

AWS re:Invent

Learn How Trend Micro Used AWS to Build their Enterprise Security Offering (Deep Security as a Service)

Mark Nunnikhoven, Principal Engineer at Trend Micro

November 14, 2013



© 2013 Amazon.com, Inc. and its affiliates. All rights reserved. May not be copied, modified, or distributed in whole or in part without the express consent of Amazon.com, Inc.

"The following story is fictional and does not depict any actual person or event"

"The following story is completely real and depicts actual people & events"

* Only the names have been changes to protect the innocent ;-)

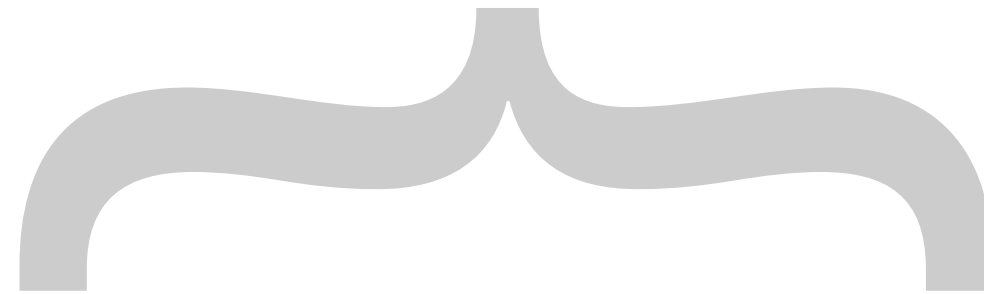
The stage

What is Deep Security?

Centralized security control management

What is Deep Security?

Centralized security control management



Manager

What is Deep Security?

Centralized security control management



What could be...



What could be...



- **For the cloud**



What could be...



- **For the cloud**
- **In the cloud**



What was



Determine what an appropriate visual here would be (old style for contrast?)

What was



- **For the data center**

Determine what an appropriate visual here would be (old style for contrast?)

What was



- **For the data center**
- **In the data center**

Determine what an appropriate visual here would be (old style for contrast?)

The story so far...

Deep Security—The Early Years

Security for servers and virtual machines

Security for servers and virtual machines

Product focus

- **Enterprise only**
- **Tight integration with virtualization platform**
- **Focused on Windows platforms**

Deep Security—The Middle Years

Security for servers and virtual machines

Security for servers and virtual machines

Big changes

- **Acquired by Trend Micro in 2009**
- **Provided more protection**
- **Agentless protection is key**
- **Expanded platform support**

Deep Security—Now

Deep Security—Now

Product changes

- **Protection regardless of location**
- **“Single pane of glass”**
- **Smart, simple, security that fits taken to heart**

Security for servers, virtual machines

Product changes

- **Protection regardless of location**
- **“Single pane of glass”**
- **Smart, simple, security that fits taken to heart**

Security for servers, virtual machines, & the cloud

Product changes

- **Protection regardless of location**
- **“Single pane of glass”**
- **Smart, simple, security that fits taken to heart**

The Decision

Time to offer Deep Security as a service

Why a Service?

Security for servers, virtual machines

Why a Service?

Security for servers, virtual machines

Drivers

- **Face the same challenges as our clients**

Why a Service?

Security for servers, virtual machines

Drivers

- **Face the same challenges as our clients**
- **Work directly with clients**

Why a Service?

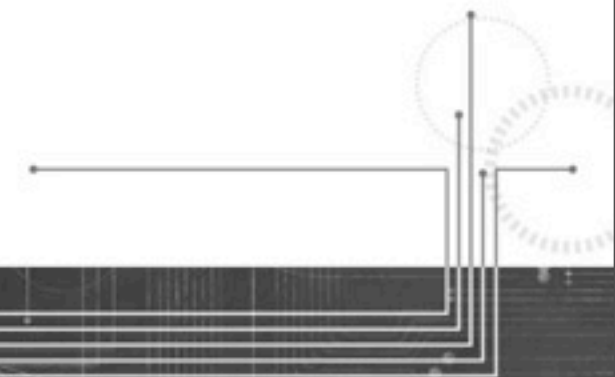
Security for servers, virtual machines

Drivers

- **Face the same challenges as our clients**
- **Work directly with clients**
- **Smaller feedback loop for new features**

The players

Internal Teams



The Service Team

Executive sponsor

**Key R&D product team
members**

DevOps*

Internal Teams

The Service Team

Executive sponsor

**Key R&D product team
members**

DevOps*

Internal Teams

The Service Team

Executive sponsor

**Key R&D product team
members**

DevOps*

People to win over

Executives

Information Security

Operations

R&D Product Team

Internal Teams

The Service Team

Executive sponsor

Key R&D product team members

DevOps*

VS

People to win over Executives

Information Security

Operations

R&D Product Team

Internal Teams

The Service Team

Executive sponsor

Key R&D product team members

DevOps*



People who helped

Executives

Information Security

Operations

R&D Product Team

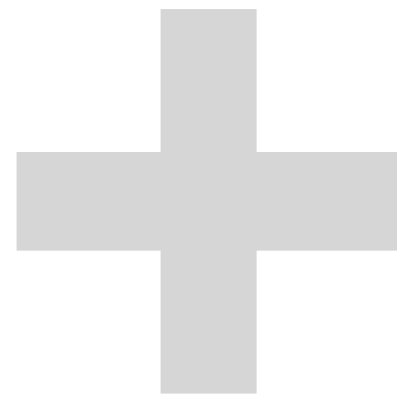
Internal Teams

The Service Team

Executive sponsor

Key R&D product team members

DevOps*



People who helped

Executives

Information Security

Operations

R&D Product Team

Team Profile

Information Security

- **Own existing security policy**

| | | | | |
|-----|-----------|--|--|--|
| 128 | OUT-G5-01 | Contingency | Responsible Business Unit Owners of Trend Micro must establish contingency arrangements to manage outsourced environments, must the outsource provider not be available (eg due to a disaster or dispute). | (http://aws.amazon.com/aup/), AWS Customer Agreement (http://aws.amazon.com/agreement/), and Service Level Agreements (which are service specific such as http://aws.amazon.com/ec2-sla/) |
| 129 | ENV-H1-01 | Security Perimeter and Physical Entry Controls | There must be documented procedures for the provision of physical protection in areas housing IT facilities (eg: data centers, communications facilities, key user areas) | Assets in the solution are deployed in AWS data centers and follow their controls for physical access. Further information is available at http://aws.amazon.com/security . Controls aimed at Trend Micro staff working on or Trend Micro locations involved in this solution are detailed in existing solutions |
| 130 | ENV-H1-02 | Security Perimeter and Physical Entry Controls | Procedures must include the protection of: buildings against unauthorized access | Assets in the solution are deployed in AWS data centers and follow their controls for physical access. Further information is available at http://aws.amazon.com/security . Controls aimed at Trend Micro staff working on or Trend Micro locations involved in this solution are detailed in existing solutions |
| 131 | ENV-H1-03 | Security Perimeter and Physical Entry Controls | Procedures must include the protection of: important papers and removable storage media against theft or copying | Assets in the solution are deployed in AWS data centers and follow their controls for physical access. Further information is available at http://aws.amazon.com/security . Controls aimed at Trend Micro staff working on or Trend Micro locations involved in this solution are detailed in existing solutions |
| 132 | ENV-H1-04 | Security Perimeter and Physical Entry Controls | Procedures must include the protection of: easily portable computers and components against theft | Assets in the solution are deployed in AWS data centers and follow their controls for physical access. Further information is available at http://aws.amazon.com/security . Controls aimed at Trend Micro staff working on or Trend Micro locations involved in this solution are detailed in existing solutions |
| 133 | ENV-H1-05 | Security Perimeter and Physical Entry Controls | Procedures must include the protection of: vulnerable staff against intimidation from malicious third parties. | Assets in the solution are deployed in AWS data centers and follow their controls for physical access. Further information is available at http://aws.amazon.com/security . Controls aimed at Trend Micro staff working on or Trend Micro locations involved in this solution are detailed in existing solutions |
| 134 | ENV-H1-06 | Security Perimeter and Physical Entry Controls | All Trend Micro buildings (new or existing) must undergo risk assessment exercise | Assets in the solution are deployed in AWS data centers and follow their controls for physical access. Further information is available at http://aws.amazon.com/security . Controls aimed at Trend Micro staff working on or Trend Micro locations involved in this solution are detailed in existing solutions |
| 135 | ENV-H1-07 | Security Perimeter and Physical Entry Controls | Trend Micro premises must be classified and separated into secured area based on risks identified in risk assessment exercise | Assets in the solution are deployed in AWS data centers and follow their controls for physical access. Further information is available at http://aws.amazon.com/security . Controls aimed at Trend Micro staff working on or Trend Micro locations involved in this solution are detailed in existing solutions |
| | | | | Assets in the solution are deployed in AWS data centers and follow their controls for physical access. Further information is available at |

Team Profile

Information Security

- **Own existing security policy**

Information Security

- **Own existing security policy**
- **400+ requirements for operational services**

Information Security

- **Own existing security policy**
- **400+ requirements for operational services**
- **Wants development of cloud best practices**

Team Profile

Operations

- **Run several data centers worldwide**

Team Profile

Operations

- **Run several data centers worldwide**
- **Rigid change management with complex schedules**

Operations

- **Run several data centers worldwide**
- **Rigid change management with complex schedules**
- **Wants development of DevOps runbook**

Team Profile

R&D Product Team

- **Develop & maintain the product**

R&D Product Team

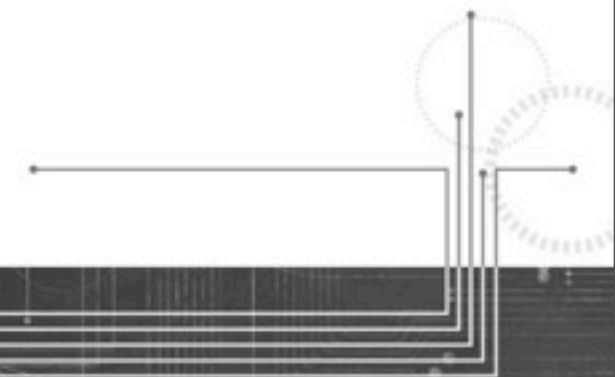
- **Develop & maintain the product**
- **Only operational work is emergency support**

R&D Product Team

- **Develop & maintain the product**
- **Only operational work is emergency support**
- **Wants tighter feedback loop**

