Architecture Dynatrace for Government

Dynatrace Training Module
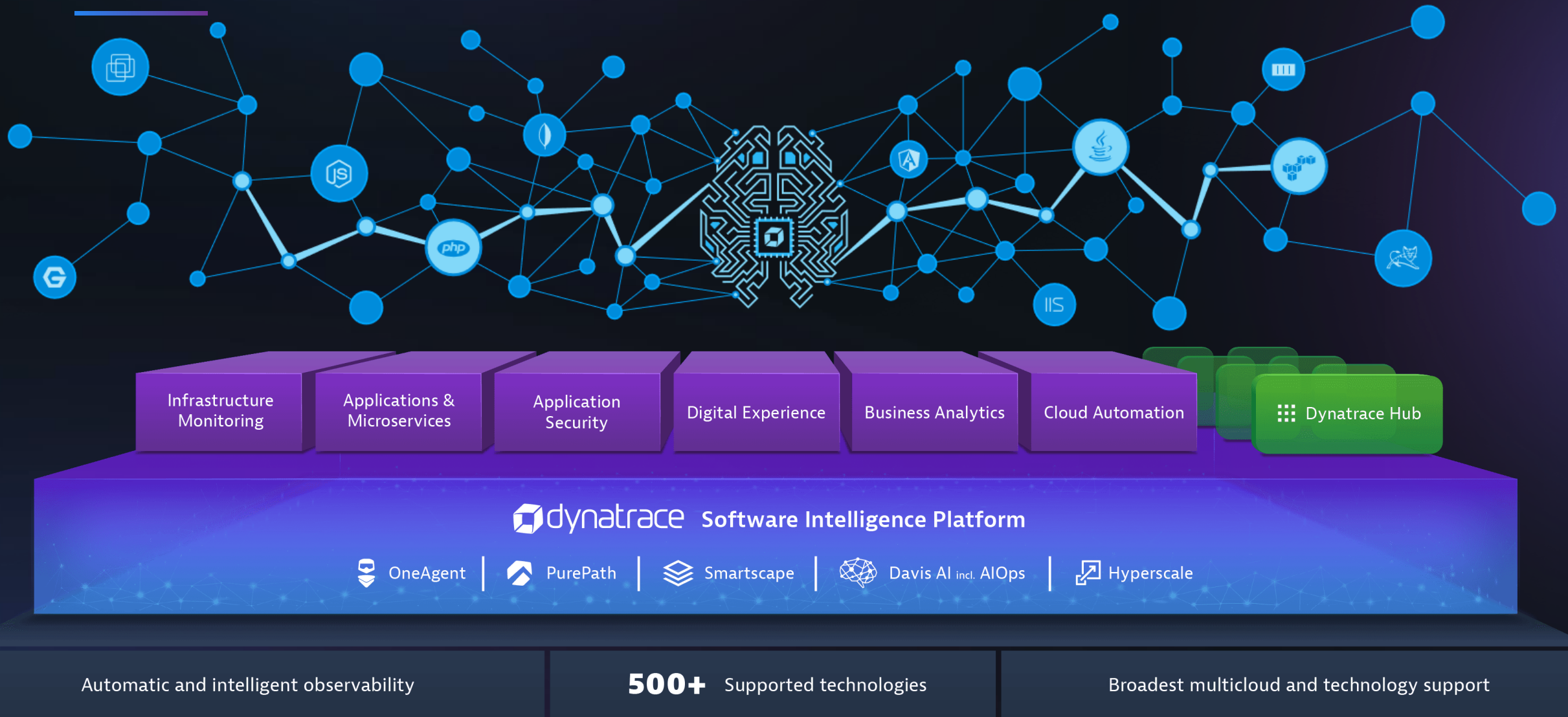
dynatrace

Agenda

- Dynatrace Capabilities Overview

- Dynatrace Offerings
  - Dynatrace for Government vs SaaS vs Managed

- Dynatrace for Government Architecture

What is Dynatrace?

