RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

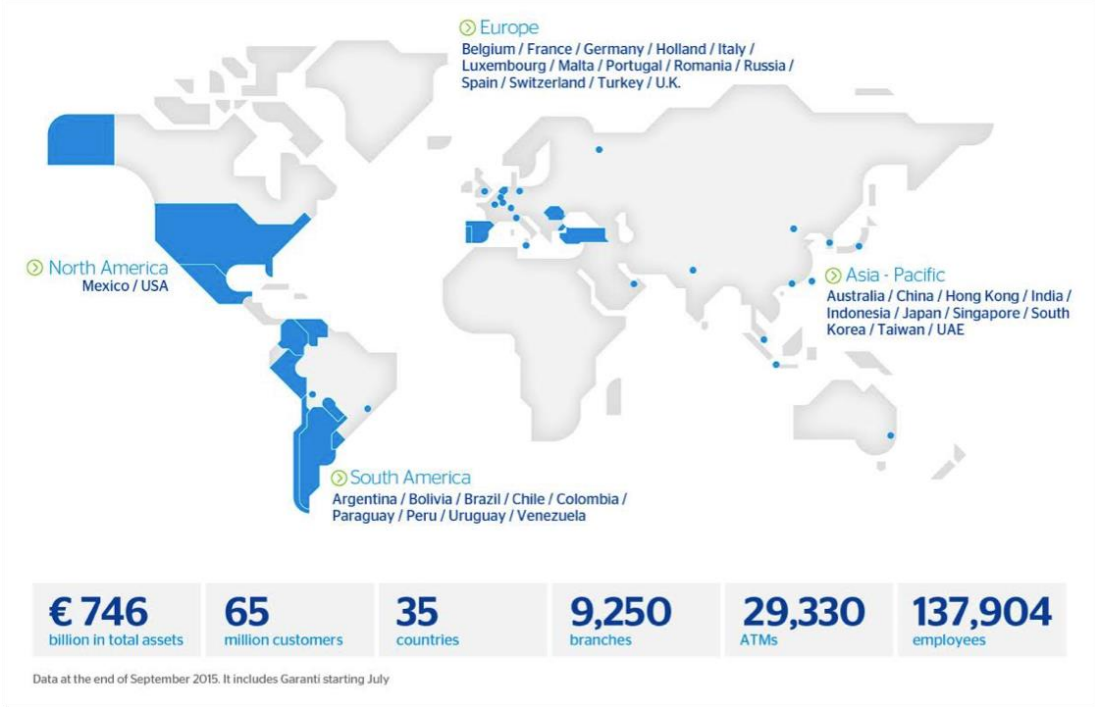
SESSION ID: ASD-F01

Security as a Service in a Financial Institution: Reality or Chimera?

Javier Losa
Cybersecurity Product Engineering
Innovation 4 Security – BBVA Group
@sealth

Iñigo Merchán
Security Architect
BBVA
@achemerchan

Our use case


Europe
Belgium / France / Germany / Holland / Italy / Luxembourg / Malta / Portugal / Romania / Russia / Spain / Switzerland / Turkey / U.K.
North America
Mexico / USA
Asia - Pacific
Australia / China / Hong Kong / India / Indonesia / Japan / Singapore / South Korea / Taiwan / UAE
South America
Argentina / Bolivia / Brazil / Chile / Colombia / Paraguay / Peru / Uruguay / Venezuela
€ 746
billion in total assets
65
million customers
35
countries
9,250
branches
29,330
ATMs
137,904
employees
Data at the end of September 2015. It includes Garanti starting July

i4s – Our security product leverage

Banks must adapt to new landscape

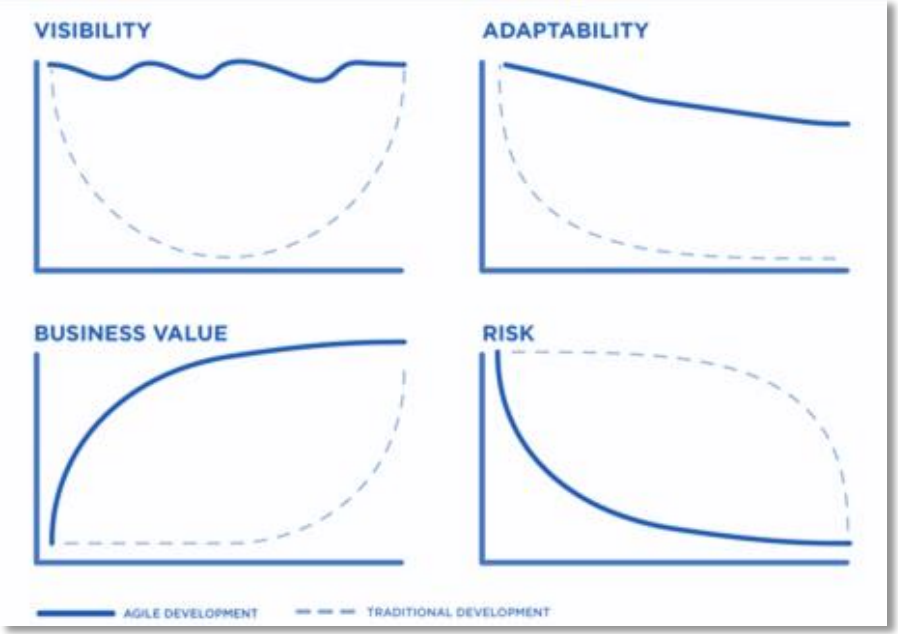
We are living a **digital revolution** that affects society as a whole (transportation, healthcare, entertainment, etc.) and Financial Services are not a exception. Banks are part of the digital revolution now because clients expect them to be.

