Spelunking The Data

splunk> turn data into doing®

Agenda

- Introduction
- AWS Use Cases
- FSI Customers Use Cases

Welcome!

Meet your Splunker

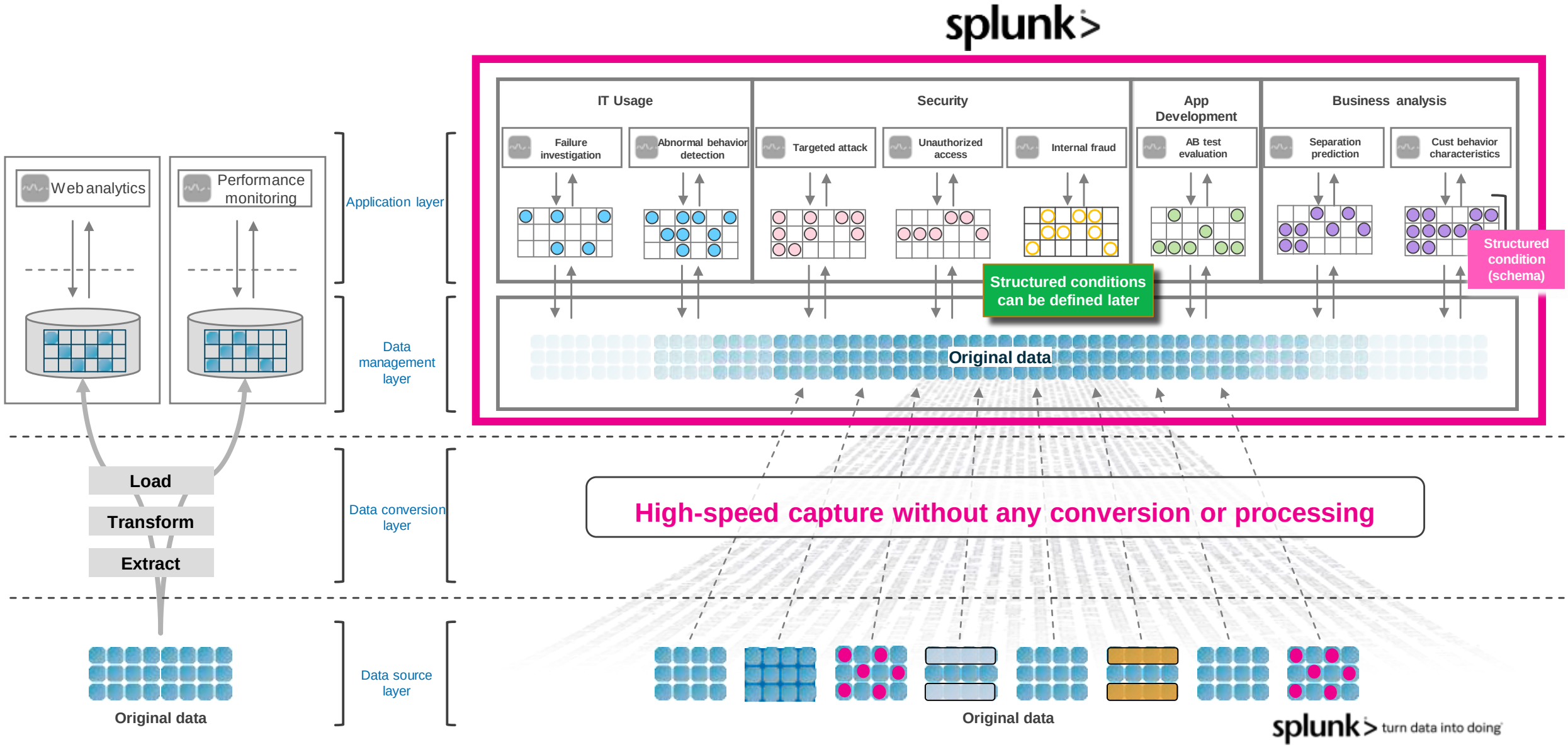
Herrick LAI

Senior Sales Engineer, Splunk HK

Introduction

splunk> turn data into doing®

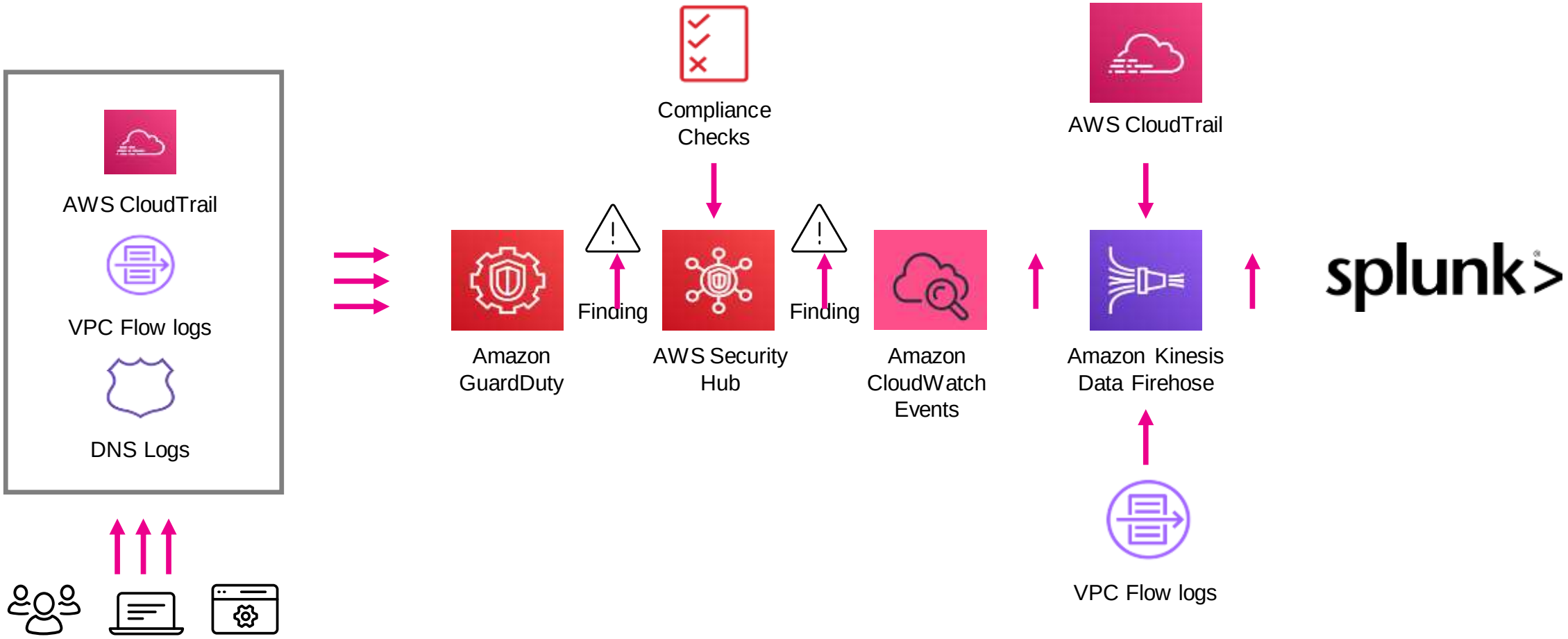
Utilize of the data



AWS Use Cases

splunk> turn data into doing®

AWS Data Flow for Use Cases



Use Case 1: Detecting ransomware activities within AWS environments

AWS Data Source: CloudTrail, CloudWatch

Cloud ransomware can be deployed when attackers obtain high-privileged credentials from targeted users or resources. The use case help to detect when users in your AWS environment are performing activities that are commonly associated with ransomware attacks, namely through the creation of KMS keys and encryption activities

- **AWS users creating KMS keys where kms:Encrypt is publicly accessible**
  - detection of newly created Key Management Service (KMS) keys or
  - keys that have been assigned a policy for access, where the action kms:Encrypt is accessible for everyone

- **AWS users with KMS keys performing encryption in S3 buckets**
  - detection of users with KMS keys performing encryption specifically against S3 buckets

Use Case 2: Detecting suspicious new instances in your AWS EC2 environment

AWS Data Source: CloudTrail

You are an Amazon Web Services (AWS) admin who manages AWS resources and services across your organization. You are aware that cryptomining or cryptojacking on your environment is a potential problem you need to be aware of

- **Abnormally high AWS instances launched by user**
  - looks for CloudTrail events where a user successfully launches an abnormally high number of instances
- **EC2 instance started in previously unseen region**
  - looks for CloudTrail events where an instance is started in a particular region in the last one hour and then compares it to a lookup file of previously seen regions where an instance was started
- **EC2 instance started with previously unseen AMI**
  - looks for EC2 instances being created with previously unseen AMIs