What is Dynatrace?

| Infrastructure Monitoring | Applications & Microservices | Application Security | Digital Experience | Business Analytics | Cloud Automation | ::: Dynatrace Hub |

dynatrace **Software Intelligence Platform**

OneAgent | PurePath | Smartscape | Davis AI incl. AIOps | Hyperscale

| Automatic and intelligent observability | **500+** Supported technologies | Broadest multicloud and technology support |

Deploying software and getting the best of both worlds

SaaS

We provide the service, you just use it.

Benefits
- No local installation
- No worries about hardware provisioning backups and data storage
- No monitoring/operator needed

Concerns
- Compliance
- Bandwidth consumption

On Premises

We provide the software, you run it.

Benefits
- Full control of data

Concerns
- System administrators need to support it: troubleshooting, patching, upgrading, backup, monitoring, failover

Deploying software and getting the best of both worlds

DT for Government
SaaS

We provide the service, you just use it.

Benefits

- No local installation
- No worries about hardware provisioning backups and data storage
- No monitoring/operator needed

Concerns

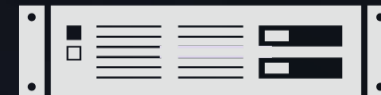- Bandwidth consumption

Managed
On Premises

You provide the platform, we manage the service.

Benefits

- Full control of data
- Self monitoring built-in
- No worries about patching, upgrading, troubleshooting, monitoring or failover

Deploying software and getting the best of both worlds

DT for Government

We provide the service, you just use it.

- No local installation
- No worries about hardware provisioning backups and data storage
- No monitoring/operator needed

