Infrastructure at your Service.

Elking your PostgreSQL Database Infrastructure

About me

Arnaud Berbier
Senior Consultant

+41 79 128 91 45
arnaud.berbier@dbi-services.com

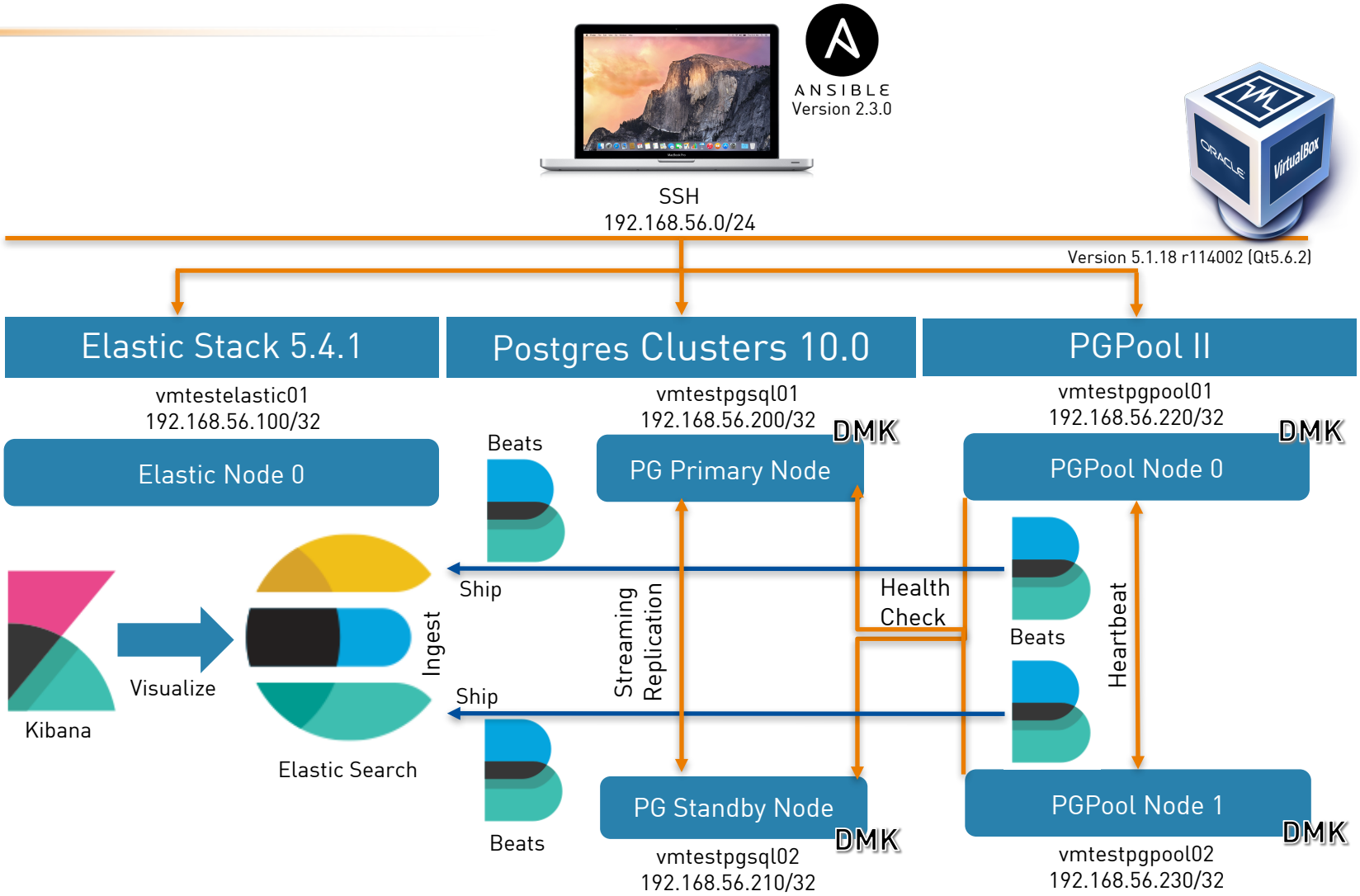
