AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

SEC302-S

SPONSORED BY DATADOG

Securing your company's next big bang

Nathan Case
Senior Director, Security Operations Resilience

Andrew Krug
Security Evangelist
Datadog

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Introductions



Nathan Case

Senior Director, Security Operations Resilience



Andrew Krug

Security Evangelist
Datadog

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

You may have seen us before at re:Invent 2019

DIY guide to runbooks, incident reports, and incident response (SEC318-R1)

youtube.com/watch?v=E1NaYN_fJUo

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

We’re living in a golden age of biology

Unprecedented development of next-generation medicines across all diseases including outright cures



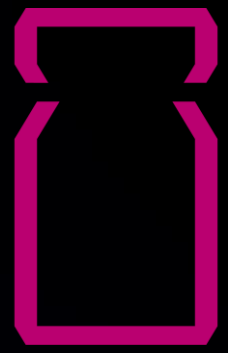
Cell Therapy



Gene Therapy



Nucleic Acids



Vaccines

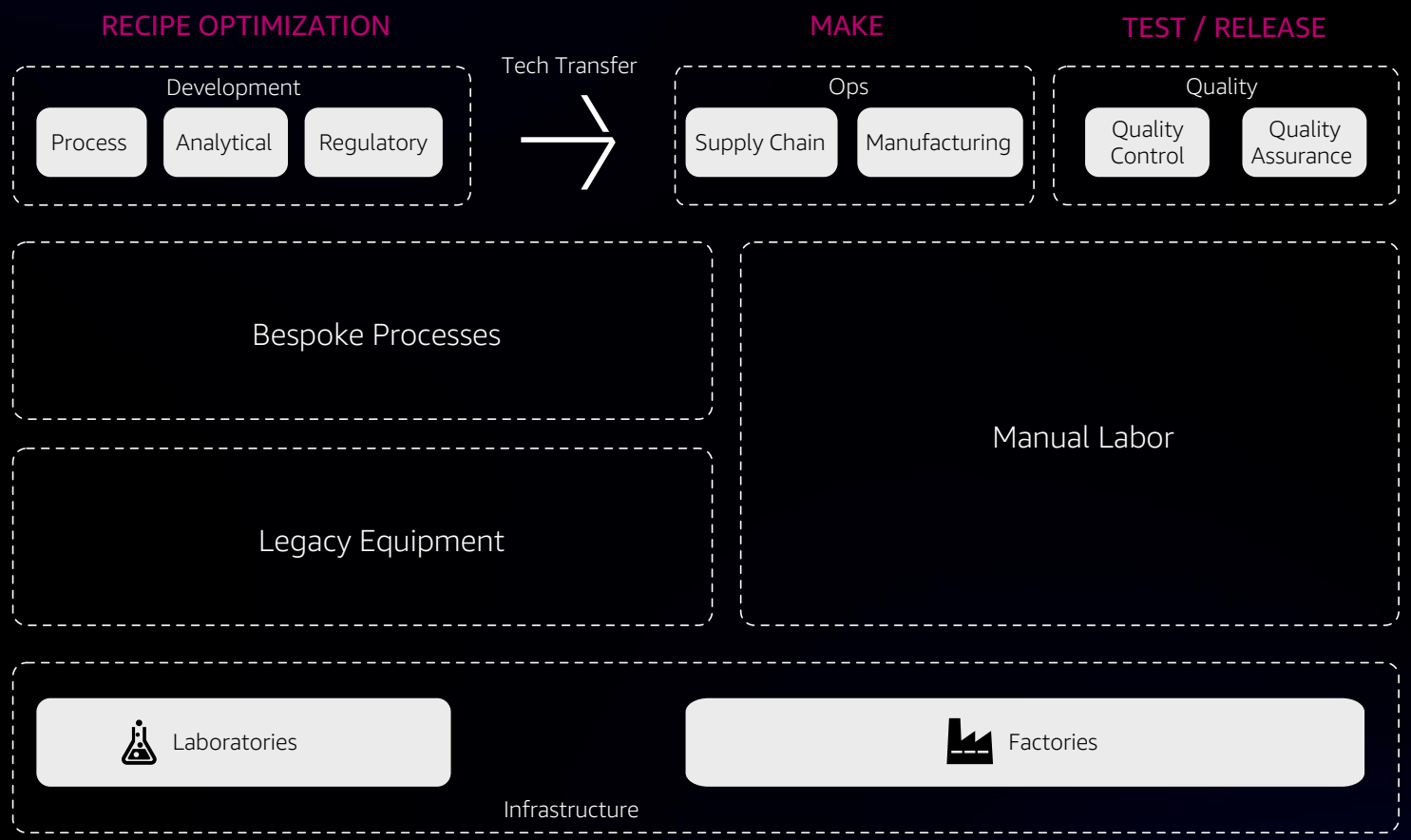


Biologics

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Manufacturing has proven to be the rate-limiter

Infrastructure and know-how available to the very few; artisanal approaches thwart scale, access, low cost

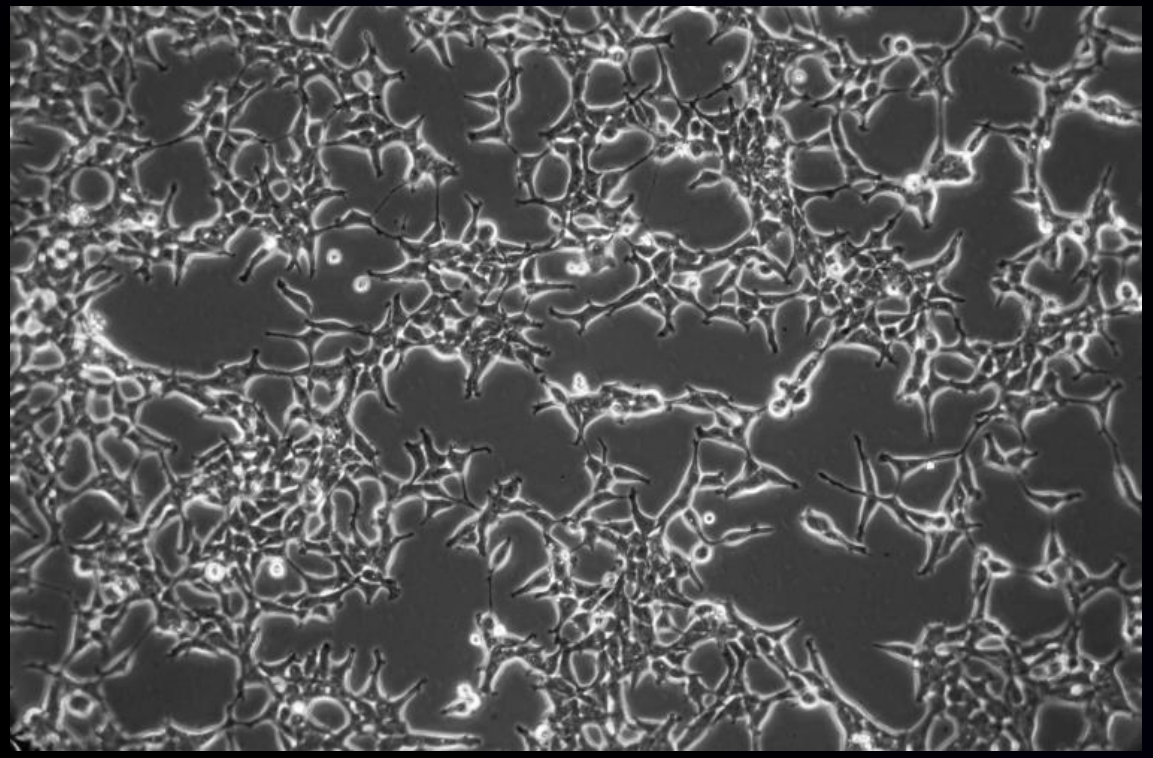


- Errors
- Delays
- Cost
- Opacity
- Regulatory failure

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

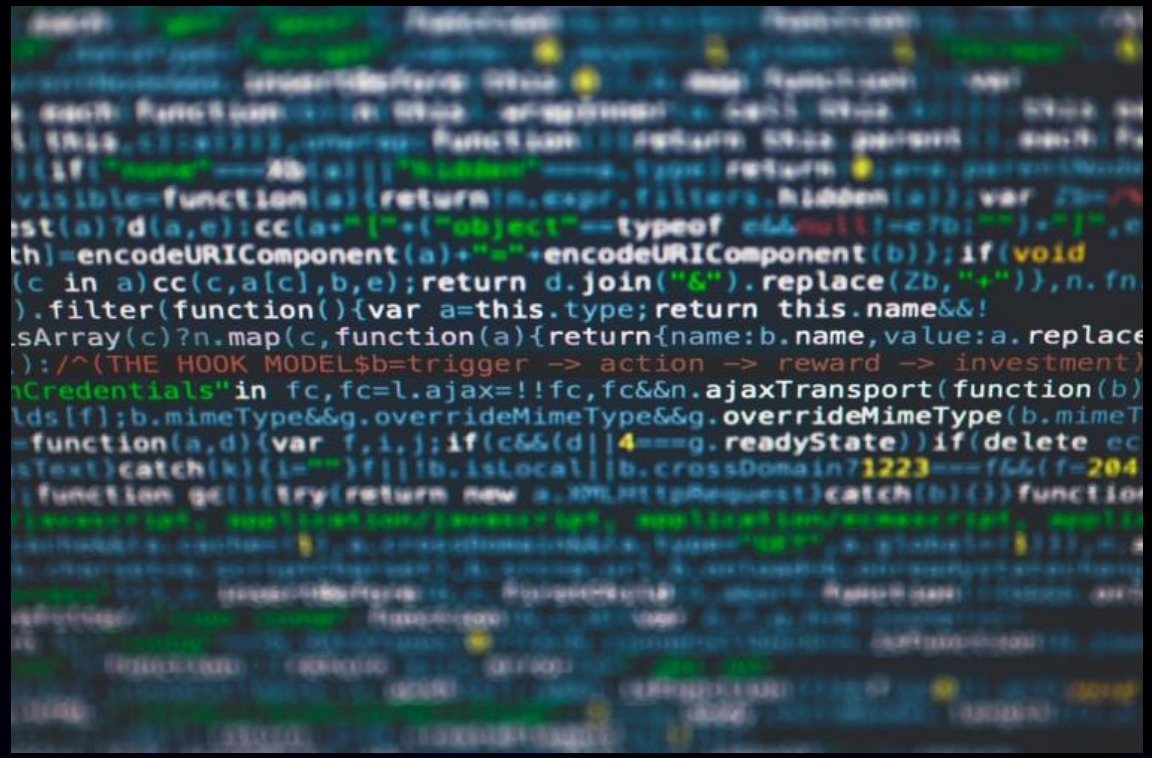
Resilience is a digitally native, cloud-first biotech

We develop new high-performance bio and digital technologies



Bioengineering/bioprocessing

New ways of *making* that are faster, smaller, cheaper, higher quality



Digital

automation, transparency, prediction, security

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Regulated workloads

What is this GxP thing of which you speak?









Santé Canada

Health Canada



Qualification proves that a physical entity (infrastructure, hardware) is fit for its ***intended use*** as defined in a set of requirements.

Validation provides evidence-based proof that a process will consistently produce a result meeting its predetermined specifications and quality attributes.

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How can we move faster while raising the quality/compliance bar?

Learn from modern software development (Agile, CI/CD, etc.) and maximize automation

Development	Traditional		Future state
Infrastructure provisioning	Manual		Automated
Integration + deployments	Manual		Automated
Testing + reports	Manual	**GxP Landing Zone GxP SDLC**	Automated
Delivery	Waterfall		Agile
Qualification + Validation			
Whitelisting of services	Lengthy		Automated
IQ/OQ/PQ processes	Manual		Automated
Document review	Lengthy	**AutoWhitelisting Automated IQ**	Reduced
Approvals	Manual		Streamlined
Ops			
Monitoring + incident reporting	Manual		Automated
Change + release management	Manual		Automated
Traceability	Semi-automated	**Compliance Dashboard**	Automated
Maintaining validated state	Manual		Automated
Backup + restoration	Manual		Automated

AWS Control Tower

AWS CloudFormation

AWS Service Catalog

AWS CloudTrail

Amazon CloudWatch

AWS Config

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

We are pioneering biomanufacturing-as-a-service

A platform for engineering and manipulating biology to produce next-generation medicines



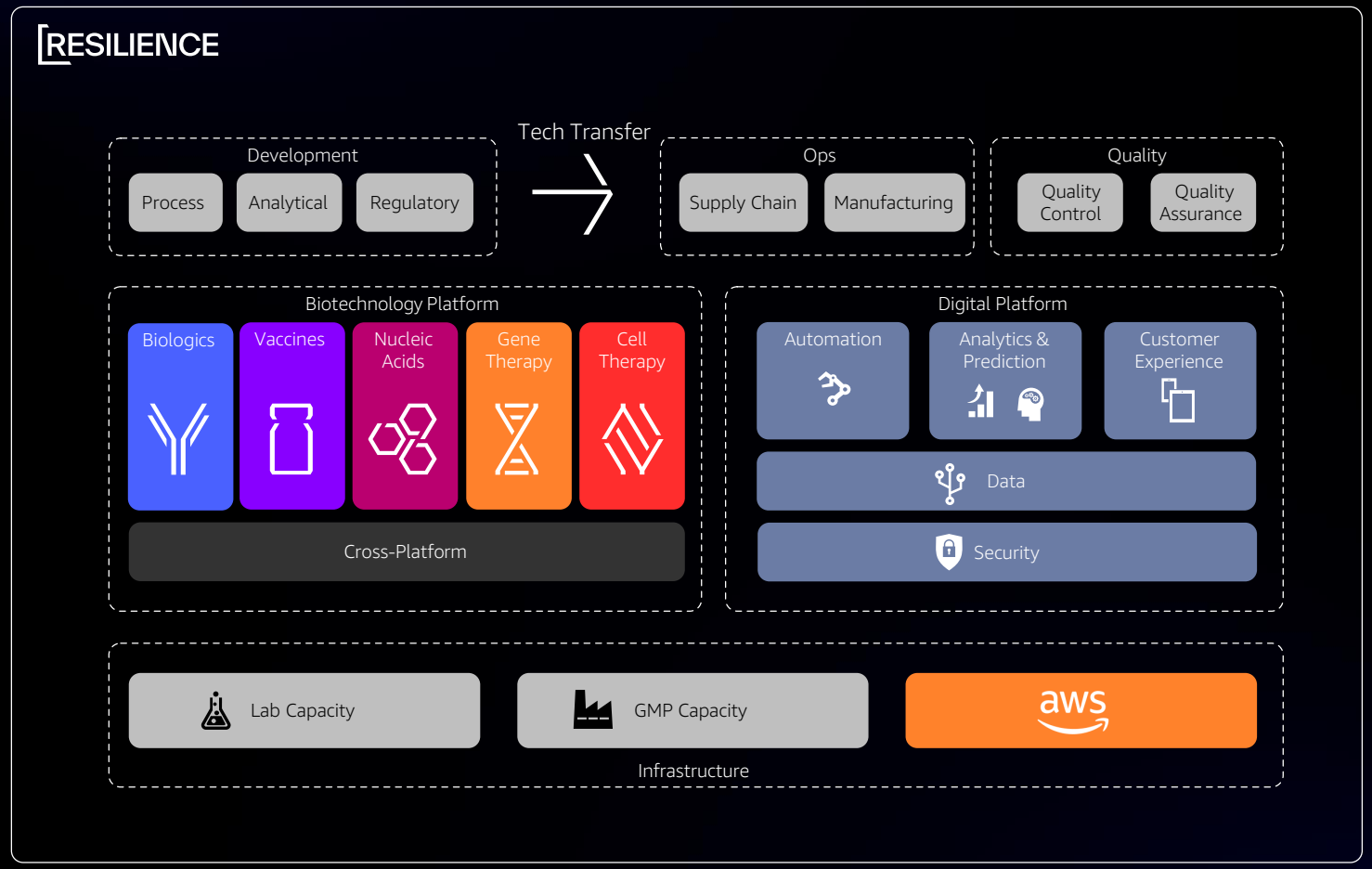




© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

We enable anyone with a next-gen therapy to make it

Faster, cheaper, more reliably without building manufacturing infrastructure or expertise