Use Case 3: Detecting Kubernetes unusual activities

AWS Data Source: CloudTrail, CloudWatch

Kubernetes implementations vary widely. Amazon Elastic Kubernetes Service (**Amazon EKS**) is a managed container service to run and scale Kubernetes applications in the cloud or on-premises

- **EKS Pod scan detection**
  - detects information on unauthenticated requests against Kubernetes' Pods API
- **EKS cluster scan detection**
  - provides information of unauthenticated requests via user agent, and authentication data against Kubernetes cluster in AWS
- **Kubernetes AWS detect suspicious kubectl calls**
  - provides information on anonymous kubectl calls with IP, verb namespace and object access context

The Security Data Journey

Splunk can meet you wherever you are

Stage 1

Security Logging & Investigation

Splunk Enterprise / Splunk Cloud

Stage 2

Continuous Monitoring

Mission Control, SSE, Splunk Enterprise Security (ES)

Stage 3

Automation

Mission Control, SSE, ES, SOAR

Stage 4

Security Nerve Center

Mission Control, SSE, ES, SOAR, UBA

Cloud is a Critical Enabler of Transformation, but Increases Complexity

What's Different

VELOCITY

COMPLEXITY

1 LIFT & SHIFT

DEV ⟷ OPS

1x Release Per Year

CLIENT SERVER

DATABASE

JAVA APPLICATION SERVER

Primarily Cloud IaaS

VM VM VM VM VM VM

DC

Private

Public

2 RE-ARCHITECT

DEV OPS

10x Release Per Quarter

More Modular, but Dependent App Components

VM VM VM

Private

Public

3 CLOUD-NATIVE

DEV OPS

100x Release Per Month

Loosely Coupled Microservices, and Serverless Functions

Private

Public

"You Build It, You Run It"

Complex Dependencies

Dynamic, Short-lived Infrastructure

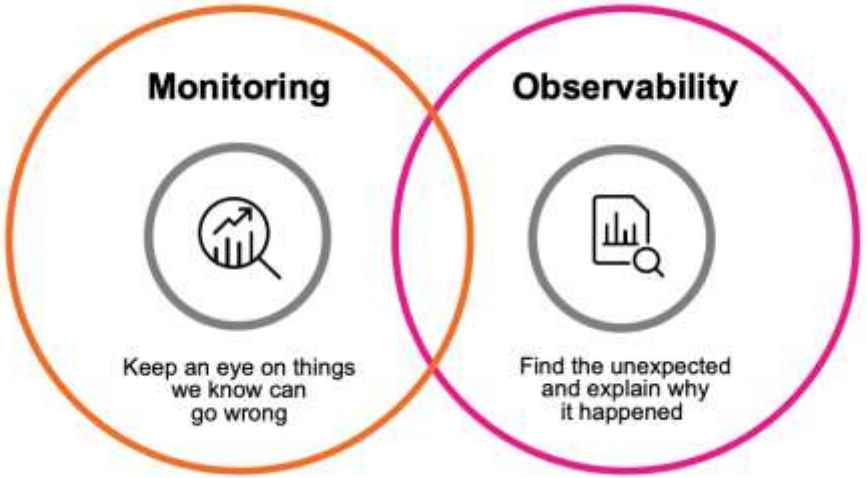
What difference btw Monitoring & Observability?

Is it just a fancy word for “Monitoring”?

Looking for expected problems, e.g.:

- Overloaded CPU
- High memory utilization
- Disk space
- High response latency
- High error rate
- Service availability

Alerting on issues that have occurred.