Agenda

1. Playground Infrastructure
2. Elastic Search Stack
3. PostgreSQL Monitoring
4. Conclusion

Playground Infrastructure

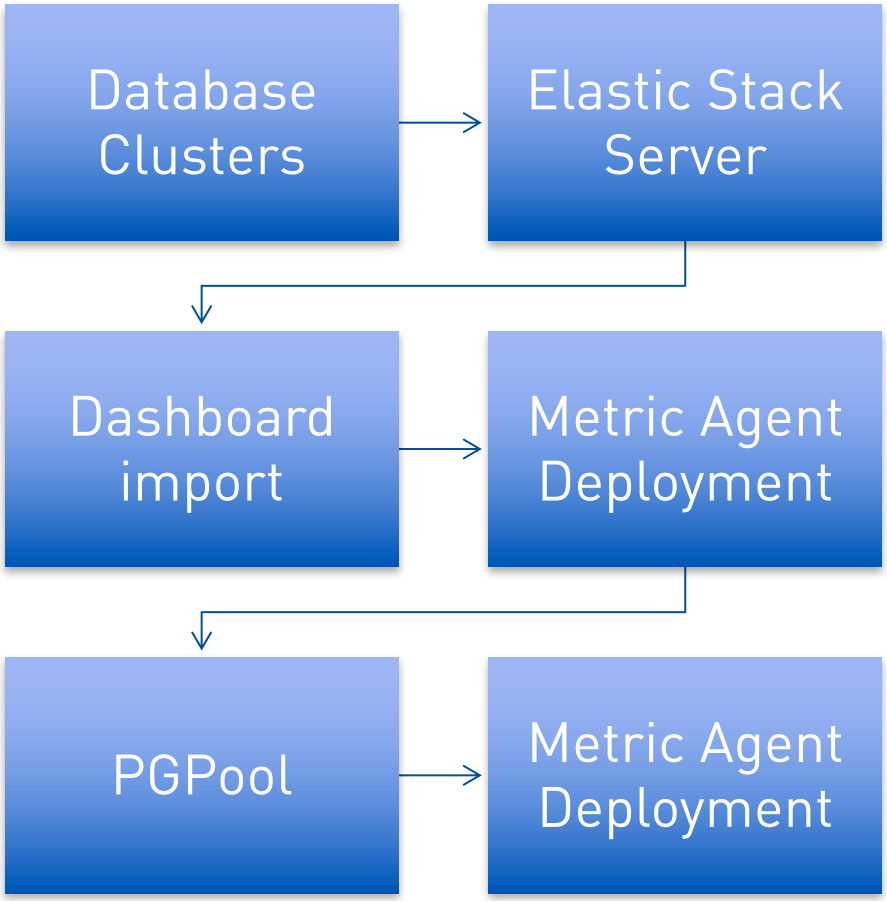
- Big Picture
- Use case and deployment process