New ecosystem, new rules

Huge changes for the industry: new customer needs, new industry players, new technologies.

Key success factors:

1. Deliver & adapt fast
2. Client & customer satisfaction
3. Better performance
4. Lower costs



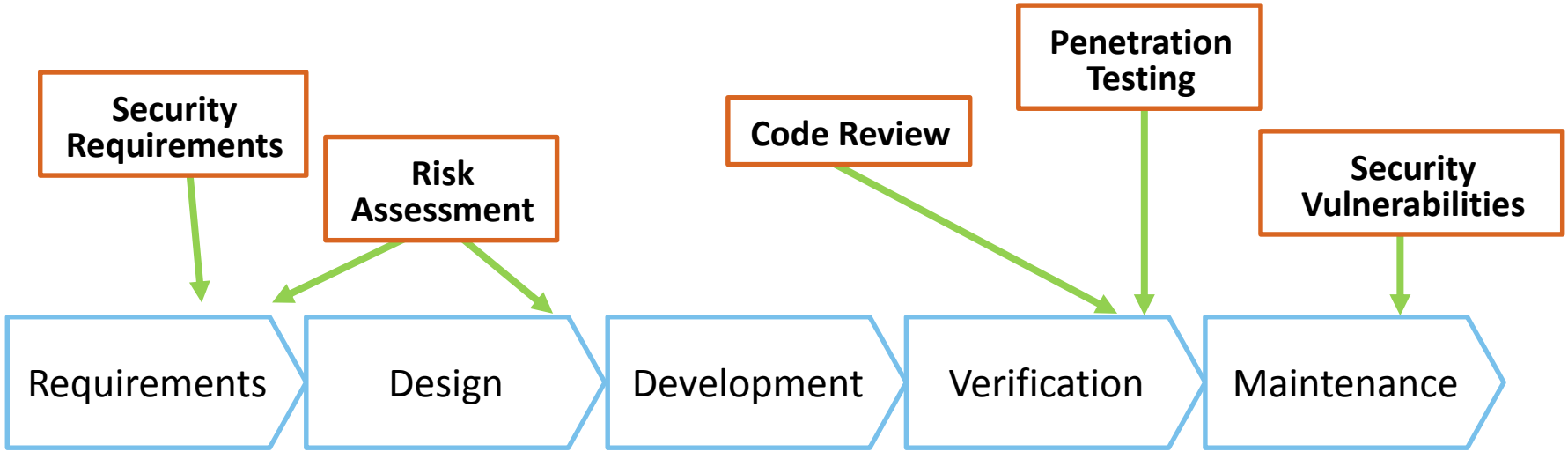
Source: Versionone

The new way of working

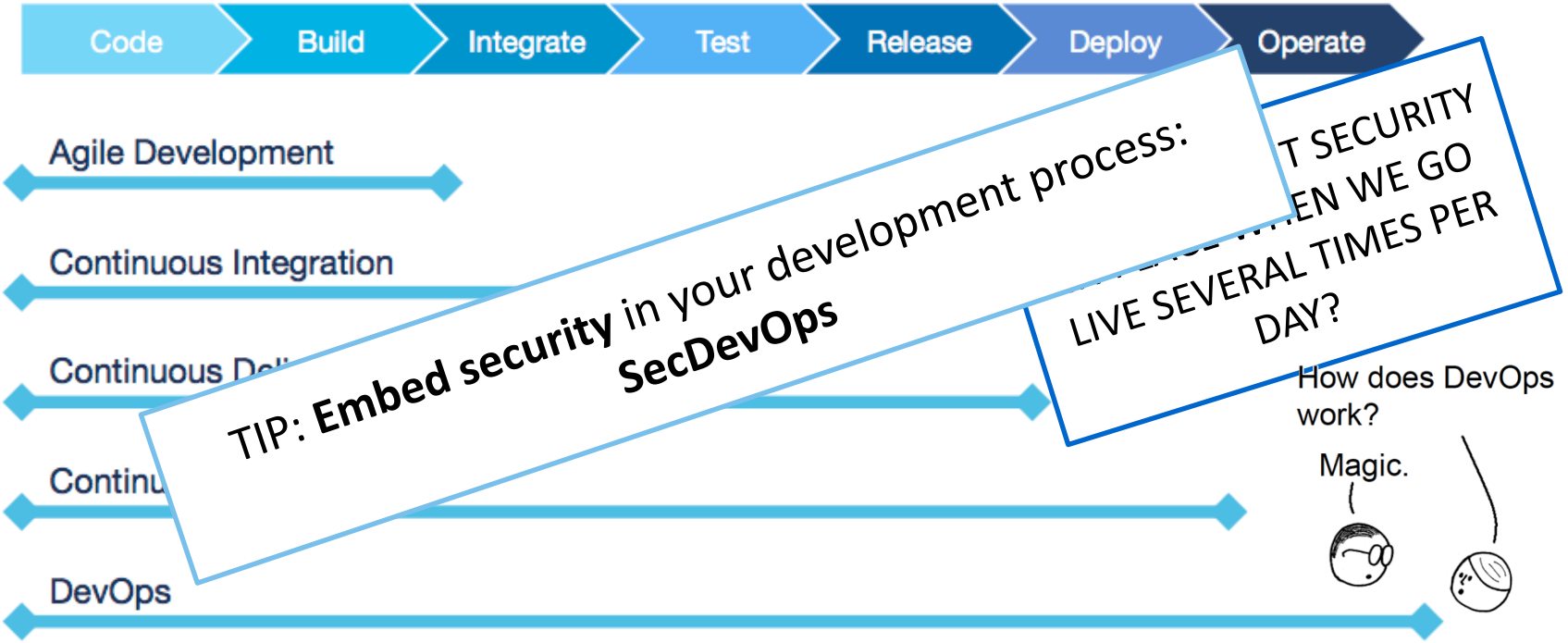
In order to meet the new paradigm, we need a different approach for security and the Digital Transformation (cloud, agile & full automation):

