splunk> .conf2017

Splunk IT Service Intelligence:

Event Management Is Dead

Event Analytics Is Revolutionizing IT

David Millis | Splunk Staff Architect, IT Operations Analytics

September 26-28, 2017 | Washington, DC

splunk> .conf2017

Or

Your Event Manager Is Driving In Circles

Time for a New Driver

David Millis | Splunk Staff Architect, IT Operations Analytics

September 26-28, 2017 | Washington, DC

Disclaimer

During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

But First, a Terminology Check

splunk> .conf2017

What is ~~Truth~~? Event Management?

- Terminology within the "Event Management" space is loose
  - event, alert, notification, alarm, incident, time-series message, ...
  - event mgr, element mgr, monitor, fault mgr, manager of managers, ...

- We have to speak the same language
  - at least during this session

Data Terms

- "Event" - time-series message describing a change of state for a target entity
  - often generated by a 3rd party entity
  - usually includes target component (server17), alert description ("node is down"), state/status/severity ("down")
  - ***NOTE**: This is different than most Splunkers think of an "event"*
- "Logged Data" - time-series message from an entity, describing something that occurred to the entity itself
  - app log, O/S log, win-event, syslog (usually)

Data Terms

- "Metric Data" - time-series message with a performance value. Usually a number.
  - Collected on a regular basis (every minute, every 15 minutes, etc)
  - "CPU % usage", "Filesystem capacity", "Interface bytes received"

- "Wire Data" - time-series message collected indirectly by capturing raw network traffic "off the wire".
  - Often metrics
  - Splunk Stream, wireshark, etc

Data Terms

- "Time-Series Data" - The stuff that Splunk indexes
  - Formerly called "events" by many Splunkers
  - Includes all of the previous data types
- "Notable Event" - an actionable message
  - intended specifically for humans in Operations
  - Splunk ITSI & ES
- "Incident" - Unplanned interruption or reduction in quality of an IT or Business service
  - Service Now, Remedy

Other Terms

- "Event Manager" - monitors stuff and spews "events"
  "Element Manager"
  "Monitor"
- "Manager of Managers" - a tool which correlates events
  "Fault Manager"
- "AI Ops" - The Latest Thing, uses Machine Learning
- "Event Analytics" - Splunk's vision for next-gen IT Ops

IT Operations' Mission:

Find What's Broken, then Fix It

splunk> .conf2017

A Brief History of Event Management

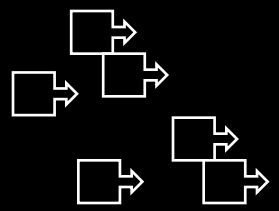
Remind Me: Why Are We Doing This?

splunk> .conf2017

A long time ago, there were very few events

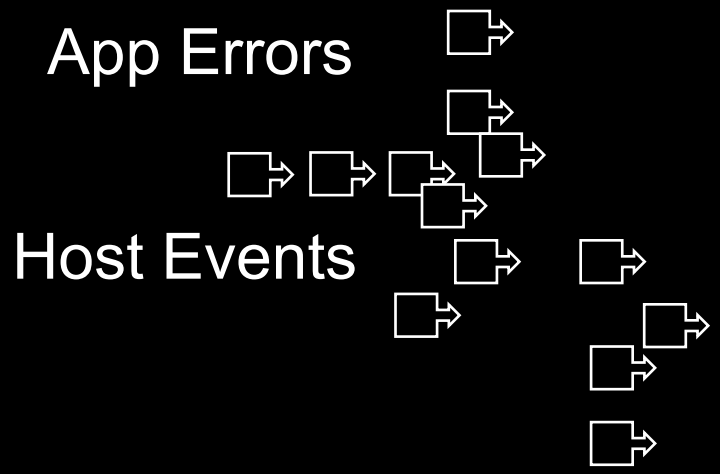
and they mostly came directly from a few large computers