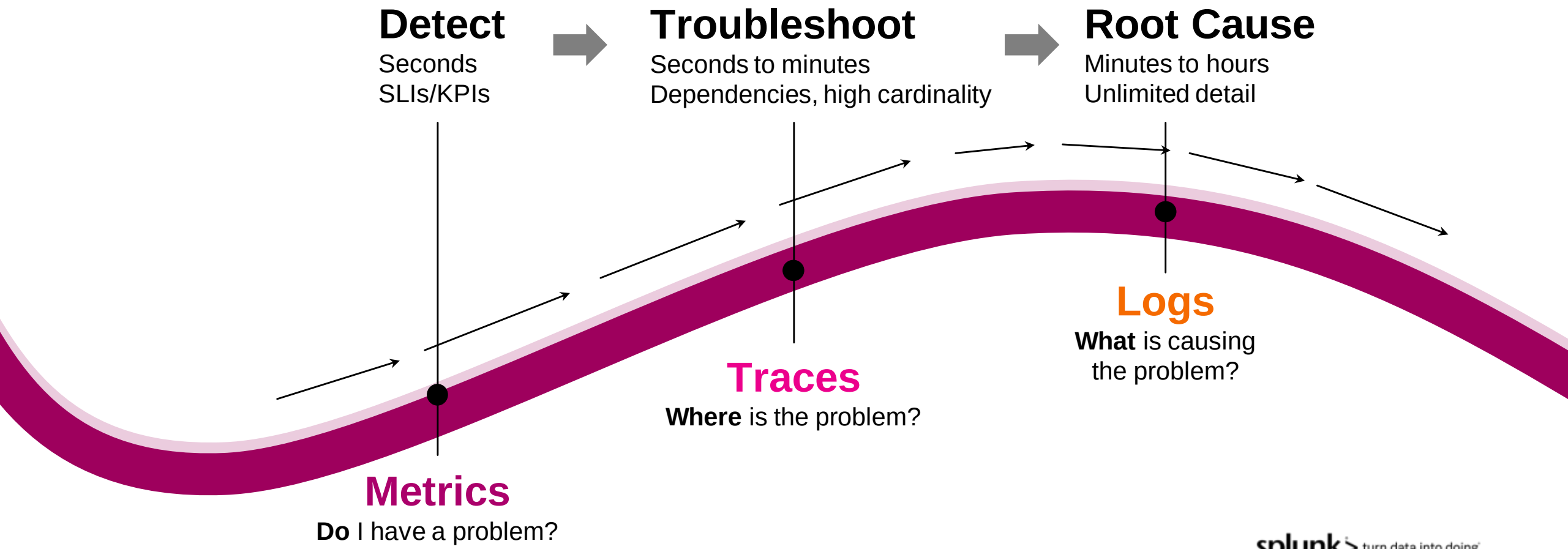
Looking for unknown unknowns, e.g.:

- Why are the alerts firing?
- What is in common between problem areas?
- Find the “needle in the haystack”
- Troubleshooting solution for complex systems

Diagnosing why issues have occurred.