The details

High Level Architecture



High Level Architecture

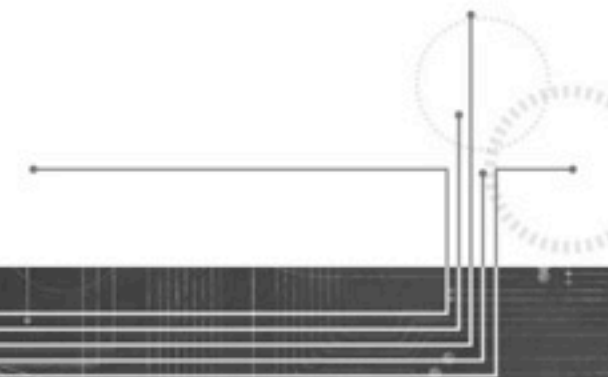


Agent

High Level Architecture



Agent



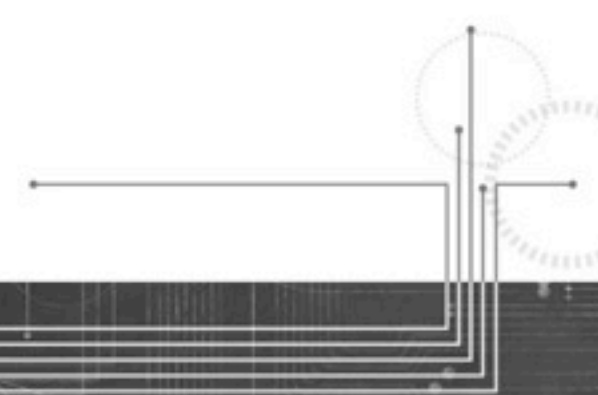
High Level Architecture



Agent



**Load
Balancer**



High Level Architecture



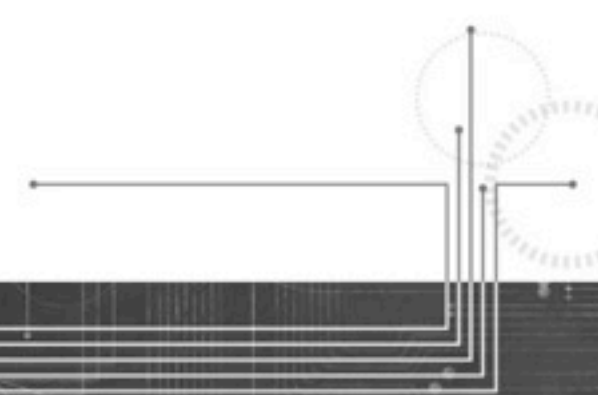
Agent



**Load
Balancer**



**Manager
+ Relay**



High Level Architecture



Agent



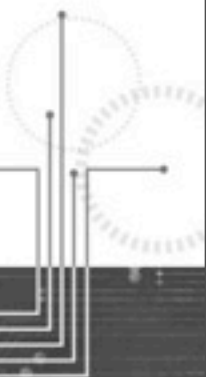
**Load
Balancer**



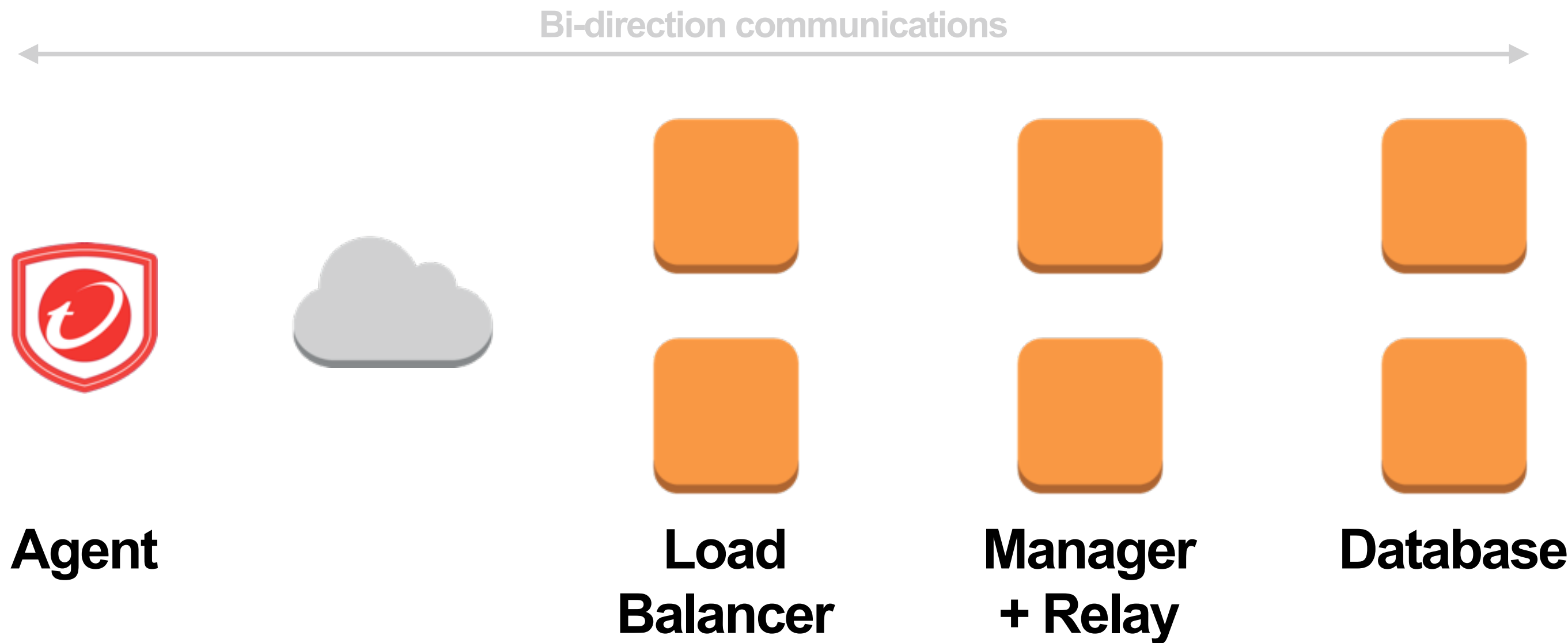
**Manager
+ Relay**



Database

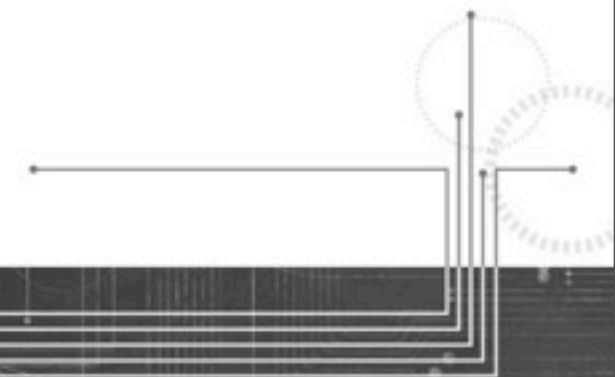


High Level Architecture



Load balancers

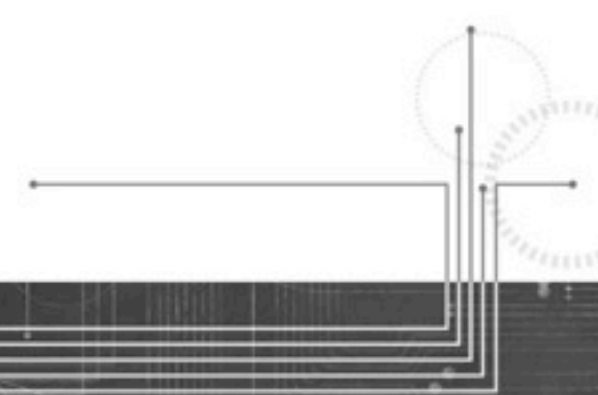
High Level Architecture



High Level Architecture



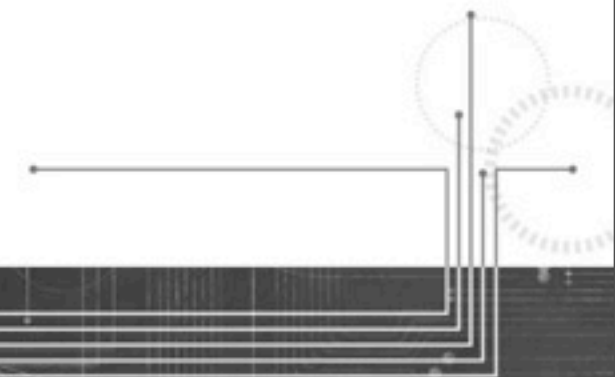
Agent



High Level Architecture



Agent



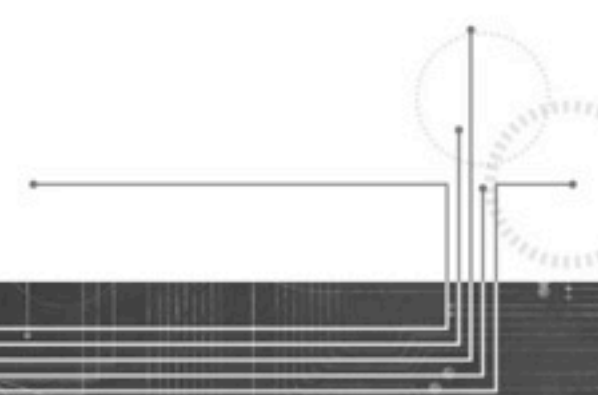
High Level Architecture



Agent



**Load
Balancer**



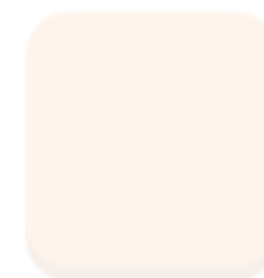
High Level Architecture



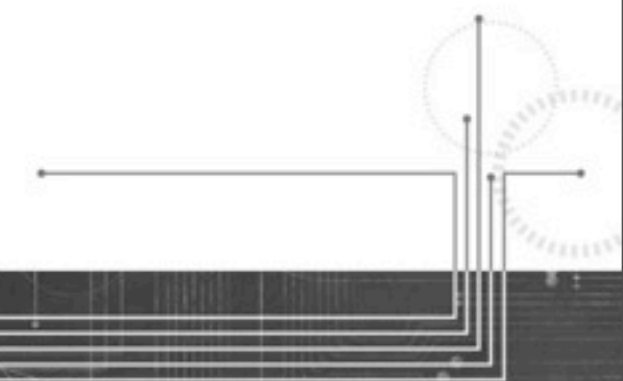
Agent



**Load
Balancer**



Manager
+ Relay



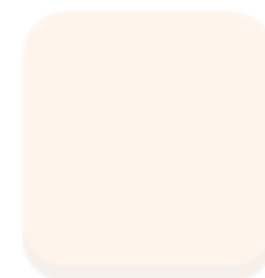
High Level Architecture



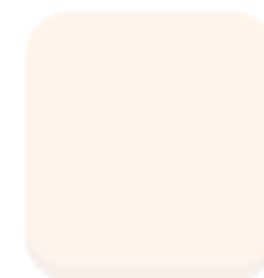
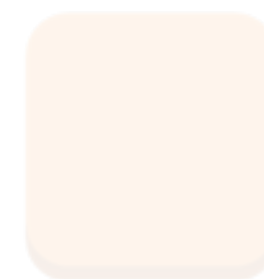
Agent