Host Events

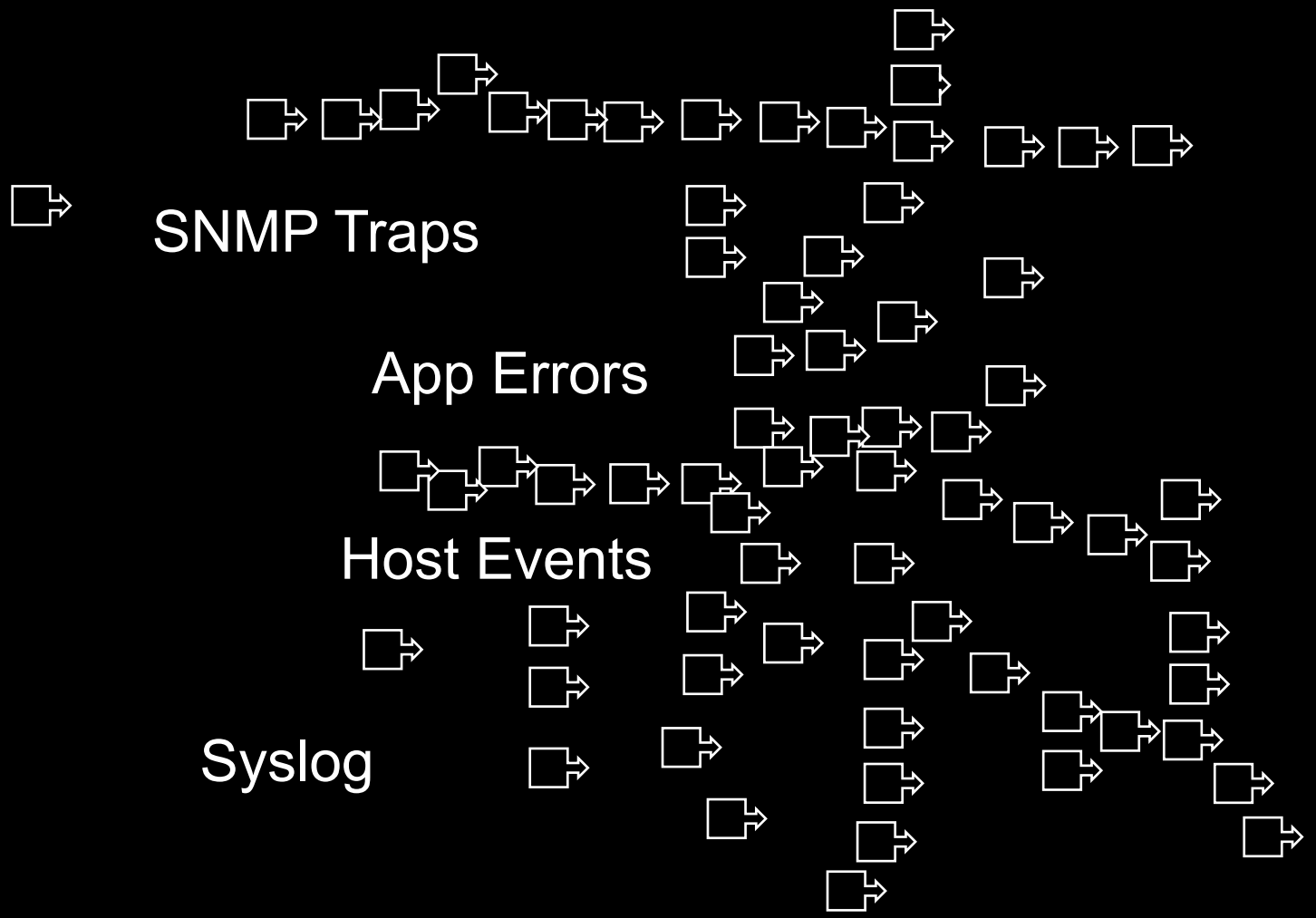


The IT Folks could handle it

But the Rate of Events Began Increasing

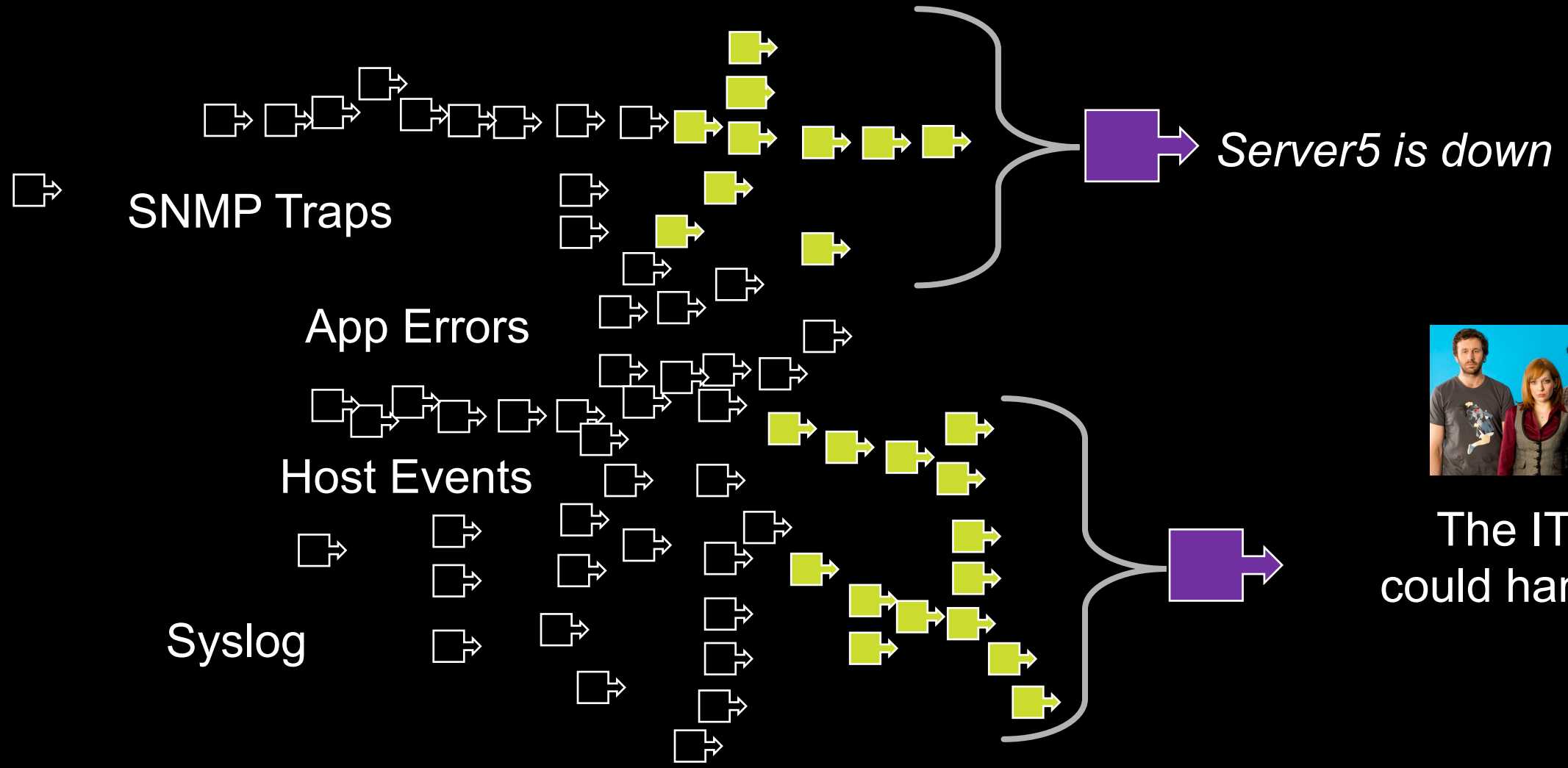


But the Rate of Events Began Increasing



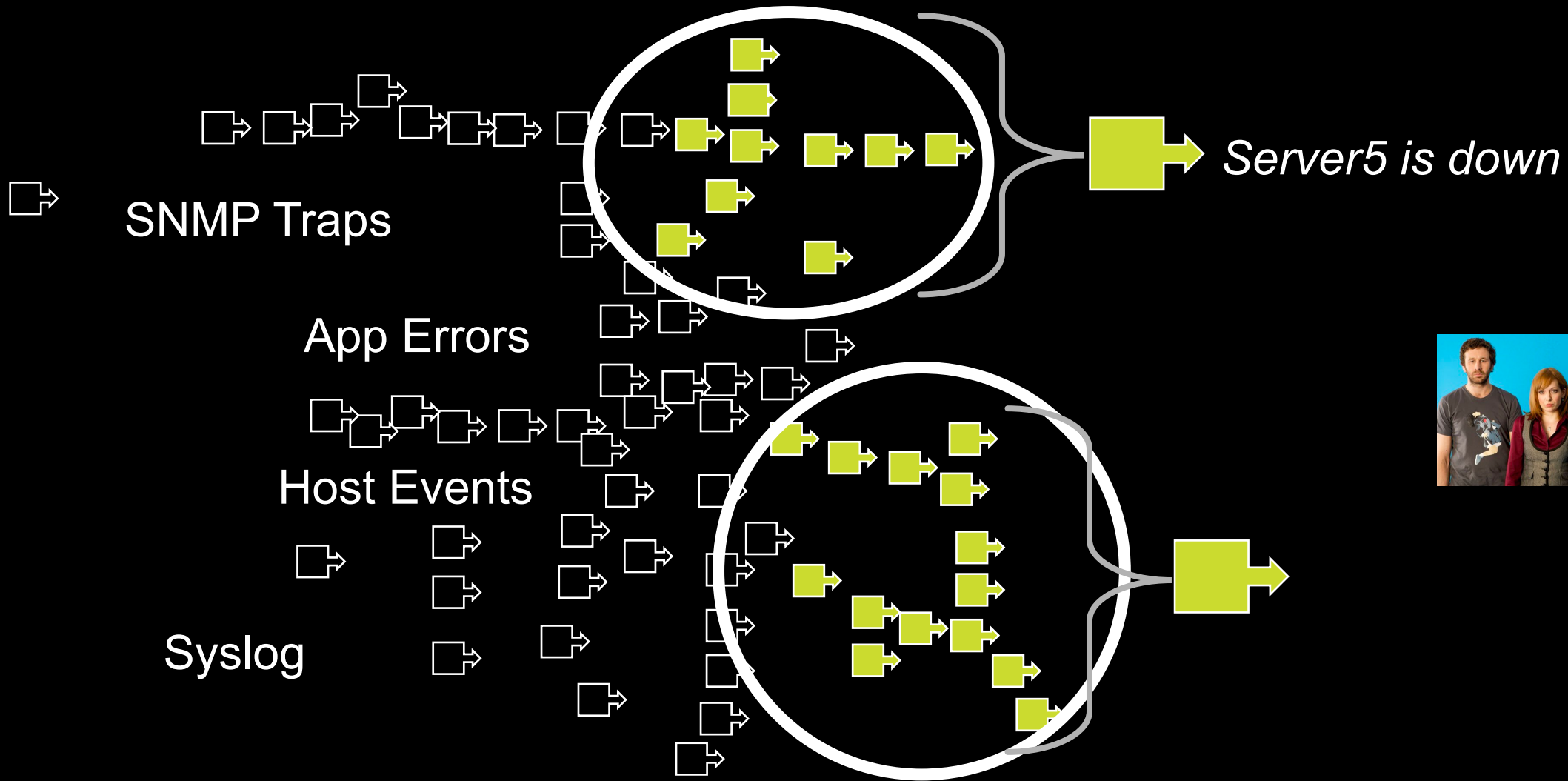
Until the IT folks couldn't handle it

The Event Manager is Born

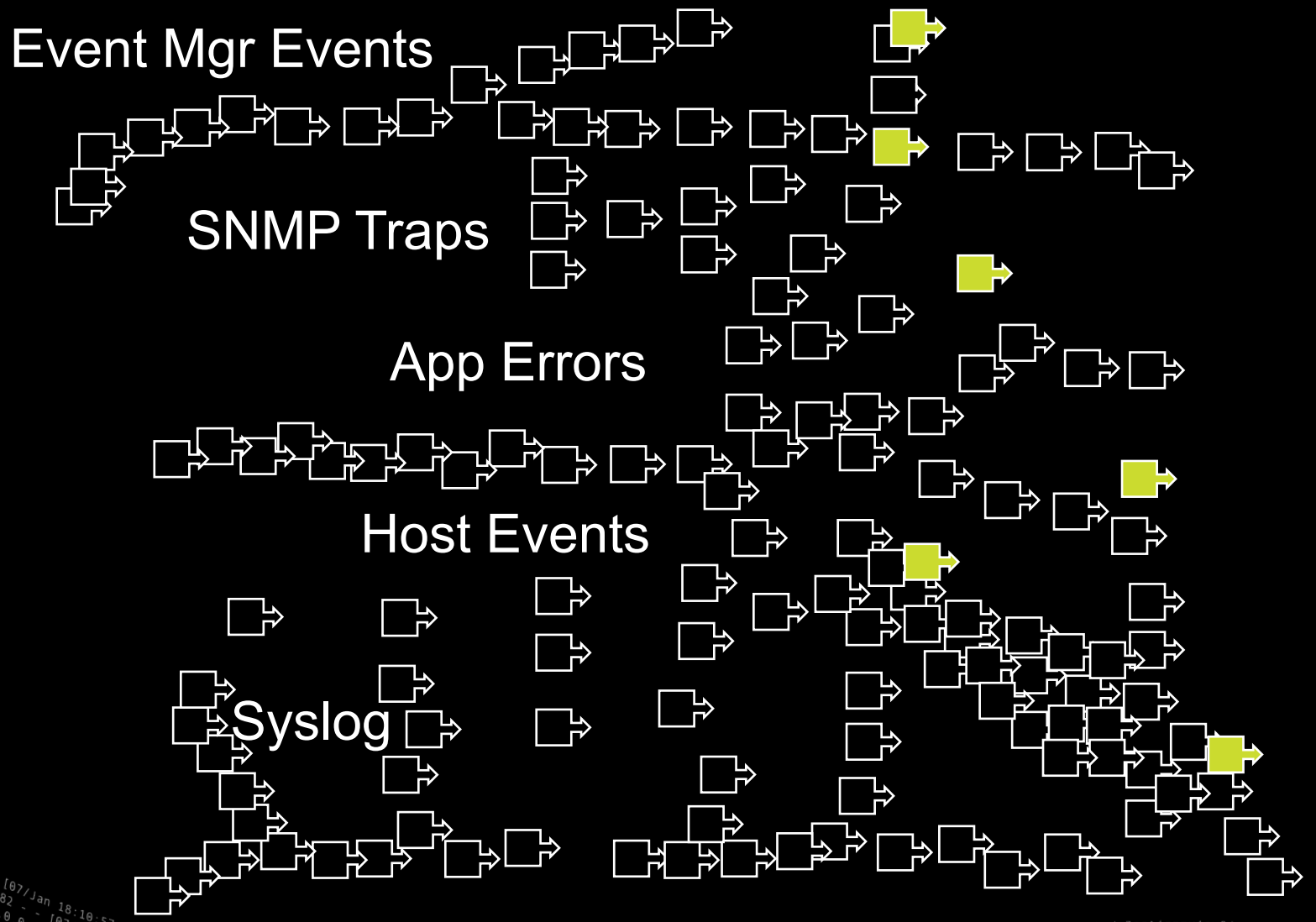


The IT Folks could handle it, again

... along with the IT Silo!