Playground Infrastructure
Big Picture



Playground Infrastructure

Use case and deployment process



Elastic Search Stack

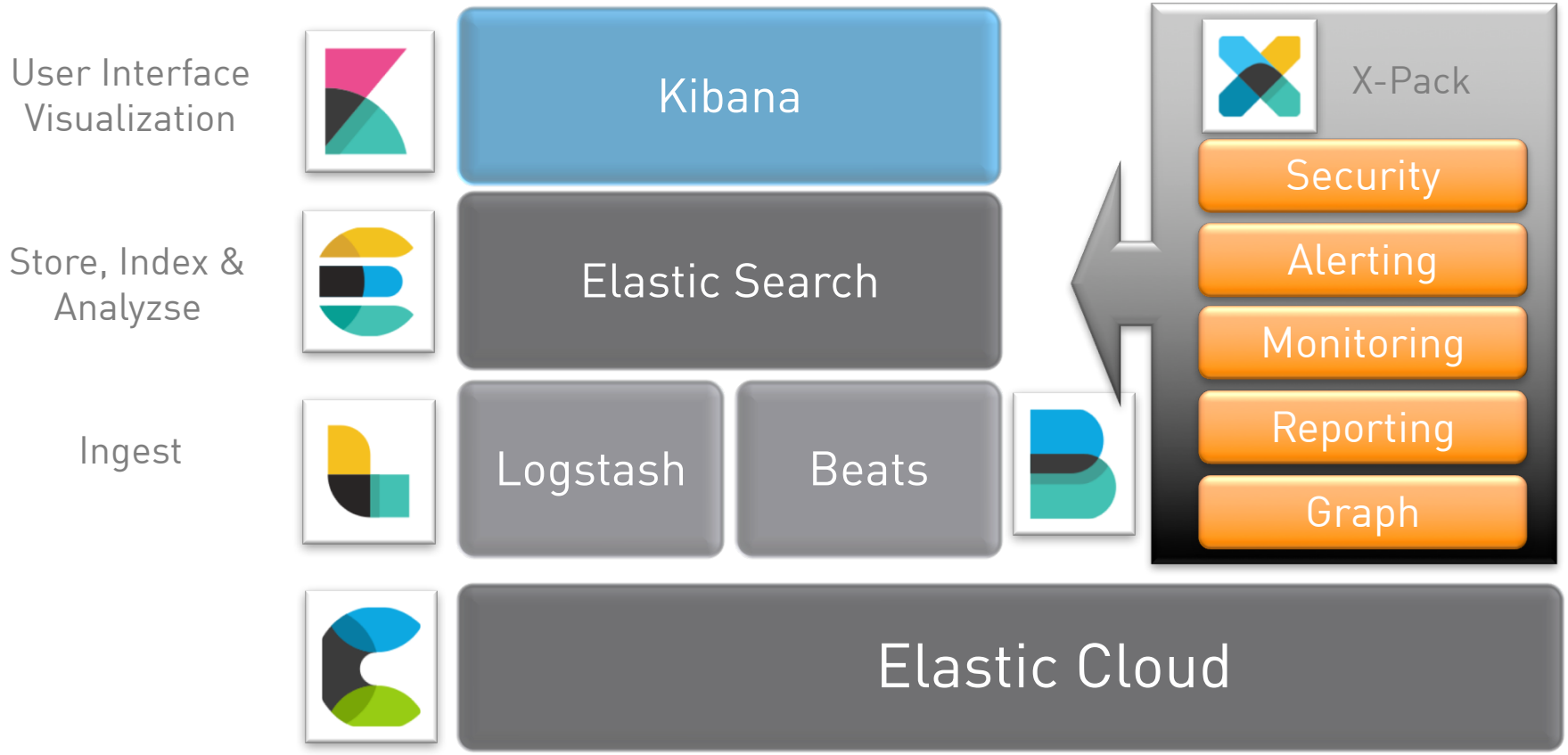
- What does ELK mean ?
- What's a Beat ?
- Is all the stack Open Source ?
- How much costs the cloud offering ?

Elastic Search Stack
What does ELK means ?

- ELK is a complete monitoring platform - Elastic Search Stack
- At the beginning Elastic Stack was commonly known as ELK
  - **E -** Elastic Search
    - Store, Search and Analyze
  - **L –** Logstach
    - Collect, Enrich and Transport
  - **K –** Kibana
    - Explore, Visualize and Share