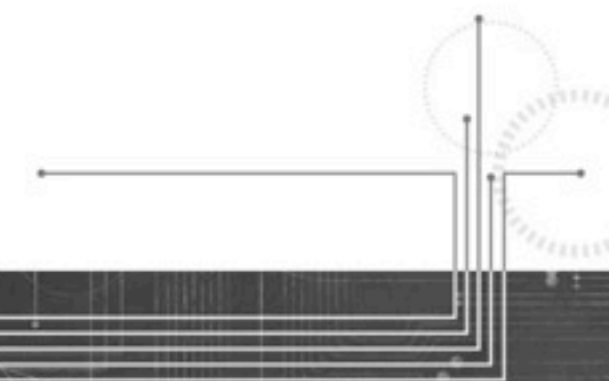
**Load
Balancer**



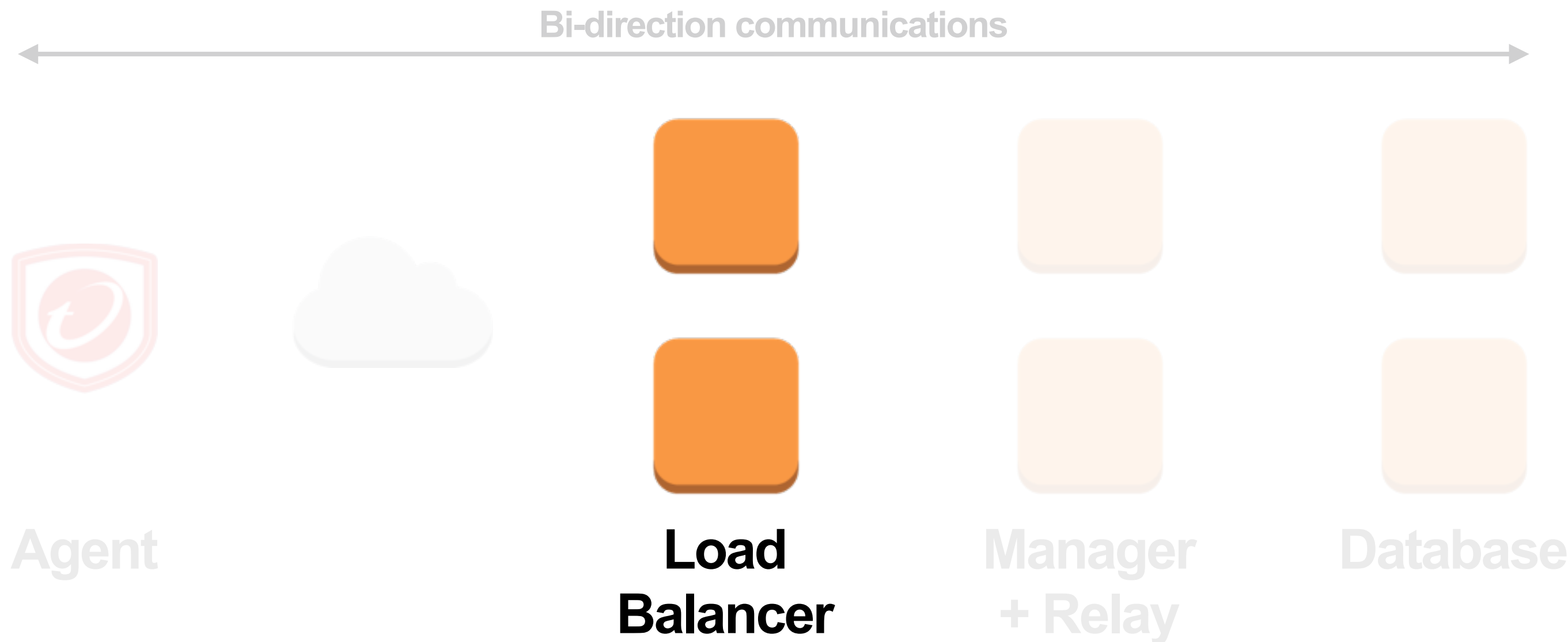
Manager
+ Relay



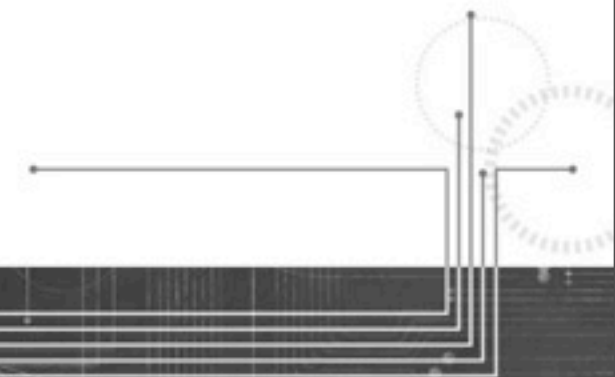
Database



High Level Architecture



Load Balancers



Load Balancers

Requirements

- **3 flows, all incoming on :443**

Load Balancers

Requirements

- **3 flows, all incoming on :443**
- **SSL off loading**

Load Balancers

Requirements

- **3 flows, all incoming on :443**
- **SSL off loading**
- **High number of concurrent connections**

Load Balancers

HAProxy

Met requirements

2+ instances required (for HA)

EC2 instance costs

More boxes to maintain

Load Balancers

HAProxy

Met requirements

2+ instances required (for HA)

EC2 instance costs

More boxes to maintain

Elastic Load Balancing

Can meet requirements

3 load balancers required (1x flow)

Cheap

Minimal maintenance

Load Balancer Architecture



**Load
Balancer**

Load Balancer Architecture



Agent

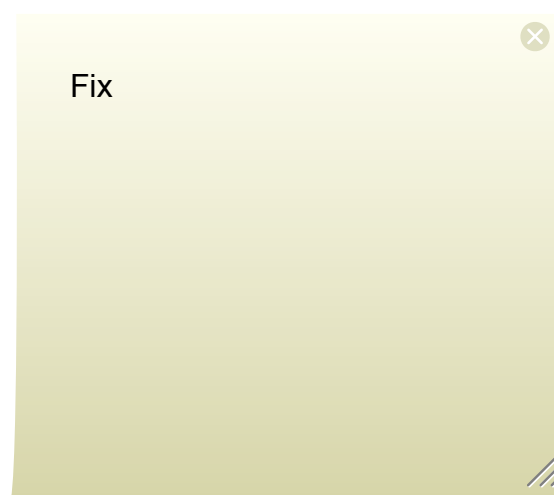


**Load
Balancer**

Load Balancer Architecture



Agent

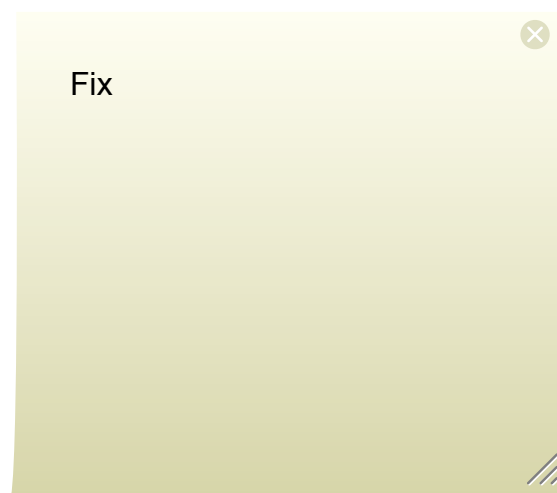


**Load
Balancer**

Load Balancer Architecture



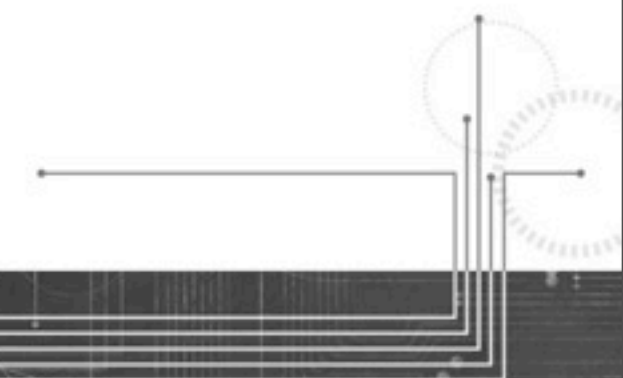
Agent



**Load
Balancer**



Manager
+ Relay



Load Balancer Architecture



Agent



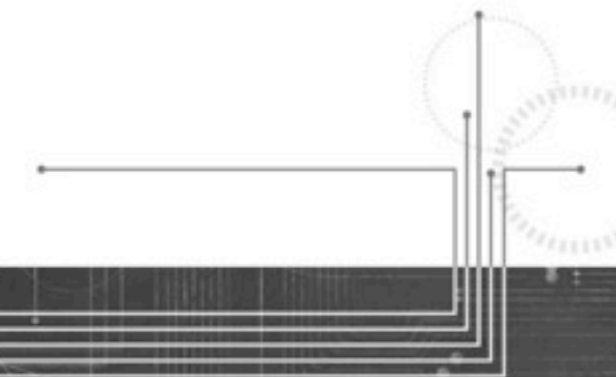
**Load
Balancer**



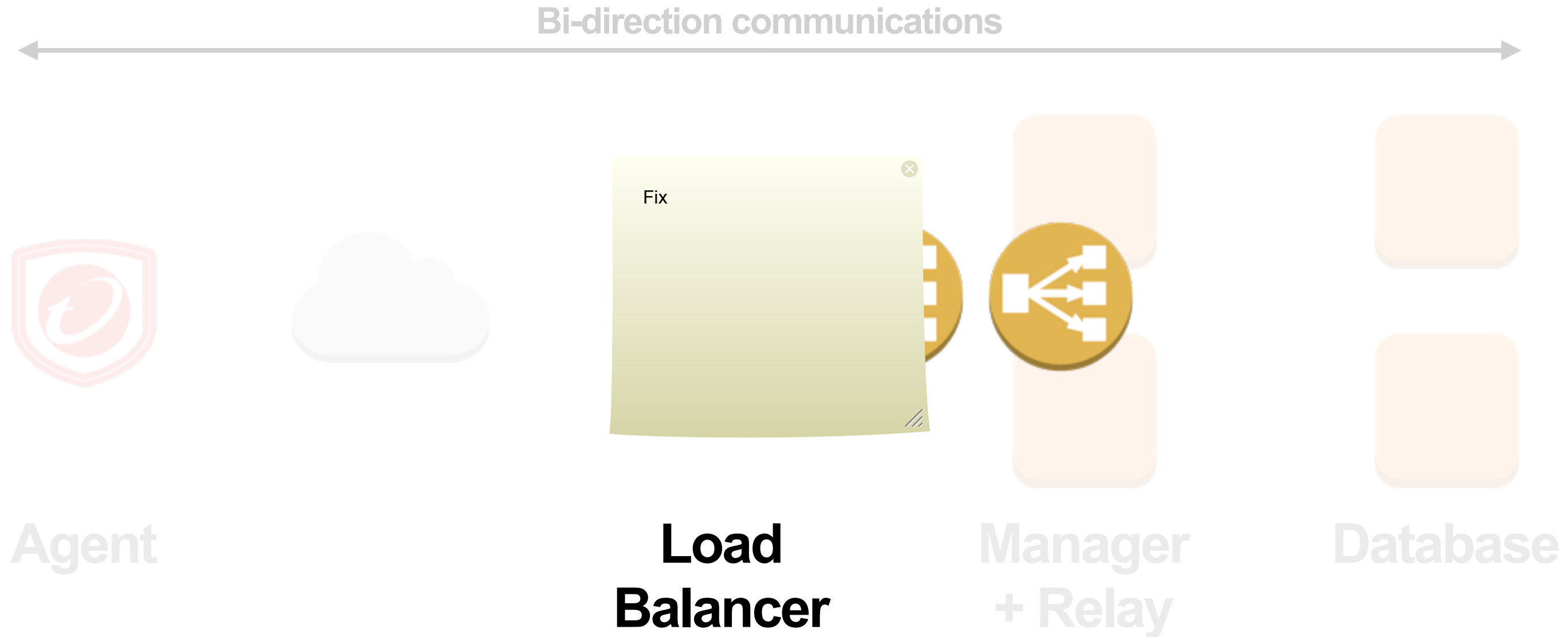
Manager
+ Relay



Database



Load Balancer Architecture



Manager + Relay

High Level Architecture



Load
Balancer

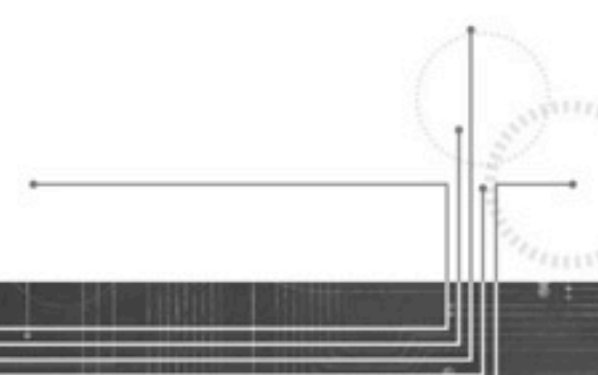
High Level Architecture



Agent



Load
Balancer



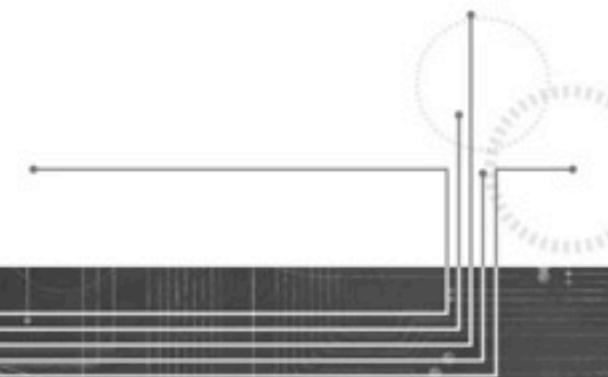
High Level Architecture



Agent



Load
Balancer



High Level Architecture



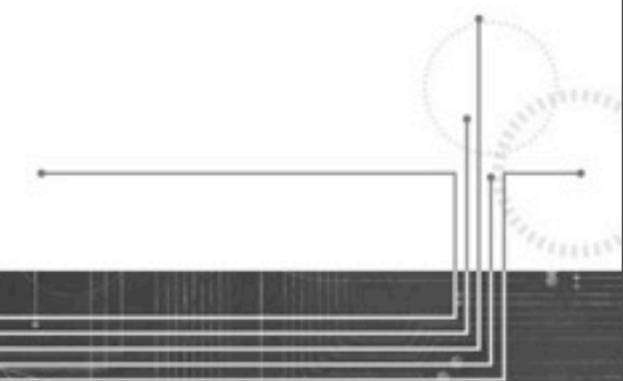
Agent



Load
Balancer



**Manager
+ Relay**



High Level Architecture



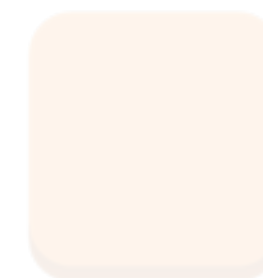
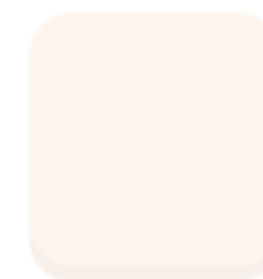
Agent