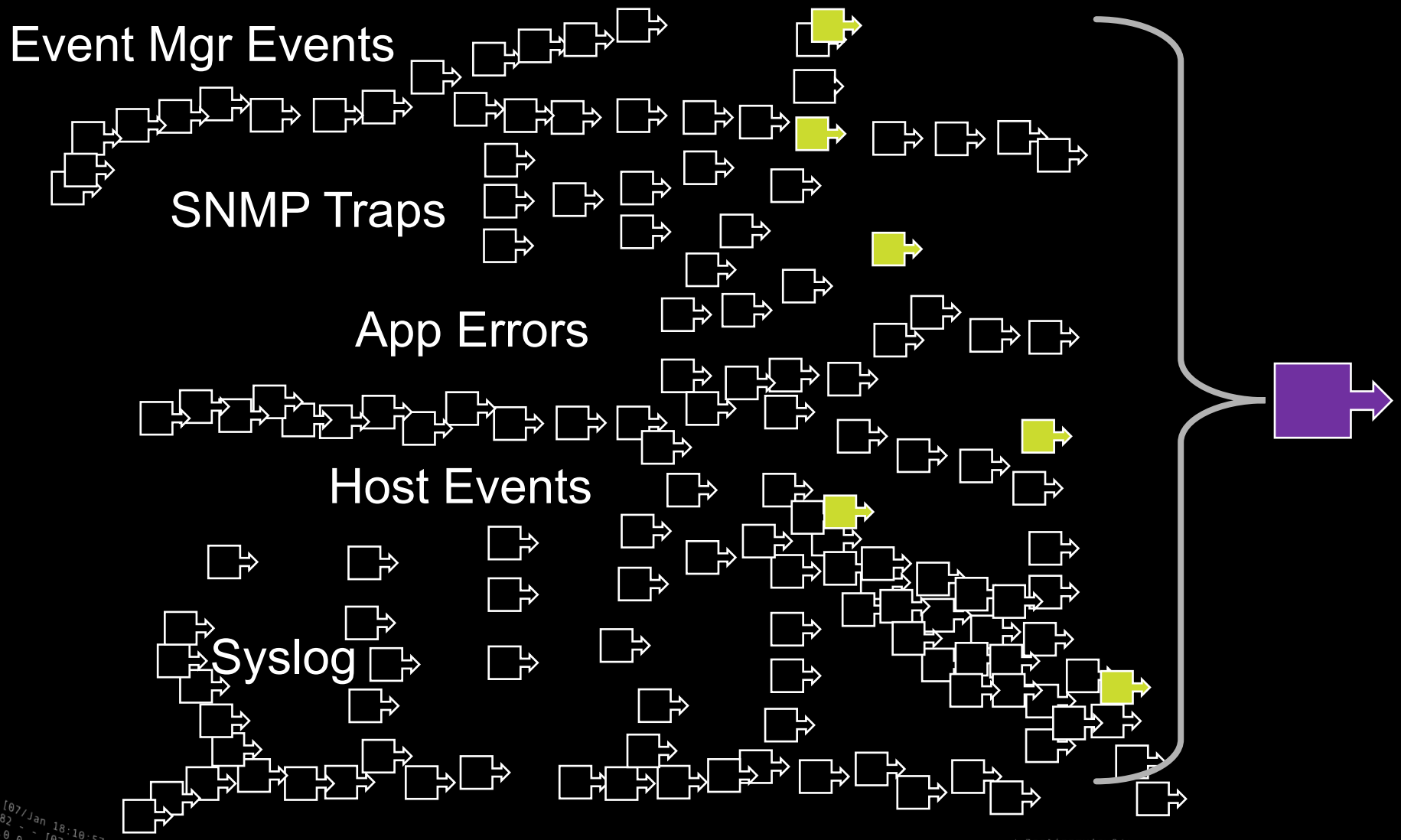
But the Rate of Events Kept Going Up



and Event Managers Multiplied

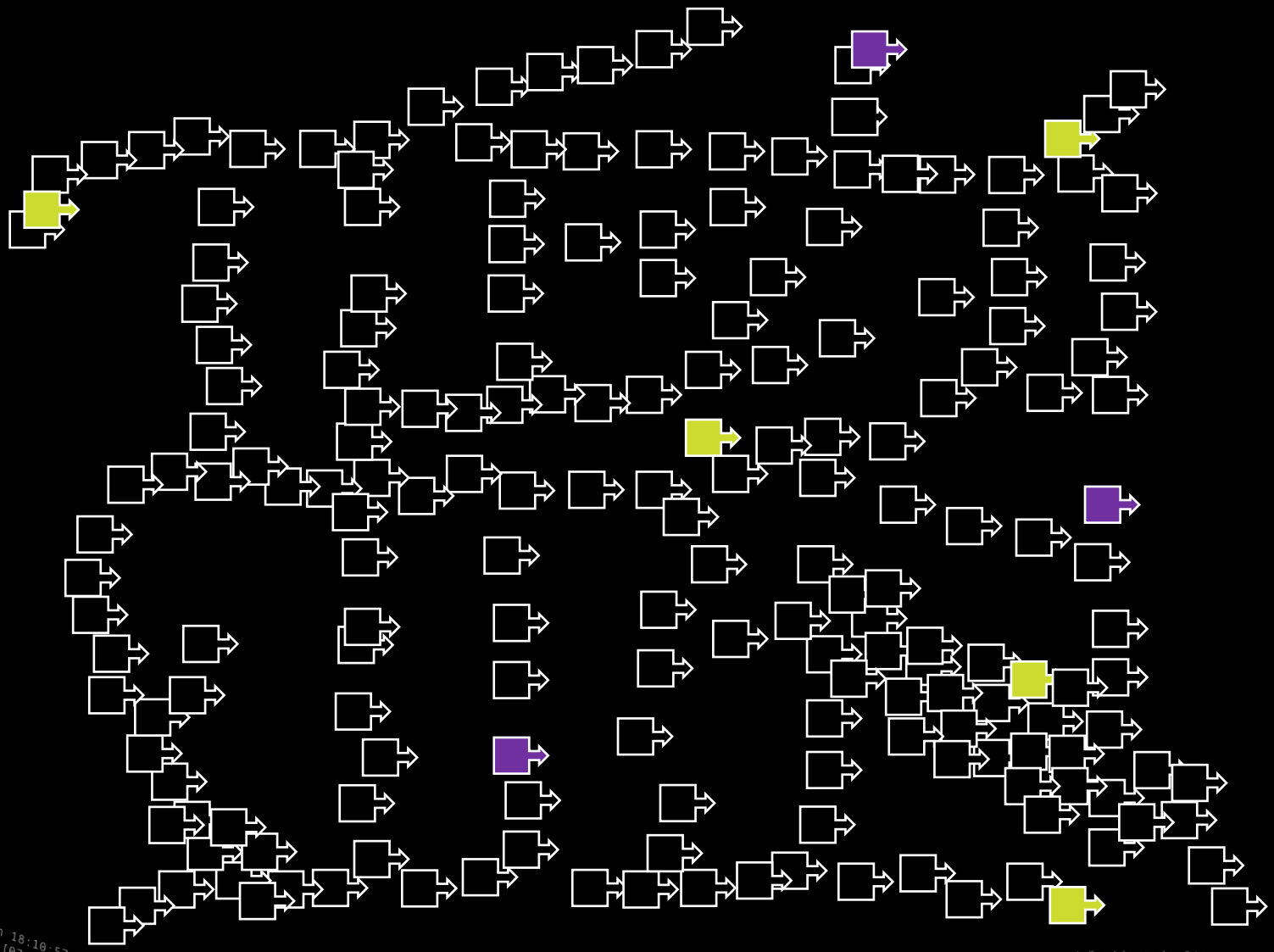
splunk> .conf2017

MoM to the Rescue

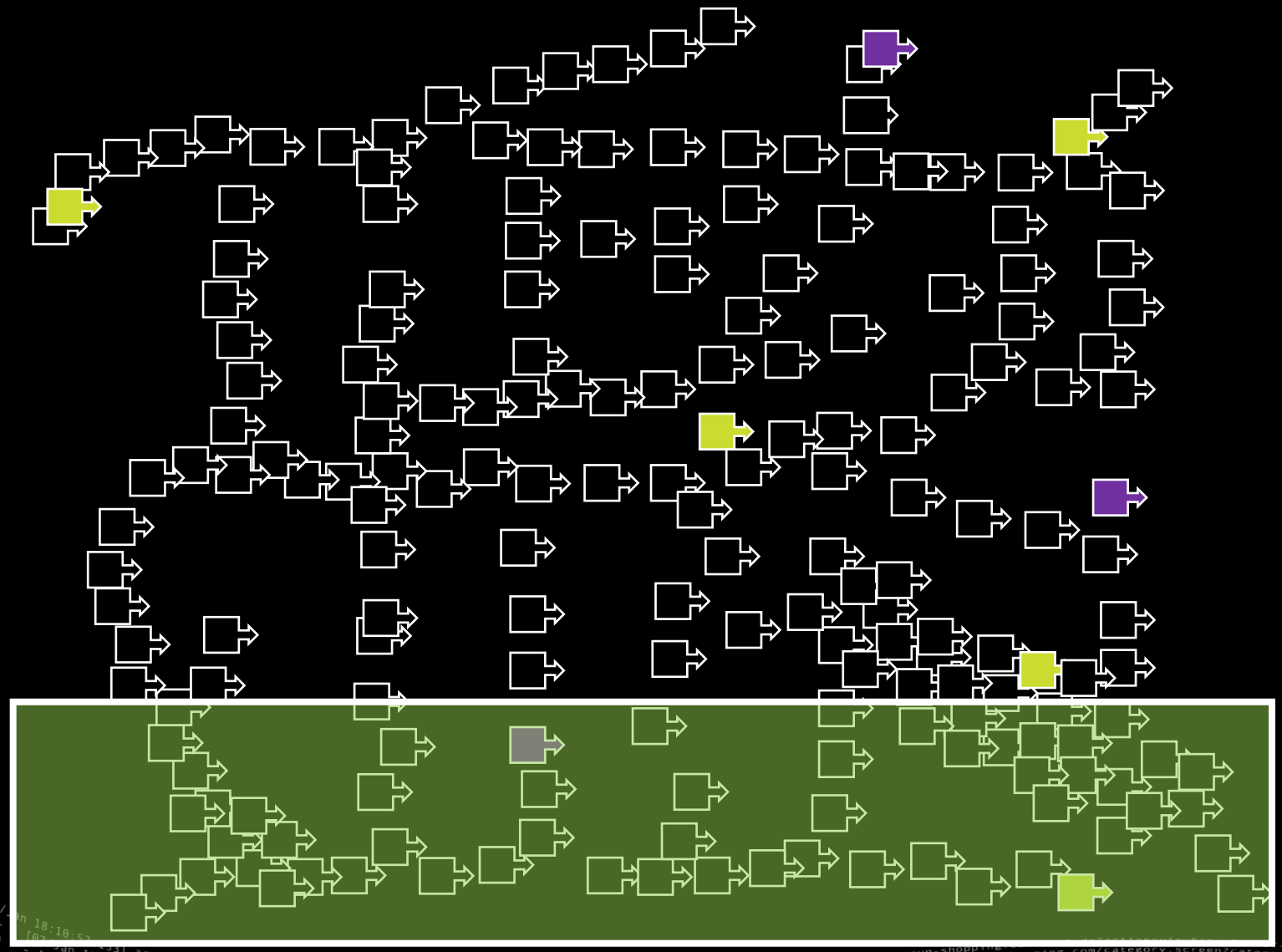


More Filtering & Reducing

Environments Became More Complex

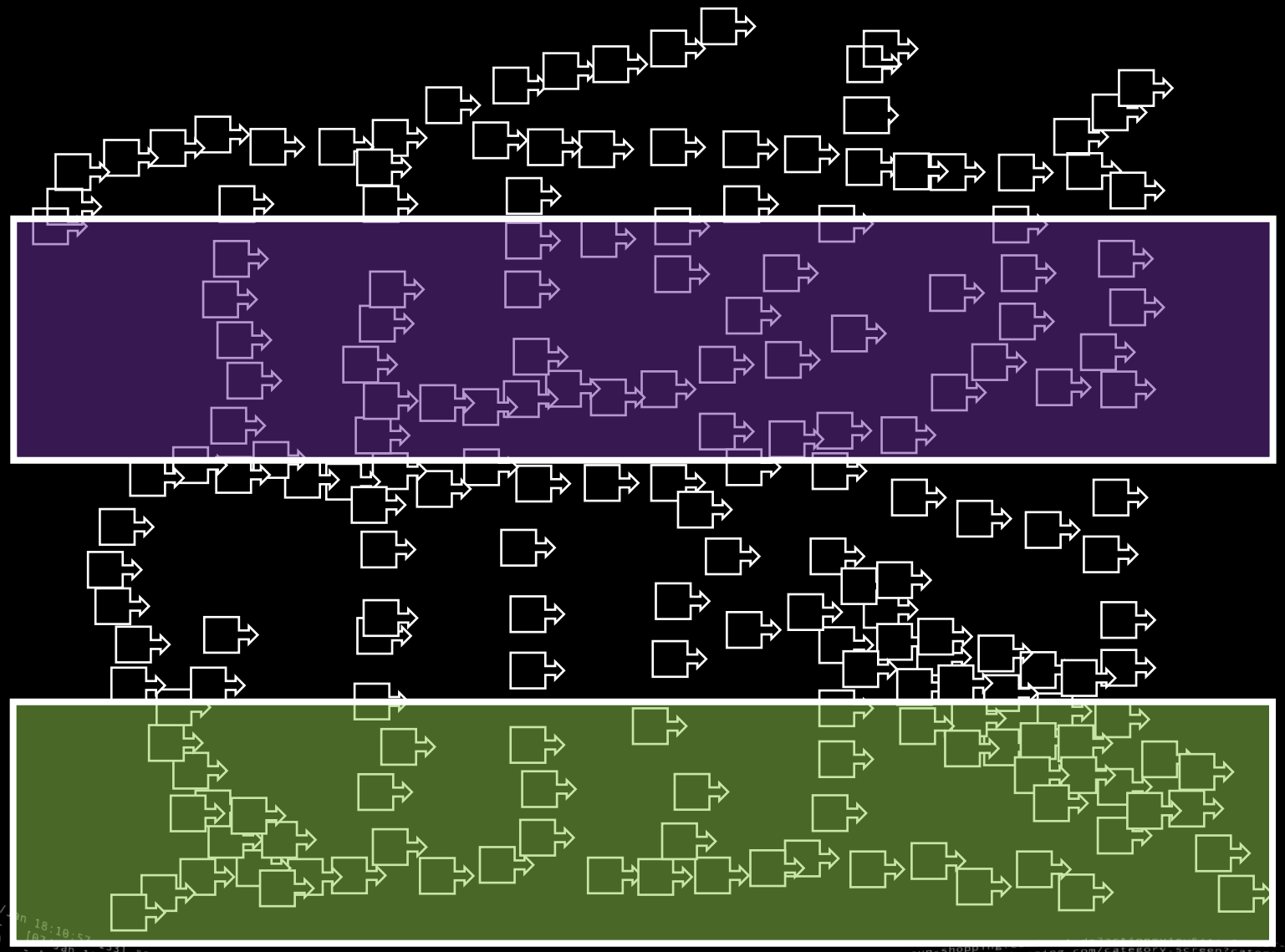