- 20+ Scrum teams
- Public, Private and Hybrid Clouds
- Security as a core for Knowledge Banking
- SecDevOps is part of our culture now
- SDx (Software Defined Everything)

How security in waterfall is addressed



How to address Security in Agile?



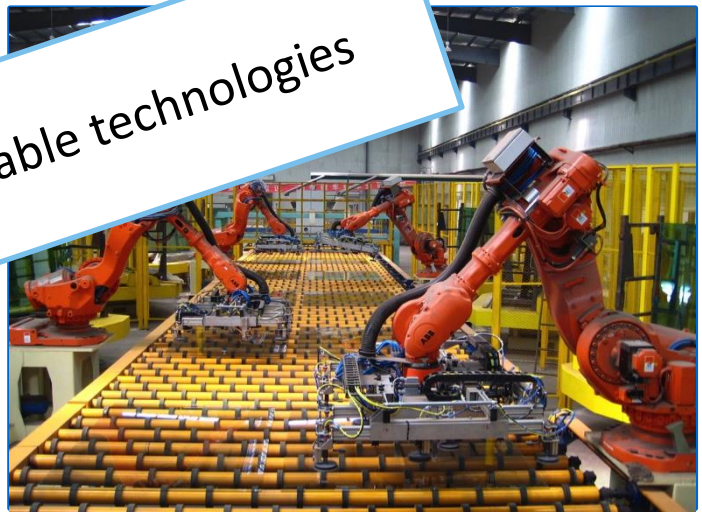
Source: RightScale

Datacenter vs. Cloud