Concerns
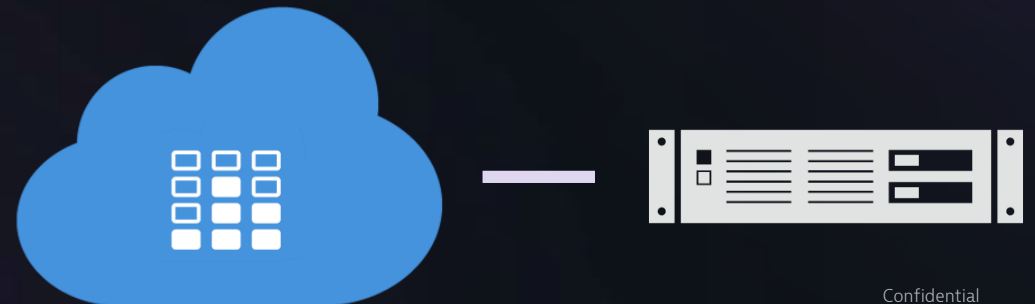- Bandwidth consumption

Managed

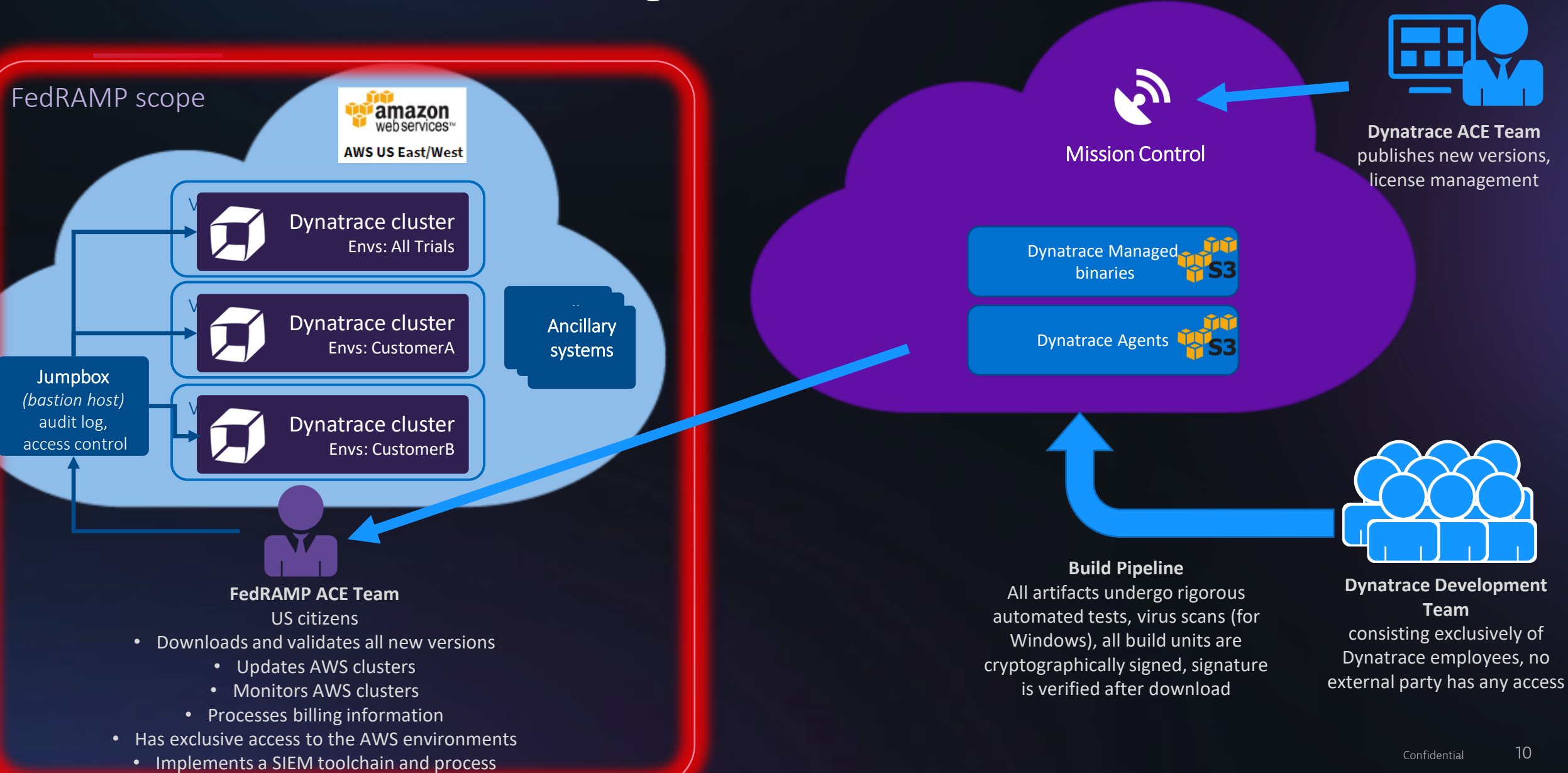*You provide the platform, we manage the service.*