Environments Became More Complex



Network

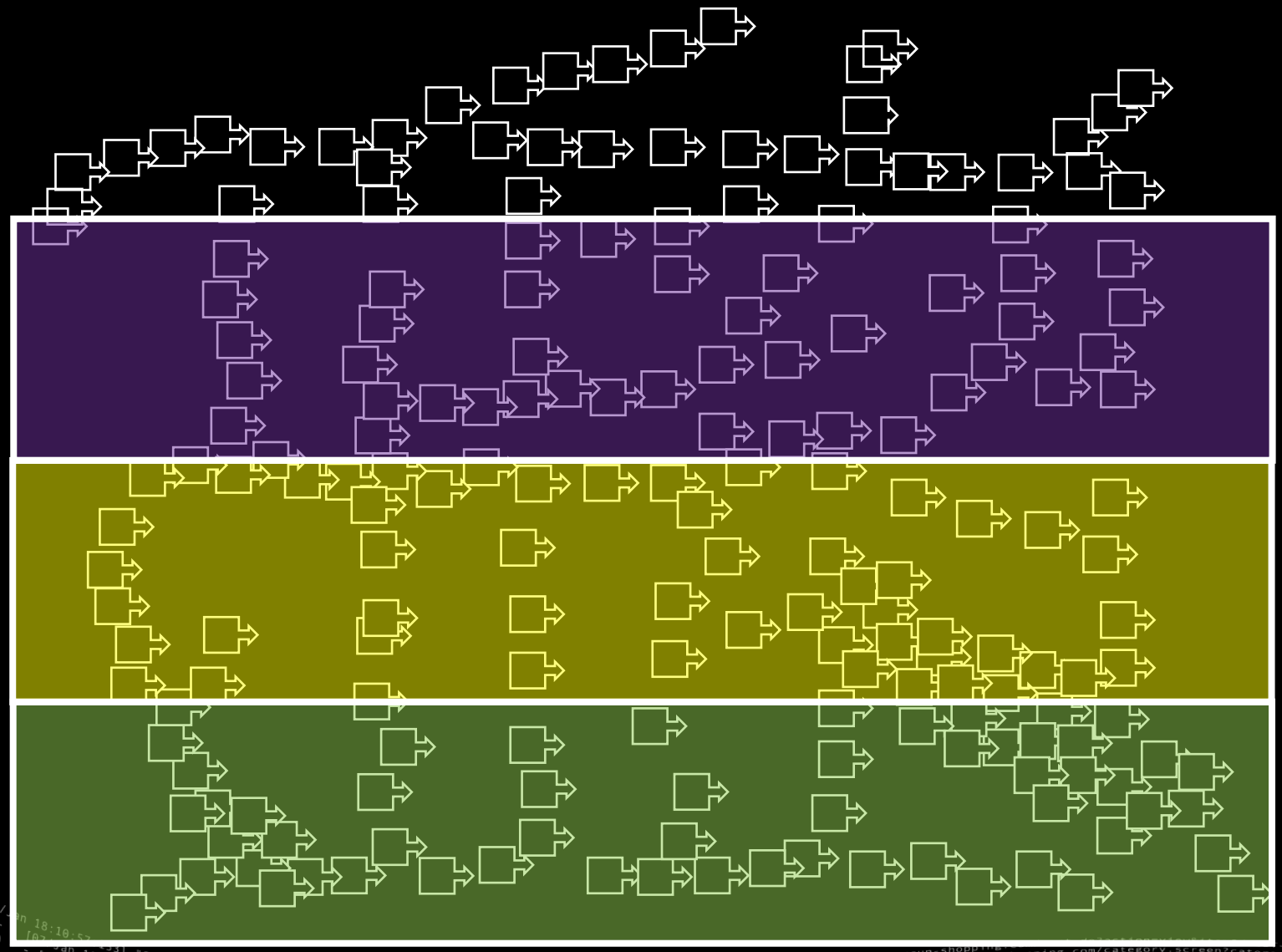
Environments Became More Complex



Virtualization

Network

Environments Became More Complex

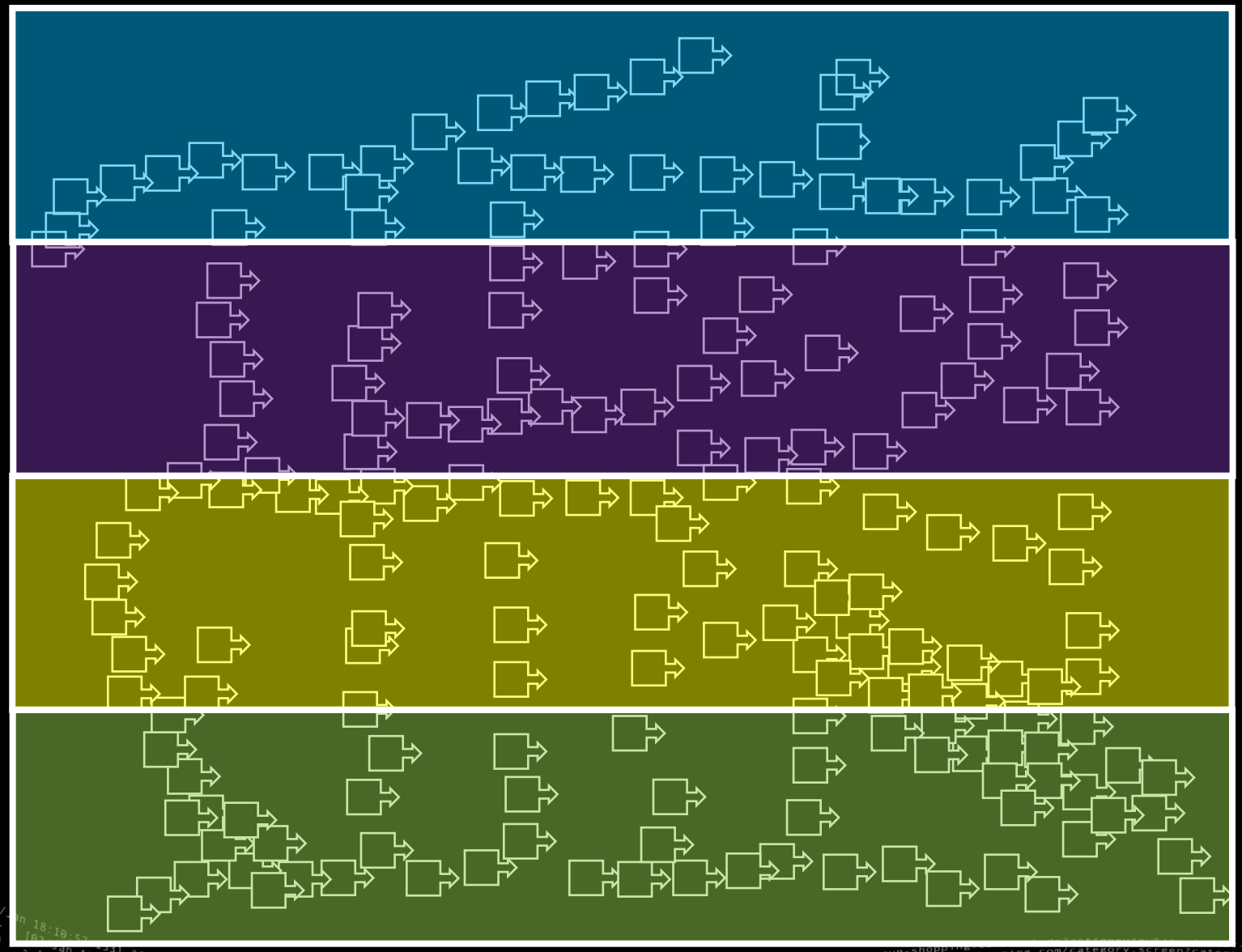


Virtualization

Storage

Network

Environments Became More Complex



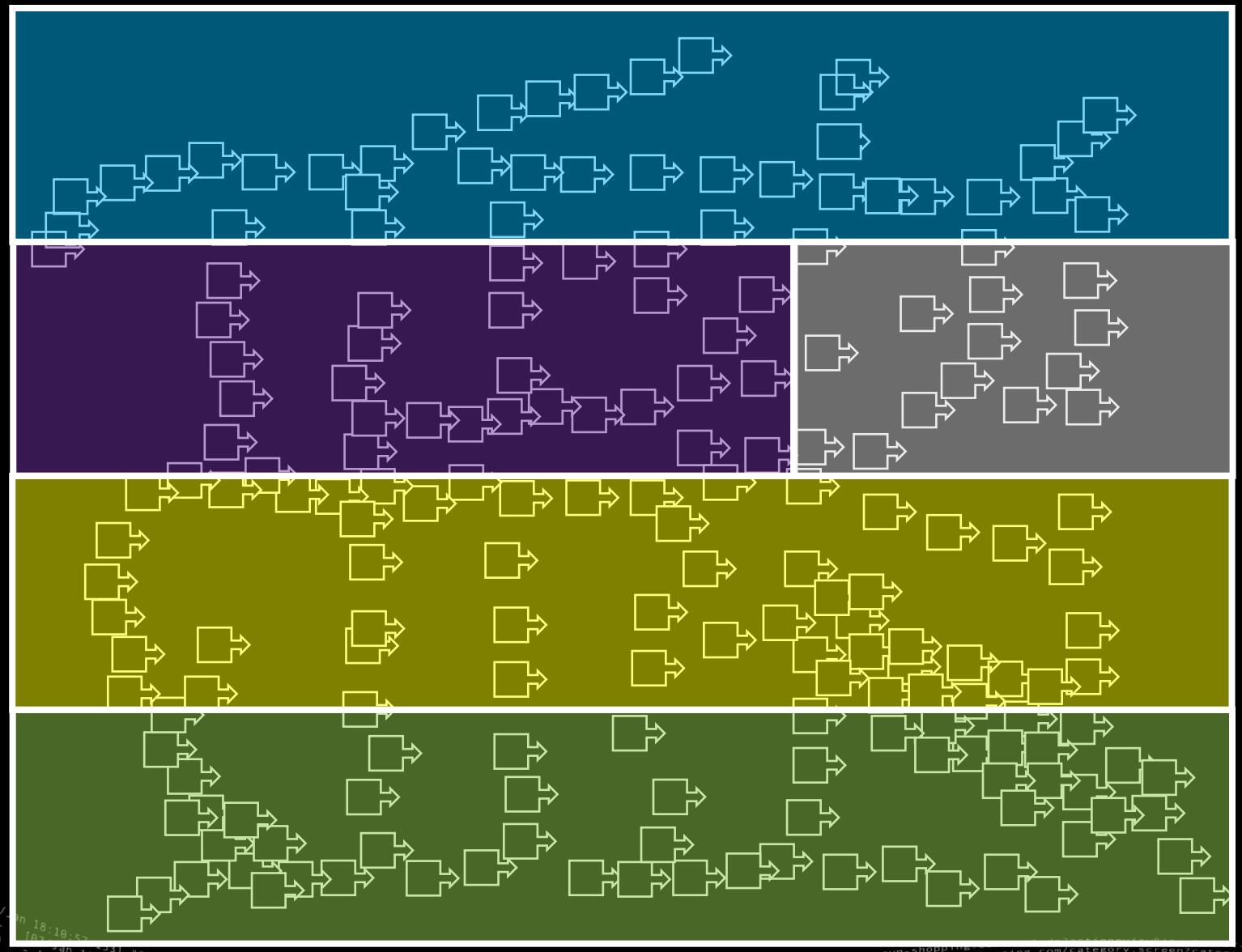
Cloud