“Three Pillars” of Observability

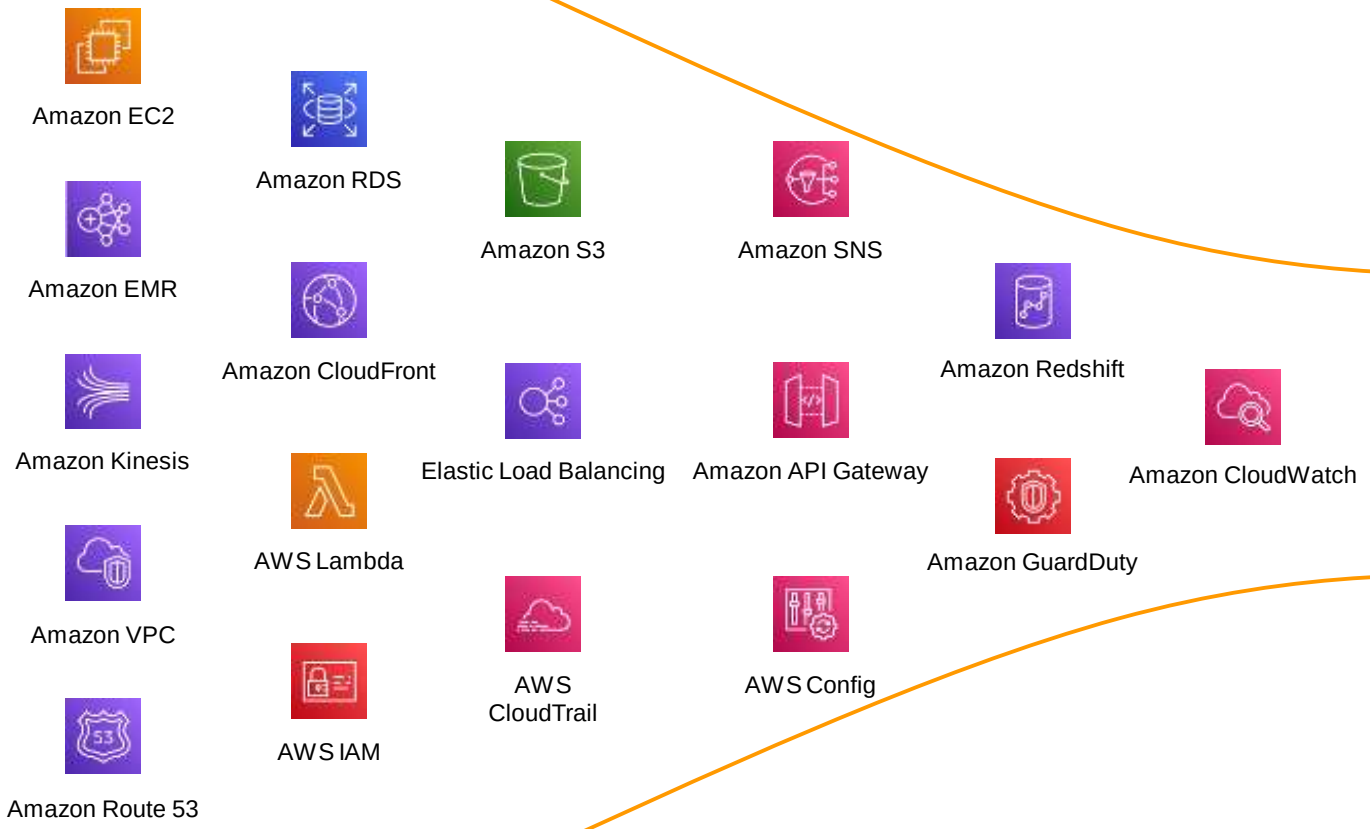
Metrics, Traces and Logs



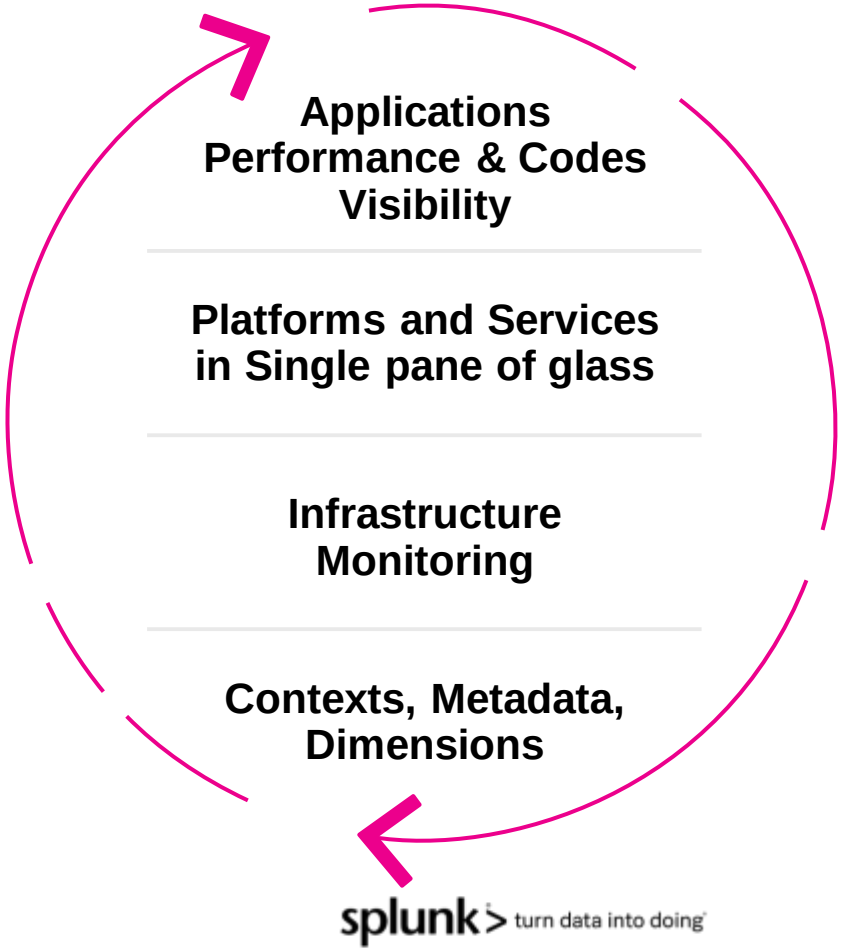
Full-Stack and End-to-end Visibility

Seamlessly integrated UX, context, and workflows

Example of AWS services



Splunk Observability Cloud



splunk> turn data into doing

Use Case 1: Monitoring AWS Lambda

AWS CloudWatch and Splunk OpenTelemetry Collector

Don't have access to underlying hosts, so you can't install agents to collect metrics and visibility into function performance so that you can make adjustments to your functions or resolve issues before customers are impacted