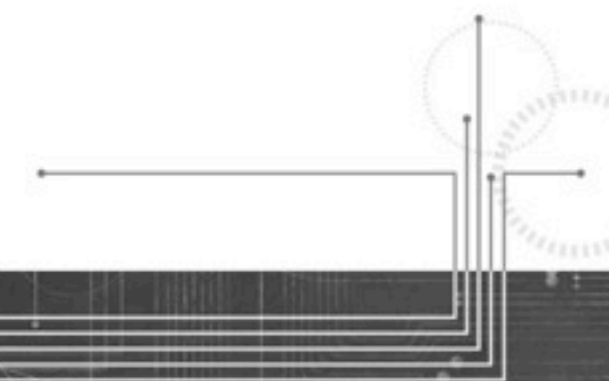
Load
Balancer



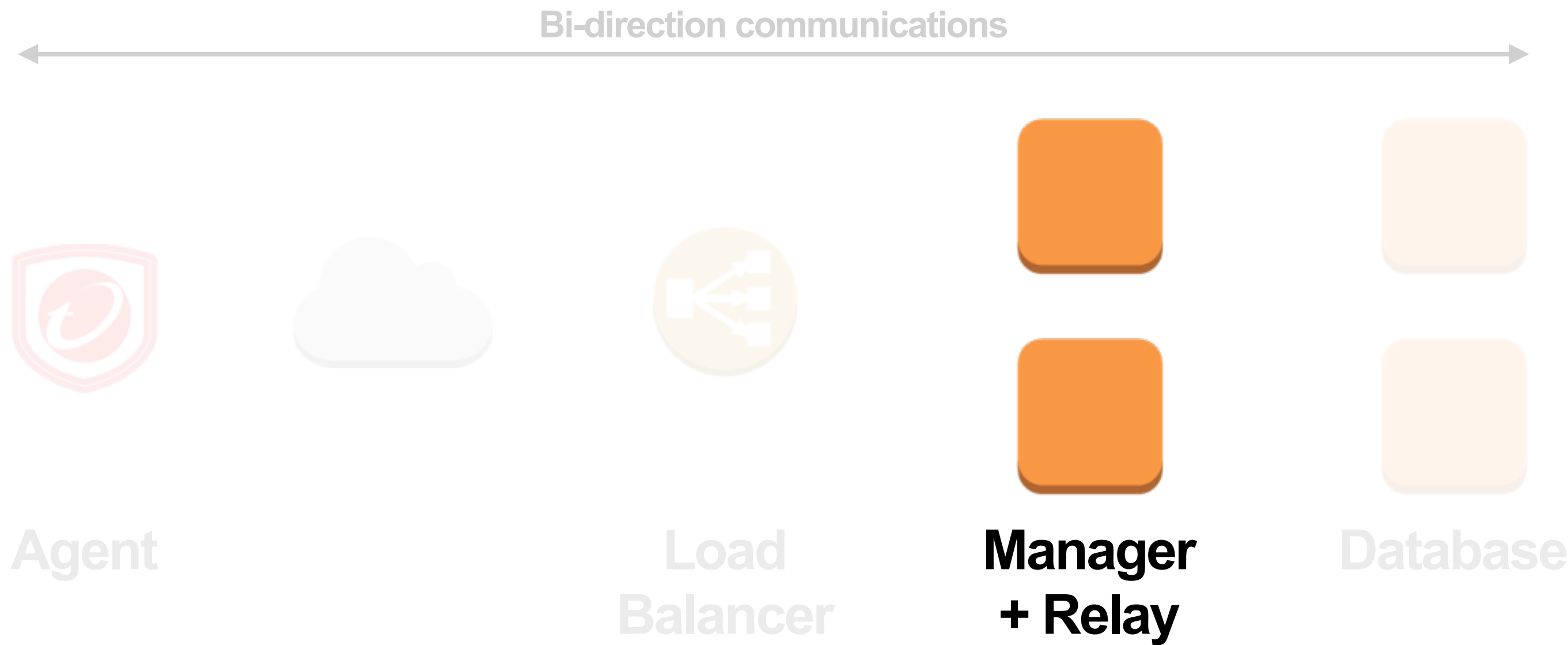
**Manager
+ Relay**



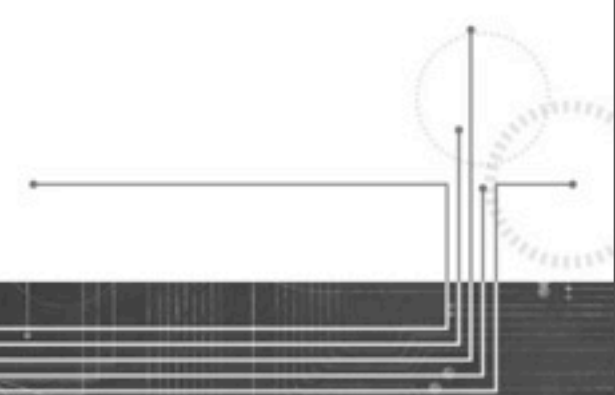
Database



High Level Architecture



Manager + Relay



Manager + Relay

Requirements

- **Hosts JVM-based application**

Manager + Relay

Requirements

- **Hosts JVM-based application**
- **Memory, CPU, and network are constraints**

AWS Windows Base

Met requirements

Harder to script

More expensive

Manager + Relay

AWS Windows Base

Met requirements

Harder to script

More expensive

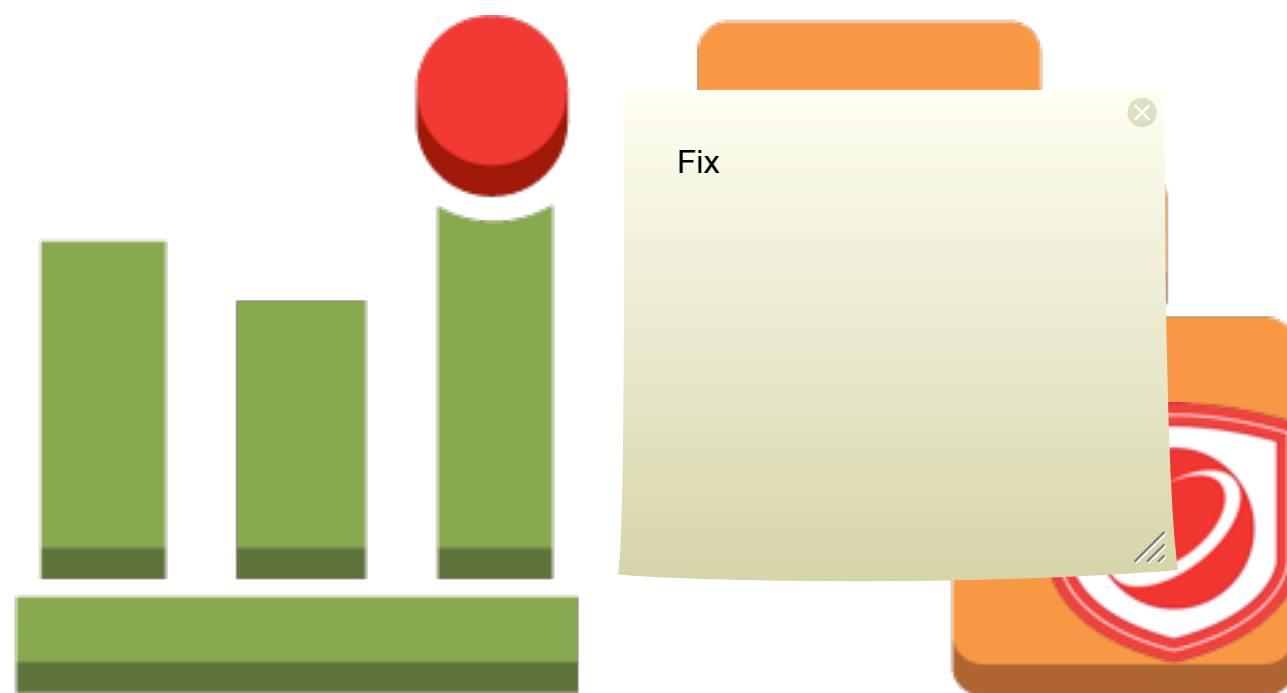
AWS Linux Base

Met requirements

Simple scripting

Cheaper

Manager + Relay Architecture



Load
Balancer

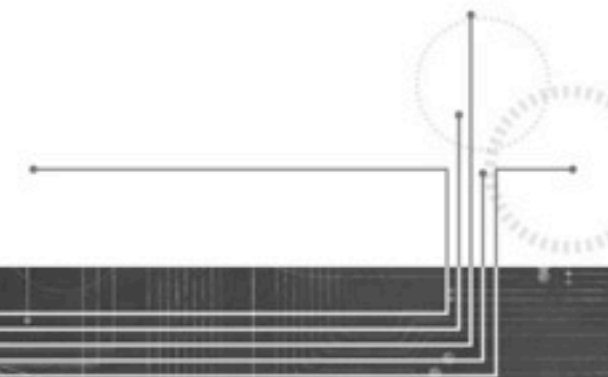
Manager + Relay Architecture



Agent



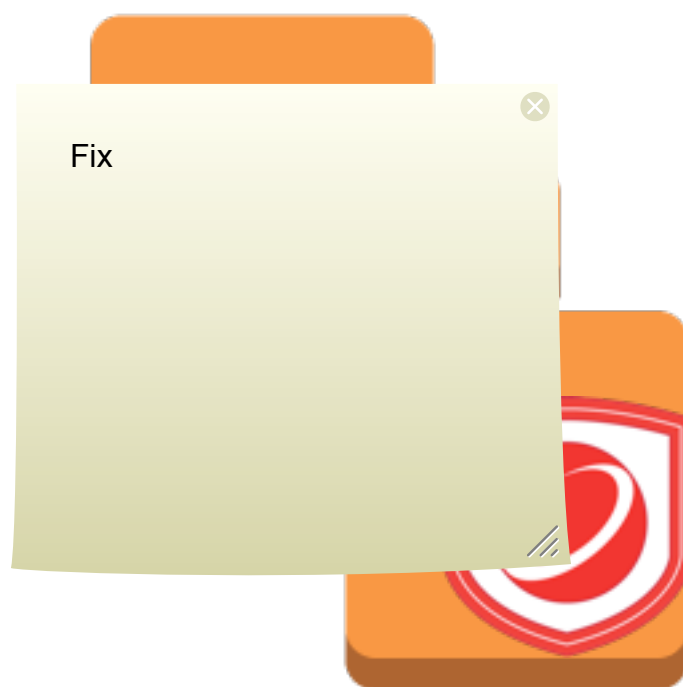
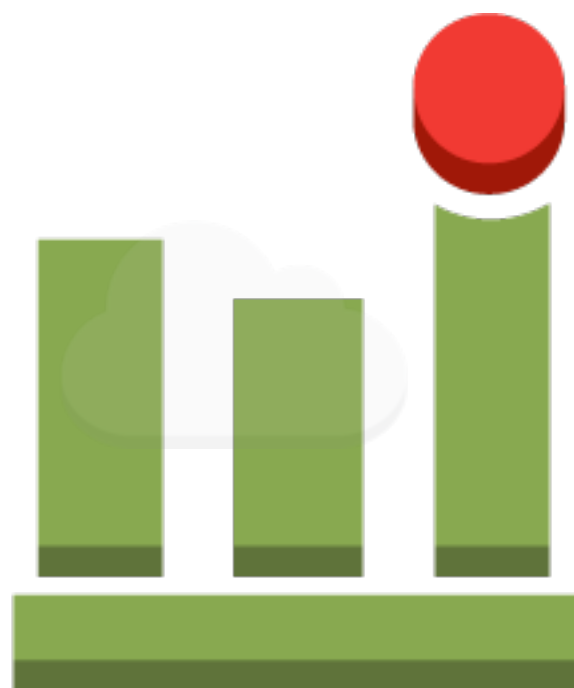
Load Balancer