Virtualization

Storage

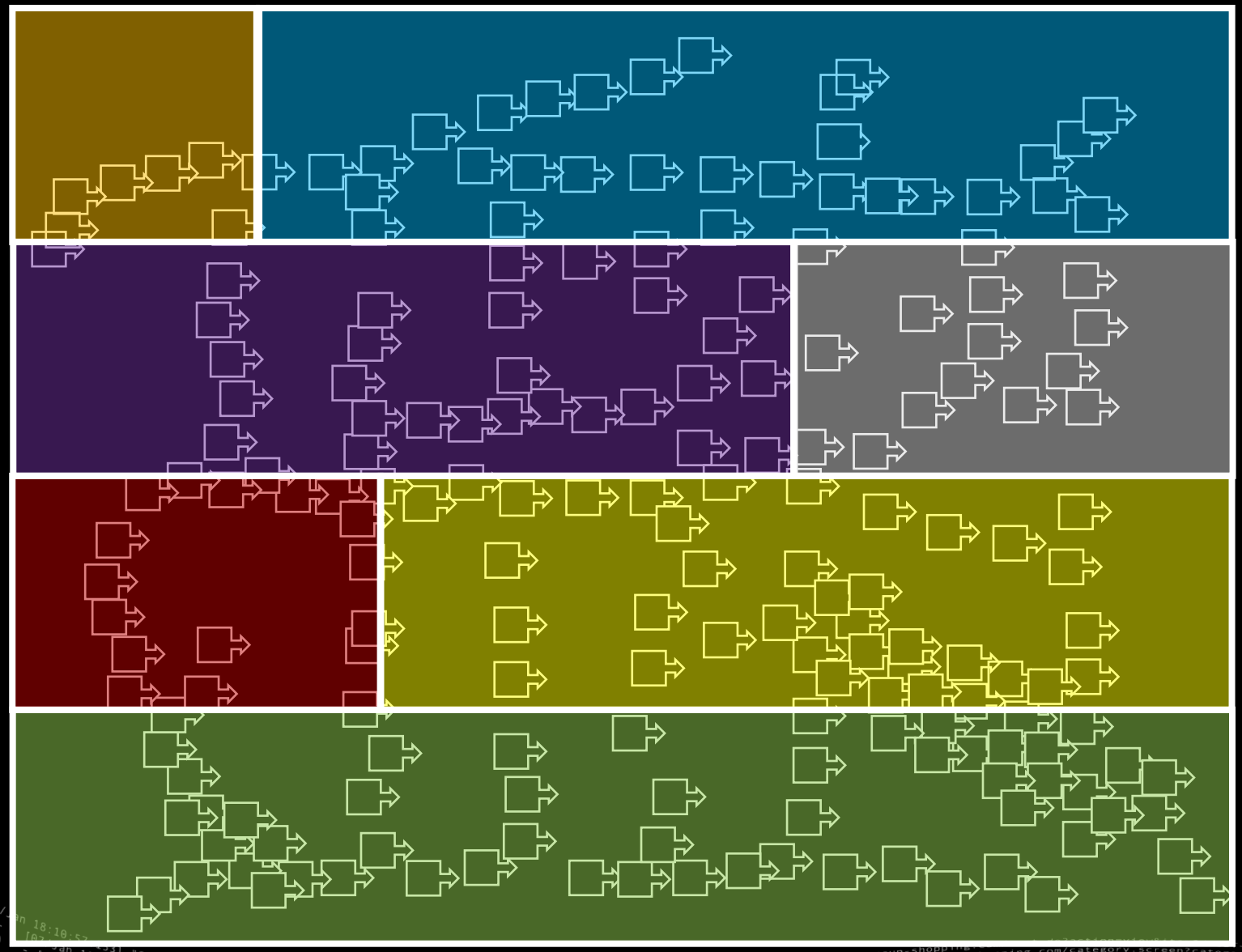
Network

Environments Became More Complex



Highly Available

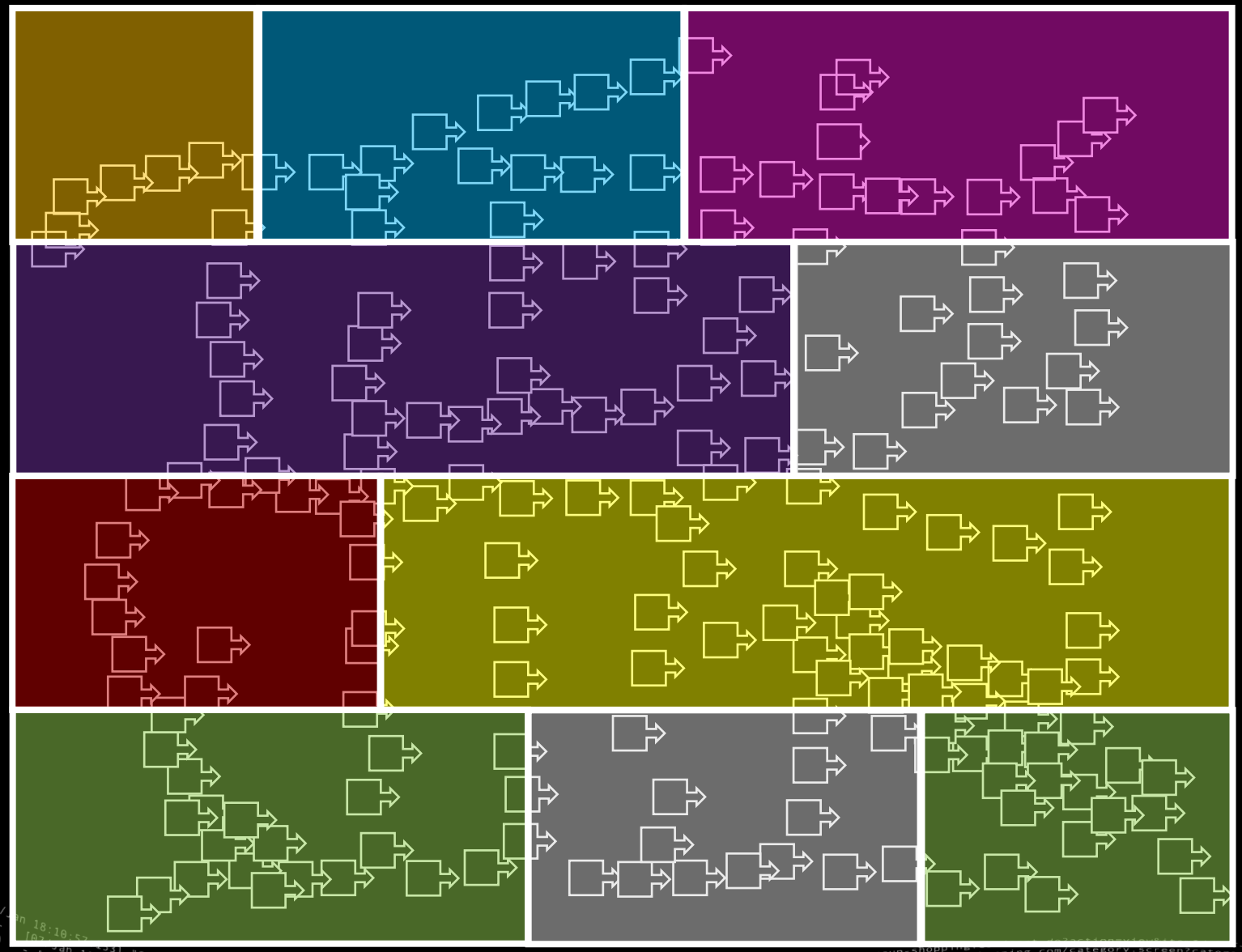
Environments Became More Complex



Highly Available

On Demand

Environments Became More Complex

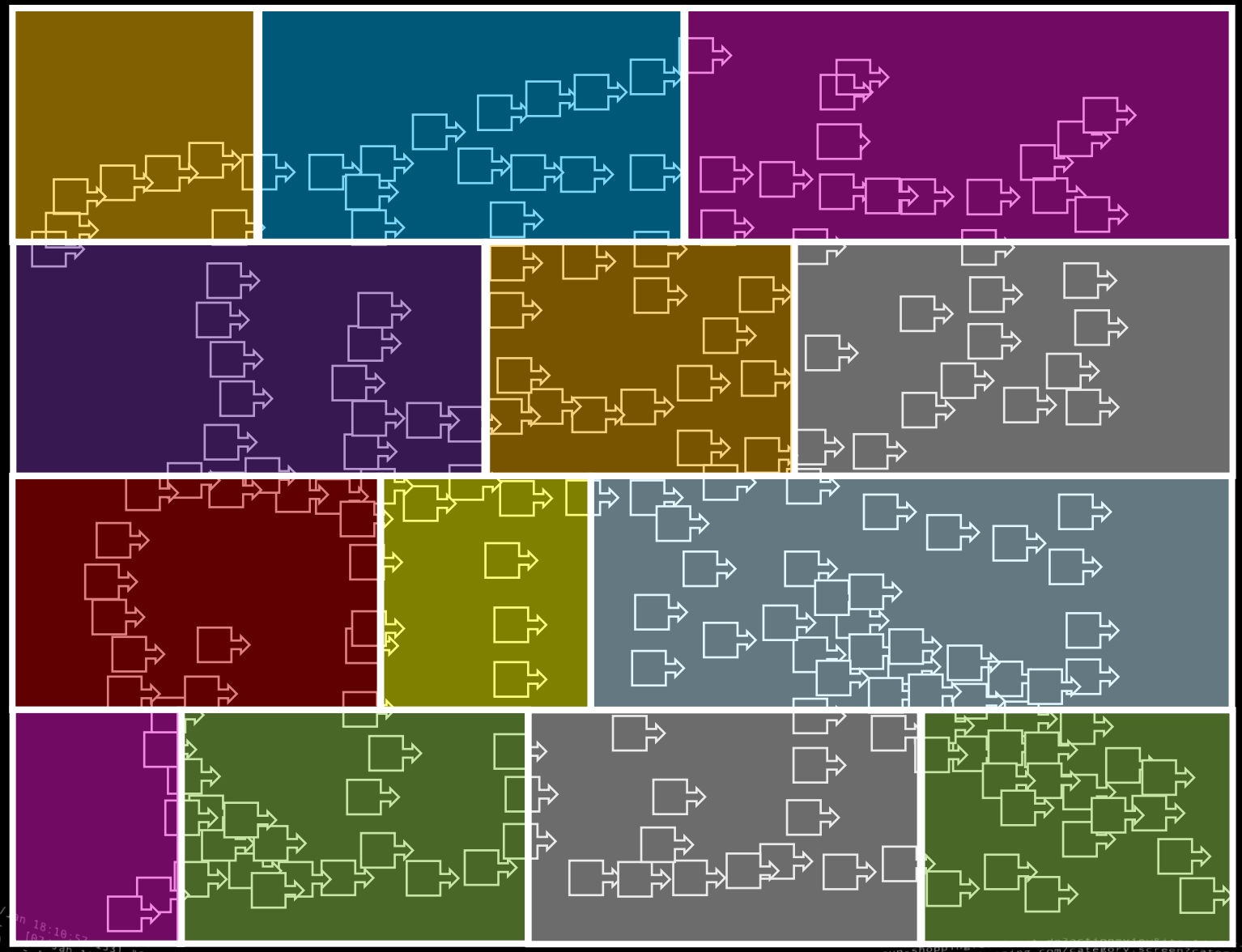


* As a Service

Highly Available

