Splunk

Turning Big Data into Actionable Insights

Big Data Challenges

Lack of effective analytical tool to handle big data

Event management and task prioritization of high velocity data

Visualization of real time data

Splunk

Splunk Capabilities

Advance Analytics Capabilities

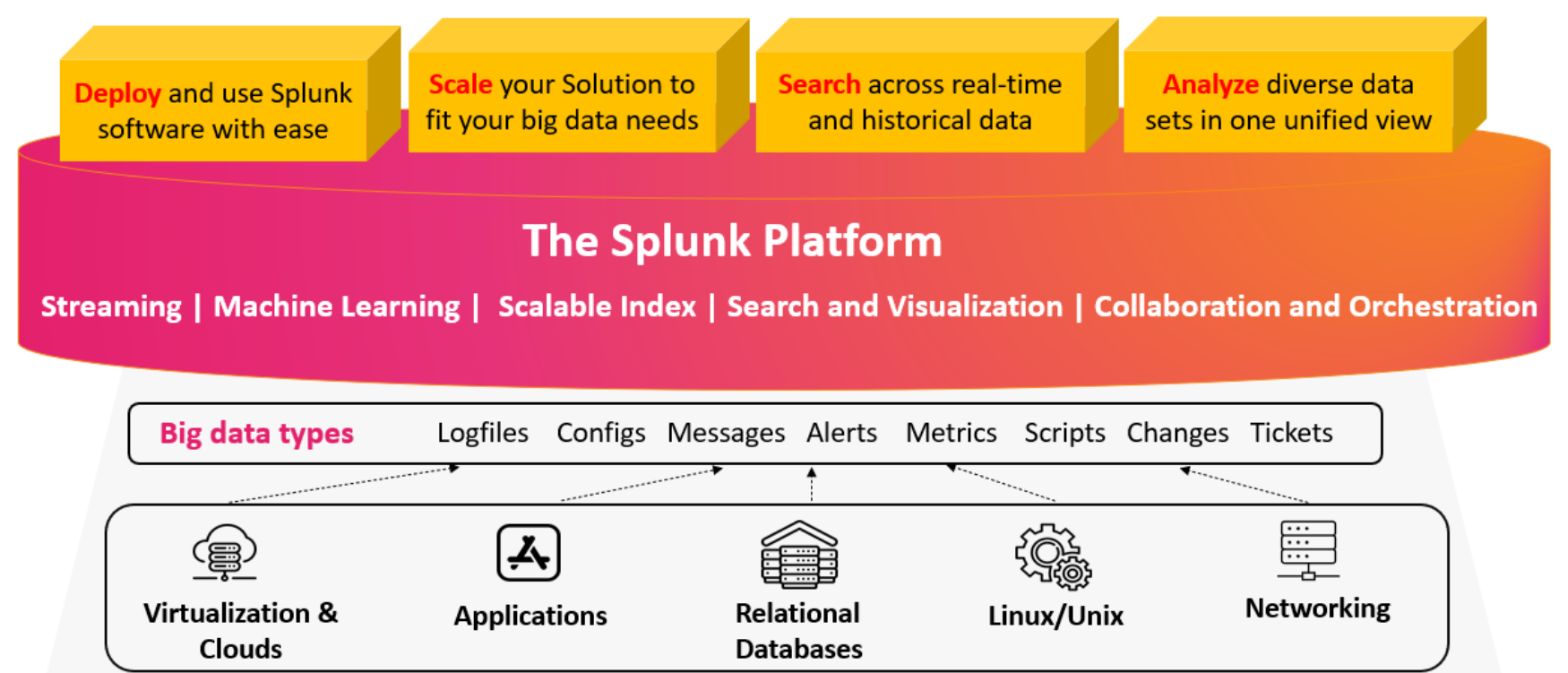Handle all kind of high velocity data

Transform data into Insights

Why Splunk

Enhance Security
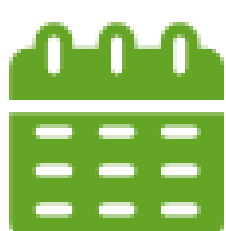
WHY?

Drive Reselience

Unlock Innovation

Deploy and use Splunk software with ease

Scale your Solution to fit your big data needs

Search across real-time and historical data

Analyze diverse data sets in one unified view

The Splunk Platform

Streaming | Machine Learning | Scalable Index | Search and Visualization | Collaboration and Orchestration

Big data types   Logfiles   Configs   Messages   Alerts   Metrics   Scripts   Changes   Tickets

Virtualization & Clouds   Applications   Relational Databases   Linux/Unix   Networking