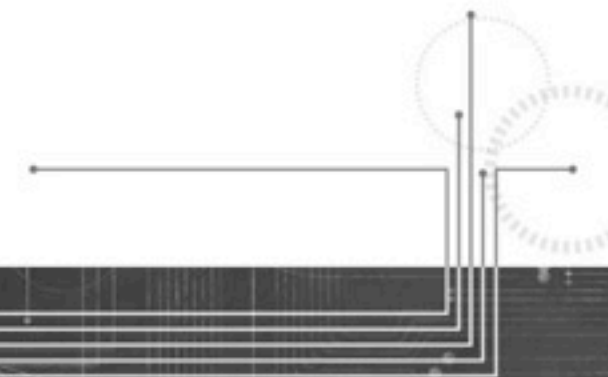
Manager + Relay Architecture



Agent



Load Balancer



Manager + Relay Architecture



Agent



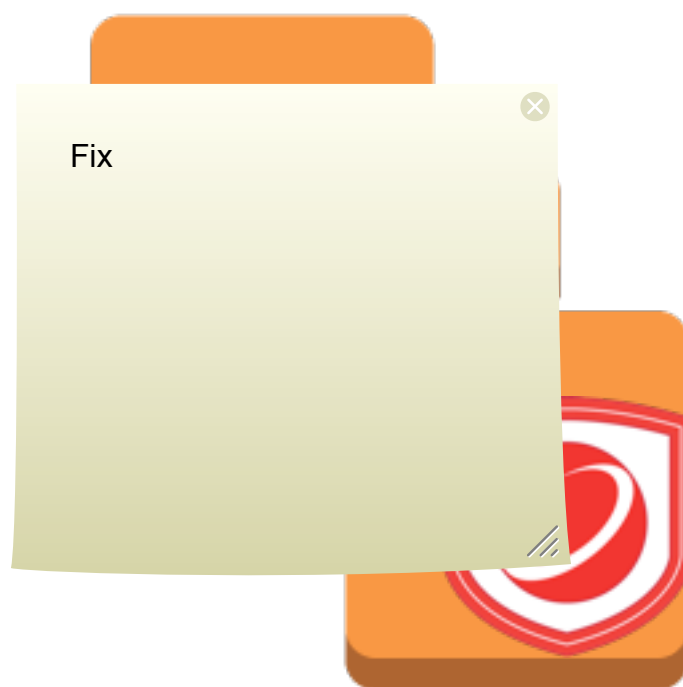
Load
Balancer

**Manager
+ Relay**

Manager + Relay Architecture



Agent



Load Balancer

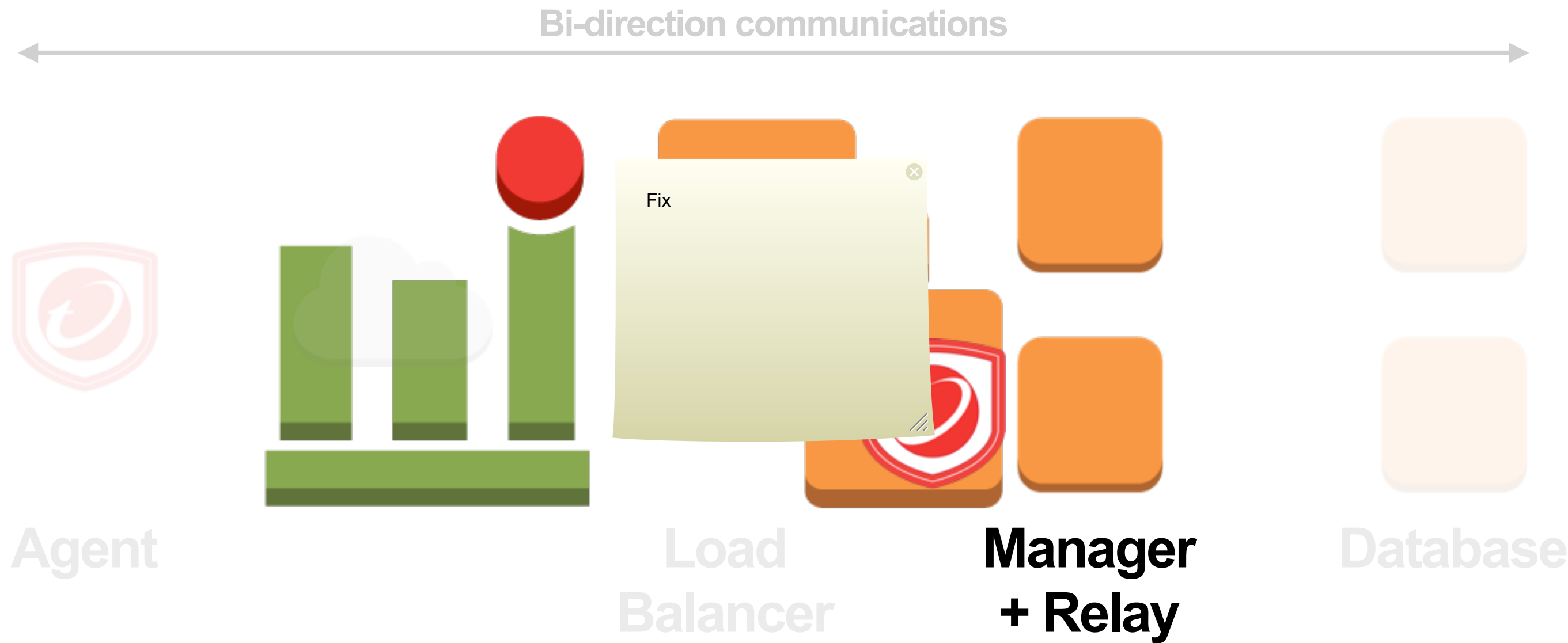
Manager + Relay



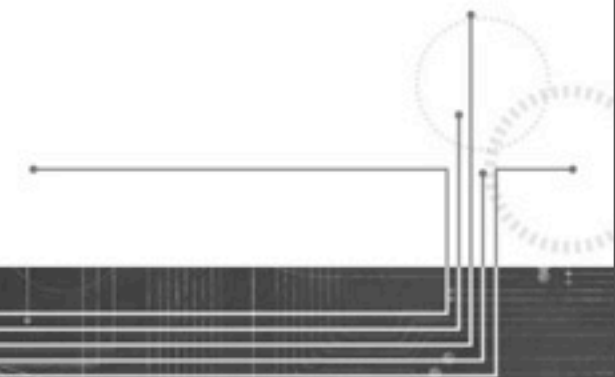
Database



Manager + Relay Architecture



Manager + Relay—Tips & Tricks



Manager + Relay—Tips & Tricks

Tips & tricks

- **We don't use AMIs**

Manager + Relay—Tips & Tricks

Tips & tricks

- **We don't use AMIs**
- **Auto-scale only for failover**

Database

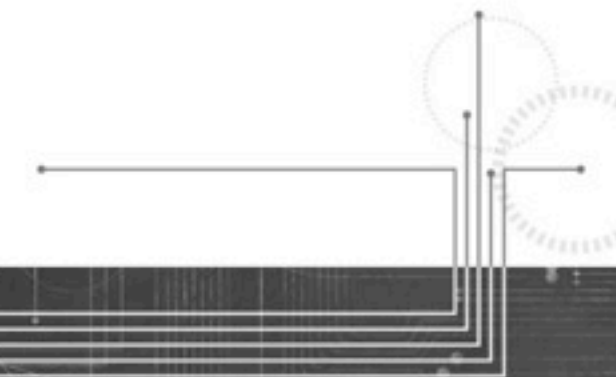
High Level Architecture



Load
Balancer



Manager
+ Relay



High Level Architecture



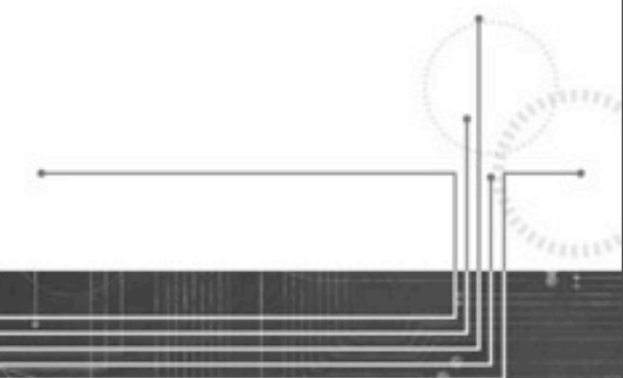
Agent



Load
Balancer



Manager
+ Relay



High Level Architecture



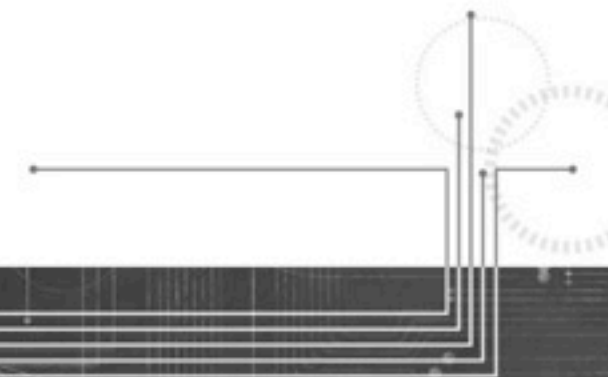
Agent



Load
Balancer



Manager
+ Relay



High Level Architecture



Agent



Load
Balancer



Manager
+ Relay

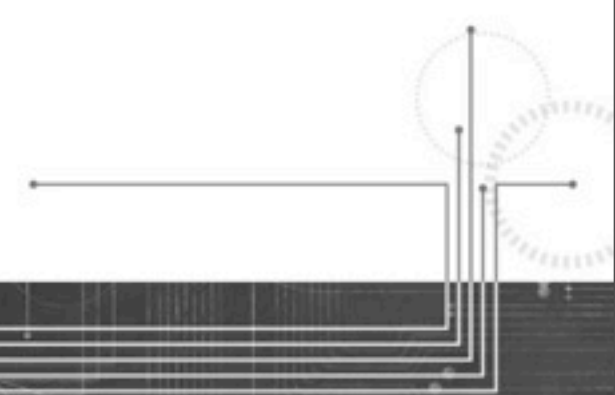


Database

High Level Architecture