Idea

Leverage
Do more with less

Speed
Faster from development to patient

Confidence
Reliable and predictable partner

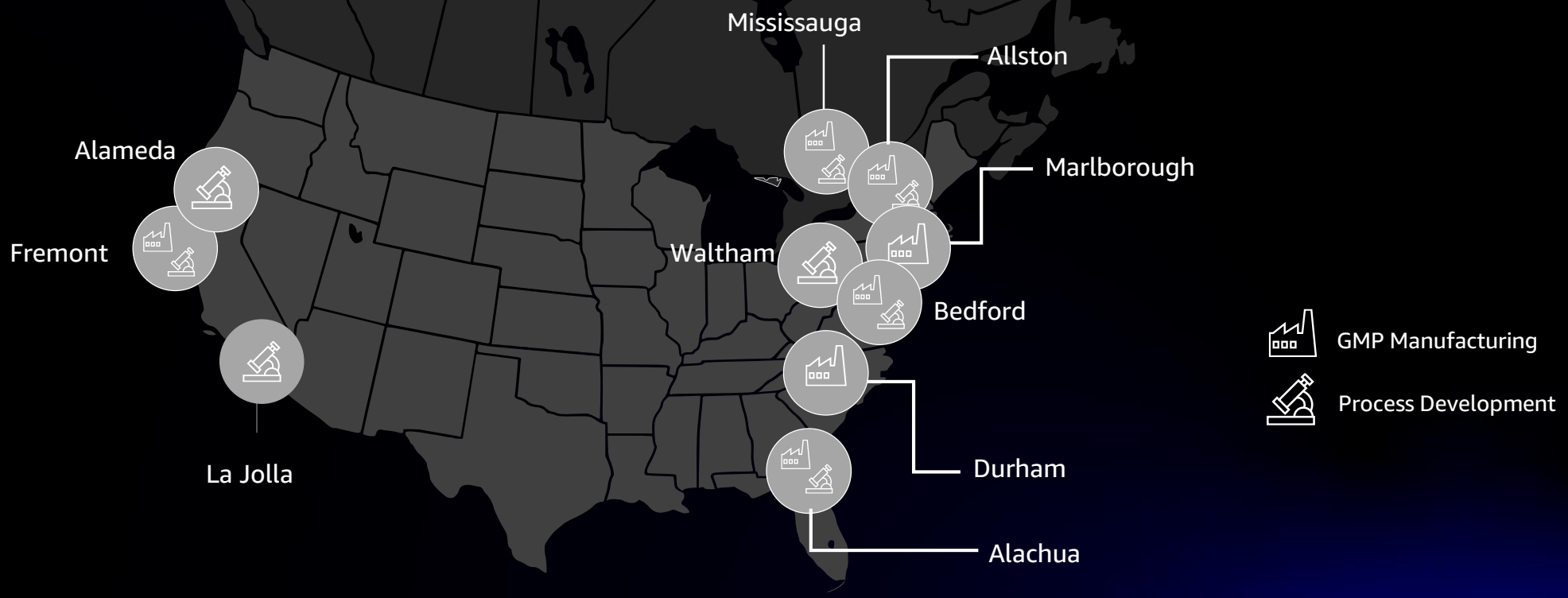
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

We deliver this capability across a global network

Smart labs and smart factories across all modalities

Cell Therapy | **Gene Therapy** | **Vaccines** | **Nucleic Acids** | **Biologics**

Resilience provides on-demand access to biomanufacturing capabilities at all scales and across all modalities; instead of building and maintaining one's own labs and factories for one-off, artisanal manufacturing, our customers access a platform of technologies and expertise, delivered across a global network of high-performance smart facilities, to more rapidly industrialize and scale the global production of their next-generation therapeutics.



aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Virtual desktops

How can something so unsexy be so useful?

Amazon WorkSpaces

Challenges

Hyper-scale growth

Chip shortage / laptop shortage

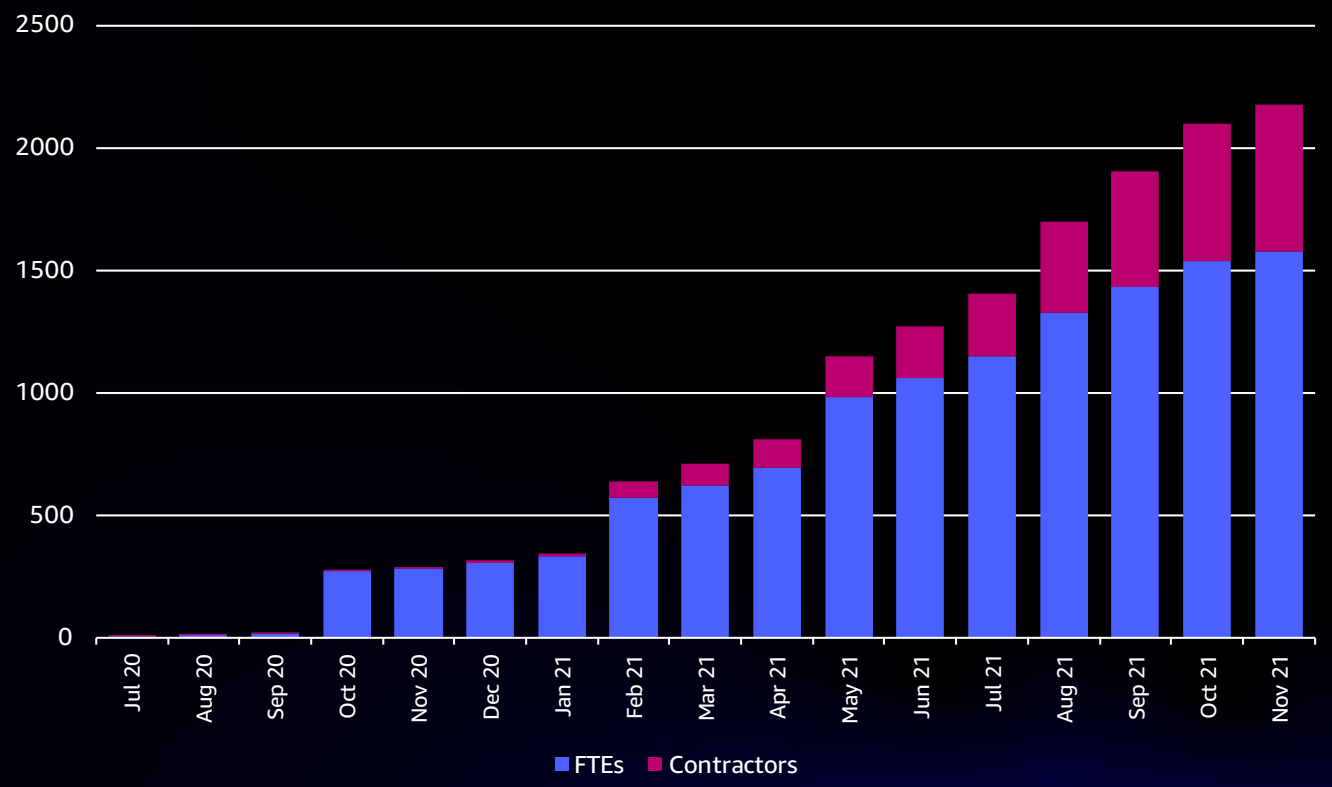
Hundreds of contractors/vendors

PC-controlled instruments

Secure remote access/maintenance

Hazardous (digital) materials

YTD headcount since birth



aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

It’s always Day 1

Among the fastest-growing tech or biotech companies in history… and just getting started

July 2020 launch – 1 employee (CEO)

Nov 2021 (today) – 2000+ workers
150+ in Digital
12 sites across US + Canada
4 operating GMP factories
3 rounds of financing
9 acquisitions

2022 estimates 3000+ workers
300+ in Digital
North America, UK, Europe, Middle East
5+ operating GMP factories

ARCH VENTURE PARTNERS

8VC

NEA®

GV

…among many other investors

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The benefits mirror those of cloud computing itself

Force-multiplying	Scalable	Flexible	Leverage
Make with proven platforms Reduced complexity Outsourced heavy lifting	Lab ↳ Pilot ↳ Clinical ↳ Commercial Global distribution	All modalities Opex not capex Pay only for what you use Shared risk	Do more with less

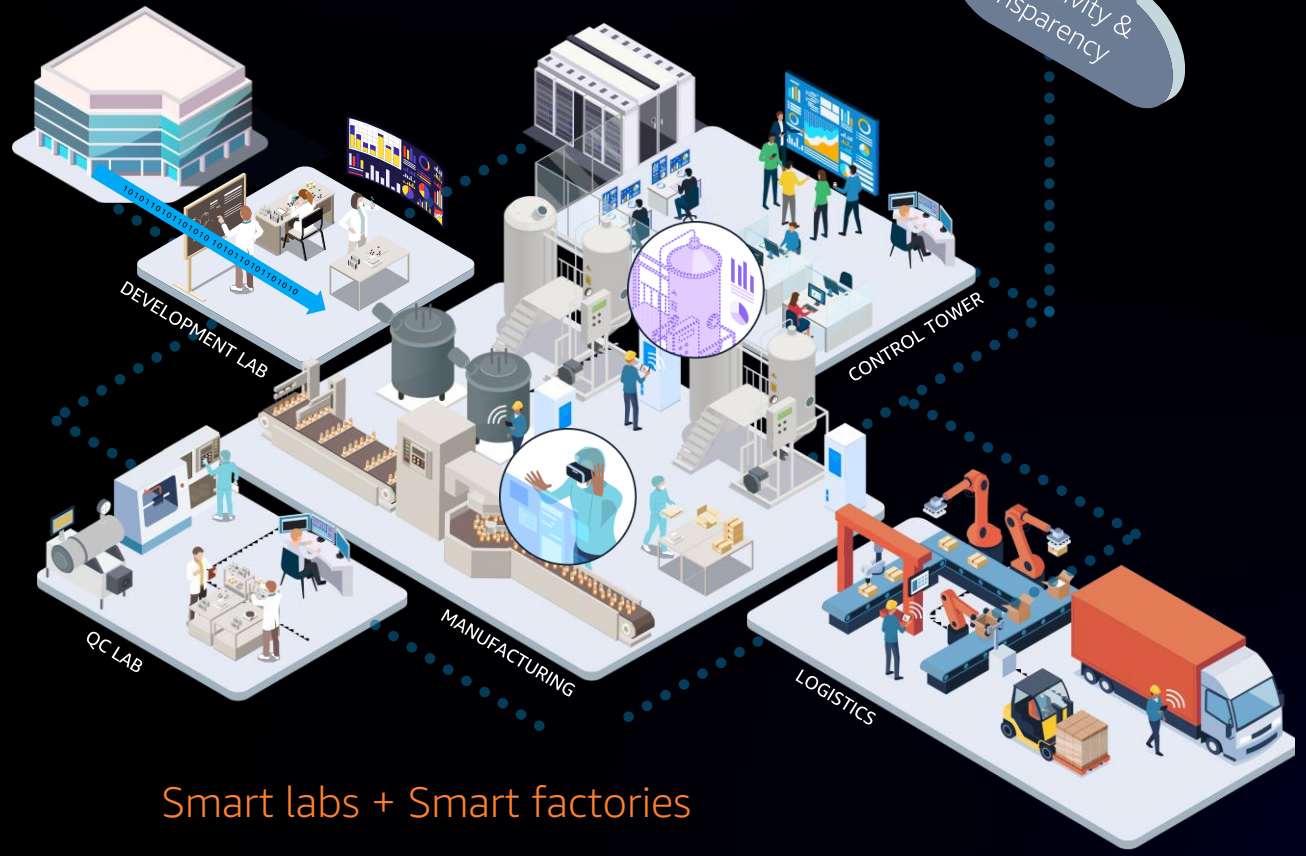
Performant	Accessible	Highly available	Speed
Quality Speed Yield/potency Reproducibility	Next-generation technology Democratized access Obsolescence-proof	Capacity and access Domestic On demand No downtime	Faster from development to patient

Compliant	Secure	Transparent	Confidence
cGMP ISO FedRAMP	Hardened facilities Fault-tolerant supply chain IP protection	Real-time visibility Real-time data transfer Accountability	A reliable and predictable partner

