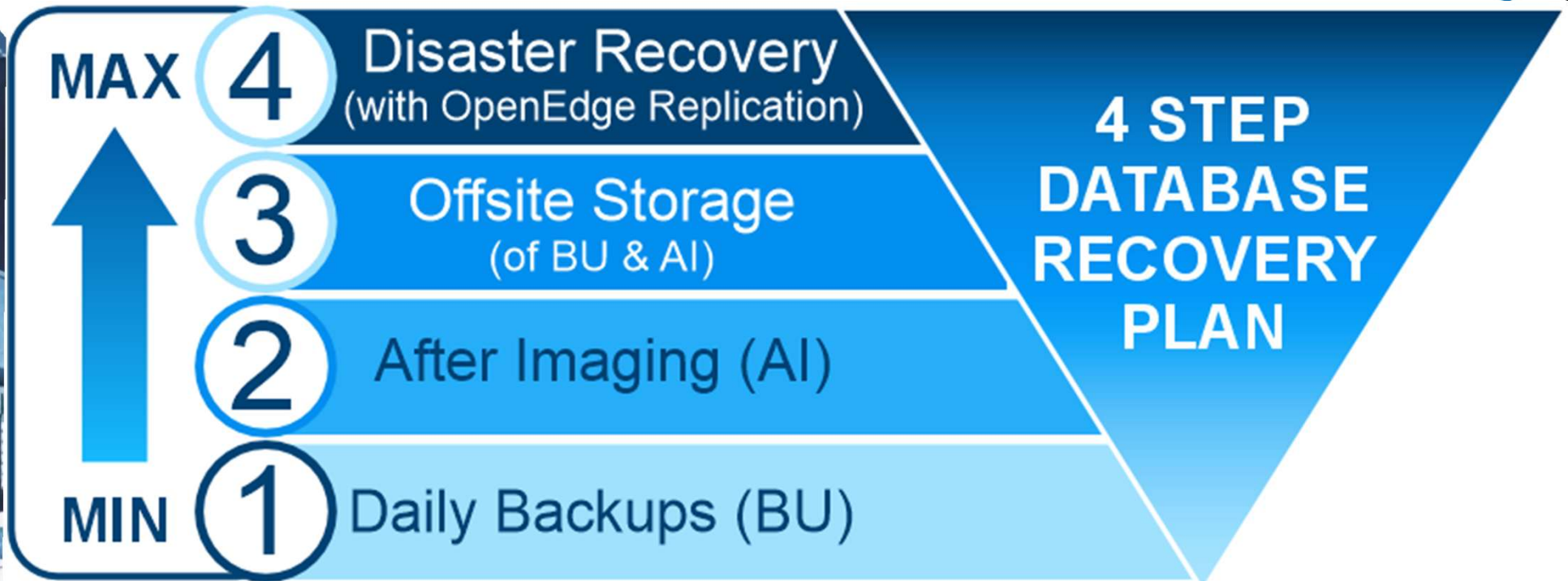
Bringing it all together...



Dealing with Disasters



Dealing with Disasters



QUESTIONS?





THANK YOU!

for more information visit:
www.omegaserve.com/cybersecurity