On Demand

Environments Became More Complex



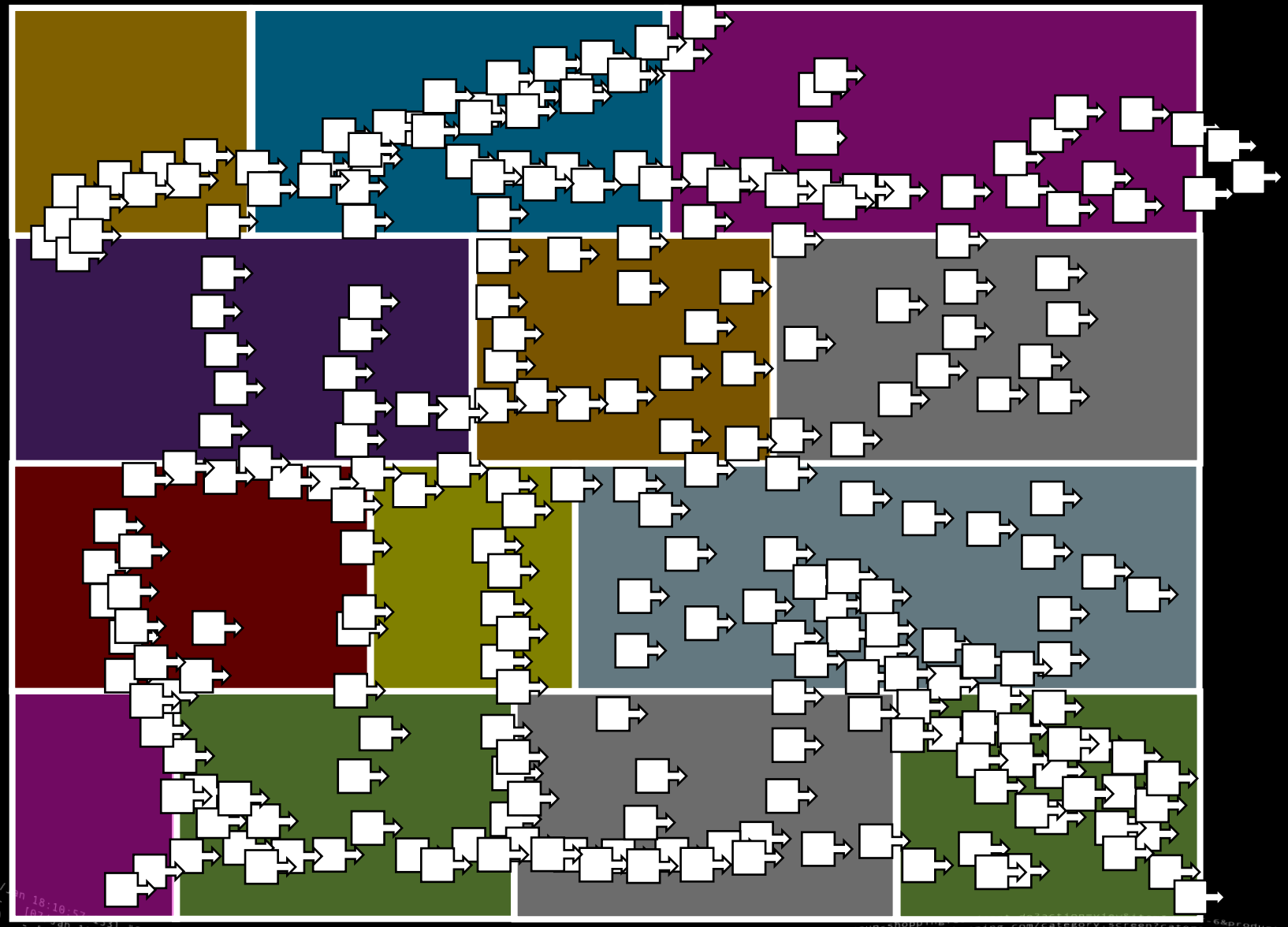
* As a Service

Highly Available

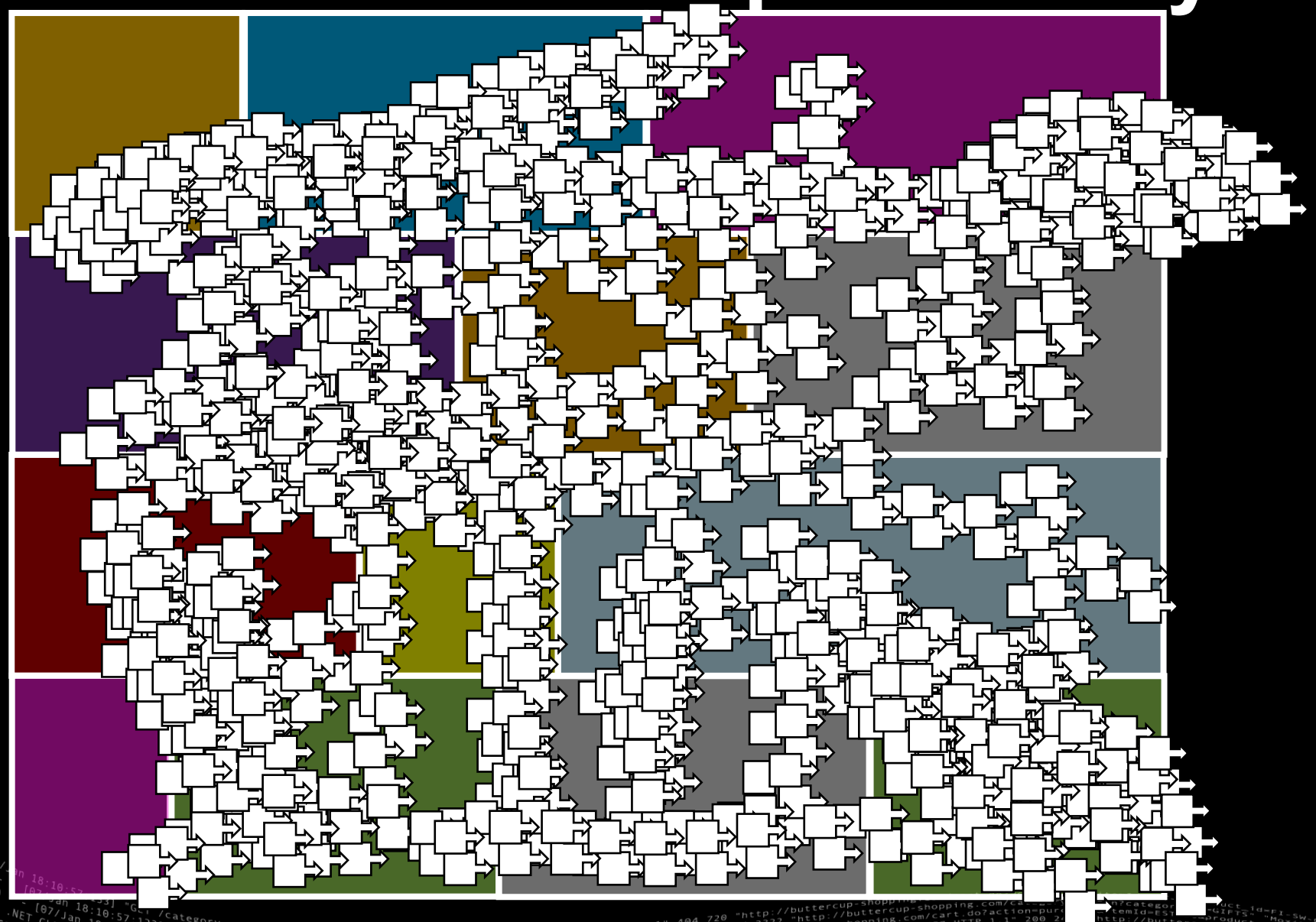
On Demand

Software Defined

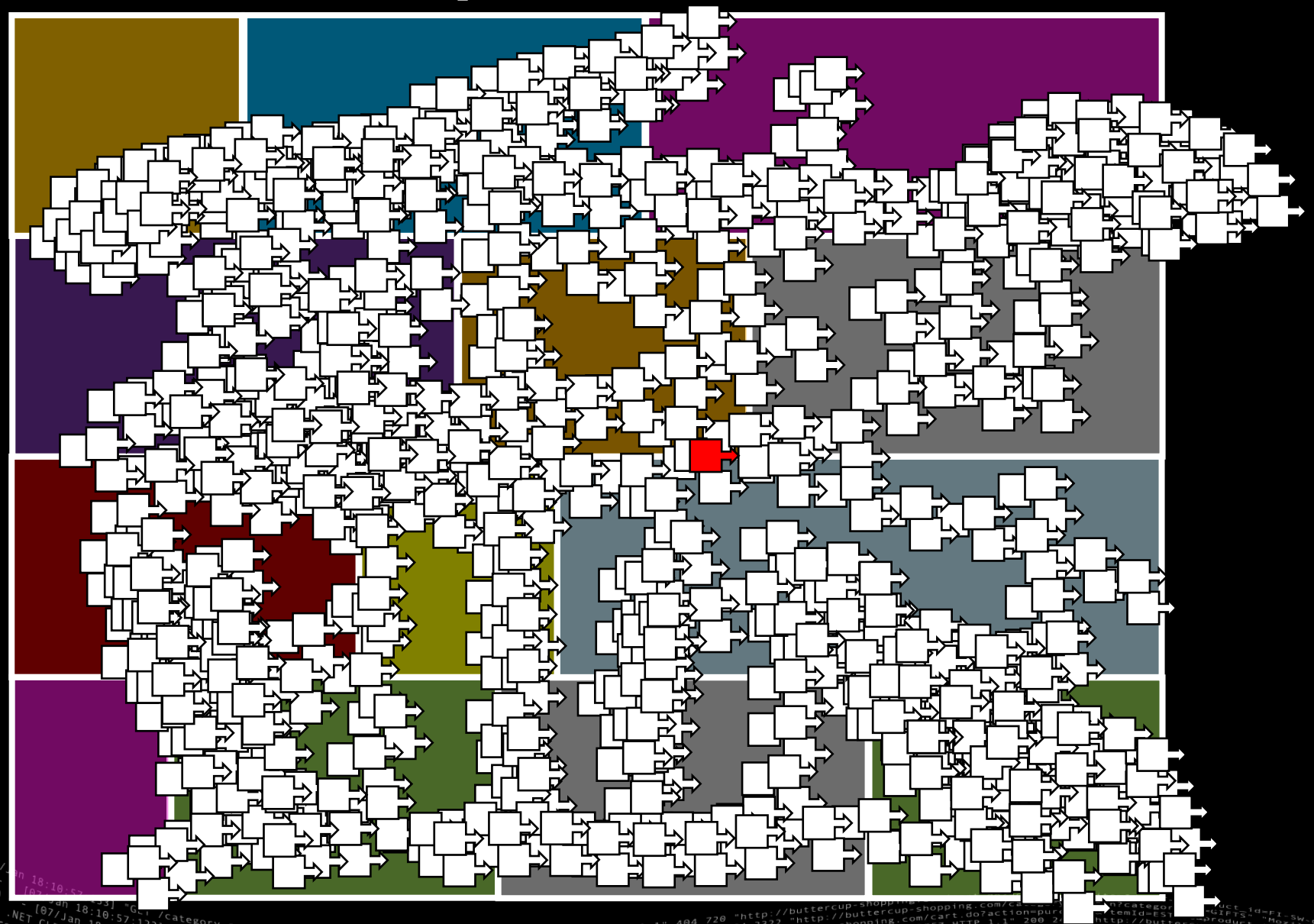
And the number of Events increased--



... Exponentially

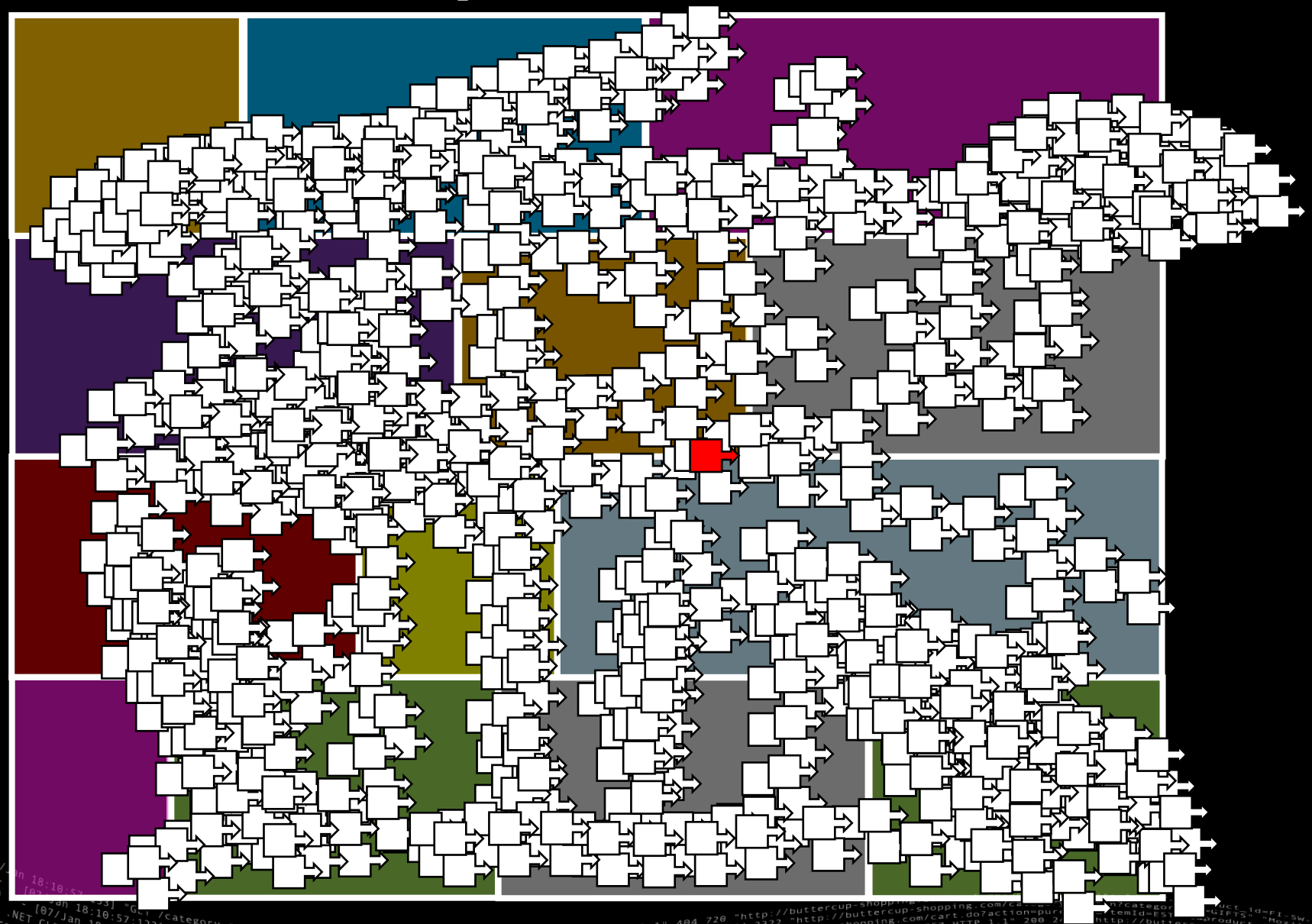