- Full control of data
- Self monitoring built-in
- No worries about patching, upgrading, troubleshooting, monitoring or failover
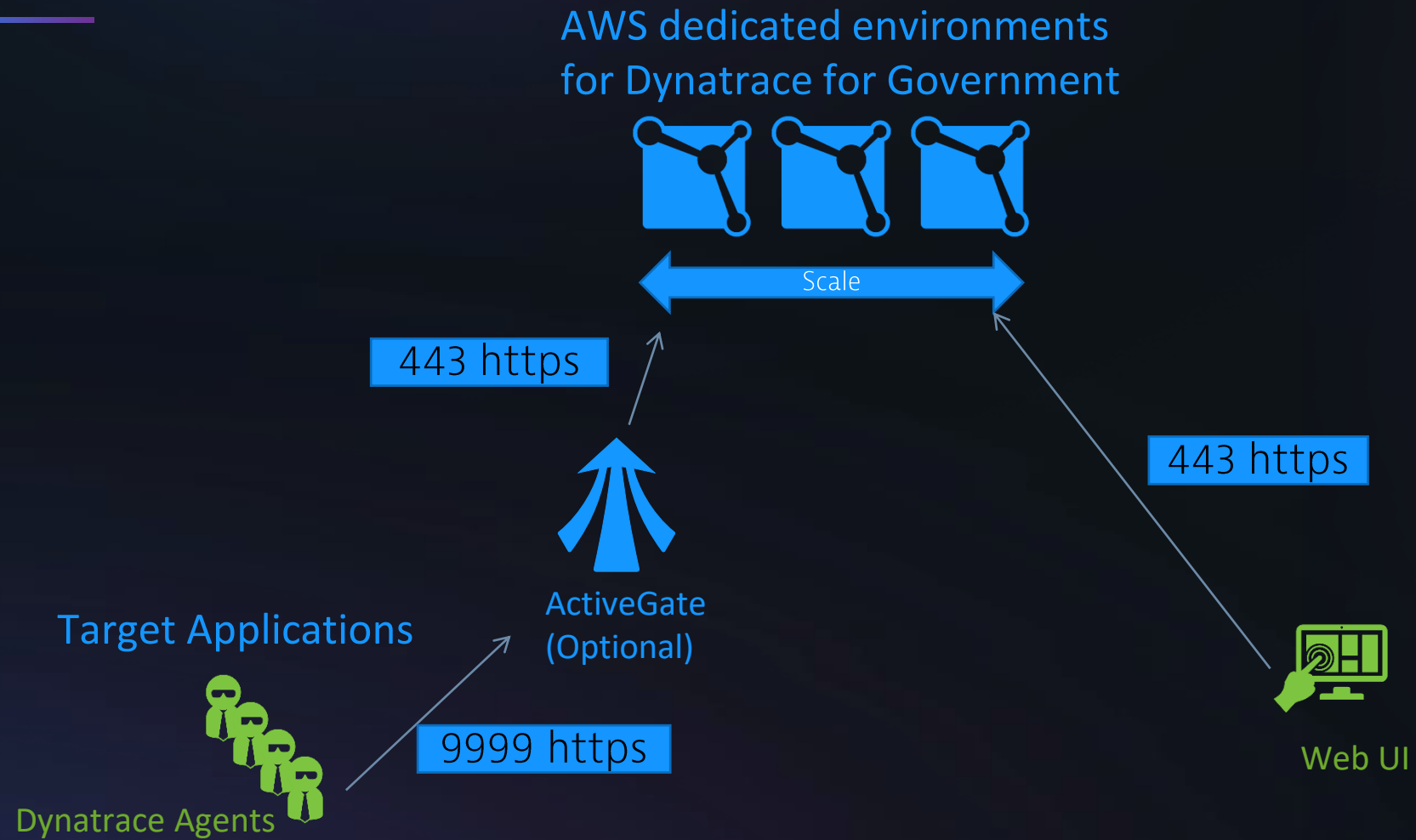
Dynatrace for Government

Dynatrace for Government Architecture
(a FedRAMP-certified, isolated SaaS offering)

FedRAMP scope

AWS US East/West

Dynatrace cluster
Envs: All Trials

Dynatrace cluster
Envs: CustomerA

Ancillary systems

Dynatrace cluster
Envs: CustomerB

Jumpbox
(bastion host)
audit log,
access control

Mission Control

Dynatrace Managed
binaries **S3**

Dynatrace Agents **S3**

Dynatrace ACE Team
publishes new versions,
license management

FedRAMP ACE Team
US citizens
- Downloads and validates all new versions
  - Updates AWS clusters
  - Monitors AWS clusters
  - Processes billing information
- Has exclusive access to the AWS environments
  - Implements a SIEM toolchain and process

Build Pipeline
All artifacts undergo rigorous
automated tests, virus scans (for
Windows), all build units are
cryptographically signed, signature
is verified after download

**Dynatrace Development
Team**
consisting exclusively of
Dynatrace employees, no
external party has any access

Ports - SaaS

AWS dedicated environments
for Dynatrace for Government

Scale

443 https

443 https

ActiveGate
(Optional)