Use Cases

Threat Detection

Event Management

Splunk

Web Analytics & Visualization

Application Dev & Modernization

Splunk Architecture for Web Analytics

Web Application → Log File → Amazon S3 Data Layer → splunk>
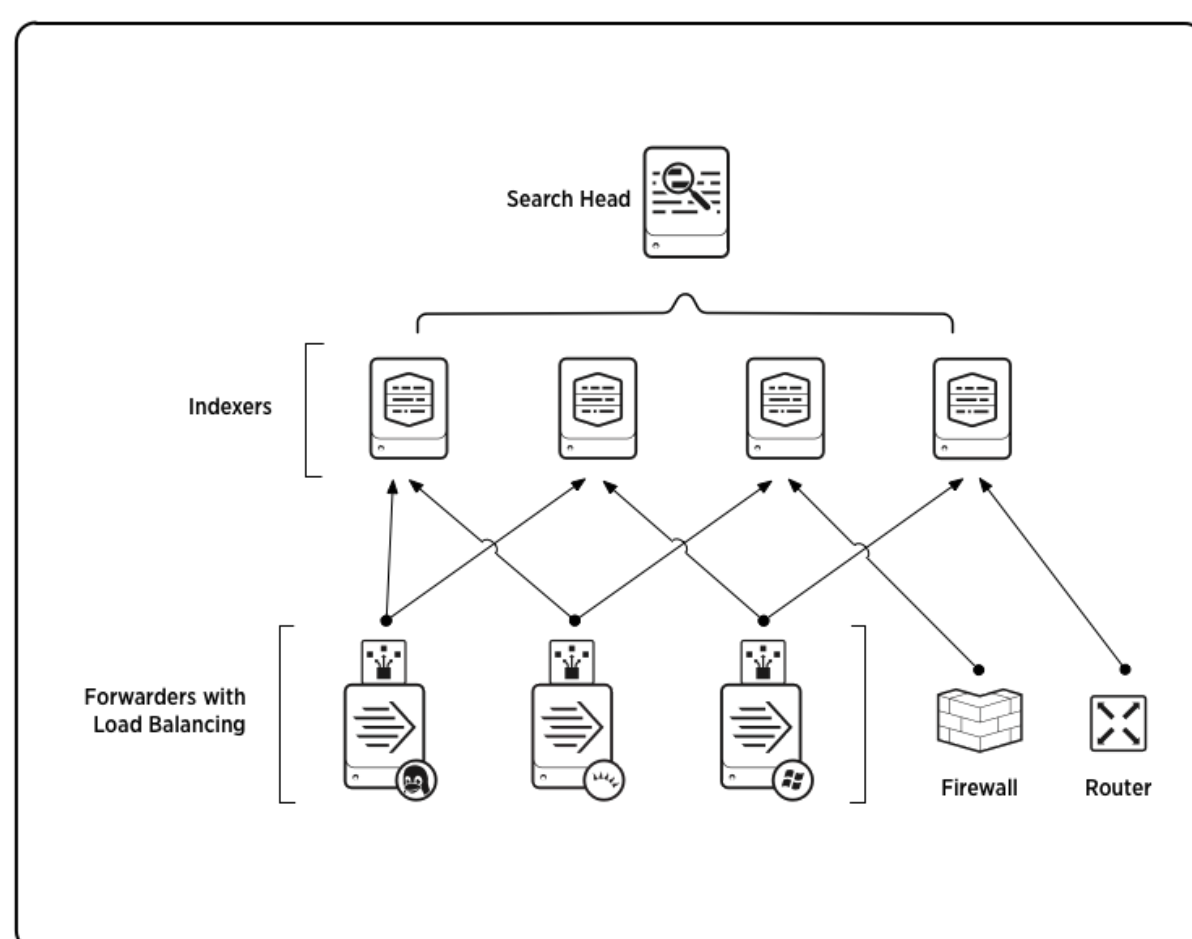
Visualize Critical Treads

Ad-hoc search capability
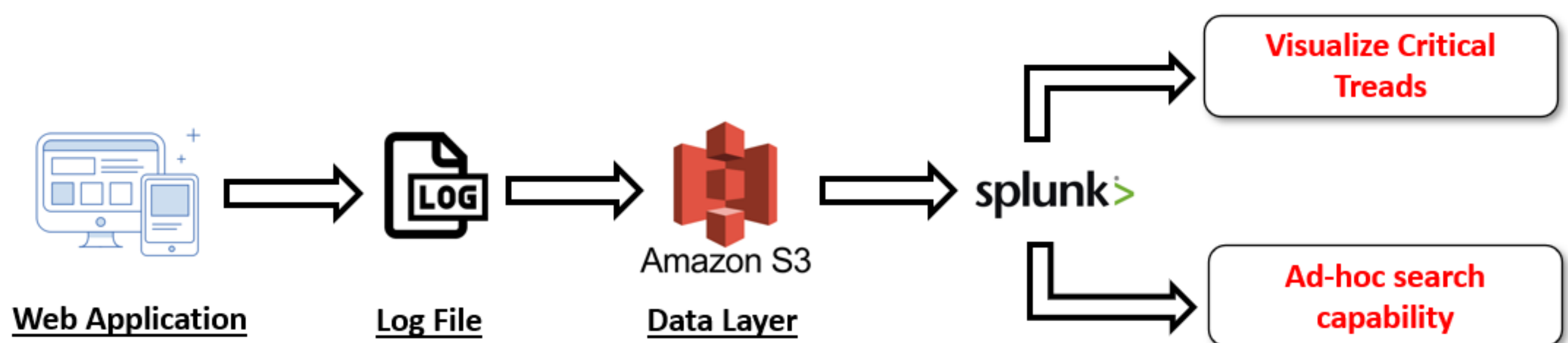
How it works

The index is the repository for Splunk Enterprise data. Splunk Enterprise transforms incoming data into events, which it stores in indexes

Companies using Splunk

2M+

**Security threats blocked
in six months**

Aflac

70%

**Faster mean time
to repair**

TESCO

2x

**Online delivery slots
made available
In five weeks during
pandemic**

HONDA

96%

**Faster application
development**

QuantumMetric

Team 10

Aleksandra Singer: singe240@umn.edu

Arv Ramchandani: ramch020@umn.edu

Harsha Moturi: motur008@umn.edu

Jingzhi Ren: ren00144@umn.edu

Naval Vaidya: vaidy100@umn.edu

Vijay Kumar: sidda015@umn.edu