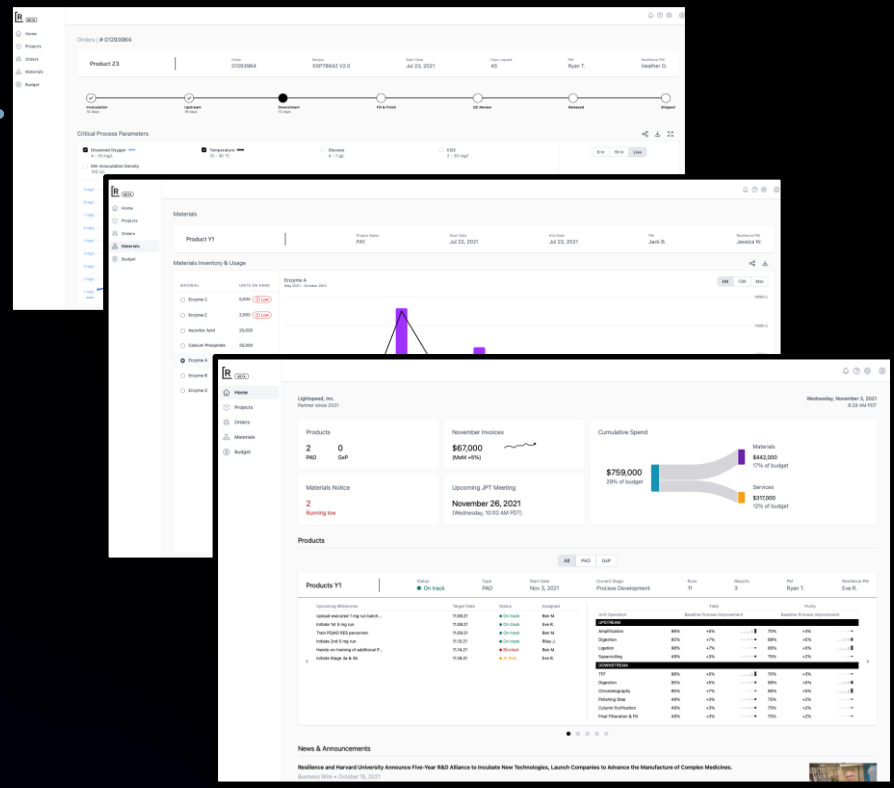
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Reinventing the customer experience

Visibility, performance, security, and scale



Smart labs + Smart factories



Visibility + Transparency

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Bringing tech to biotech is a challenge

Legacy is everywhere… people, process, technology

Infrastructure

On-prem
Heterogeneous
Aging-to-obsolete
Regulated

Devices / OT

Proprietary
Disconnected
Low security posture

Applications

Monolithic
Heterogeneous
Cloud unfriendly
Low security posture
Some low-latency

Data

Limited visibility
Siloed when it exists
Paper is everywhere

Processes

Highly manual
Highly regulated

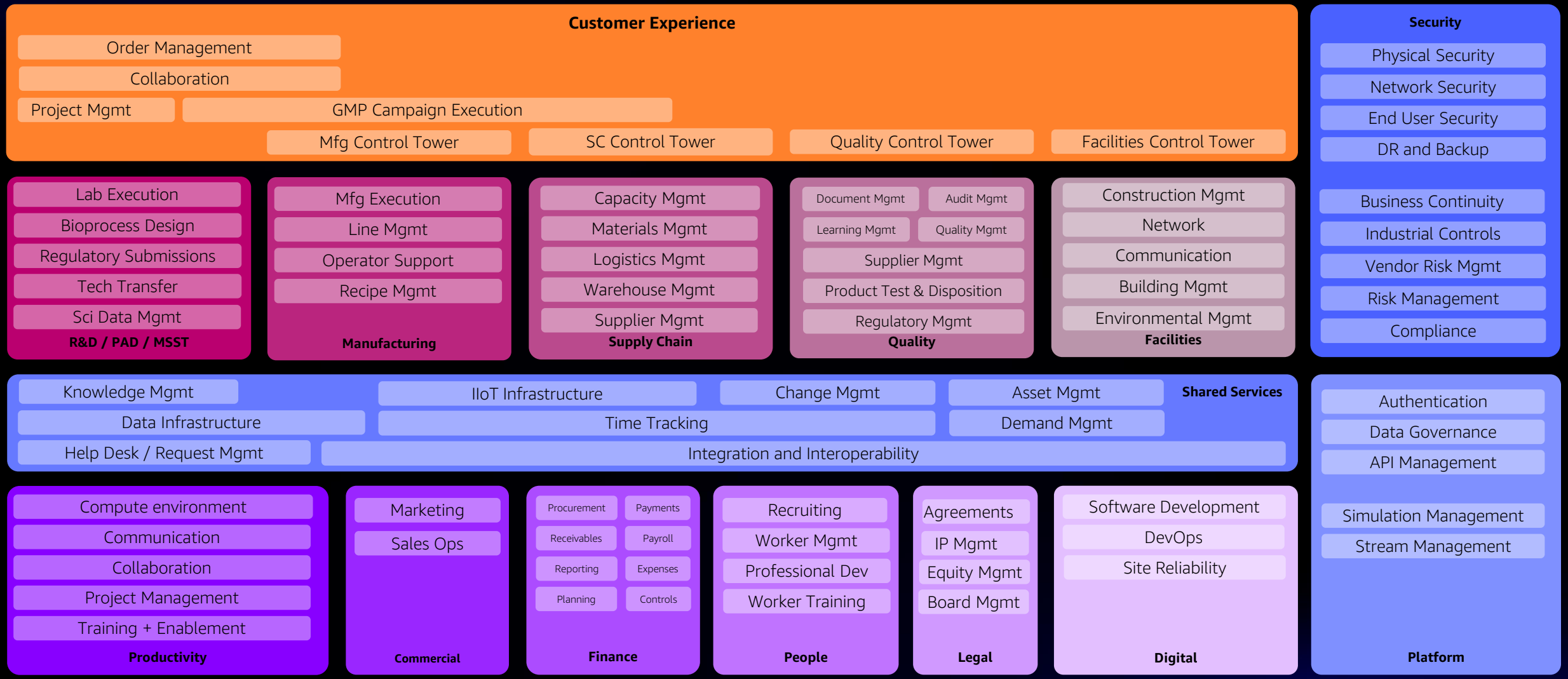
People

Globally distributed workforce
Site-based concentrations
Contractors and vendors everywhere

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

We think and design around a “microservices” architecture

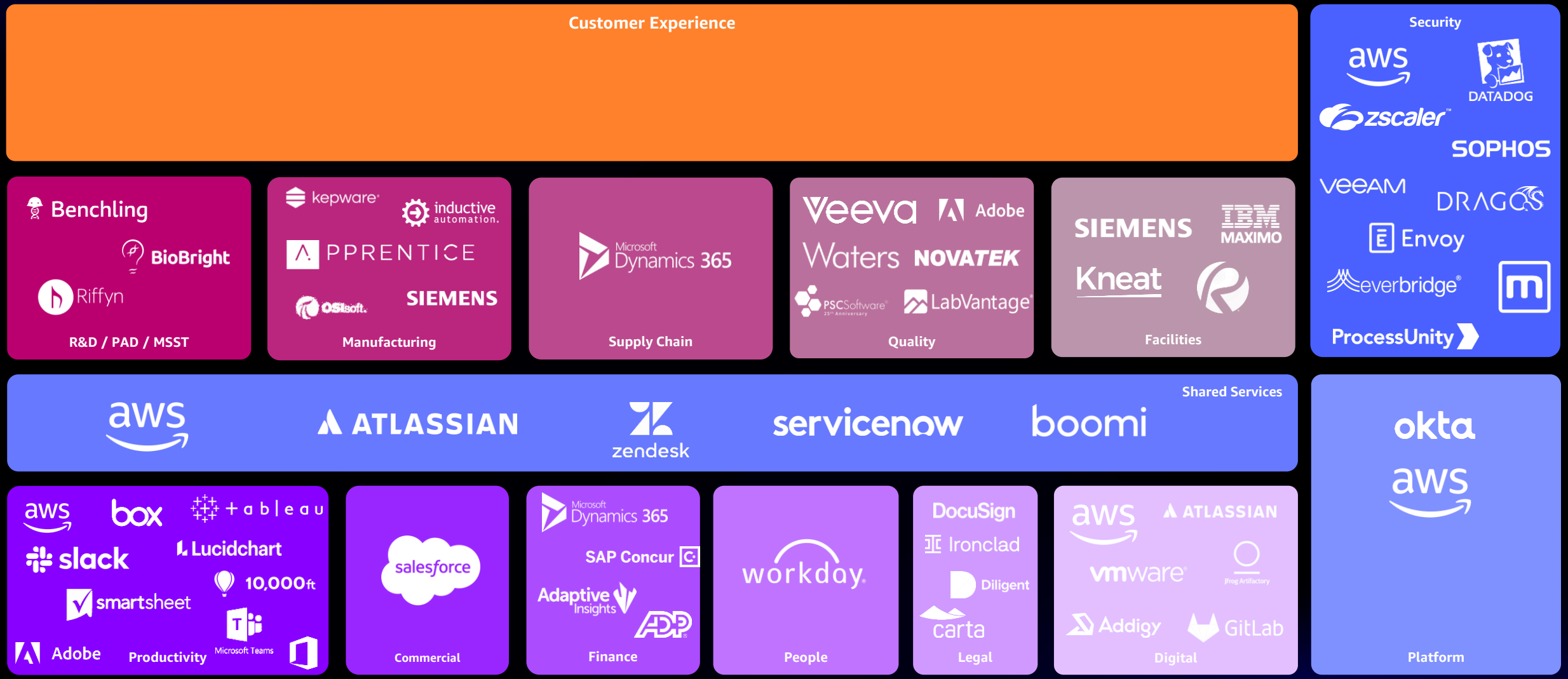
We start with use cases/capabilities; we insist on standardization and modularization; we decide build vs. buy



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

We insist on best-in-breed applications (where they exist)

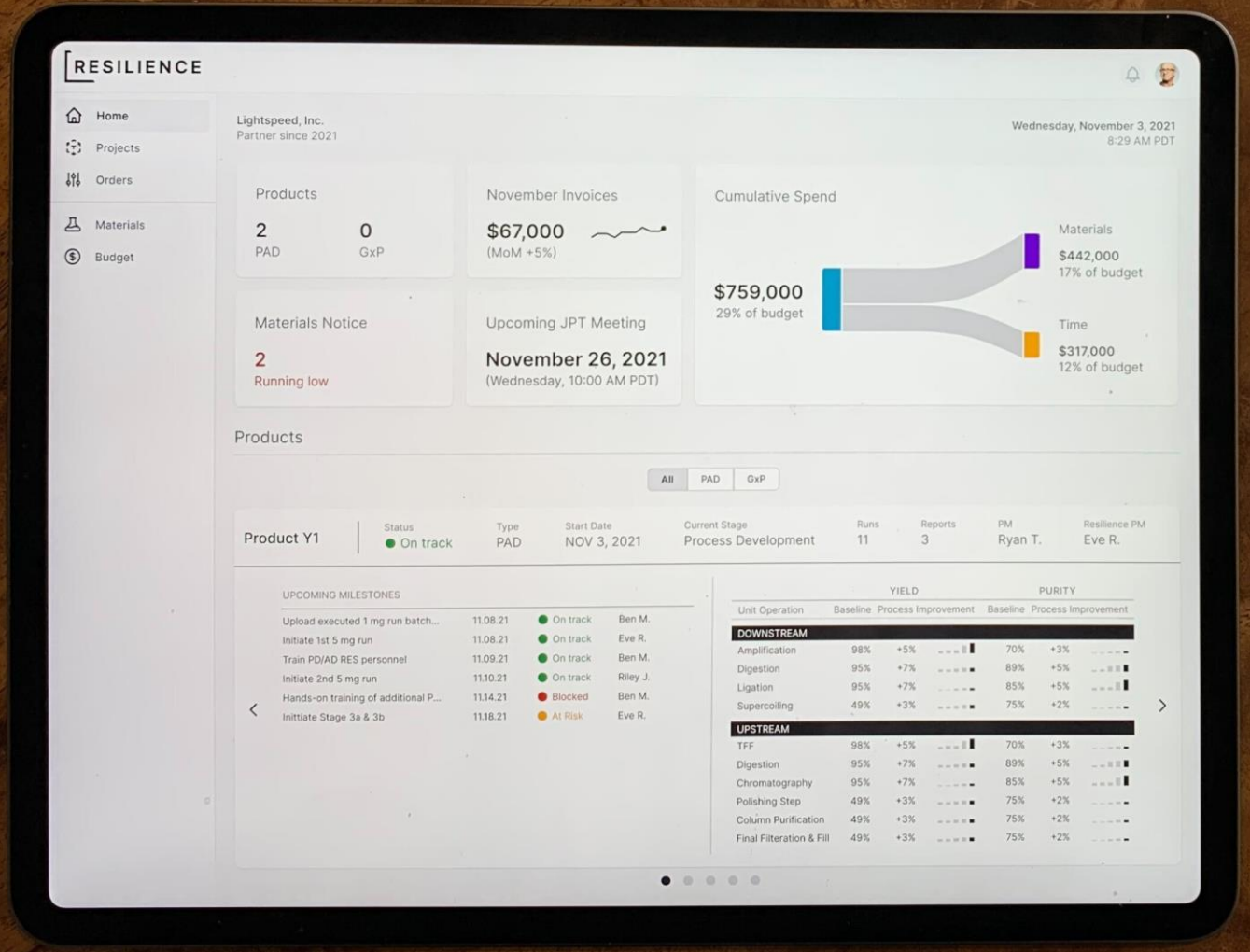
Optimized for functionality, interoperability, security, cloud-compatibility