Database



Database

Requirements

- **MS SQL or Oracle**

Database

Requirements

- **MS SQL or Oracle**
- **Low latency path to Manager + Relay nodes**

Manager + Relay

on Amazon EC2

Met requirements

2x cost for clustered pairs

More maintenance

Manager + Relay

on Amazon EC2

Met requirements

2x cost for clustered pairs

More maintenance

on Amazon RDS

Can meet requirements

1.3x cost for clustered pairs

Less effort

MS SQL

Teams are more familiar

Better tools available*

**30 DB limit per Amazon RDS
instance**

Manager + Relay

MS SQL

Teams are more familiar

Better tools available*

30 DB limit per Amazon RDS instance

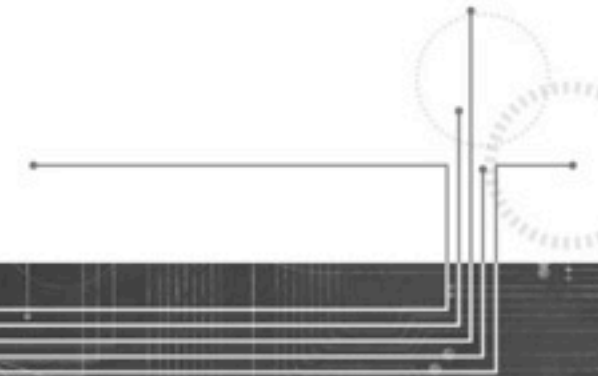
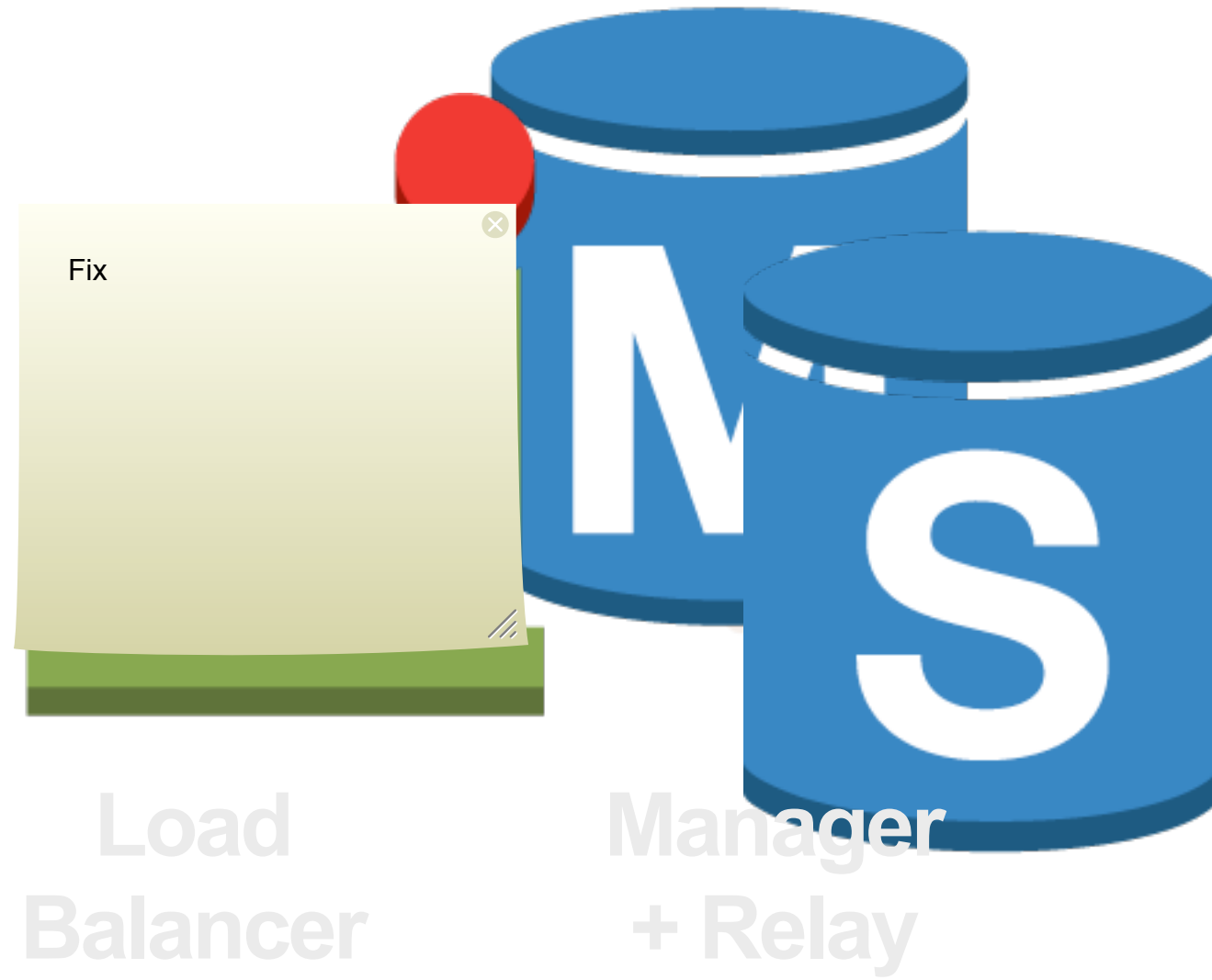
Oracle

Forces product improvements

“Encourages” learning

No tablespace limits

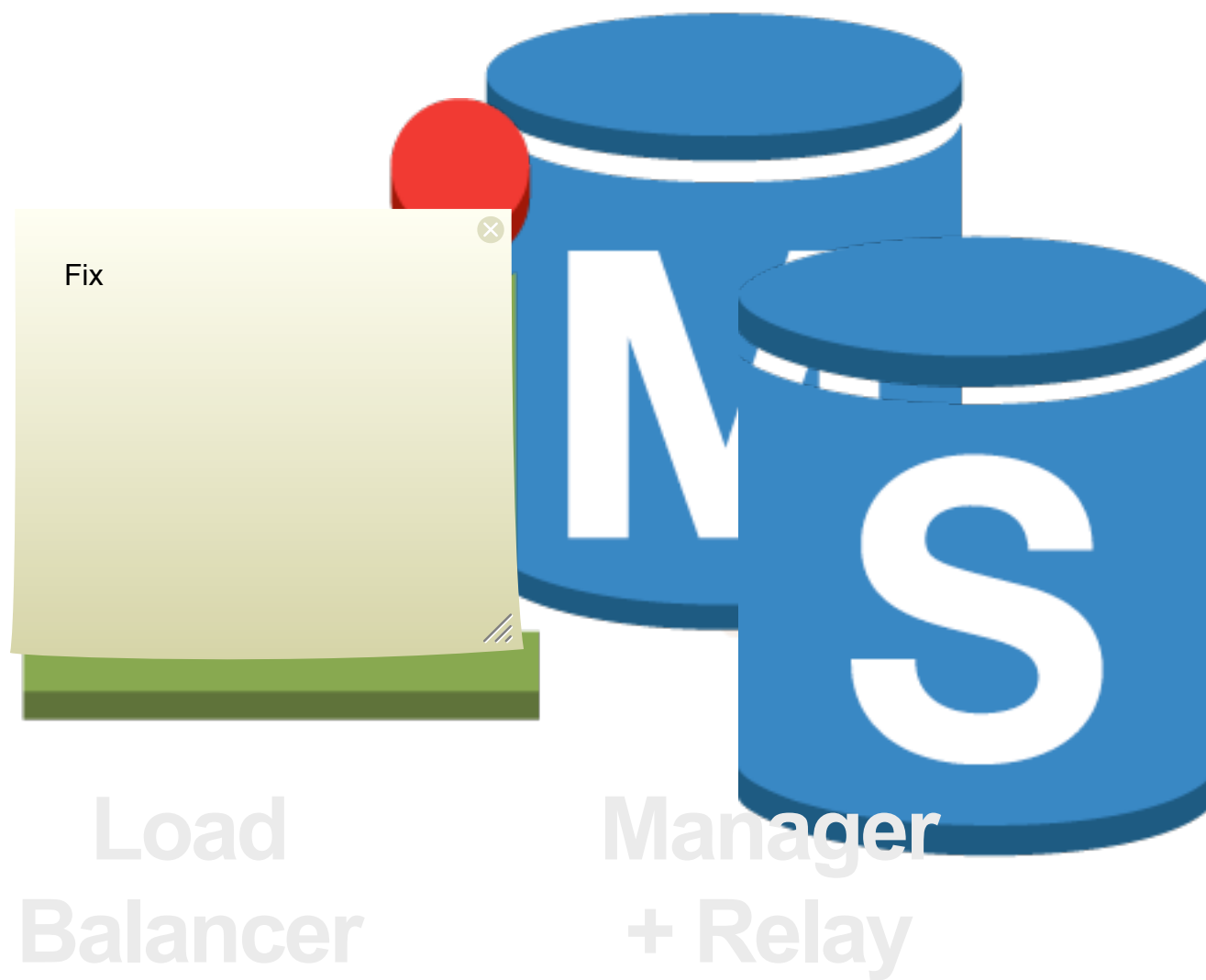
Database Architecture



Database Architecture



Agent



Load
Balancer

Manager
+ Relay

Database Architecture

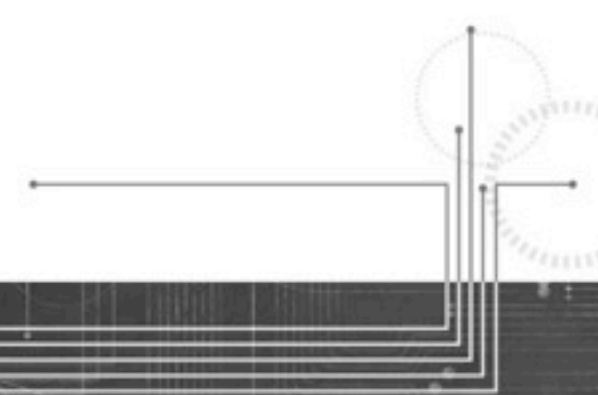


Agent



Load Balancer

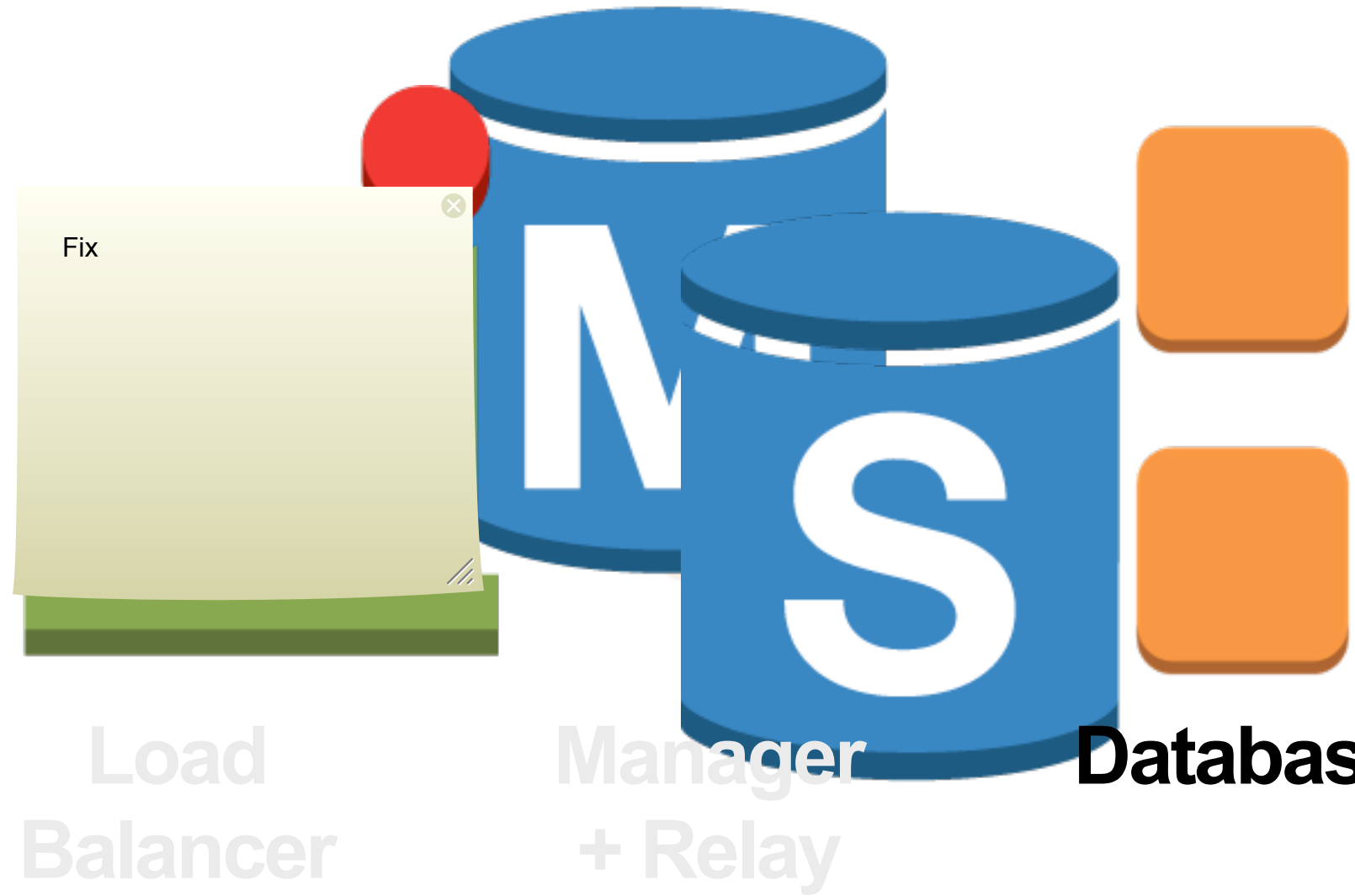
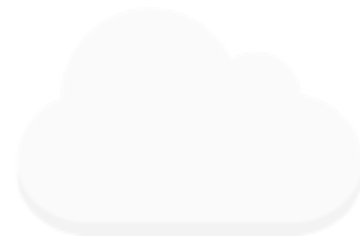
Manager + Relay