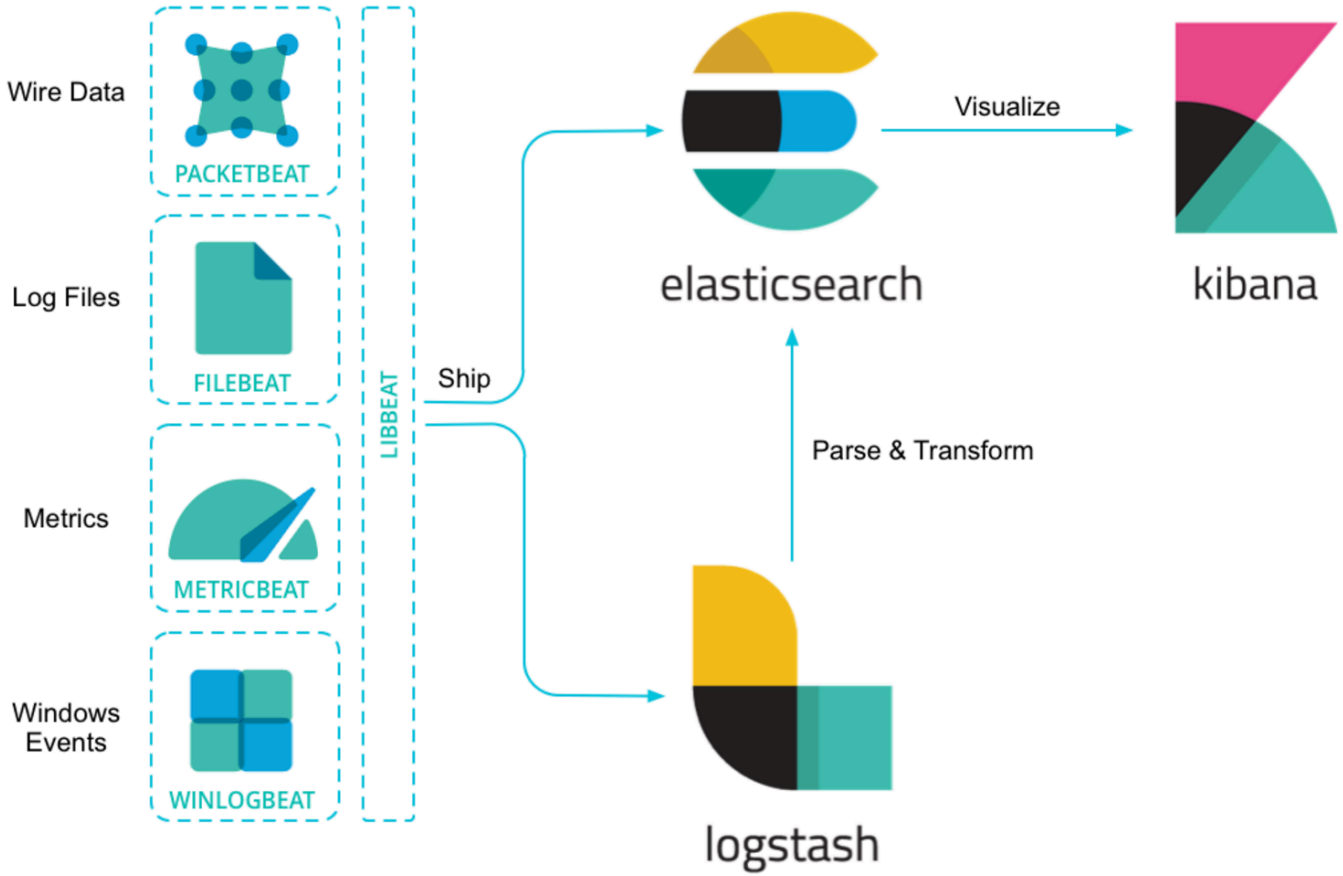
Elastic Search Stack
What does ELK means ?

- It evolved to be a full Monitoring Stack



Elastic Search Stack
What's a Beat ?

- Lightweight Data Shippers to ingest data into Elastic



Elastic Search Stack
Is all the stack open source ?

Elastic Search Stack
Is all the stack open source ?

- Components support over subscriptions

		Open Source	Basic	Gold	Platinum
Elastic Search	Elasticsearch	✓	✓	✓	✓
	Kibana	✓	✓	✓	✓
	Beats	✓	✓	✓	✓
	Logstash	✓	✓	✓	✓
X-Pack	Monitoring		✓	✓	✓
	Multicluster			✓	✓
	Configurable Data retention			✓	✓
X-Security	Authentication + Encryption			✓	✓
	Role-Based access ctrl			✓	✓
	Audit			✓	✓
	Encryption at rest support				✓

Elastic Search Stack
Is all the stack open source ?