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

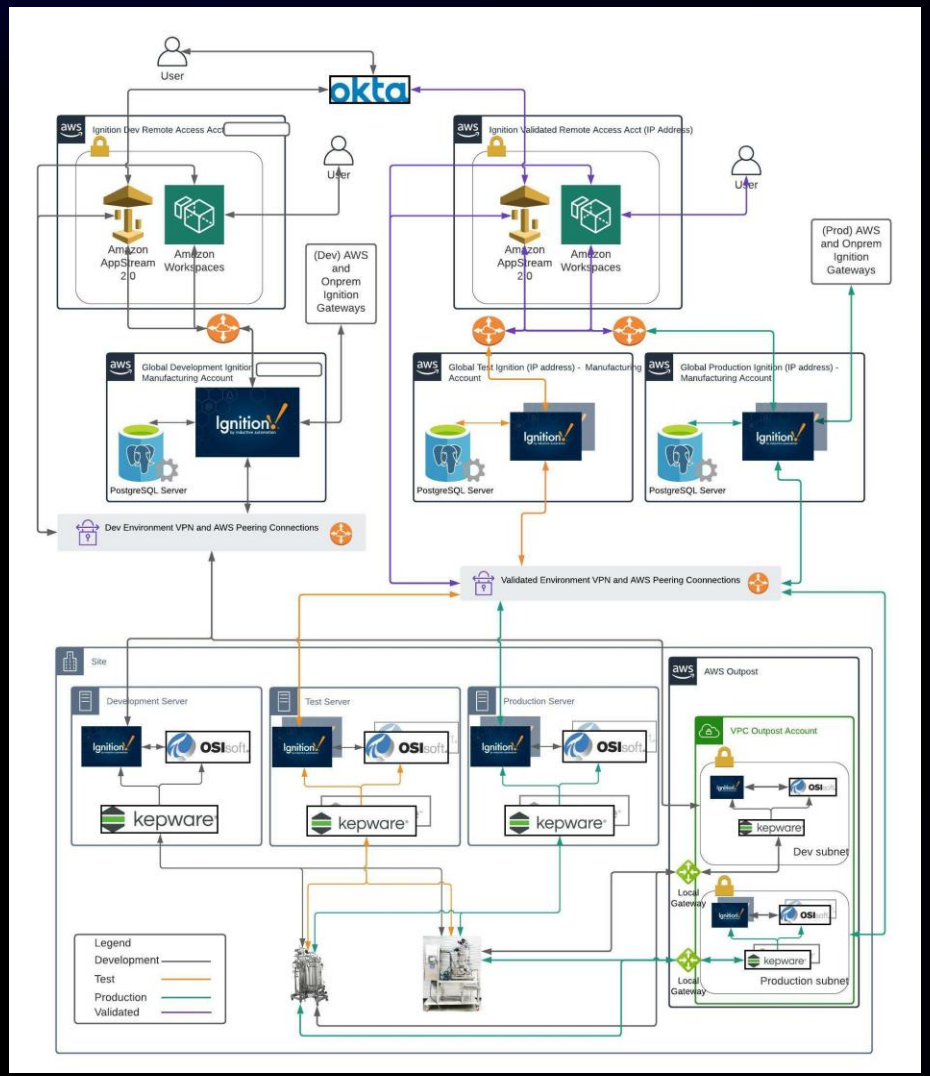
We build what doesn't exist but should

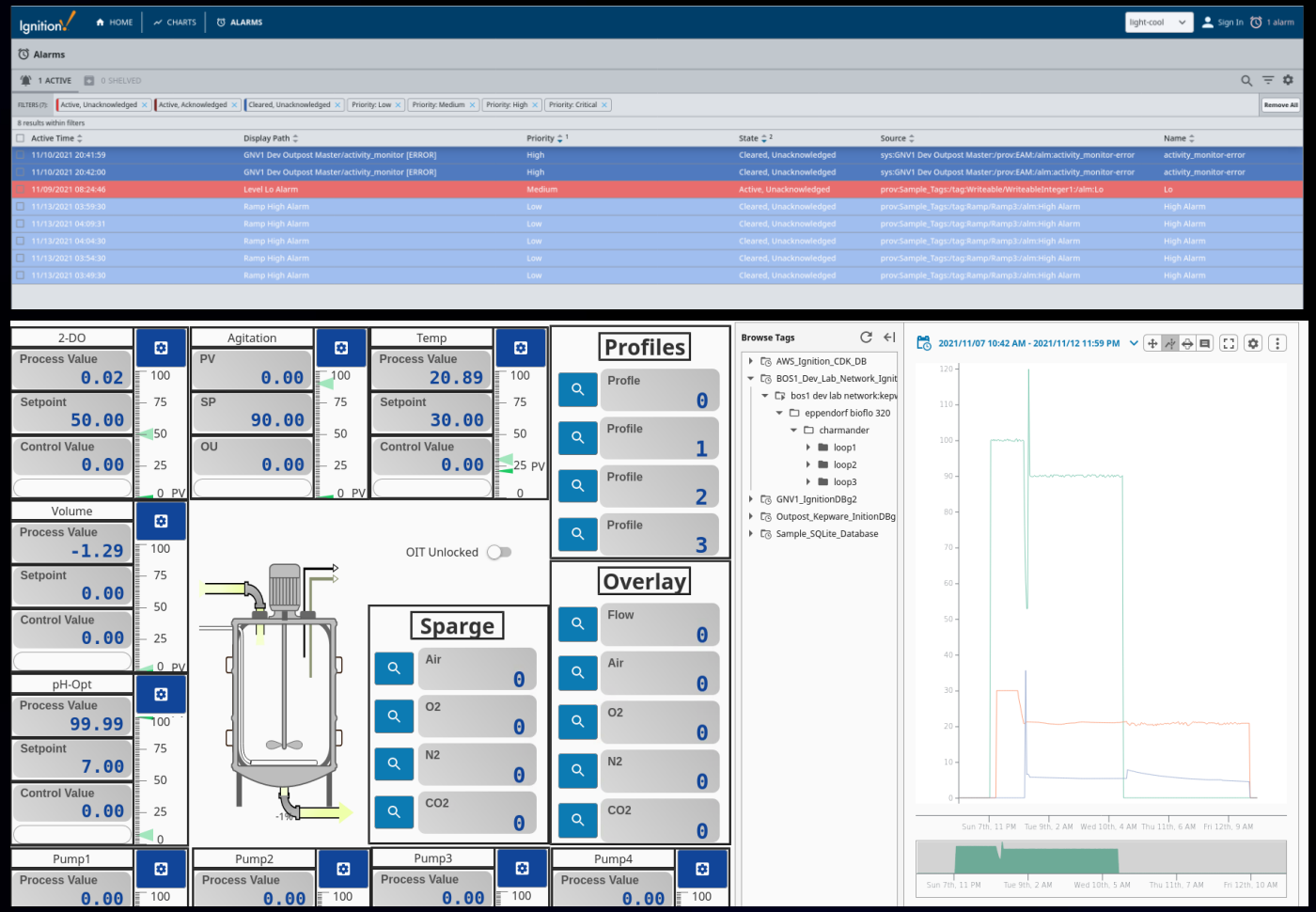
A digital interface to move from therapeutic concept to physical creation and patient delivery



Site infrastructure

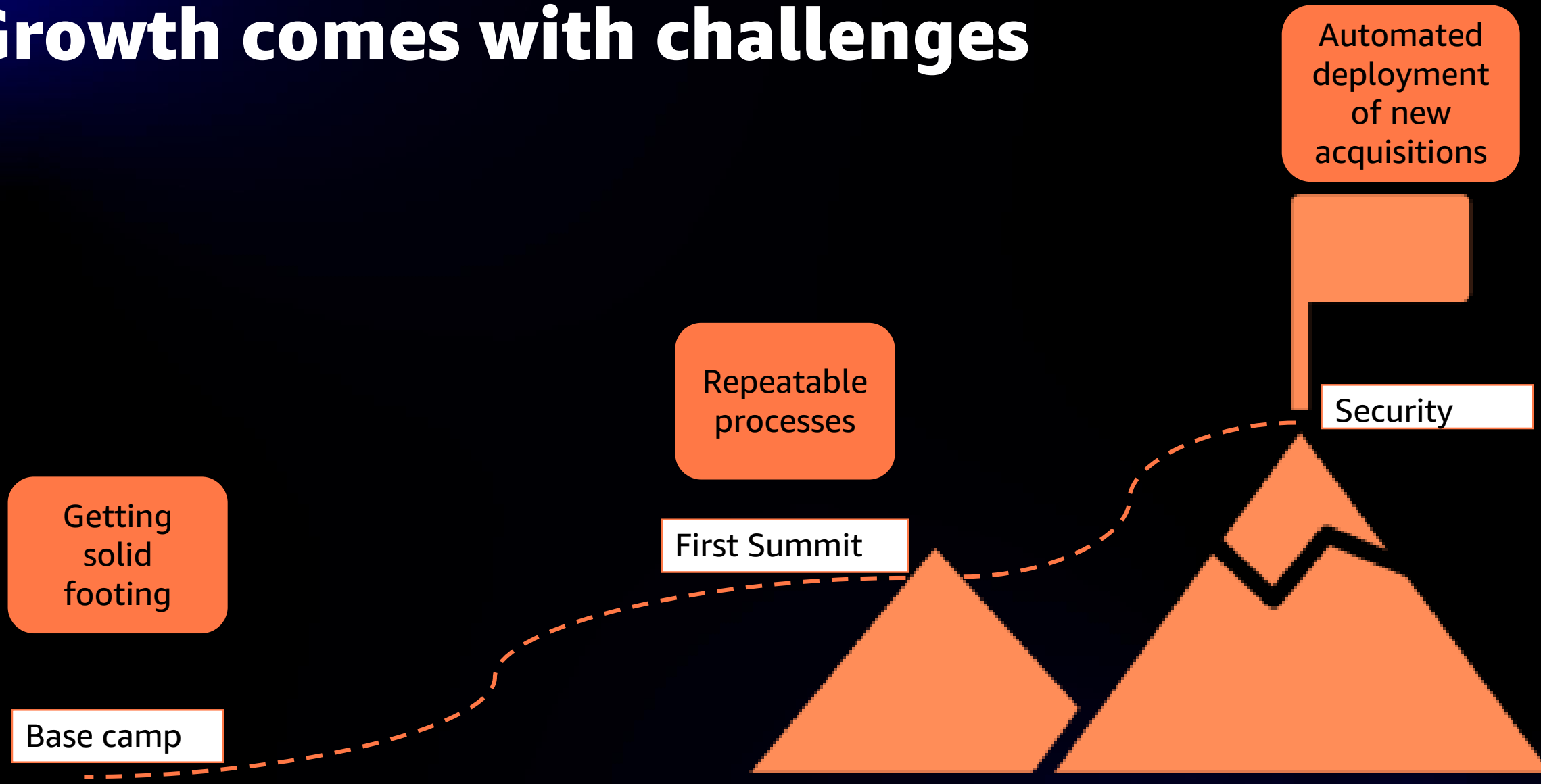
One backplane, unlimited environments for low-latency OT data acquisition, alarming, control





© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Growth comes with challenges



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

About the fundamentals

Fundamentals

- Security foundations
- Cloud native

Tools

- AWS Well-Architected Framework
- NIST Framework

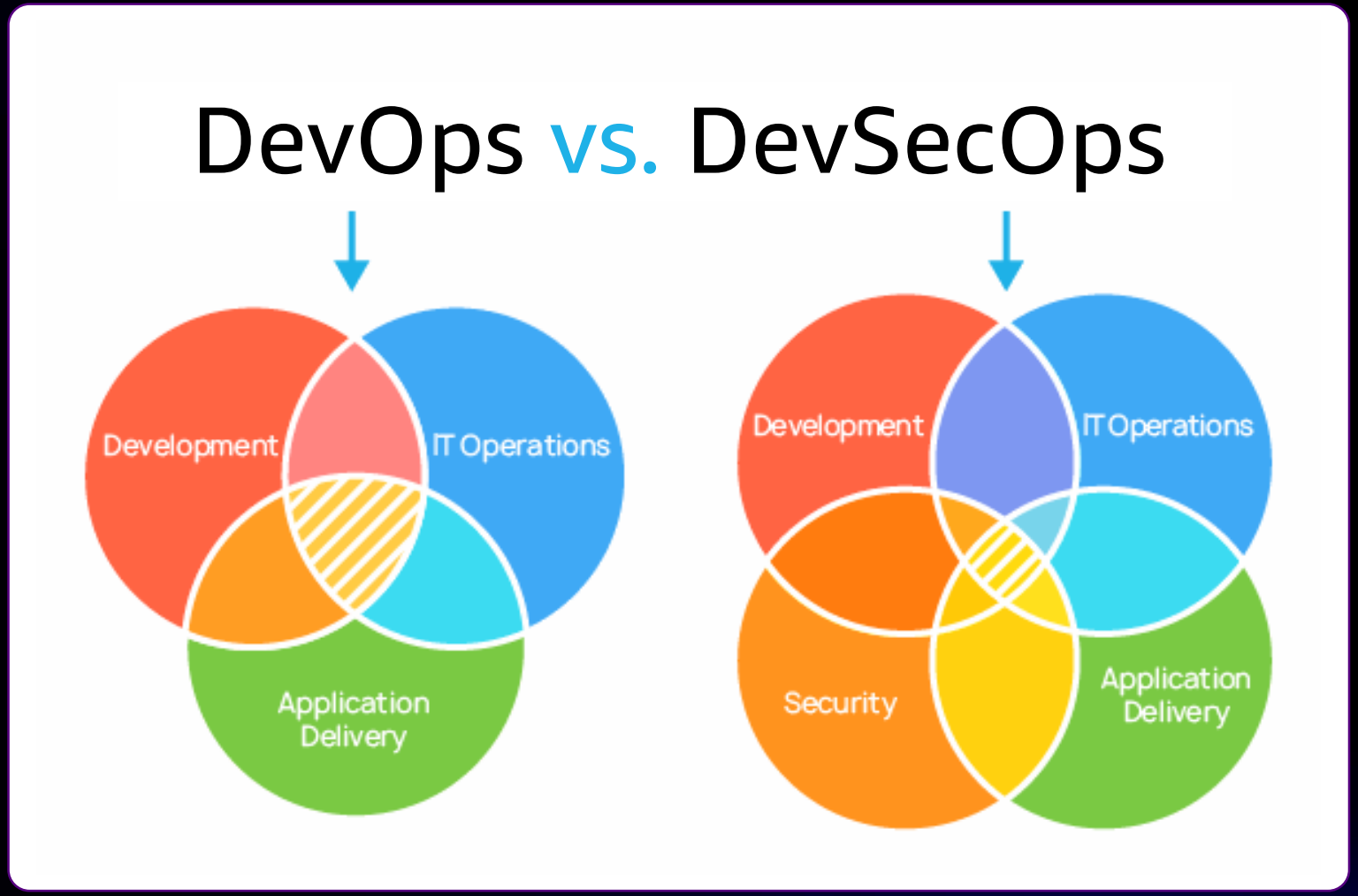
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is DevSecOps?