Database Architecture



Agent

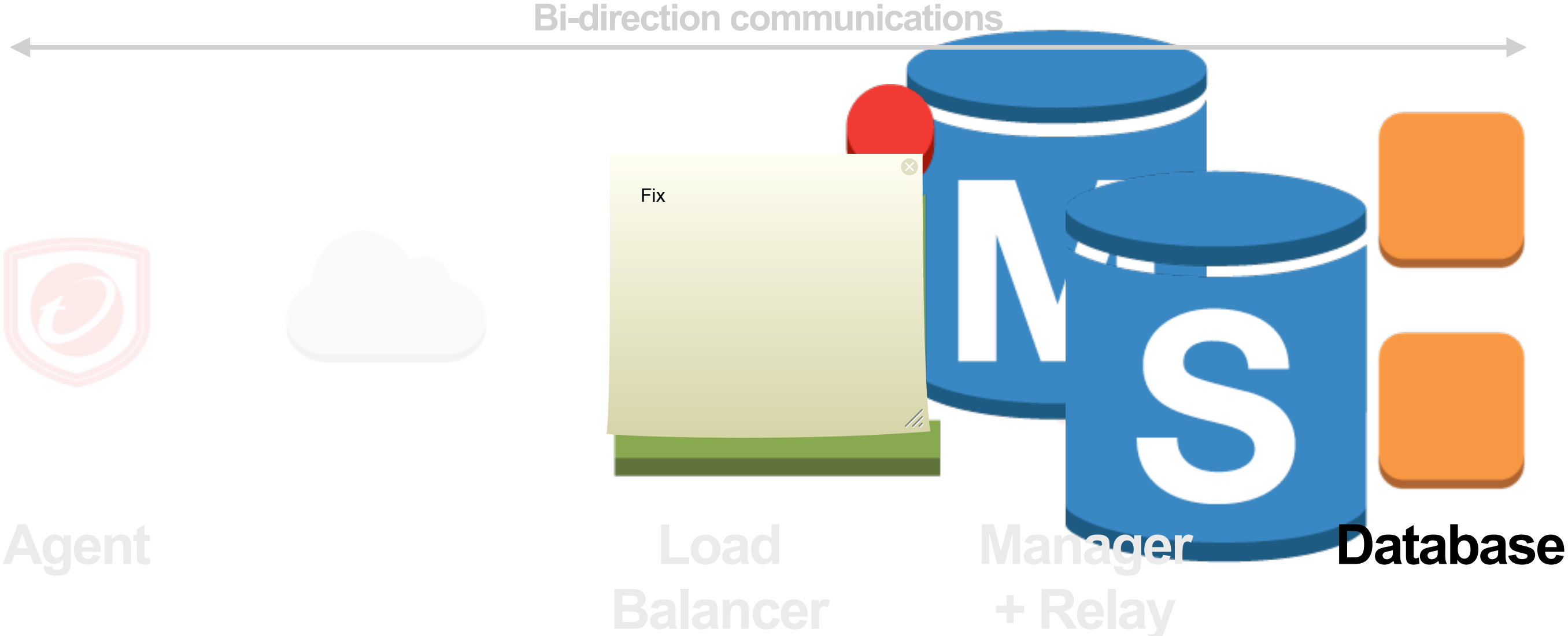


Load
Balancer

Manager
+ Relay

Database

Database Architecture



Final(ish) Design

High Level Architecture



Agent



**Load
Balancer**



**Manager
+ Relay**



Database

High Level Architecture



Agent



**Load
Balancer**

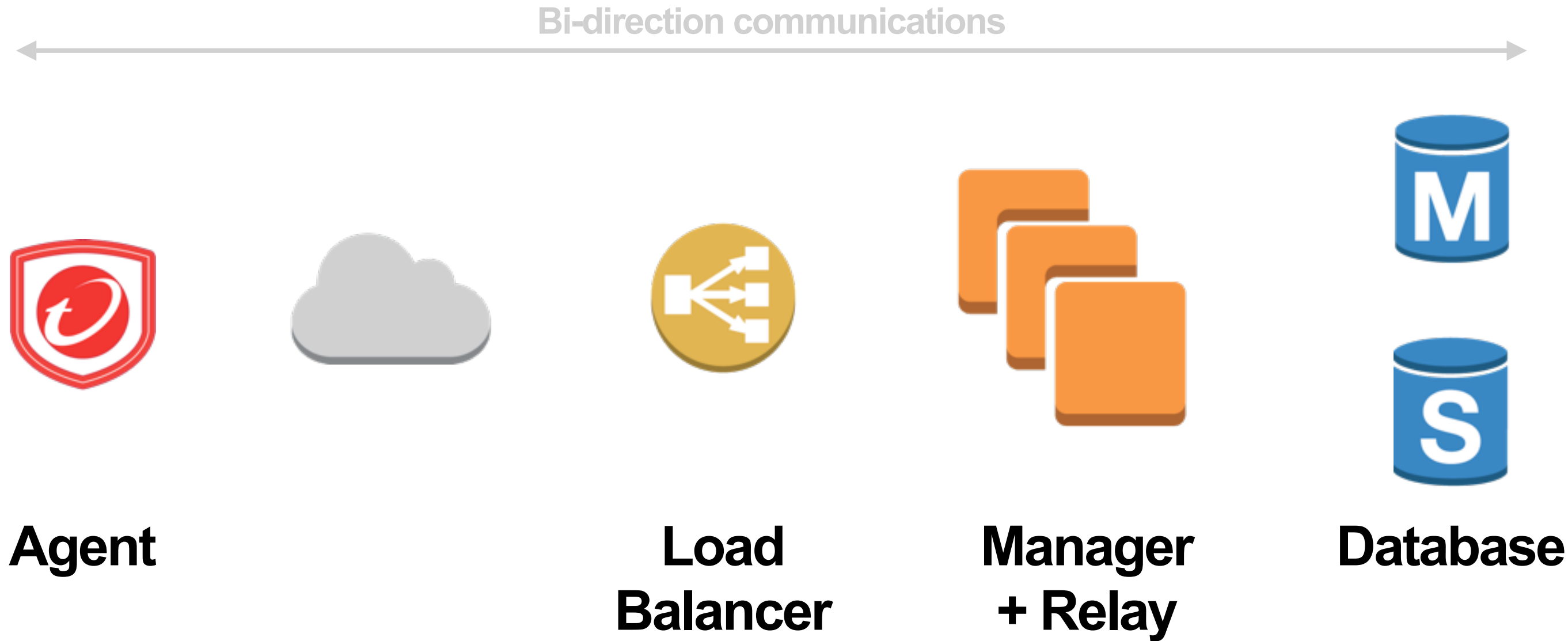


**Manager
+ Relay**



Database

High Level Architecture



High Level Architecture



Agent



**Load
Balancer**



**Manager
+ Relay**

Add highly detailed graphic here



Database

High Level Architecture



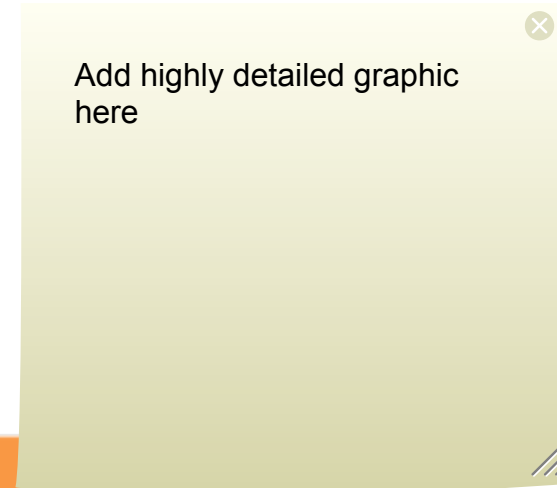
Agent



**Load
Balancer**

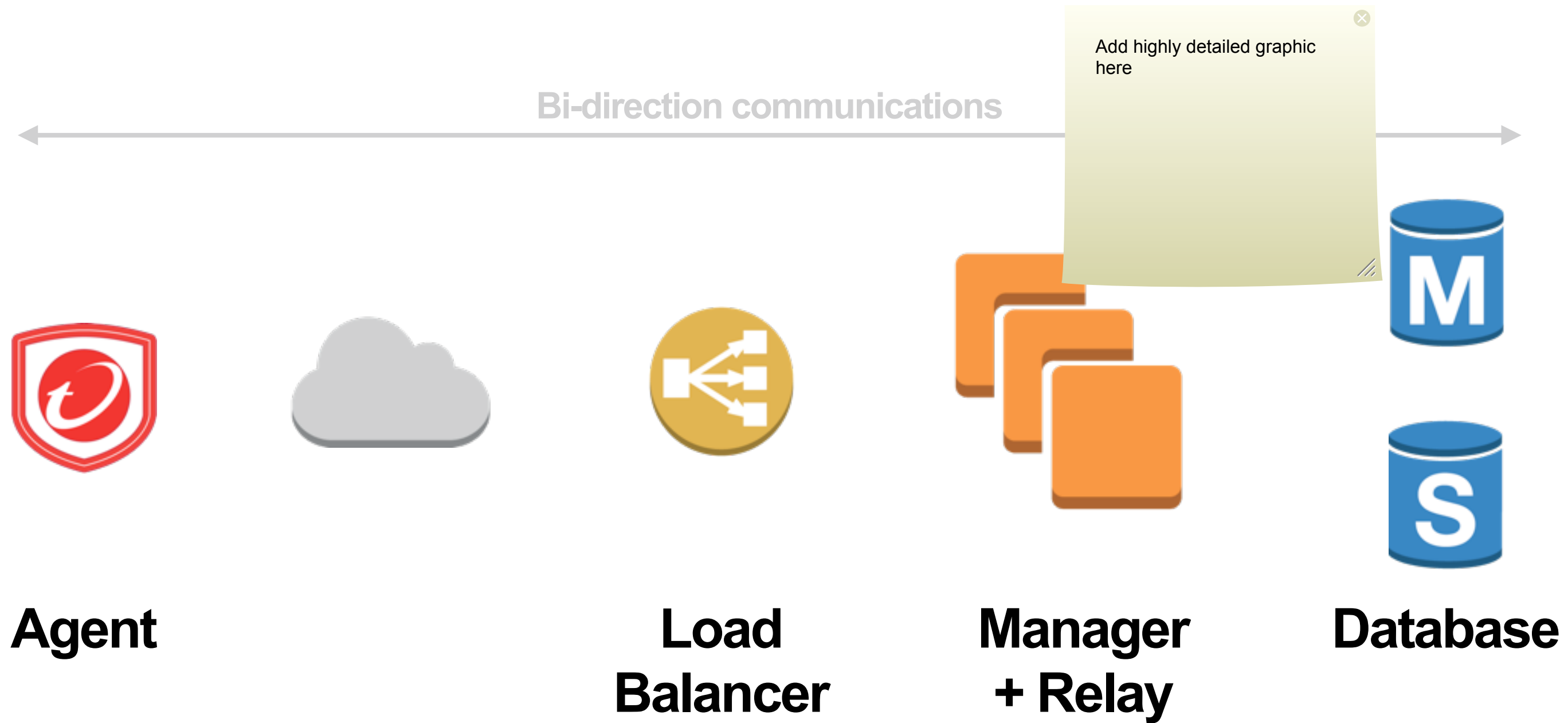


**Manager
+ Relay**



Database

High Level Architecture



Supporting Services

Supporting Services



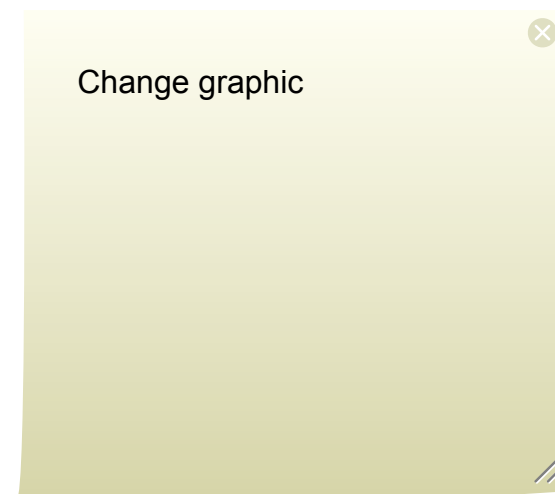
**Amazon Route 53 for all
DNS**

Supporting Services

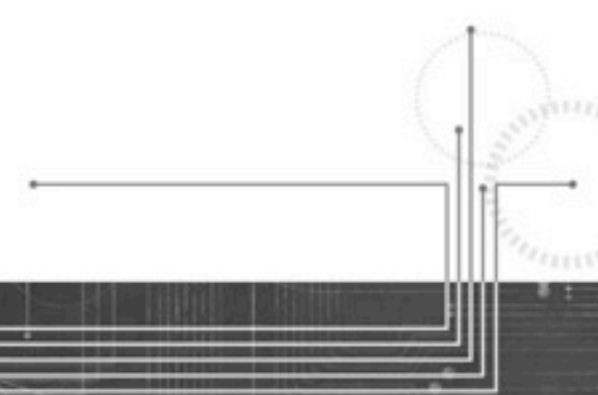


**Amazon S3 for
deployment storage**

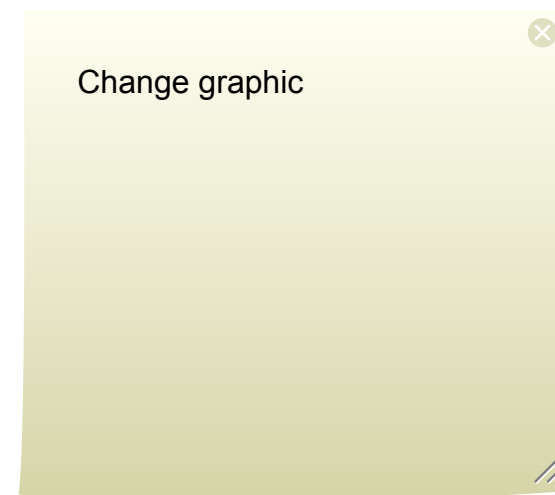
Supporting Services



**AWS Trusted Advisor for
sanity checks**



Supporting Services




Premium Support for CYA

“Soft” (not easy) changes

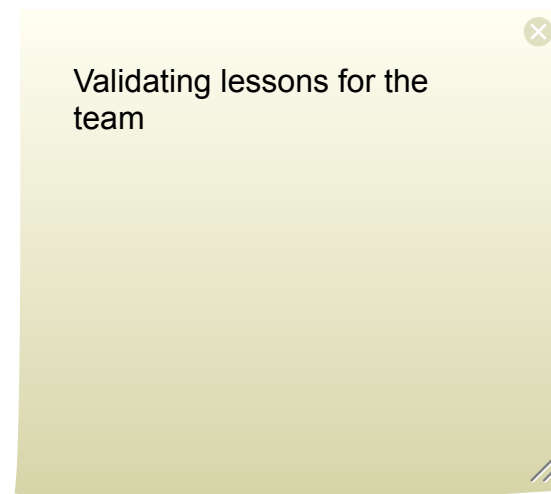
Team Profile

Information Security

- **Own existing security policy**

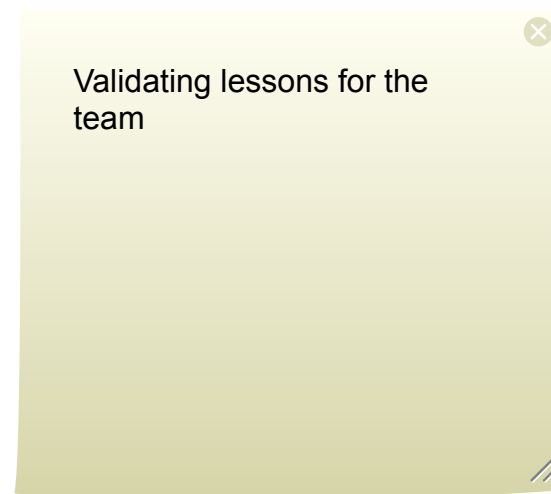


Validating lessons for the team



Information Security

- **Own existing security policy**
- **400+ requirements for operational services**



Information Security

- **Own existing security policy**
- **400+ requirements for operational services**
- **Wants development of cloud best practices**

Team Profile



Operations

- **Run several data centers worldwide**

Team Profile

Validating lessons for the team

Operations

- **Run several data centers worldwide**
- **Rigid change management with complex schedules**

Team Profile

Validating lessons for the team

Operations

- **Run several data centers worldwide**
- **Rigid change management with complex schedules**