Traditional IT Datacenter

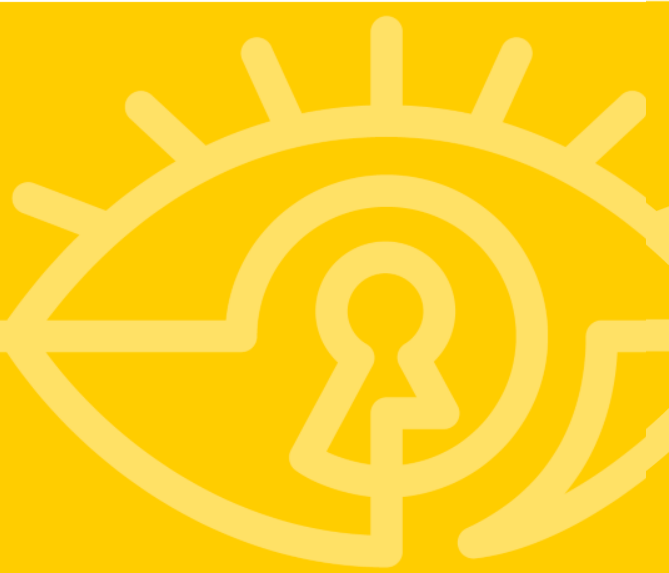
Source: MVM

Public/Hybri[illegible]ivate Cloud



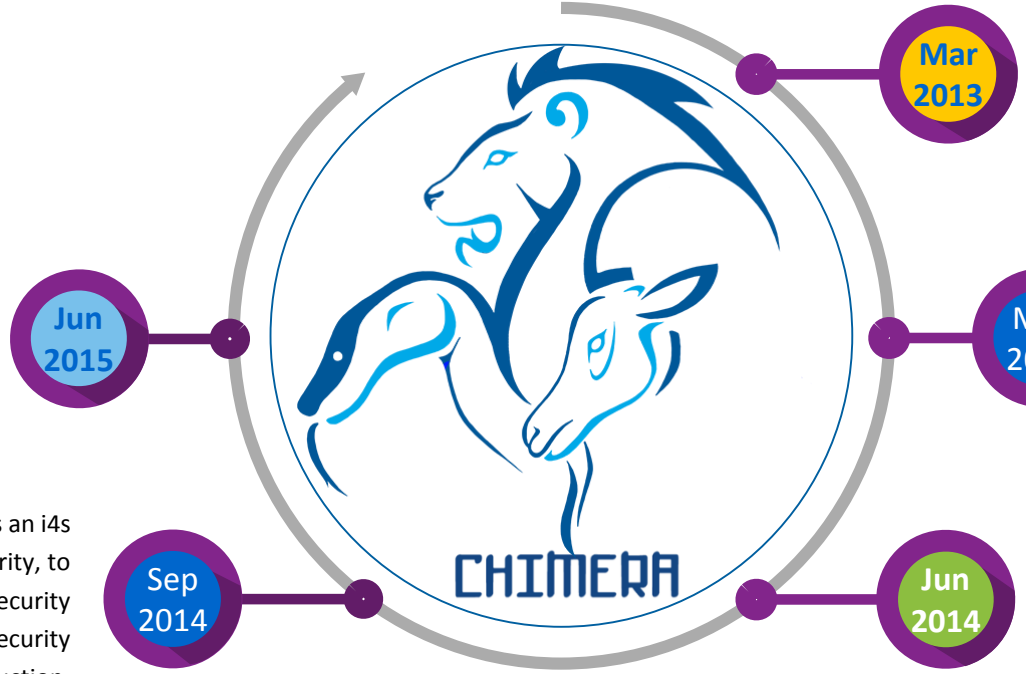
Source: Wikipedia

TIP: Take **advantage** of new available technologies

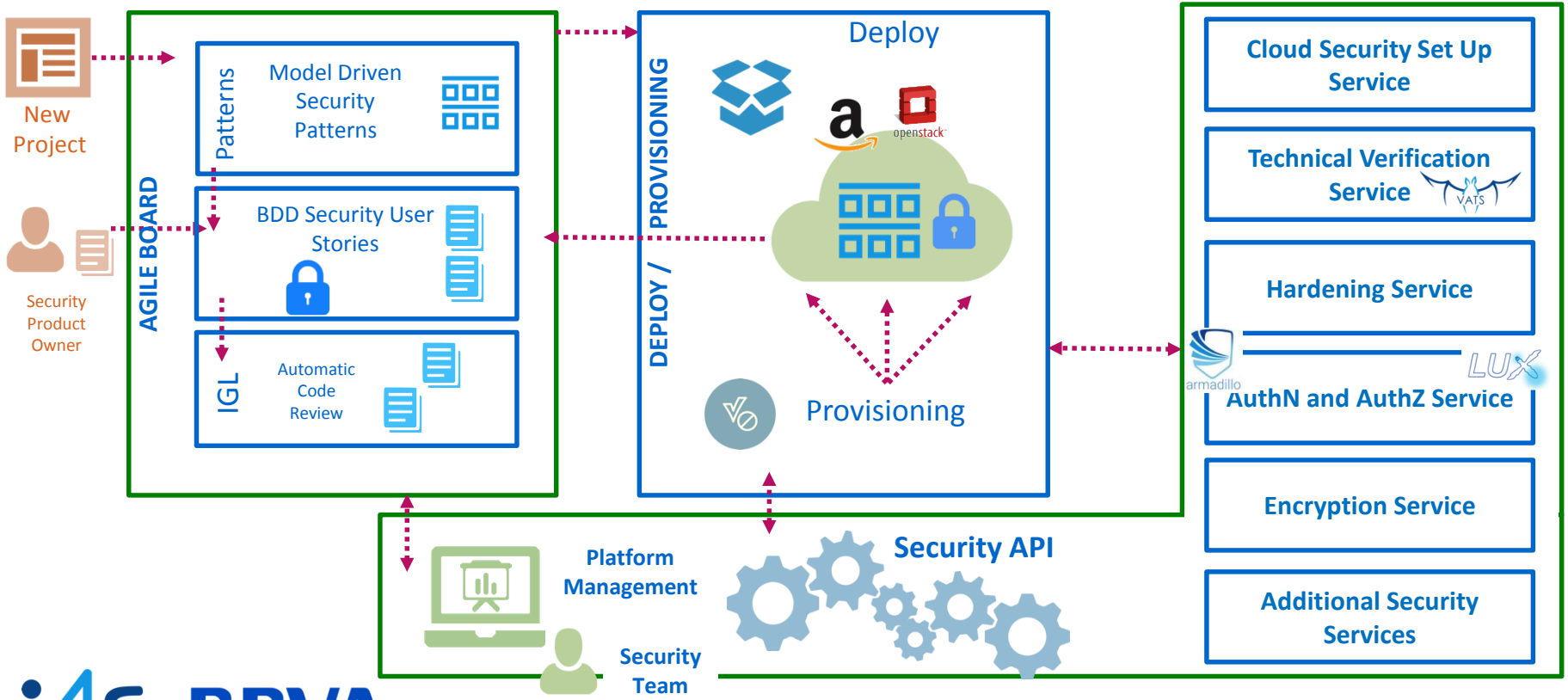


Security as a Service process (Chimera platform)