Evolution of DevOps: Security cannot be ignored or a bottleneck

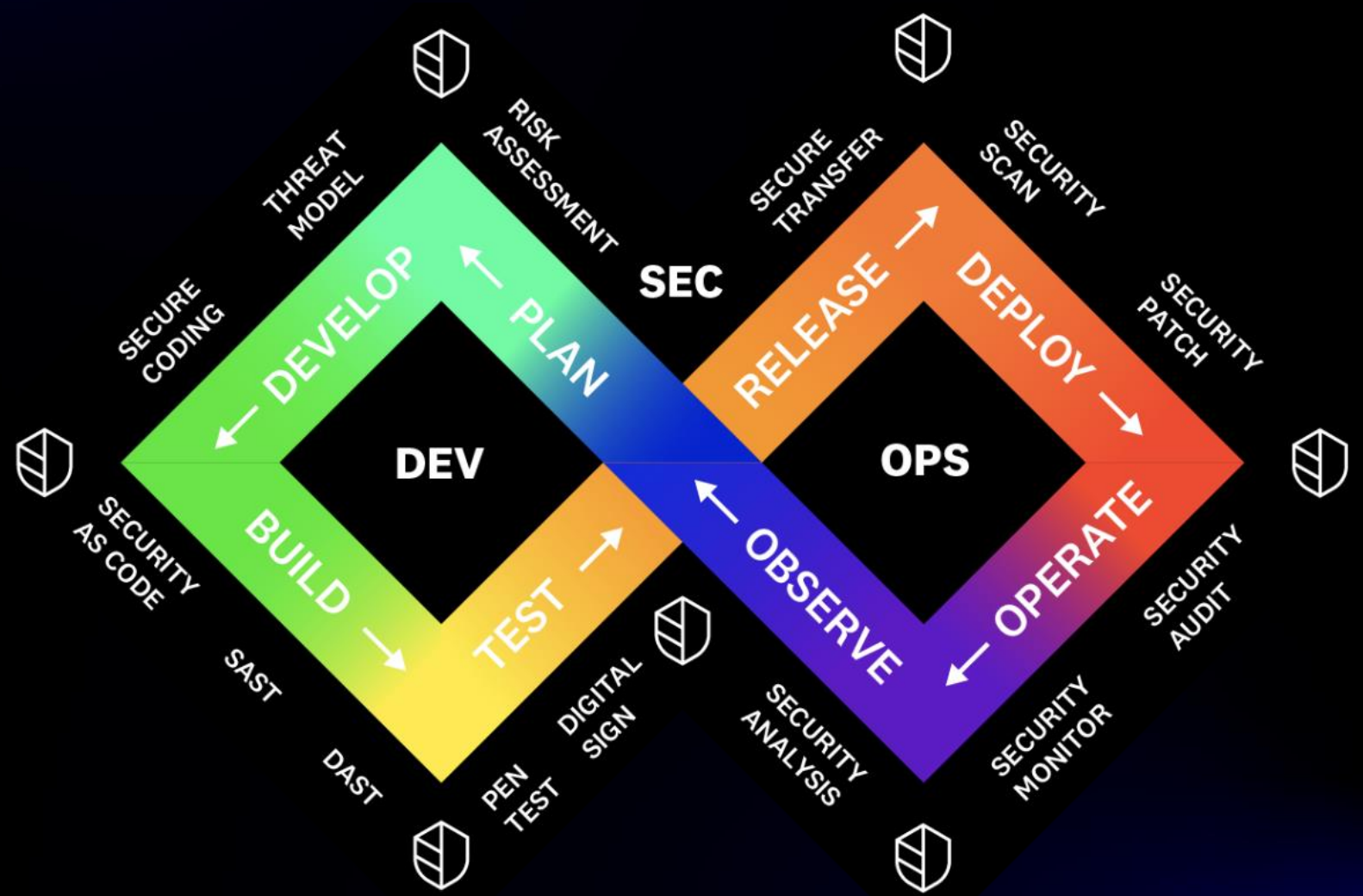
Shift left: infuse security across the SDLC

Emergence of DevSecOps



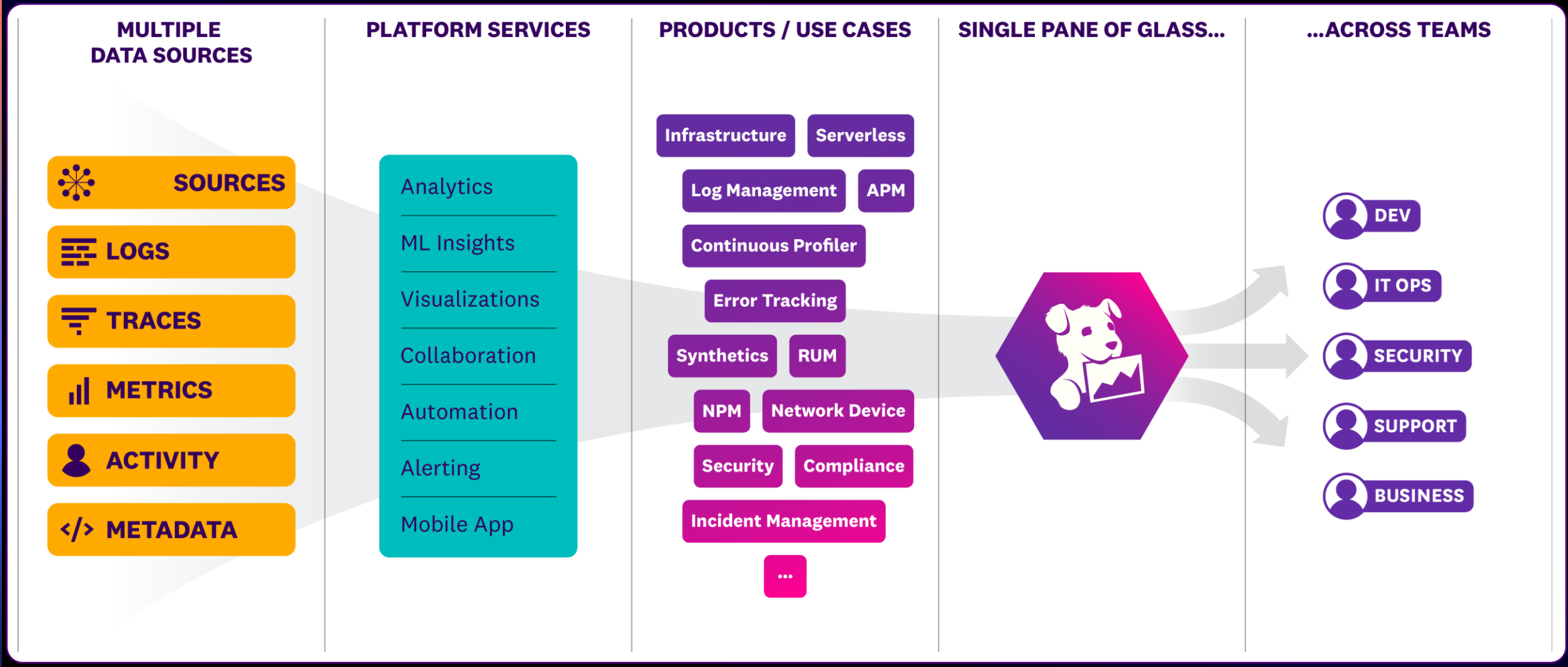
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The DevSecOps lifecycle



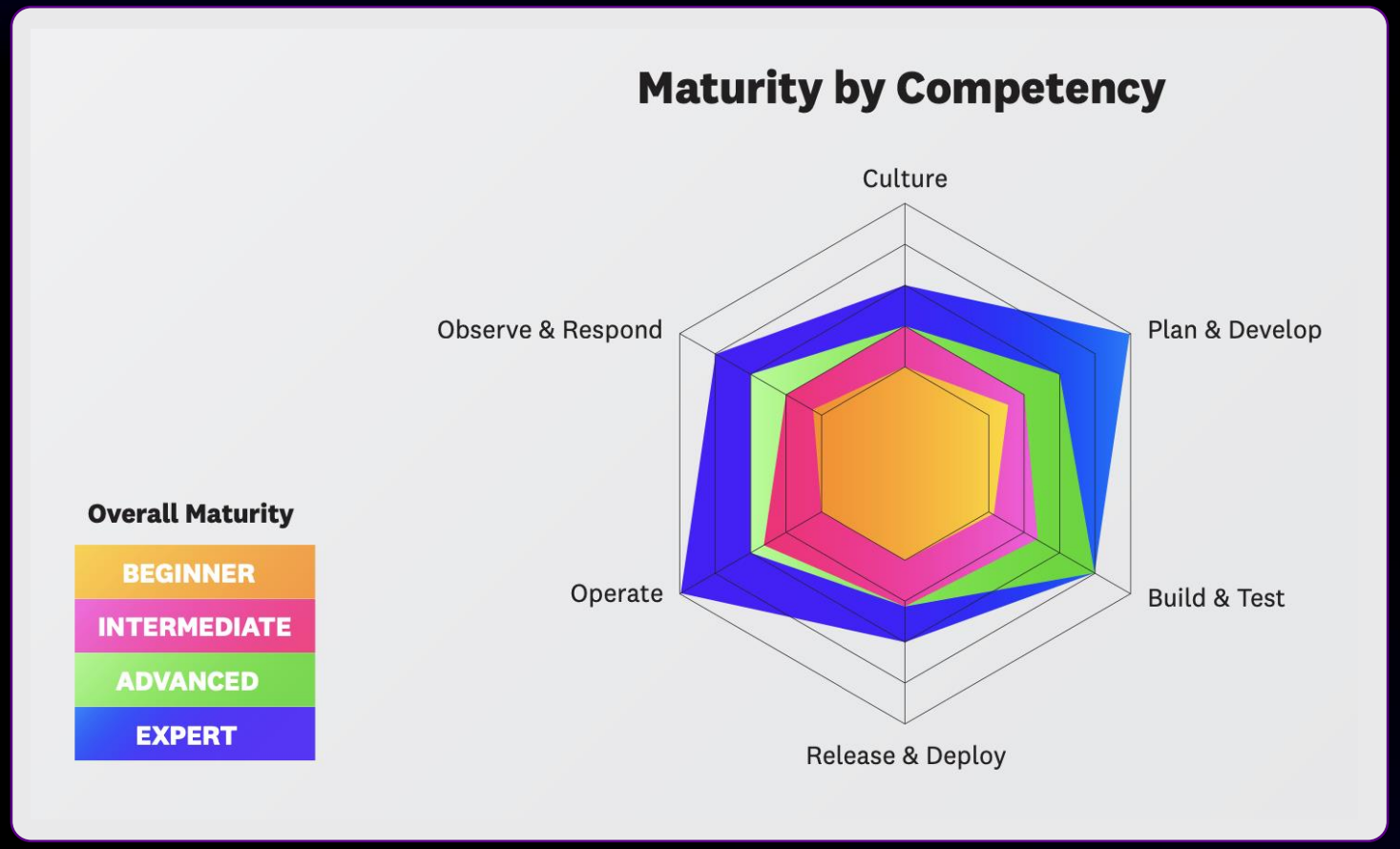
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Where does Datadog come into the story?



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Datadog's DevSecOps maturity model



People & Culture

Plan & Develop

Build & Test

Release & Deploy

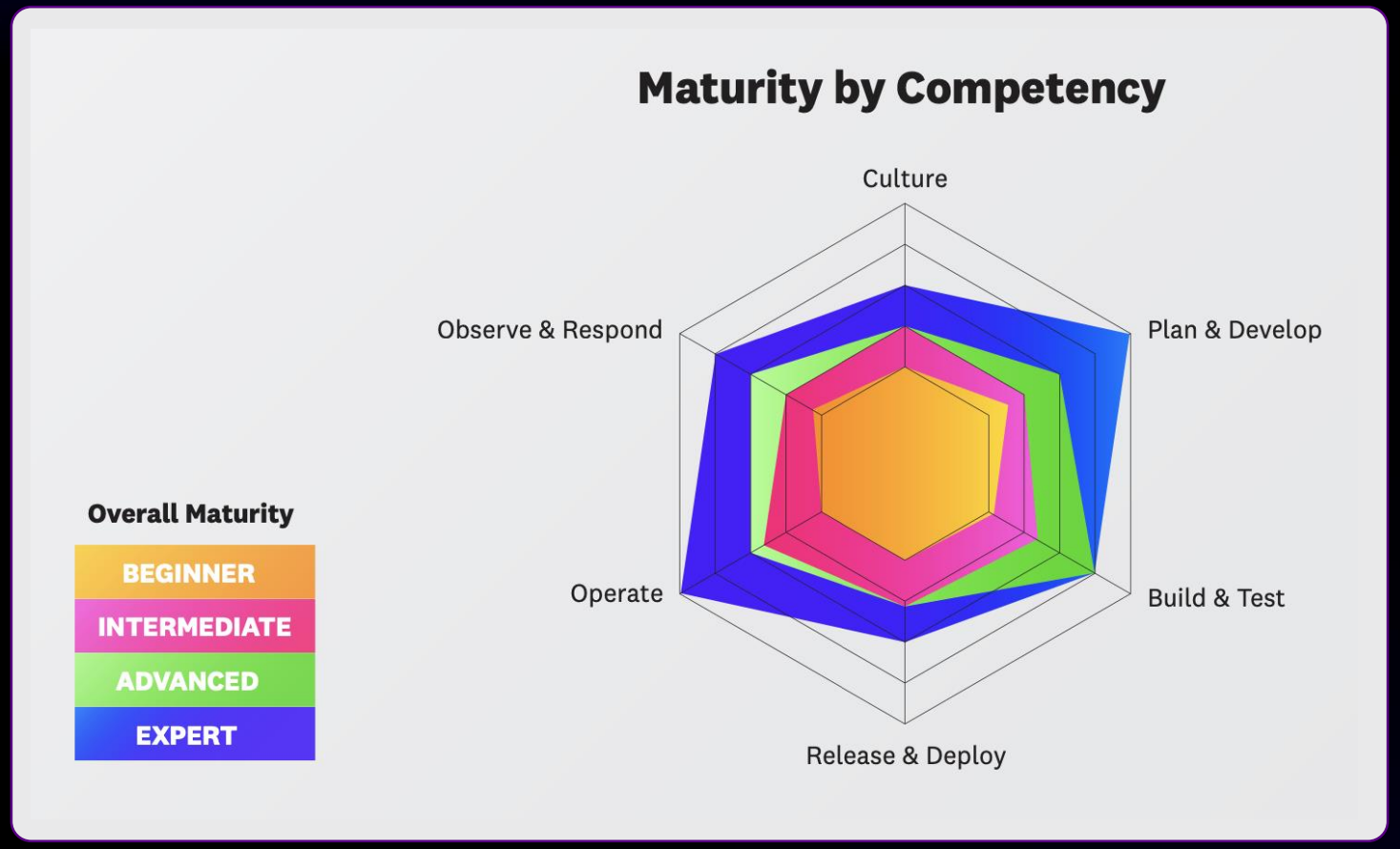
Operate

Observe & Respond

Source: "DevSecOps Maturity Model," **dtdg.co/devsecops-whitepaper**

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Today's focus



Source: "DevSecOps Maturity Model," **dtdg.co/devsecops-whitepaper**

Observe & Respond

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Applying these ideas to “ludicrous growth”