You want to be able to monitor these key Lambda metrics:

- Cold starts. The average latency, and total number of function cold starts
- Errors. The number of invocations that failed due to errors associated with the function
- Invocations. The number of times a function is invoked in response to an event or invocation API call This includes successful and failed invocations, but not throttled attempts
- Compute duration. The time from when your function code starts executing as the result of an invocation to when it stops executing. This metric directly affects AWS billing
- Business and customer experience metrics. Custom metrics relevant to how your functions are supporting your business, including user requests, checkout abandonment, revenue per location, and more

Use Case 2: Monitoring AWS Fargate deployments with Graviton2

AWS ECS Fargate data and Splunk Observability Collector

A large image photo sharing organization has a number of microservices running as containers in multiple AWS ECS Fargate clusters. DevOps and IT teams can visualize the CPU and memory utilization for each cluster and service, but they are unable to deeply analyze the tasks, containers, and resource utilization along with the dependencies

With Splunk Observability Cloud and AWS ECS Fargate with Graviton2

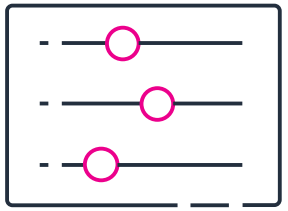
- Developers and cluster administrators can easily track each cluster, service level resource utilization, identify the root cause for task crashes, create alerts, and respond in real time to prevent a bad customer experience
- Cloud workloads running on Fargate powered by AWS Graviton2 processors achieve performance with lower costs than comparable Intel x86-based Fargate

Values of Observability

Customer Experience

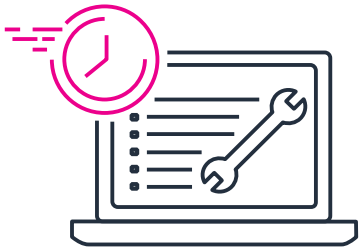
- Reduce risk of lost revenue
- Improve & maintain response times
- Provide high service availability
- Anticipate and prevent issues
- Fast issue resolution time before customers experience degradation
- Real-time visibility into the End User Experience
- Real-time visibility into Customer Journeys

Accelerate Development



- On-time projects, cloud deployments, modernisation
- Accelerate speed of cloud migration/modernisation initiatives
- Validate success of deployments to cloud
- Visibility into business AND technical KPIs and performance
- Attract & retain top talent

Reduce Unplanned Work



- Mitigate outages and service impacts
- Reduce MTTD/MTTR
- Identify and resolve issues before being deployed into production
- Pinpoint root causes to minimise the number of people and teams involved in issue resolution
- Incorporate performance into deployment pipelines to prevent surprises