When a component fails in such an environment,



What does it even mean?

When a component fails in such an environment,



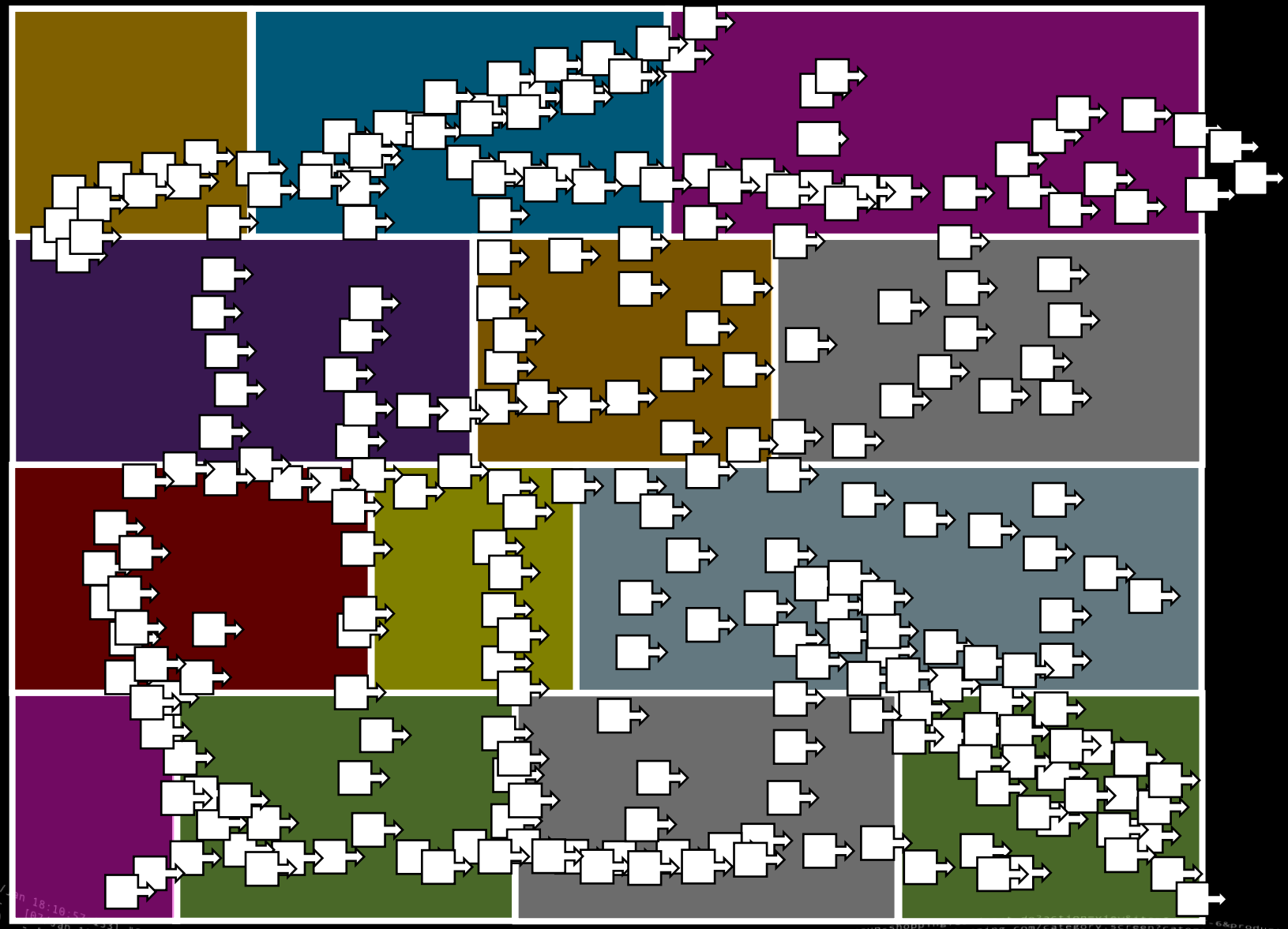
How does it affect the Bottom Line?

splunk> .conf2017

A Story about Denver Traffic

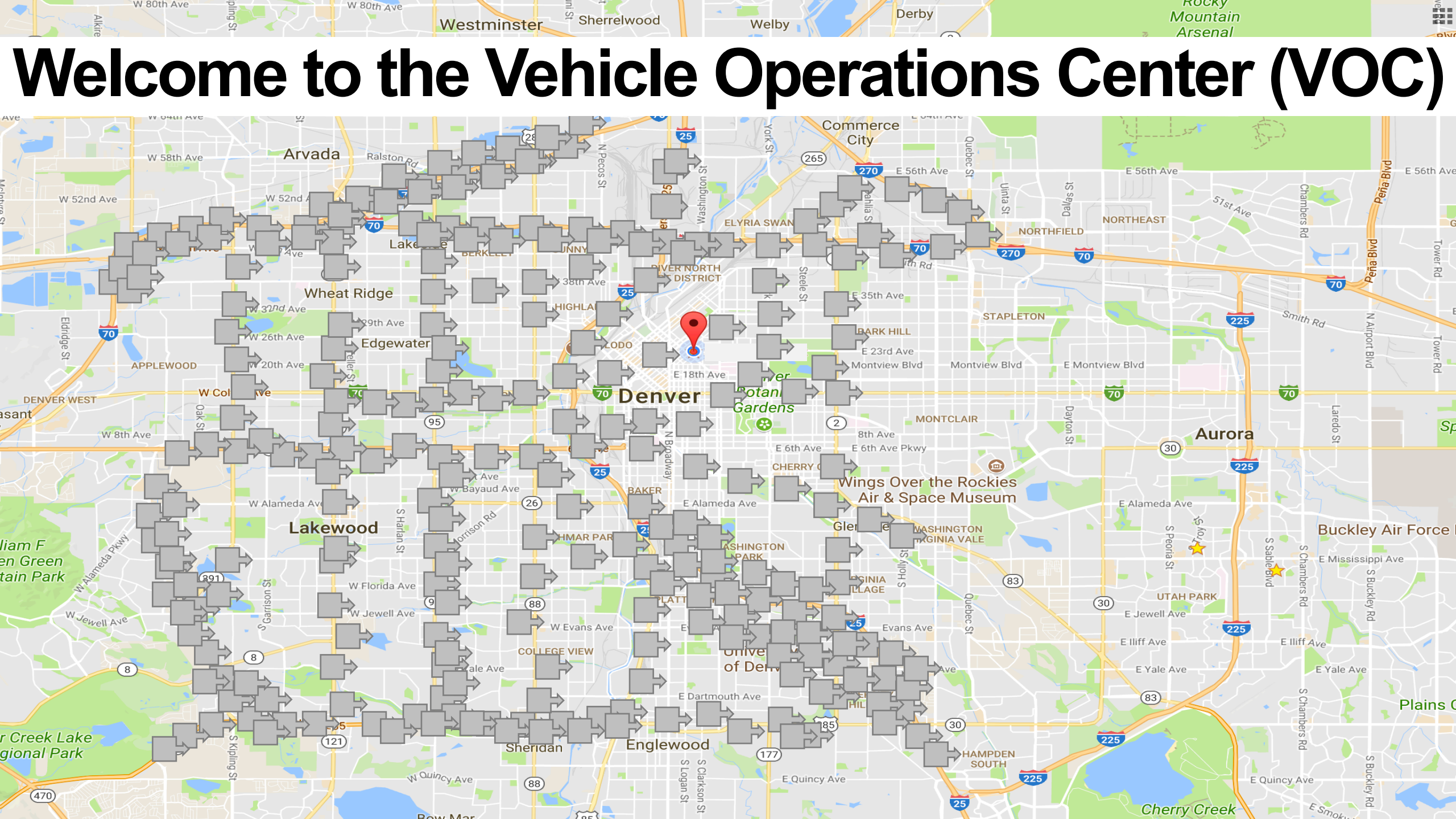
Managing Events is Lot Like Managing Vehicles