Target Applications

9999 https

Dynatrace Agents

Web UI

Storage and Retention - Dynatrace for Government

- Code Level and Performance data
  - Service Requests – 35 days (can be adjusted)
  - Service Code Level – 10 days (can be adjusted)
- Time Series
  - **1 minute** intervals – **14 days**
  - **5 minute** intervals – **28 days**
  - **1 hour** intervals – **400 days**
  - **1 day** intervals – **5 years**
- RUM
  - Sessions and User Actions – **35 days** (can be adjusted)
  - Session Replay – 35 **days**
  - Waterfall analysis– **10 days** (can be adjusted)
- Synthetic
  - Transactions – **35 days** (can be adjusted)

Tooltips provide info on where data is coming from

Updates

- The components are updated on the schedules below:

- SaaS Cluster
  - Every 4 weeks (automatic)

- OneAgent
  - Every 4 weeks (optional)
  - OneAgent versions are supported for 9 months (12 months with Premium support)

Environments

What is a monitoring environment?

- Dynatrace environments contain all of the monitoring data

- It is an independent instance (tenant) where root cause analysis and fault domain isolation take place

- Your monitoring tenant is where Dynatrace OneAgent sends its monitoring data

- It also includes the dashboards, charts, and reports that you use to stay on top of your environment's performance

- Think of your monitoring environment as the analysis server that provides all application performance analysis

Multiple Environments

- Generally it is best to have one environment.

- For usability purposes or licensing there may rise a need to have multiple DT environments
  - Sample use cases:
    - To separate Prod from Non-Prod
    - Security or process and procedure requirements
    - Custom data retention periods
    - To handle license allocation

- Agent Deployment
  - Every environment has its own agent (preloaded configurations)
  - Make sure to obtain the deploy script from the specific environment (Dynatrace Hub)

- Navigating between the multiple environments
  - Navigating between different environments can be done by clicking on the Top Right Menu and selecting the environment name

How many Environments do I need?

Dynatrace Component	Level	Use Cases	Control User Access	Cross Transaction Monitoring
Environment	1	• License Quotas • Control access to global Settings (typically used to limit configuration access for Prod)	Yes (per User Group)	No
Host Group	2	• Separate processes into logical groupings • Pass in additional metadata for tagging/naming	No	Yes
Management Zone	2	• Separate Applications, Services, and resources into logical groupings (used in combination with Host Groups) • Control edit access to individual entities • Filter a single tile or an entire Dashboard • Global filtering of the data • Filter Alert notifications	Yes (per User Group)	Yes
Tag	2	• Filter a single tile on a Dashboard • Advanced filtering • Filter Alert notifications	No	Yes

Security

Security

- FedRAMP Moderate Authorization

- Our security measures include best practices such as firewalls and regular security updates

- We also perform regular security scans and vulnerability assessments using external parties

- Dynatrace benefits from Amazon's secure, world-class data centers

- Our security team relies on industry best practices, such as:
  - Encrypted transmissions, cross-site scripting prevention, protection against code or SQL injection, hardening against DoS attacks, firewalls, regular security updates, security scans, and vulnerability assessments to ensure the security of your data

- The OneAgent undergoes continuous and extensive penetration testing and expert security reviews

- All communication between Dynatrace OneAgent and Dynatrace Cluster is handled over secure socket https communication (port 443) with strong cryptography, to guarantee your data privacy

- Metric and transaction data are encrypted even while at rest, and each customer's data are programmatically partitioned from each other customer's data

SOC 2 Type II certified

- Dynatrace has received SOC 2 Type II certification for security and availability

- View our publically available SOC 3 Report to learn more about Dynatrace adherence to the Security and Availability Service Organization Controls 3 (SOC 3) Criteria established by the American Institute of Certified Public Accountants (AICPA)

Questions?

Simply smarter clouds