- **Wants development of DevOps runbook**

Chart Example

■ Region 1

■ Region 2

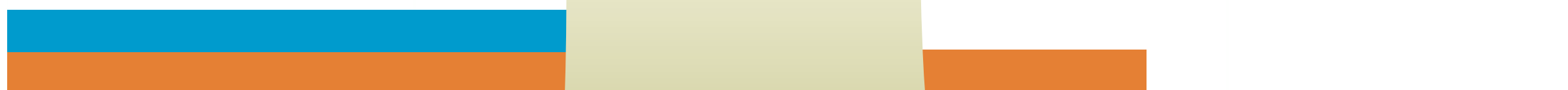
2007



2008



2009



2010



0

25

50

75

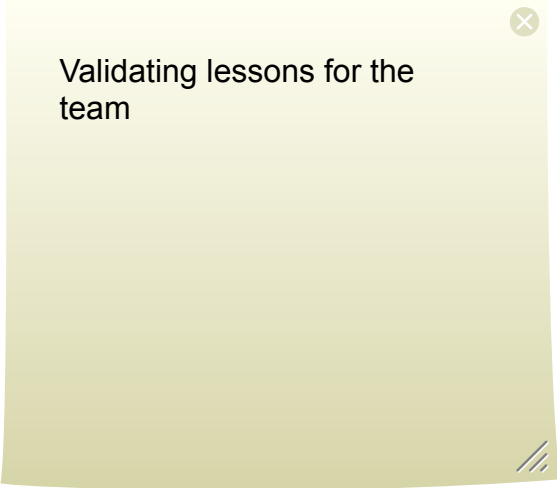
100

Add stats for Service
Add goals for other Trend services

Team Profile

R&D Product Team

- **Develop & maintain the product**



Validating lessons for the team

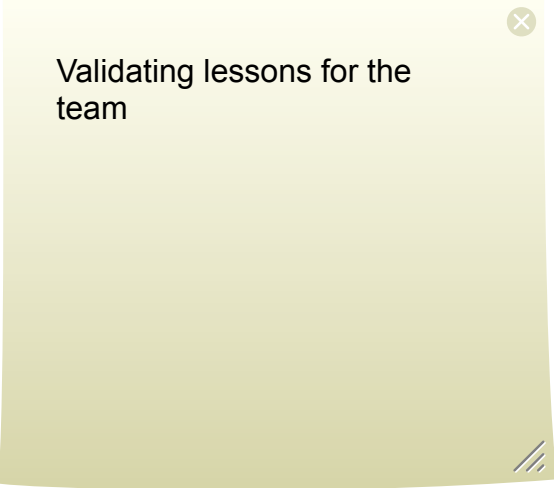
Team Profile

Validating lessons for the team

R&D Product Team

- **Develop & maintain the product**
- **Only operational work is emergency support**

Team Profile

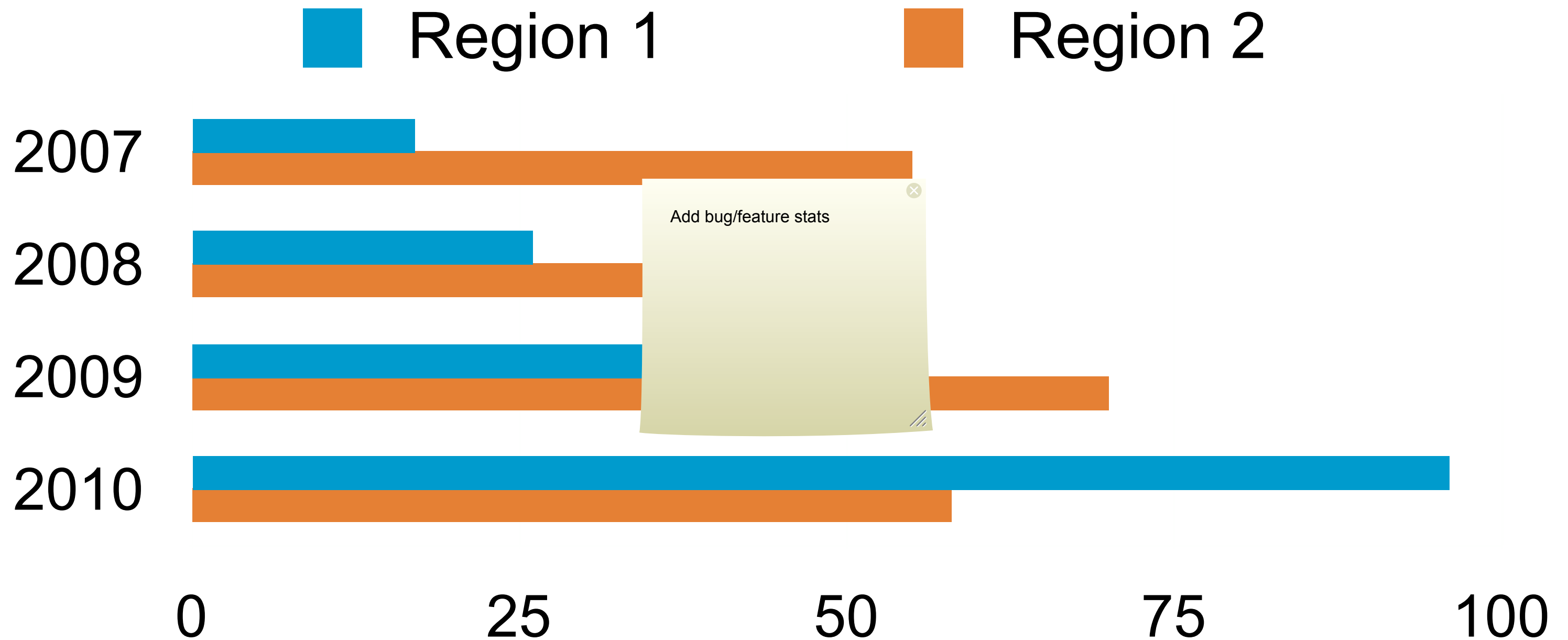


Validating lessons for the team

R&D Product Team

- **Develop & maintain the product**
- **Only operational work is emergency support**
- **Wants tighter feedback loop**

Chart Example



Team Profile



Service Team

- **Own existing security policy**

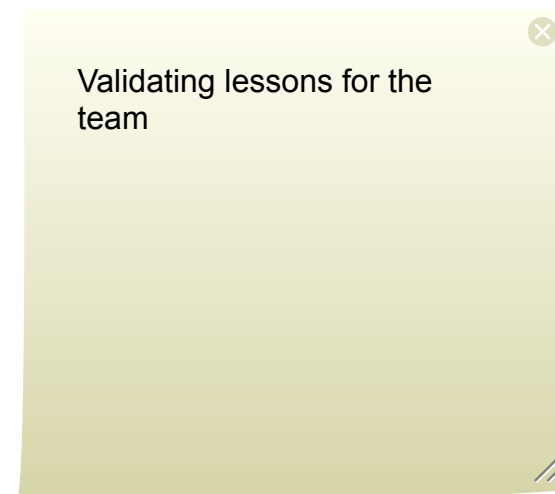
Team Profile



Service Team

- **Own existing security policy**
- **400+ requirements for operational services**

Team Profile



Service Team

- **Own existing security policy**
- **400+ requirements for operational services**
- **Wants development of cloud best practices**

Chart Example

■ Region 1

■ Region 2

2007

2008

2009

2010

0

25

50

75

100

Add stats for support?



Well?

Why a Service?

Security for servers, virtual machines

Why a Service?

Security for servers, virtual machines

Drivers

- **Face the same challenges as our clients**

Why a Service?

Security for servers, virtual machines

Drivers

- **Face the same challenges as our clients**
- **Work directly with clients**

Why a Service?

Security for servers, virtual machines

Drivers

- **Face the same challenges as our clients**
- **Work directly with clients**
- **Smaller feedback loop for new features**

AWS re:Invent

Please give us your feedback on this presentation

SEC307

As a thank you, we will select prize winners daily for completed surveys!

Thank You