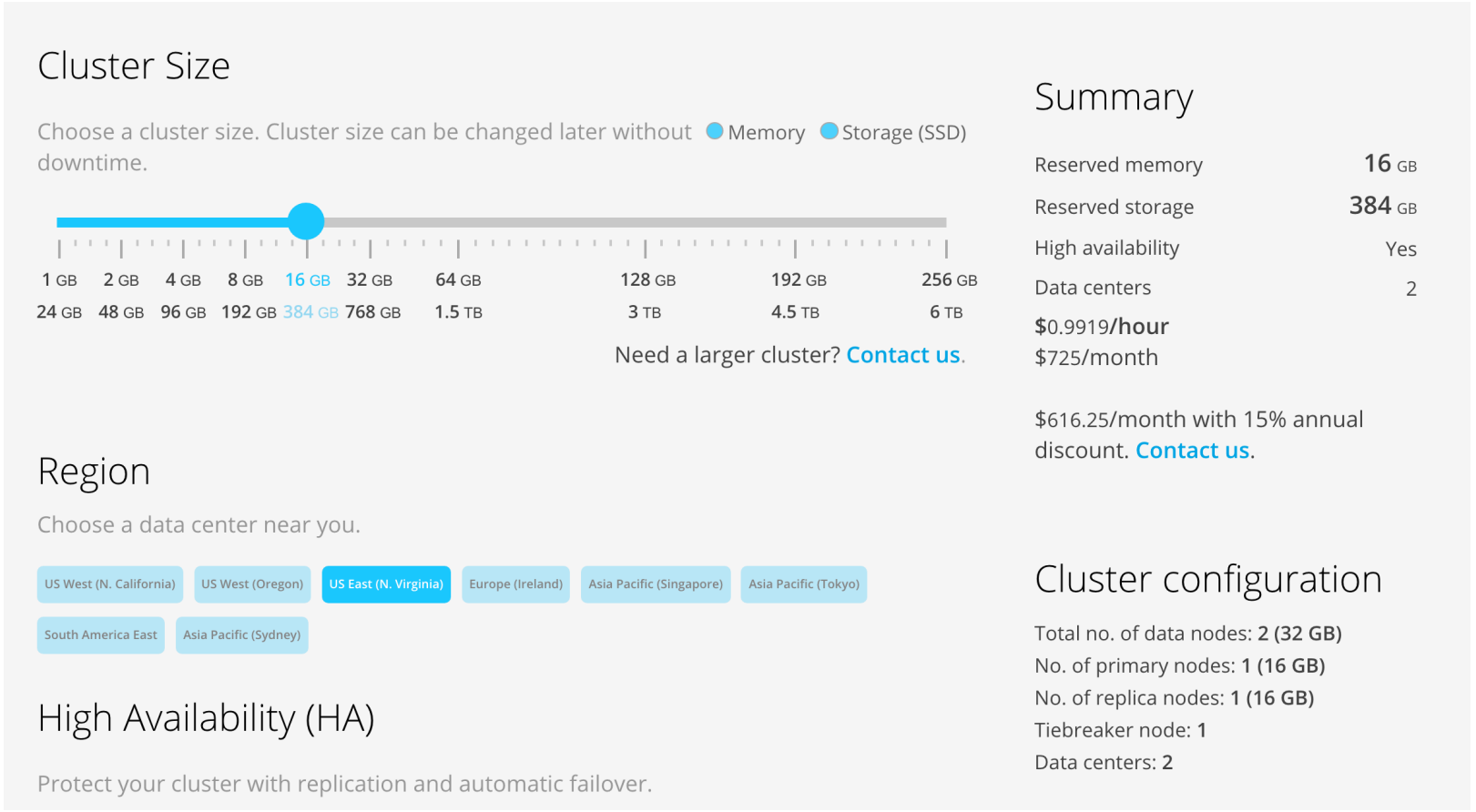
- Components support over subscriptions

		Open Source	Basic	Gold	Platinum
X-Pack	Alerting via Watcher			✓	✓
	Reporting				✓
	Graph Analytics & Visualization				✓
	Dev Tools – Search Profiler				✓
Support	Support Coverage			BH	24x7
	Response Times			Crit. 4h L2: 1d L3: 2d	Crit. 1h L2: 4h L3: 1d
	Unlimited # of Incidents			✓	✓

- Details : https://www.elastic.co/subscriptions

Elastic Search Stack
How much cost the cloud offering ?

> Elastic Cloud Offering – Host Elastic Search and Kibana



PostgreSQL Monitoring

> Postgres Cluster Settings

PostgreSQL Monitoring
Postgres Cluster Settings

- What's need to be done on the Postgres Clusters
  - Filebeat log harvesting
    - The elastic stack process owner needs access to the Postgres log files
    - log_file_mode in pg_settings parameters

```
postgres=# select name, setting, unit from pg_settings where name
like '%log_file%' or name like '%log_dir%';
name      |                  setting                          | unit
----------+---------------------------------------------------+------
log_directory | /app/postgres/admin/dbixchange01/pg_log |
log_file_mode | 0776                                    |
log_filename  | postgresql-%a.log                       |(3 rows)
```

- This correspond to file mode 666

PostgreSQL Monitoring
Postgres Cluster Settings

- What's need to be done on the Postgres Clusters
  - Metric Beat postgresql
    - A dedicated user for DB connection
    - Allowed access to the database
  - Elastic servers need to be accessible by the deployed beat agents
    - Firewall
    - Network

Conclusion
Pro & contra

- Easy to deploy
- Ingest lots of data of any log type
- Already have predefined metric such as

- Most of the required features needs subscription

Any questions? Please do ask

Arnaud Berbier
Senior Consultant

+41 79 128 91 45
arnaud.berbier@dbi-services.com

We look forward to working with you!