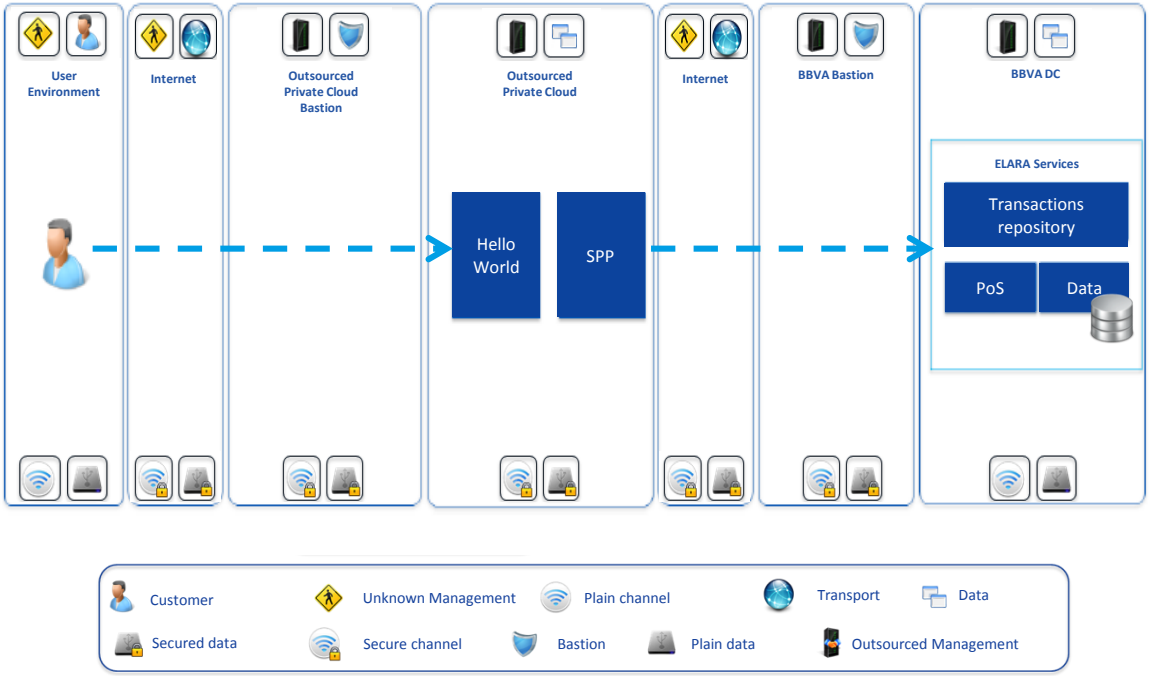
How Chimera was born…



SECaaS (Security as a Service)