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Observability on entry





Identify

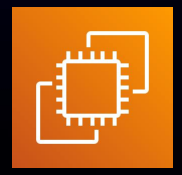
- Install simple hardware modules
- Create a simple CMDB
- Evaluate the current environment

Protect

- Automate deployments
- Evaluate infrastructure
- Segment!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Multiple paths to instrumentation and protection



Amazon Elastic Compute Cloud (Amazon EC2)

Deploy using AWS CloudFormation

Include in the AMI

Use AWS Systems Manager Agent (SSM Agent)

bit.ly/3jCgcr2



AWS Fargate

Datadog sidecar pattern

Simple instrumentation per task

Logs ship through FireLens for Amazon ECS

bit.ly/316wdPx



AWS Lambda

Serverless functions instrumented

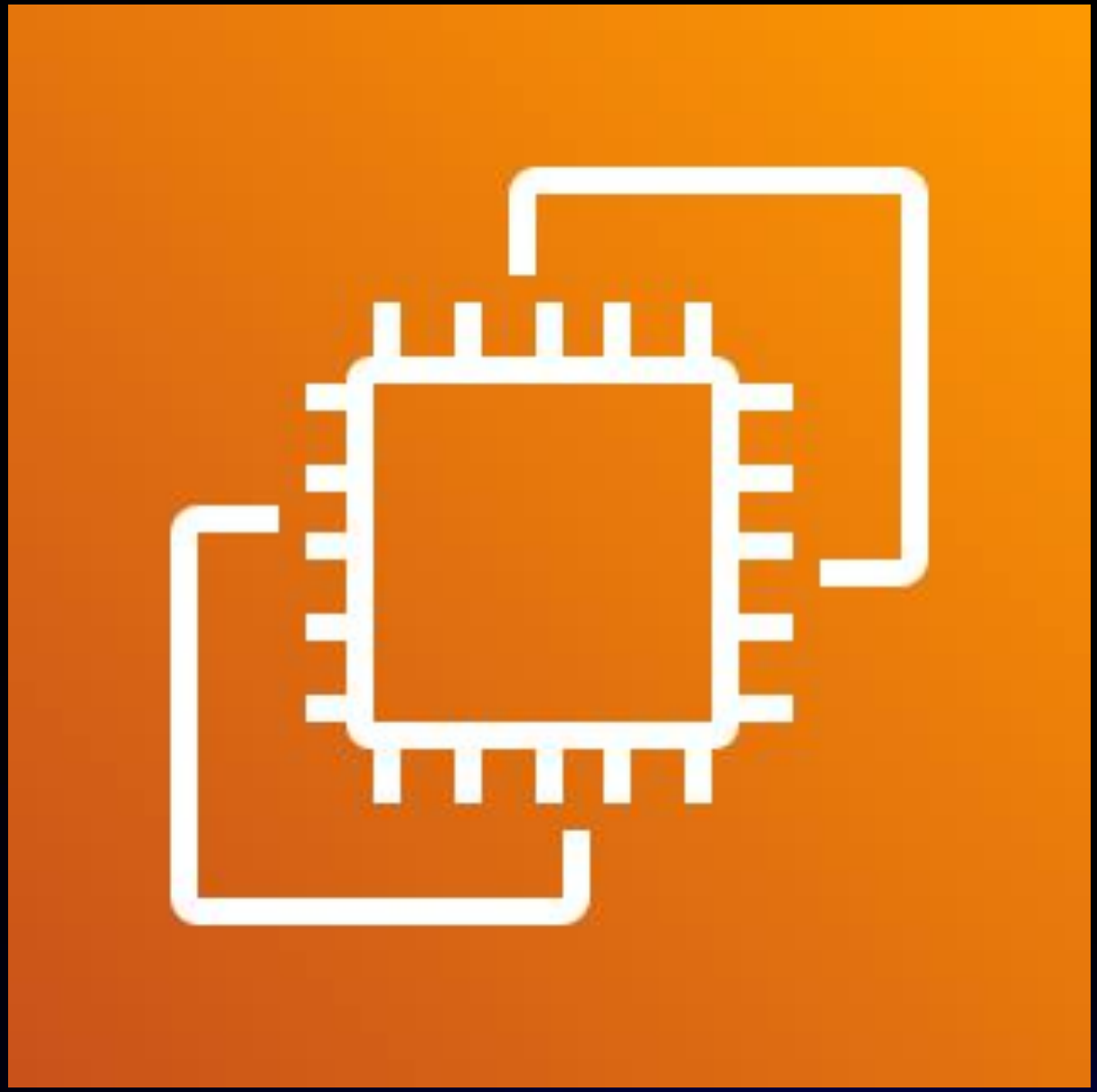
Logs ingested via Amazon CloudWatch

bit.ly/3bga1nH

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why SSM Agent for deploying monitoring?

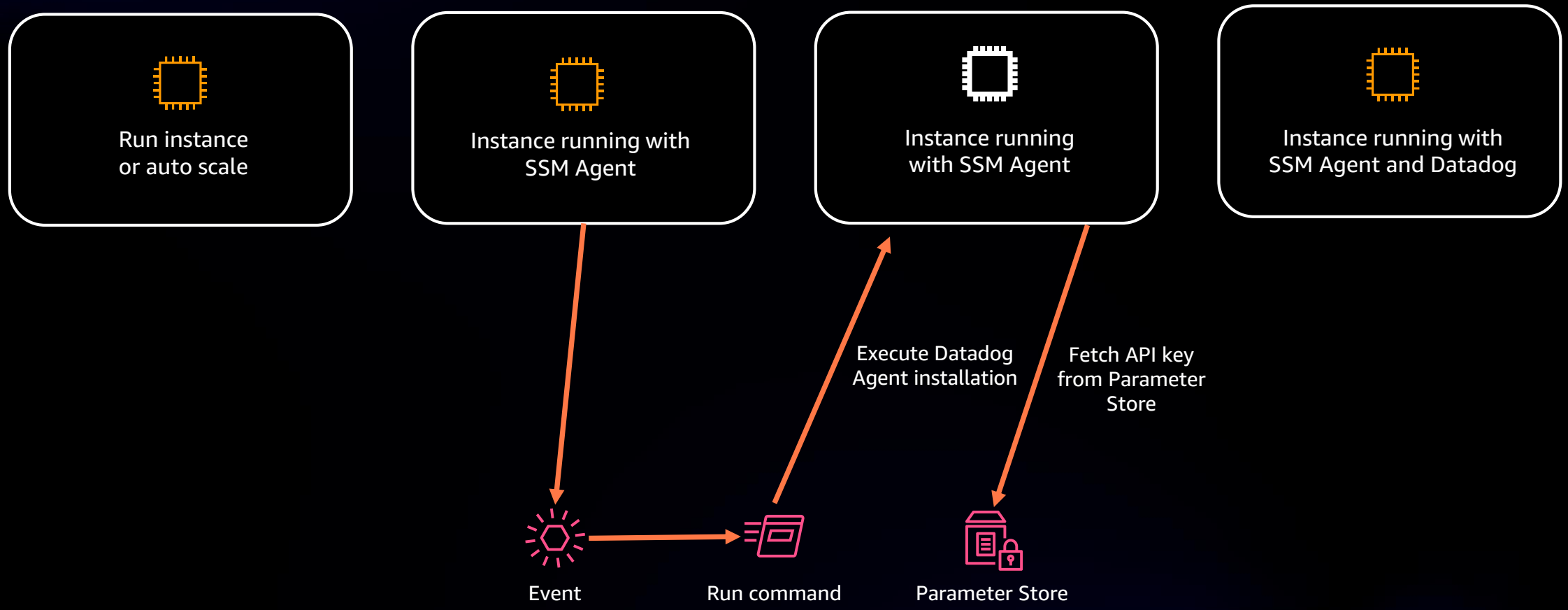
- SSM Agent is available by default in a host of images
- Other products from the AWS Systems Manager family can be used, like Parameter Store, to safeguard things like API keys
- Scales well to thousands of instances firing on demand
- Easy to report on installation compliance over time



aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Deploying Datadog Agent with SSM Agent



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

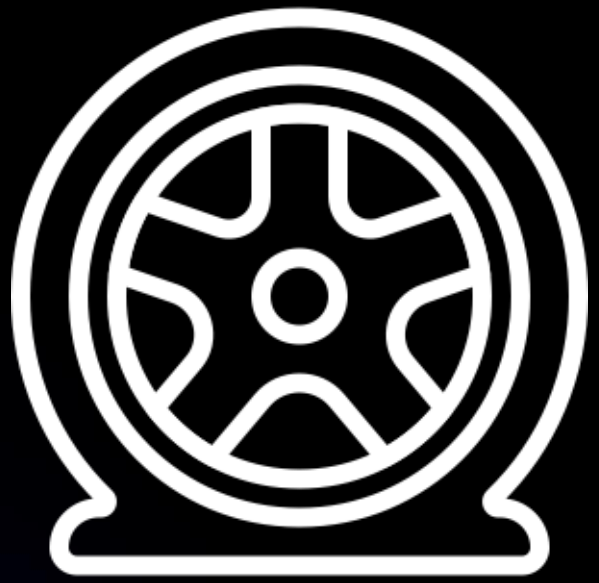
SSM Agent document

```
mainSteps:
- precondition:
    StringEquals:
    - "platformType"
    - "Linux"
  action: "aws:runShellScript"
  name: "runShellScript"
  inputs:
    runCommand:
      - sudo pip install awscli --upgrade
      - DD_AGENT_MAJOR_VERSION=7 \
        DD_API_KEY=$(aws ssm get-parameters --names dd_api_key --with-decryption --region us-west-2 --
        output text | awk '{ print $7 }') \
        DD_SITE="datadoghq.com" \
        bash -c "$(curl -L https://s3.amazonaws.com/dd-agent/scripts/install_script.sh)"
    workingDirectory: "{{ workingDirectory }}"
    timeoutSeconds: "{{ executionTimeout }}"
```

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

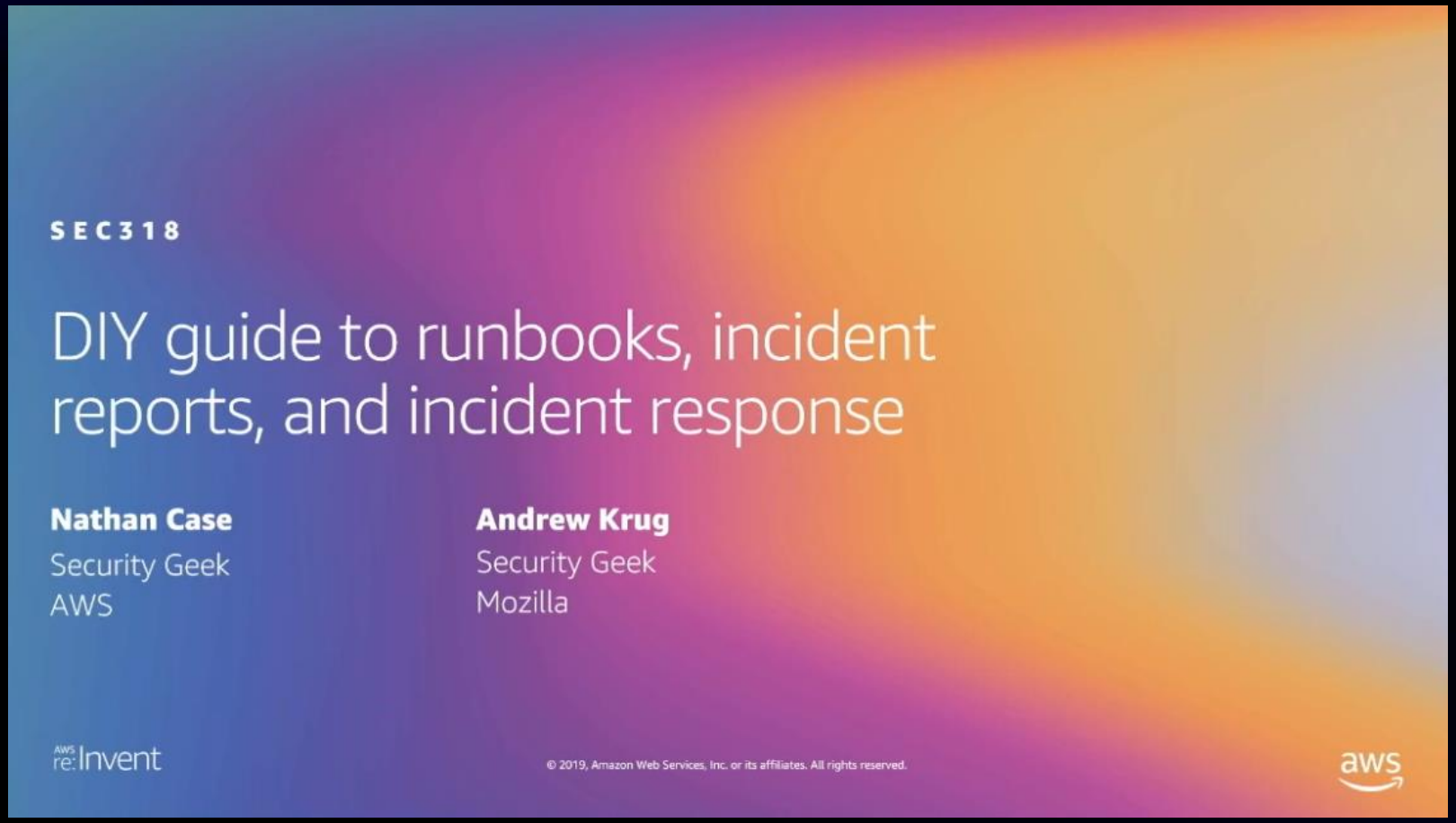
Planning for things to go bad . . .