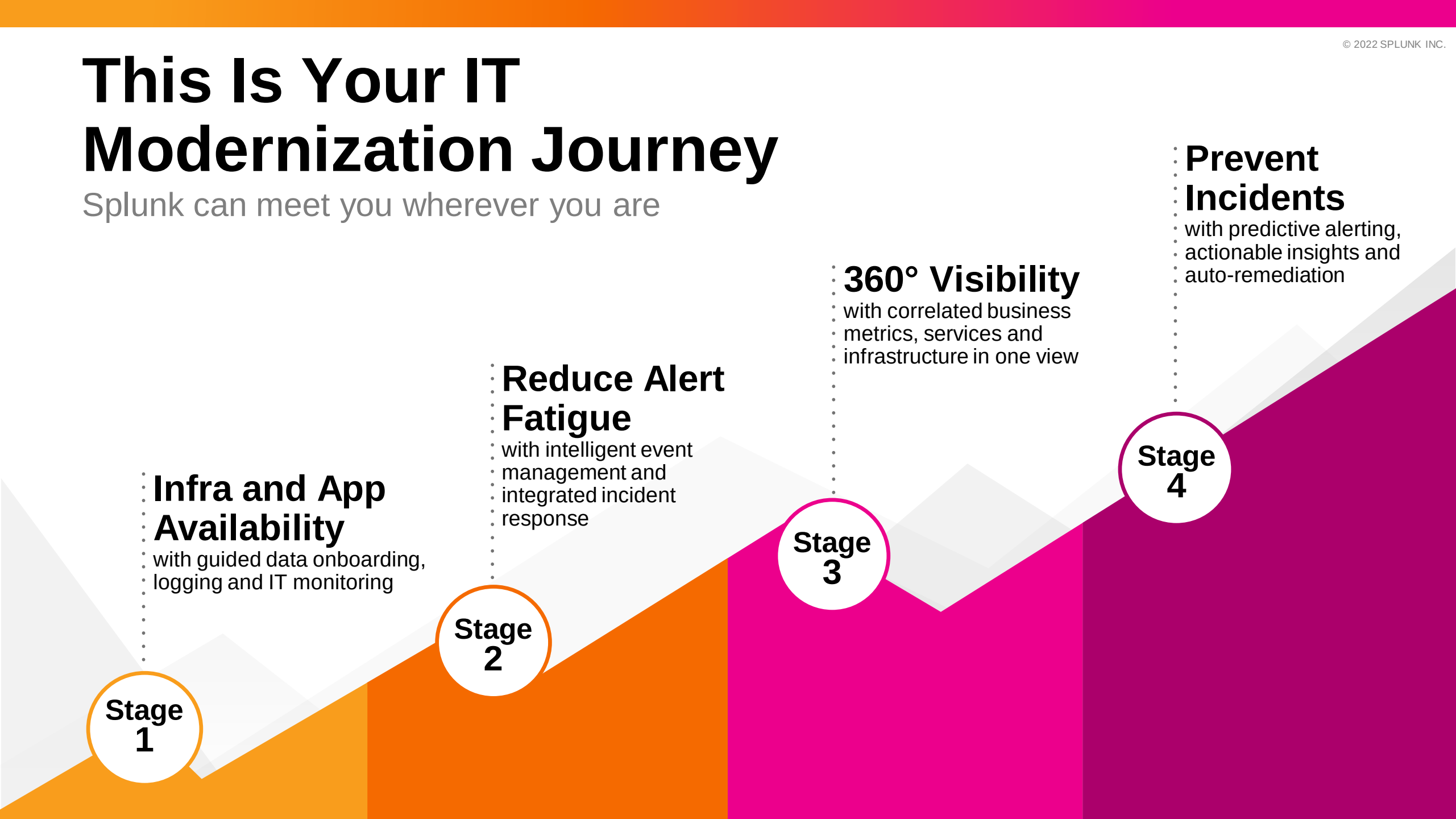
Optimize Cost

- Baseline and track costs of cloud services
- Compute optimisation recommendations to reduce cloud spending
- Visibility into the costs of APIs & Services
- Visibility into the costs of service for each customer or business unit
- Reduce Total Cost of Ownership

splunk> turn data into doing

This Is Your IT Modernization Journey

Splunk can meet you wherever you are



Detailed Use Cases

IT Operations

- What is my EBS footprint and posture across all my accounts and all my regions?
- Who started/stopped/restarted what instances and when?
- What EC2 instances are underutilized and perhaps overprovisioned?
- What is the traffic volume into my VPC and where is it originating from?
- Why are certain resources unreachable from certain subnets/VPCs?
- List resources with missing or non-conforming tags

Security

- Who added that rule in the security group that protects our application servers?
- Where is the blocked traffic into that VPC coming from?
- What was the activity trail of a particular user before and after that incident?
- Alert me when a user imports key-pairs or when a security group allows all ports
- What instances are provisioned outside of a VPC, by whom and when?
- What security groups are defined but not attached to any resource?

Cost Management

- How many instances am I running?
- What reserved instances have I purchased in the past?
- What is my reserved instance utilization?
- How much am I paying per account?
- How much am I using per service across all accounts?
- How many reserved instances should I buy based on usage?
- Is this account within budget this month, and how has it tracked in the last year?