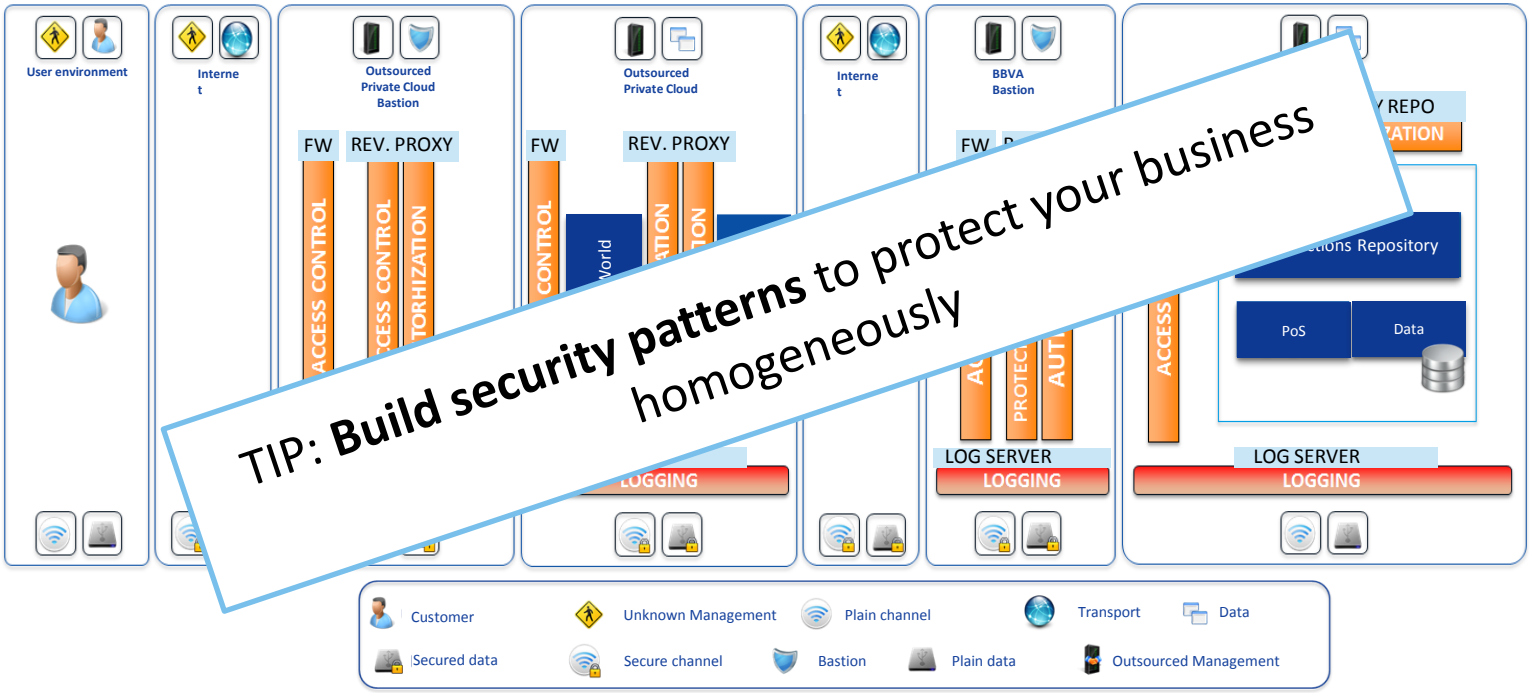


Agile Board – Security Patterns



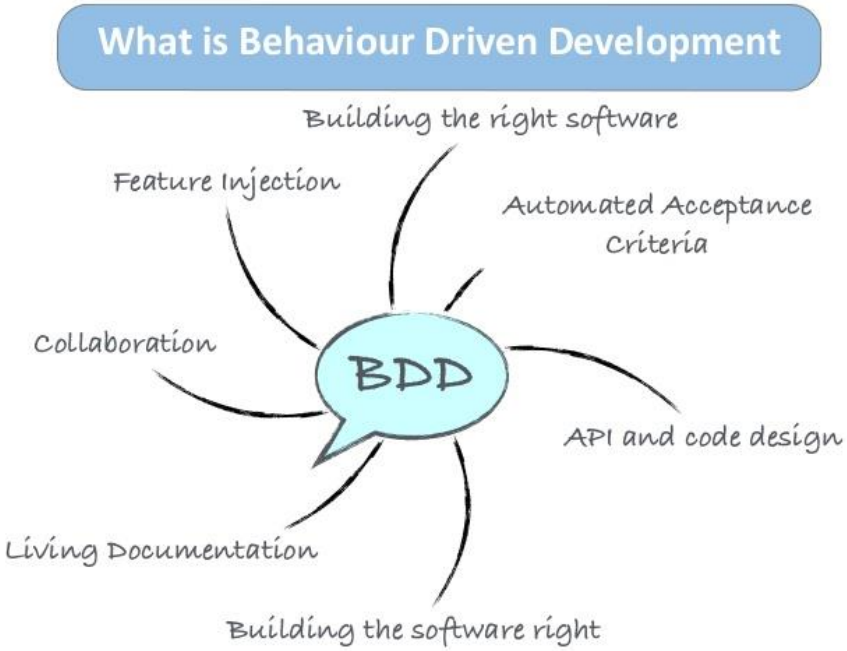
Model Driven Security: Build security patterns to automatically apply security to new projects.

Agile Board – Security Patterns



Source: Roberto Ortiz (BBVA). A methodology to build secure information systems based on patterns

Agile Board – Security with BDD



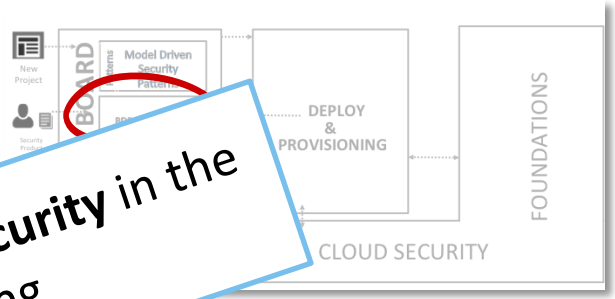
Source: Wakaleo

Behaviour Driven Development: Automate Security acceptance tests and establish a common set of user stories depending on the project and its architecture

Agile Board – Security with BDD

As an app owner
I want to ensure the app does not suffer from SQLi vulnerabilities
So that I protect user data

Example

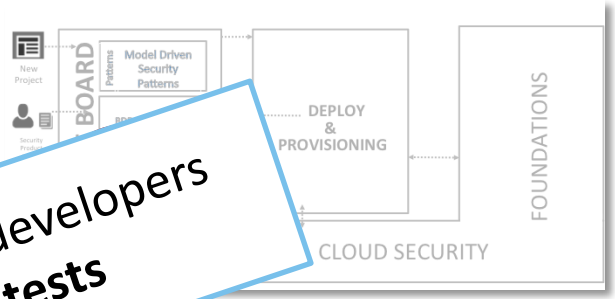


TIP: **Automate security tests to embed security** in the development from the beginning

```
Scenario: The application should not contain
Meta: @id scan_sql_injection @cwe-89
Given a scanner with all polici
And all existing alerts
And the URL regular exp                    e_urls.table are excluded from the scanner
And the SQL-Injection p
And the attack strength
And the alert threshold
When the scanner is run
And the following false po                 are removed: tables/zap.false_positives.table
And the XML report is written to the file sql_injection.xml
Then no Medium or higher risk vulnerabilities should be present
```