Preparing for an incident



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

For more information on that . . .



youtube.com/watch?v=E1NaYN_fJUo

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Runbooks and playbooks review

1. Assume the worst **will** happen
2. Start small and iterate
   - First, create docs with instructions
   - Next, write scripts
   - Finally, create automations
3. Runbooks for your engineers and playbooks for leadership

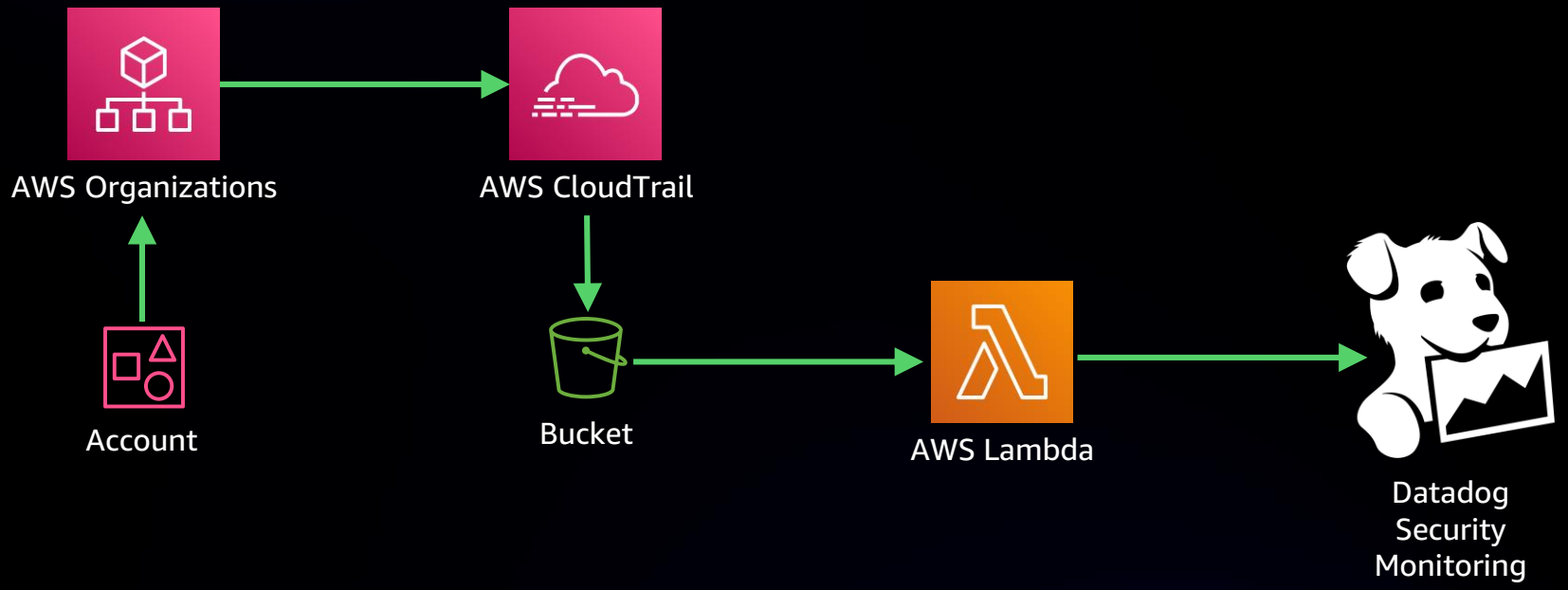


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Detecting incidents

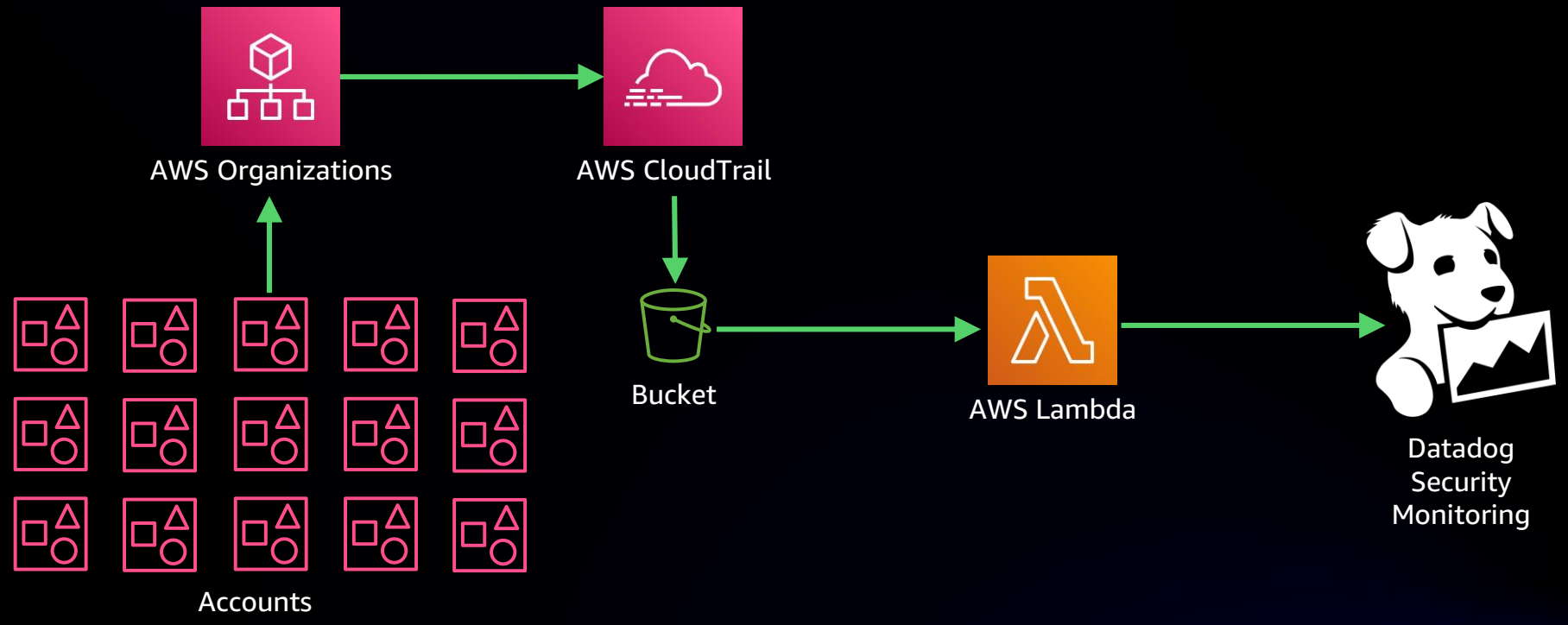
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Detecting using Datadog and control plane



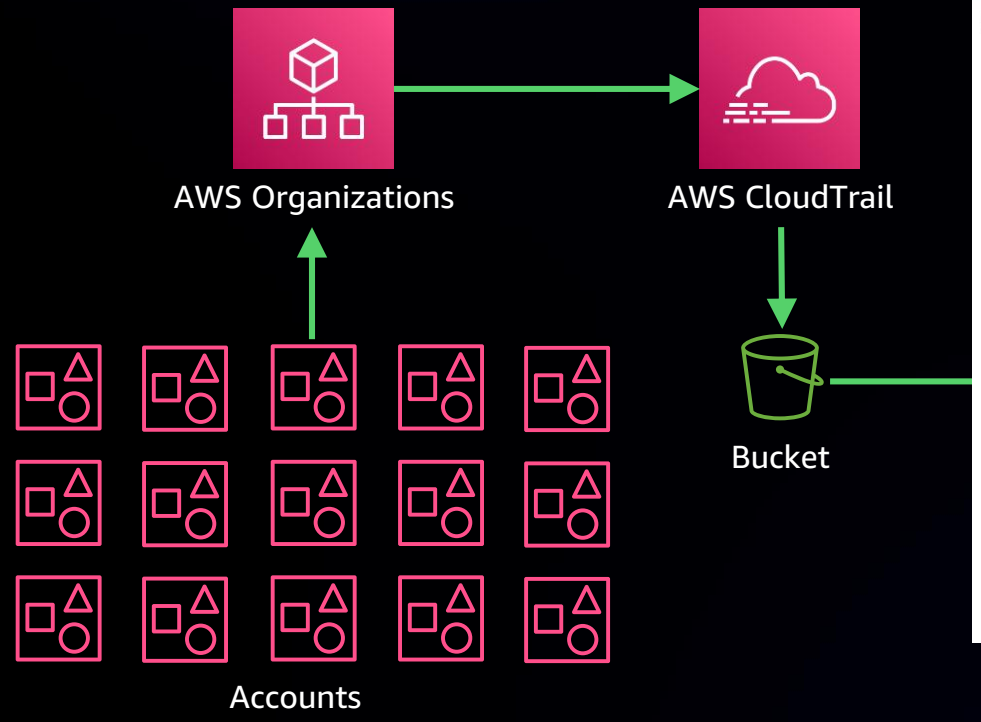
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

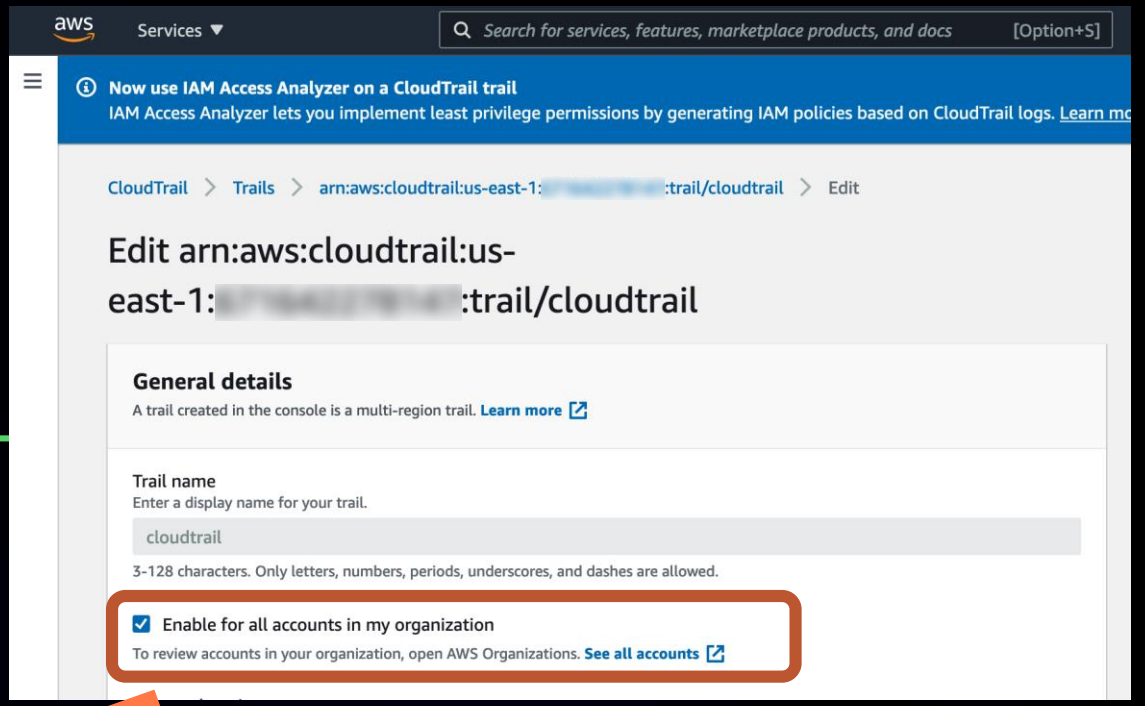
Scales automatically with growth



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Automatically enforced logging