FSI Customers Use Cases

splunk> turn data into doing®

Splunk Use Cases for Financial Services

Decisive actions for financial excellence

Financial Crimes

Fraudsters are constantly looking to exploit deficiencies in existing controls and gaps in monitoring

- Fraud
- Money Laundering
- Sanctions Compliance
- Market Abuse

Retail Banking Operations

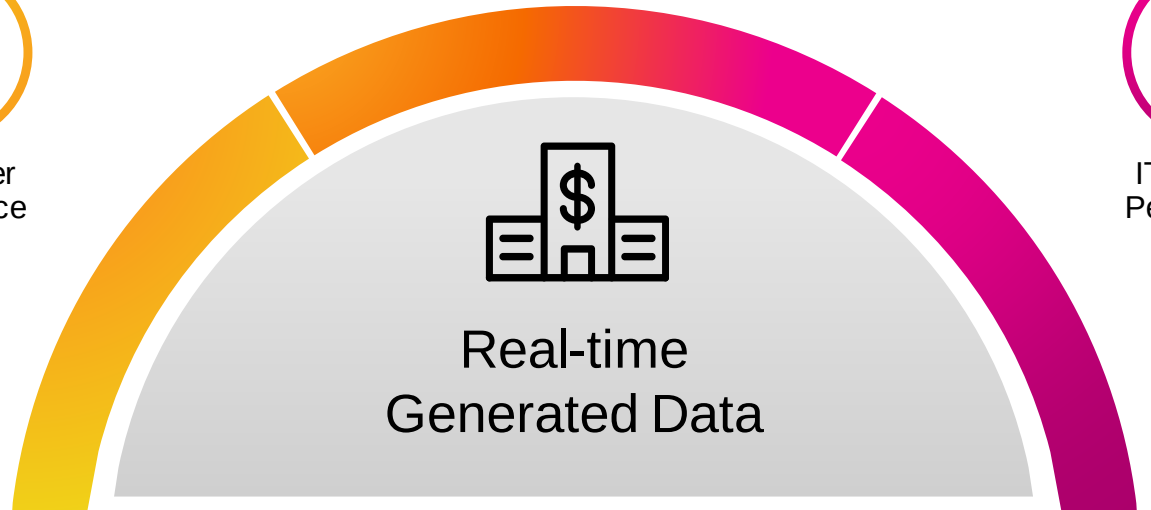
Retail Banks face costly battles to maintain their branch operations and ATM network

- ATM Monitoring & Analytics
- IT Operations & Security
- Customer Experience

Trading Operations

Capital Markets must run on the highest levels of service excellence to effect business strategy

- IT Systems Performance
- Compliance Monitoring
- Threat Detection



splunk> turn data into doing

Fintech Digital Payments Platform

Products:

- IM, APM

Use Cases:

- Observability
- Infrastructure Monitoring and Troubleshooting
- Application Performance Monitoring

Increase Market Share in Digital Wallets and Payments

Key Challenges:

- Was unable to timely resolve issue or find root cause in the first place not only impacts CX, but also liability of Fintech Digital Payments Platform vs Banks e.g. FinTech's user complains about found transferred but didn't see funds in their account

Key Results:

- is able to increase its market share in the digital wallets and payments space by offering a more reliable service, improve CX, while delivering new innovations

Data-Driven Outcomes:

Real-time streaming metrics platform – real-time transactions, helped with SLO of MTTR, 100s of transactions per second

Open Telemetry - Open standards important for FinTech to share data between different systems and avoid vendor lock-in

Full- Fidelity tracing out of the box every transaction tracing, **FundLoss** situations to determine liability - saved FinTech $

"The number one key factor that we weighed highly when it came to our partnership with Splunk was that it's not sampling -- it's 100% of all the data. As we serve 80 million users and have 5 million transactions per day, if the Observability solution only gives us 90% of traces due to sampling, that 10% loss is huge. We need to see everything, we cannot afford this loss of visibility especially as we are a payments platform."

splunk> turn data into doing

Financial Services

Products:

- Splunk Observability Cloud

Use Cases:

- IT Operations
- DevOps
- Platform

Streamlines DevOps for Real-Time Observability and 8x Faster Infrastructure Deployment

Key Challenges:

- As continued business growth created increasing complexity in Hyphen Group's IT environment and cross-functional processes, tracking errors effectively and resolving issues efficiently became more difficult. Heads of engineering had to come in at 2am or 3am because they were the only ones who knew how to dig through the error logs. Major infrastructure outages often took several hours

Key Results:

- Data-driven observability improves full-stack, end-to-end visibility into complex systems in real time, which has enhanced DevOps collaboration, enabled automation at scale and accelerated troubleshooting and infrastructure deployment.

Data-Driven Outcomes:

- Mins to resolve issues rather than hours
- 8x faster infrastructure deployment
- 275 software updates released with unprecedented efficiency

"Splunk helps streamline the problem-solving process and allows both our developers and infrastructure operations teams to focus on adding value to the business."

splunk> turn data into doing

Thank You!