Source: BDD Security - Continuum

Agile Board – IGL



Code Repository (software, infrastructure and security)

Recipe Syntax

Build and Unit Testing

Security

Code Review Engine

Integration Testing

OK

Deployment & Configuration

OK

Dev / Prod Environment

Verify

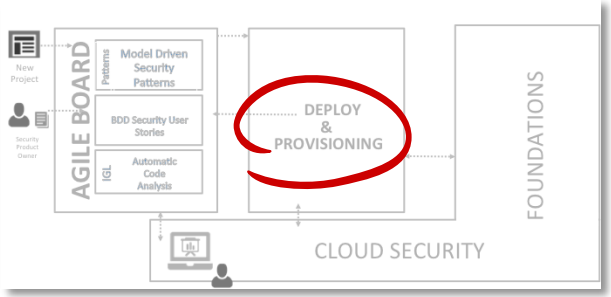
TIP: Provide **faster security feedback** to developers using (almost) **automatic security tests**

Deploy & Provisioning: IaaC

CloudFormation

SCALR

Cloud Orchestration/Management Platform



Public cloud

Hybrid cloud

Private cloud

Google Cloud Platform

rackspace

amazon web services

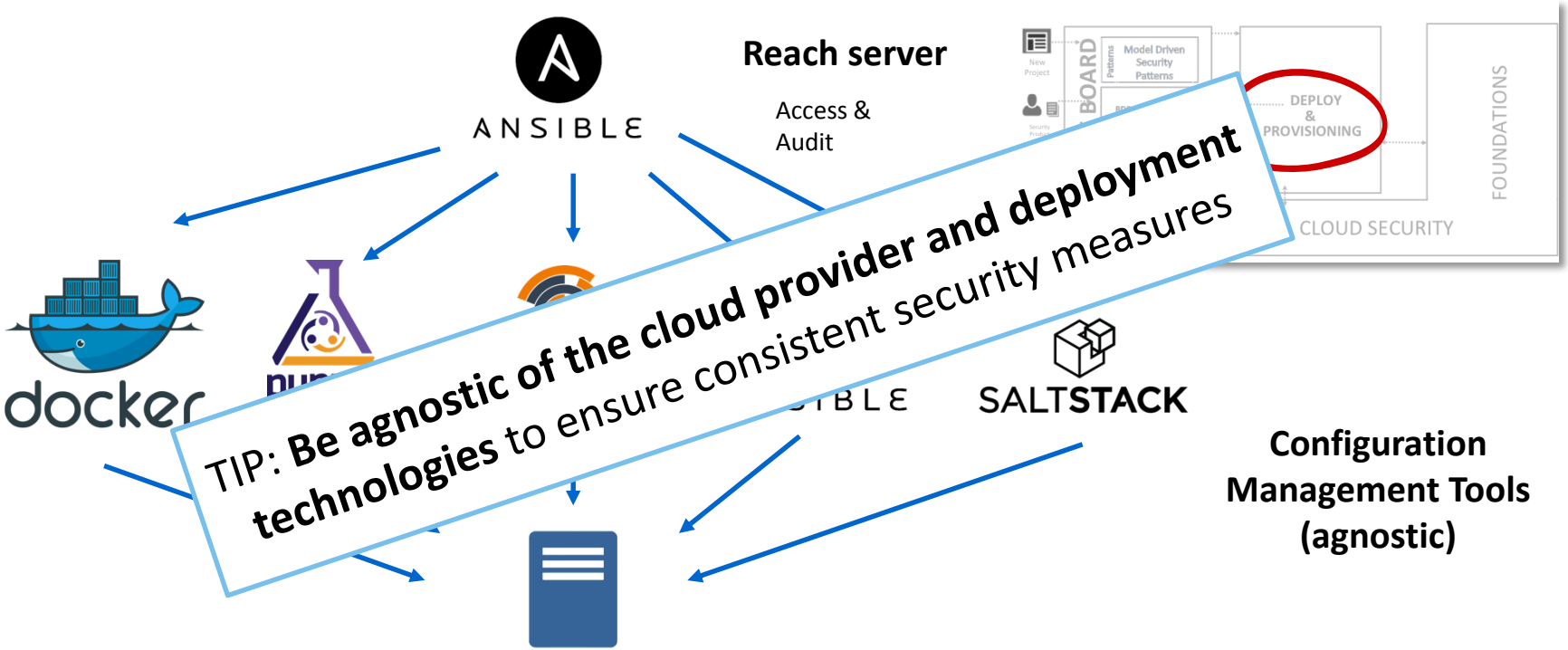
vmware vCLOUD POWERED

openstack CLOUD SOFTWARE

apachecloudstack

i4S BBVA

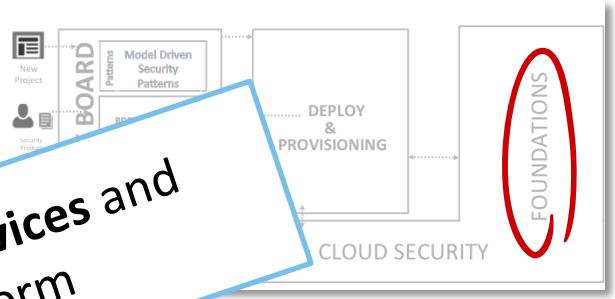
Deploy & Provisioning: CMT



Deploy & Provisioning

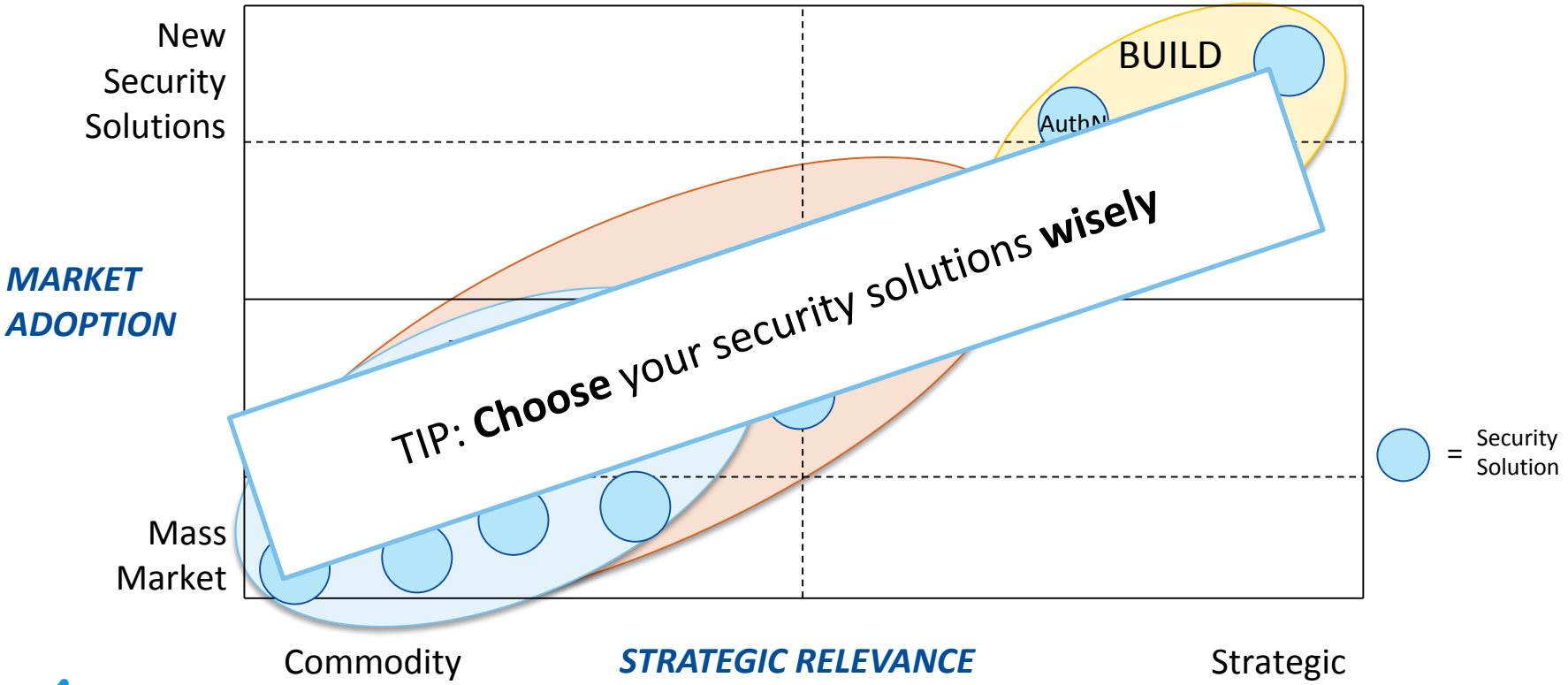
Cloud Security Foundations

- **Technical security checking**: Do the deployed services comply with the defined policies and regulations?
- **Hardening services**: security configuration and basic security components installation.
- **Security events collection & analytics** (Logs, IDS
- **Network & traffic filtering**: L7
- **Identity assura**
- **Crypto as a Se** tokenization API, etc.
- **"Agile" self servi** SDLC, Risk Management, BDD Security.
- **- INSERT ANY SECURITY SERVICE HERE -**



TIP: **Build your baseline of security services** and connect them in an unified platform

Cloud Security Foundations



Takeaways - Apply

- To secure the cloud, use the same technology the cloud is built upon (agile and DevOps are here to stay!), so **embrace SecDevOps**…the sooner, the better.
- Start thinking about your **security patterns**, you will need them to support massive deployments and achieve SECaaS (Security as a Service).
- Identify points of security interaction within your business processes and **automate** them.
- **Don’t be afraid of Open Source Software**: it can be helpful in many ways…but don’t forget **internal security development** can have its use cases.
- **Digital Trust** needs to be your long term value, use it as your compass.

RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: ASD-F01

Security as a Service in a Financial Institution: Reality or Chimera?

Javier Losa
Cybersecurity Product Engineering
Innovation 4 Security – BBVA Group
@sealth

Iñigo Merchán
Security Architect
BBVA
@achemerchan