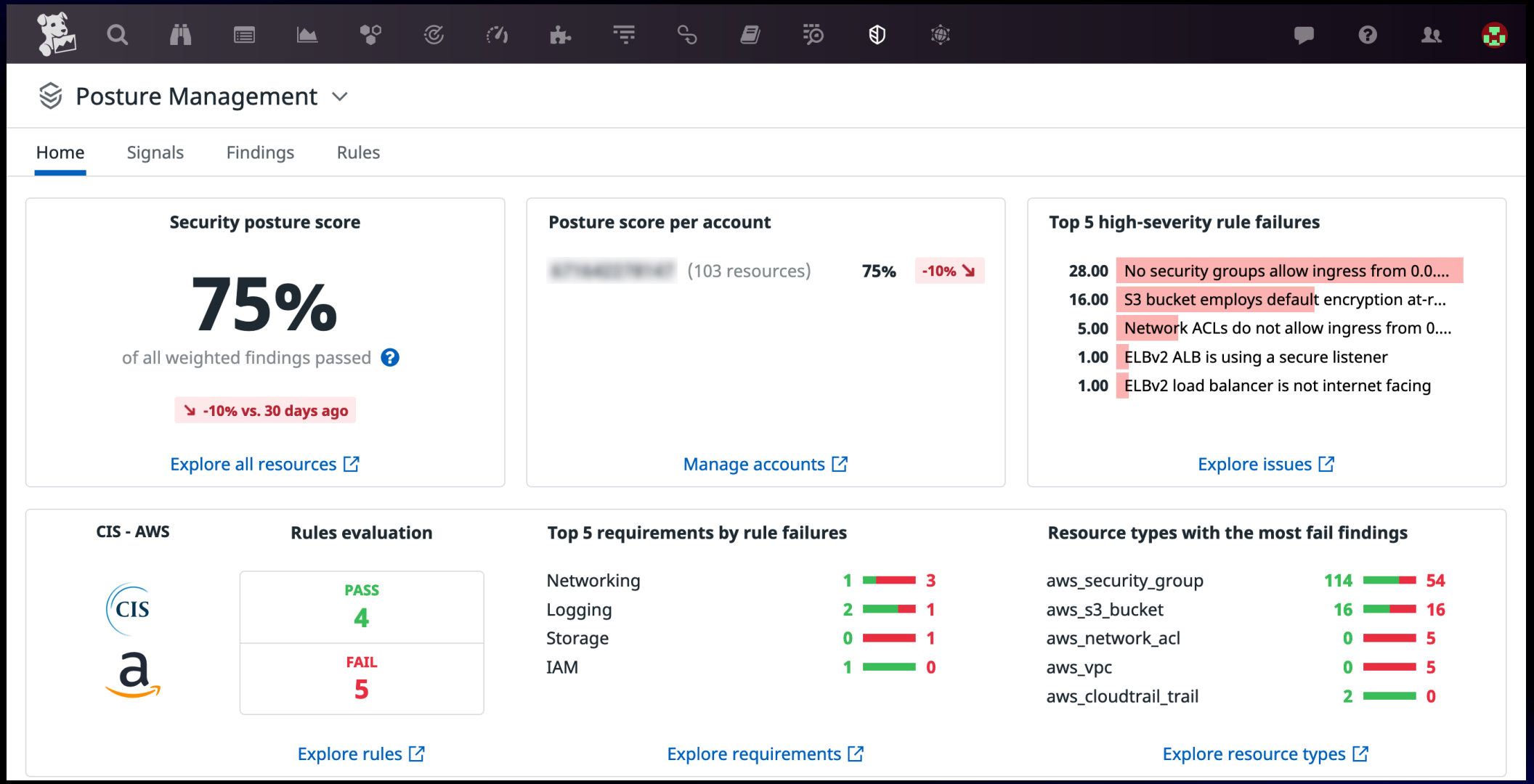


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Adding more context

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

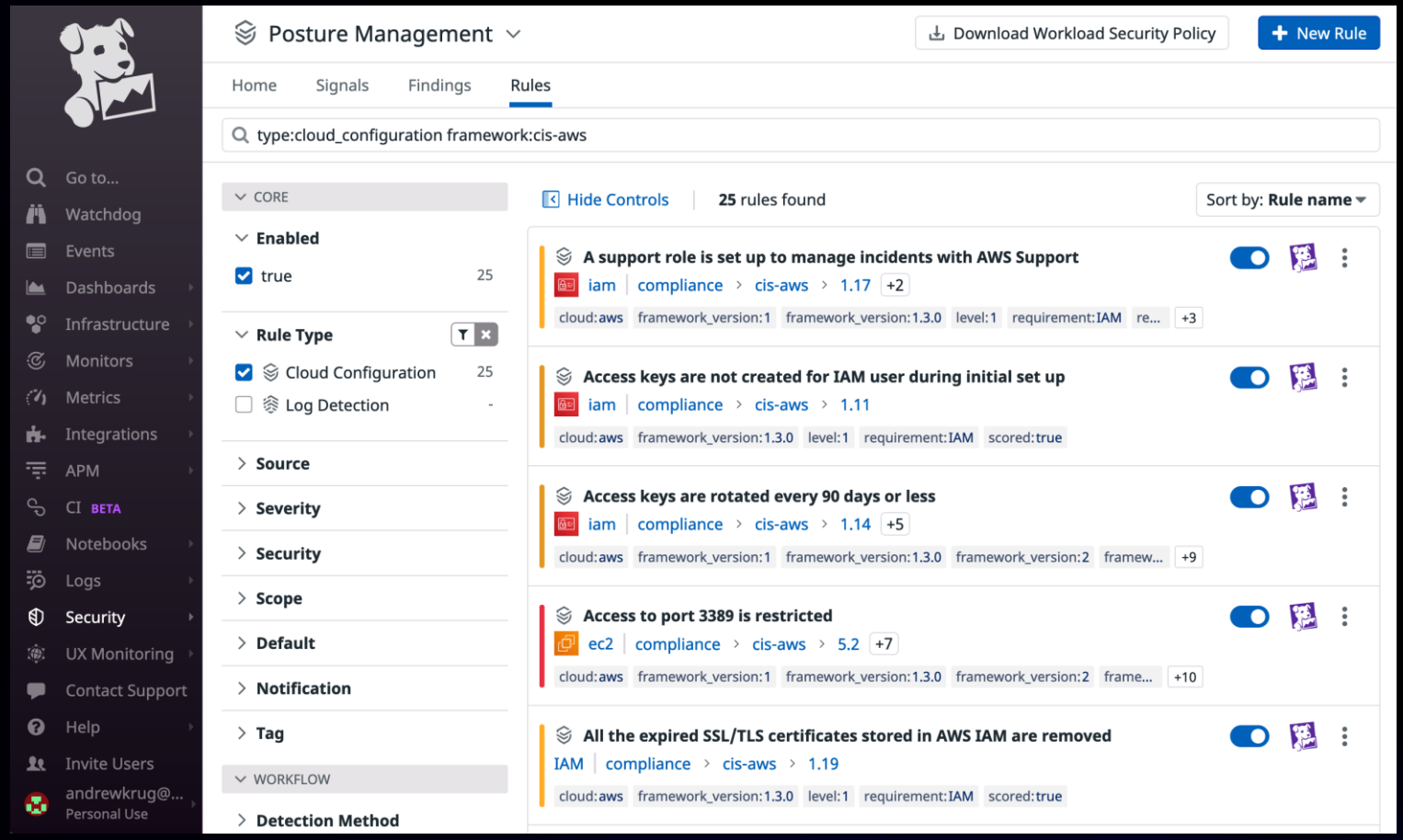
See more with continuous auditing



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cloud security posture management

- Speedy analytics to give you health metrics
- Continuously scans for misconfigurations or mistakes
- Supports a variety of checks for the AWS Cloud

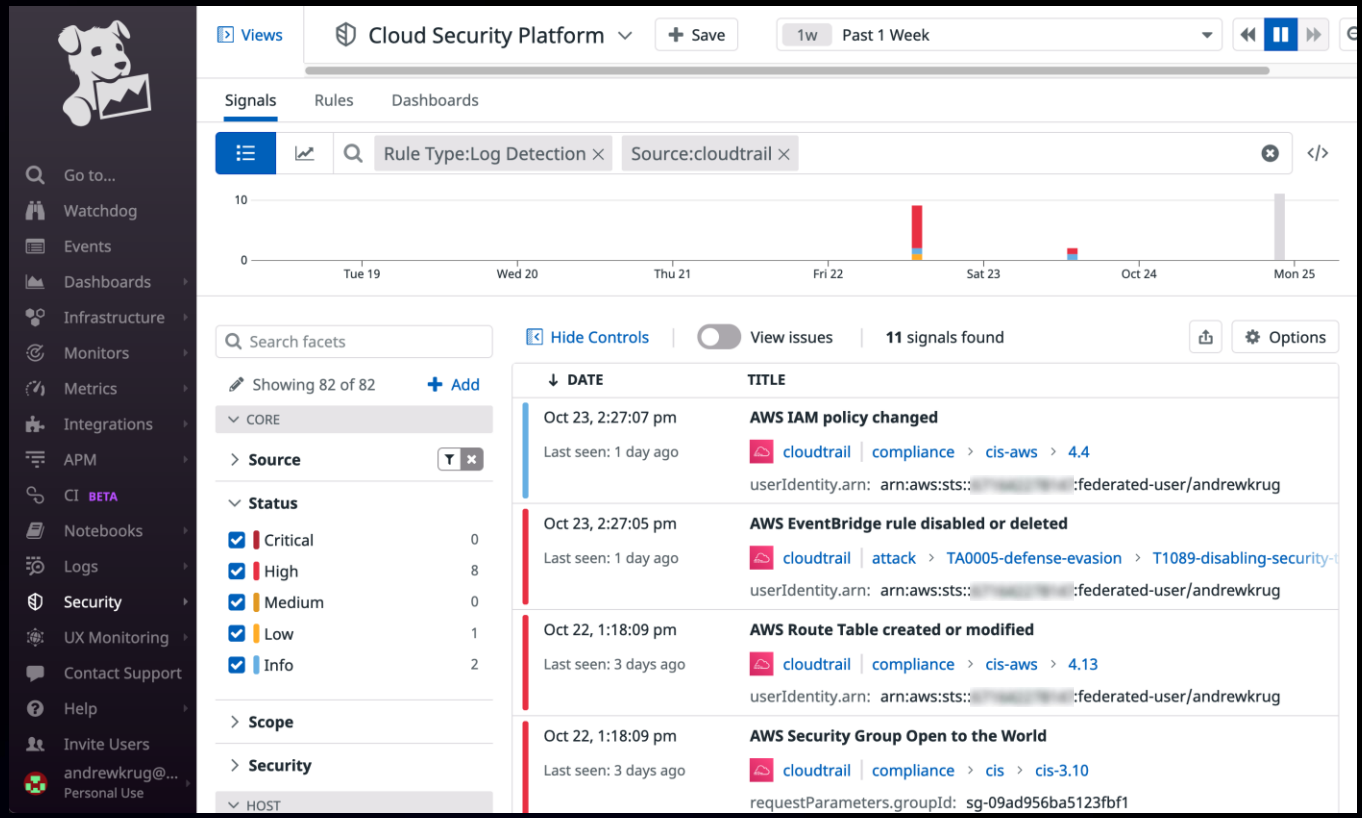


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Log-based alerting

- Supports detection using CloudTrail logs
- CloudTrail is highly rich

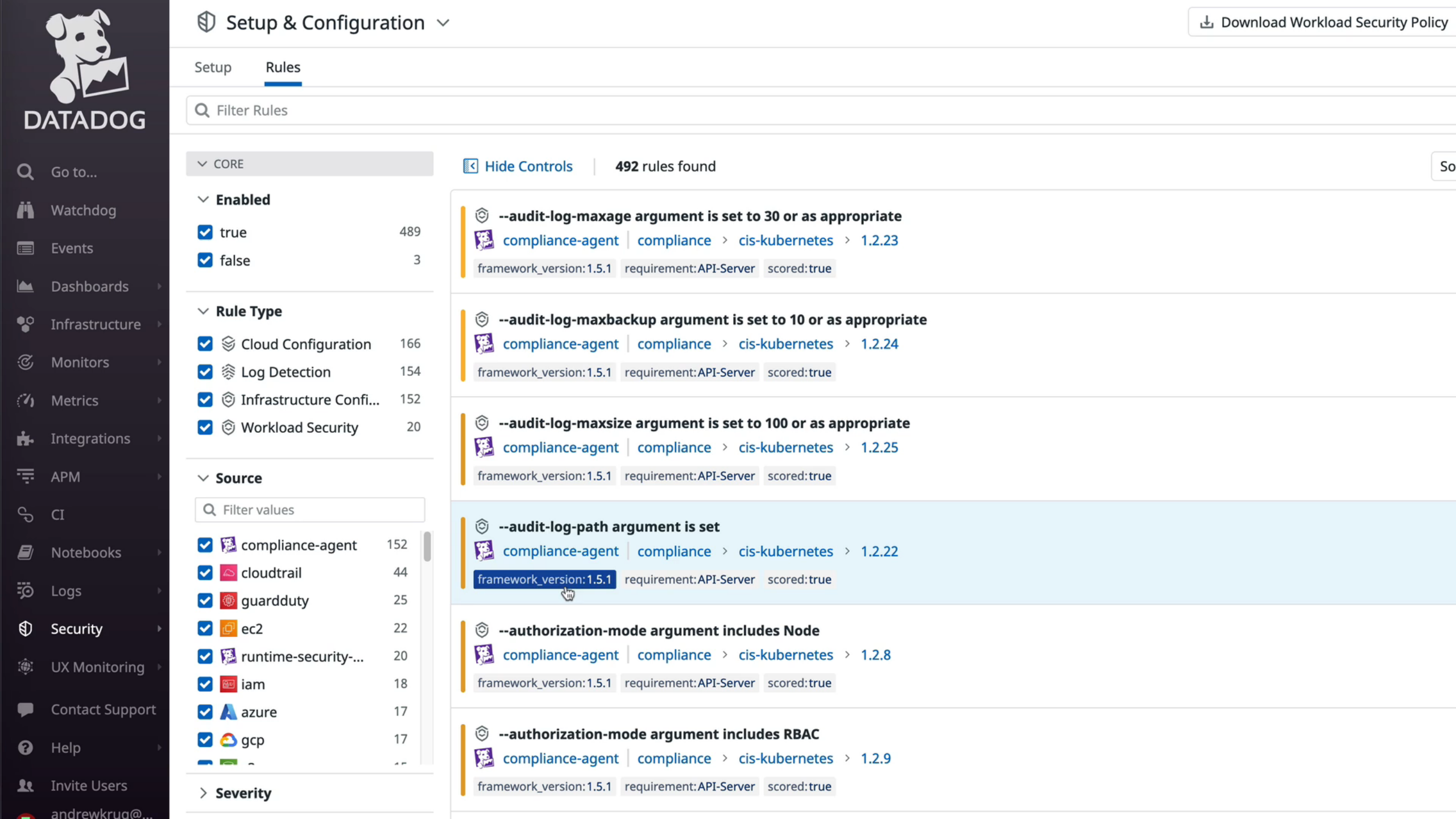
Sometimes you need more context than what is in the default JSON structure



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Inspirational Demo 2: Adding more context to alerts

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.


DATADOG
Go to...
Watchdog
Events
Dashboards
Infrastructure
Monitors
Metrics
Integrations
APM
CI
Notebooks
Logs
Security
UX Monitoring
Contact Support
Help
Invite Users
Setup & Configuration
Download Workload Security Policy
Setup
Rules
Filter Rules
CORE
Hide Controls
492 rules found
Enabled
true 489
false 3
Rule Type
Cloud Configuration 166
Log Detection 154
Infrastructure Confi... 152
Workload Security 20
Source
Filter values
compliance-agent 152
cloudtrail 44
guardduty 25
ec2 22
runtime-security-... 20
iam 18
azure 17
gcp 17
Severity
--audit-log-maxage argument is set to 30 or as appropriate
compliance-agent | compliance › cis-kubernetes › 1.2.23
framework_version:1.5.1 requirement:API-Server scored:true
--audit-log-maxbackup argument is set to 10 or as appropriate
compliance-agent | compliance › cis-kubernetes › 1.2.24
framework_version:1.5.1 requirement:API-Server scored:true
--audit-log-maxsize argument is set to 100 or as appropriate
compliance-agent | compliance › cis-kubernetes › 1.2.25
framework_version:1.5.1 requirement:API-Server scored:true
--audit-log-path argument is set
compliance-agent | compliance › cis-kubernetes › 1.2.22
framework_version:1.5.1 requirement:API-Server scored:true
--authorization-mode argument includes Node
compliance-agent | compliance › cis-kubernetes › 1.2.8
framework_version:1.5.1 requirement:API-Server scored:true
--authorization-mode argument includes RBAC
compliance-agent | compliance › cis-kubernetes › 1.2.9
framework_version:1.5.1 requirement:API-Server scored:true

How these things and more help Resilience grow

- Governance is key
- Planning beats rework every day of the week
- Adding developers to your budget is worthwhile if you are a security leader
- Building recipes instead of doing similar things repeatedly

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.