splunk> .conf2017

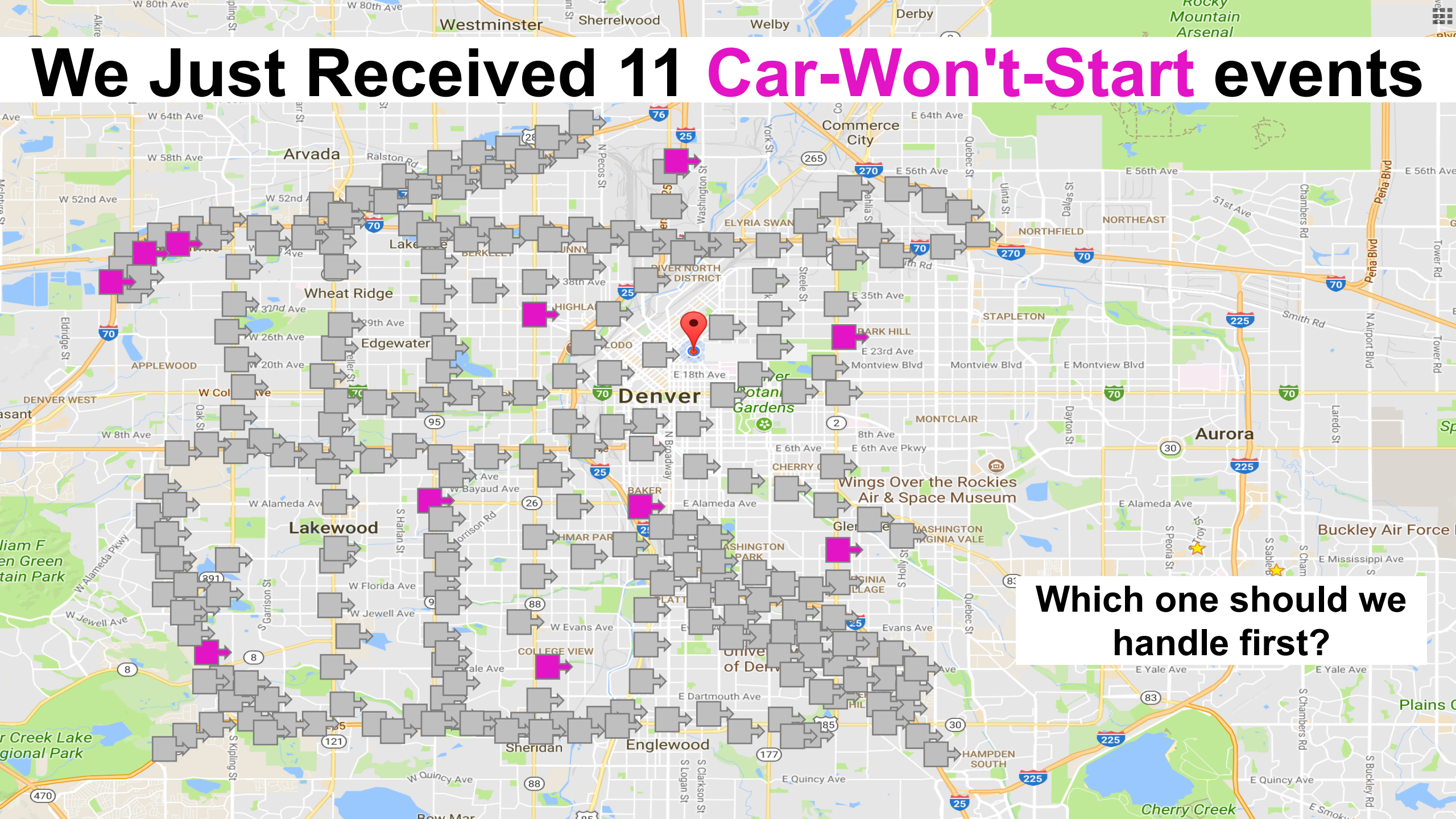


splunk> .conf2017

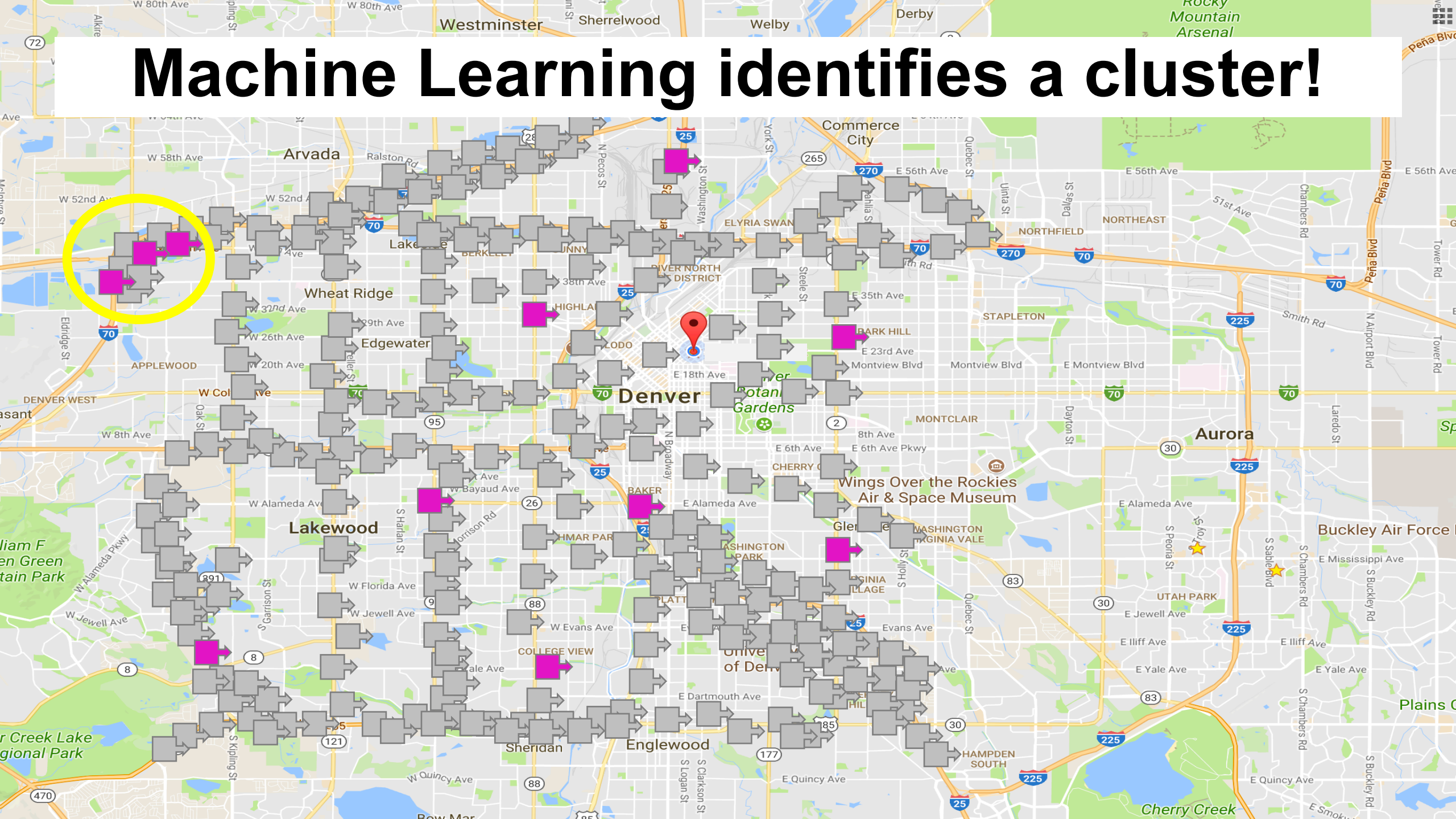
Welcome to the Vehicle Operations Center (VOC)



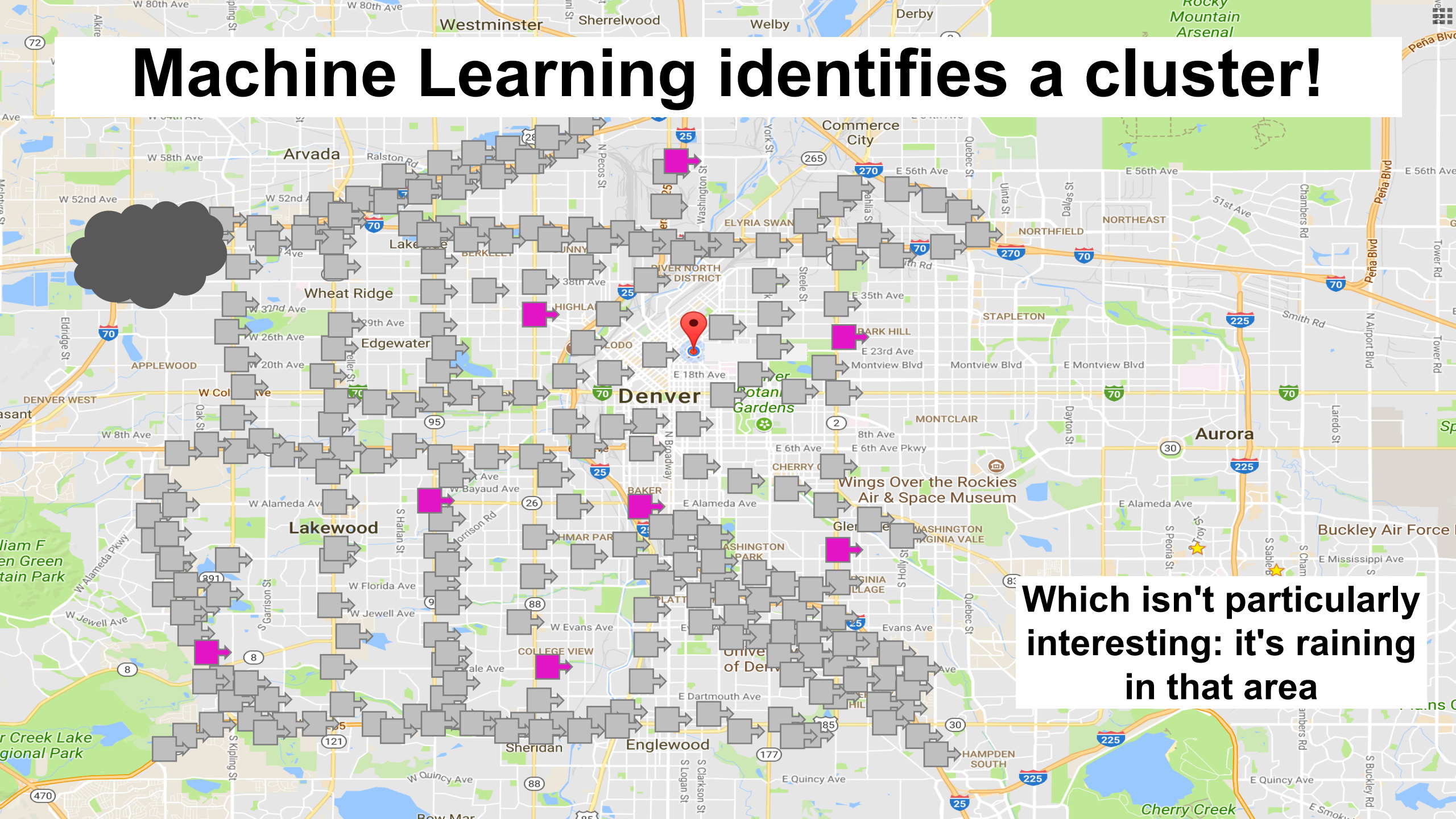
We Just Received 11 Car-Won't-Start events



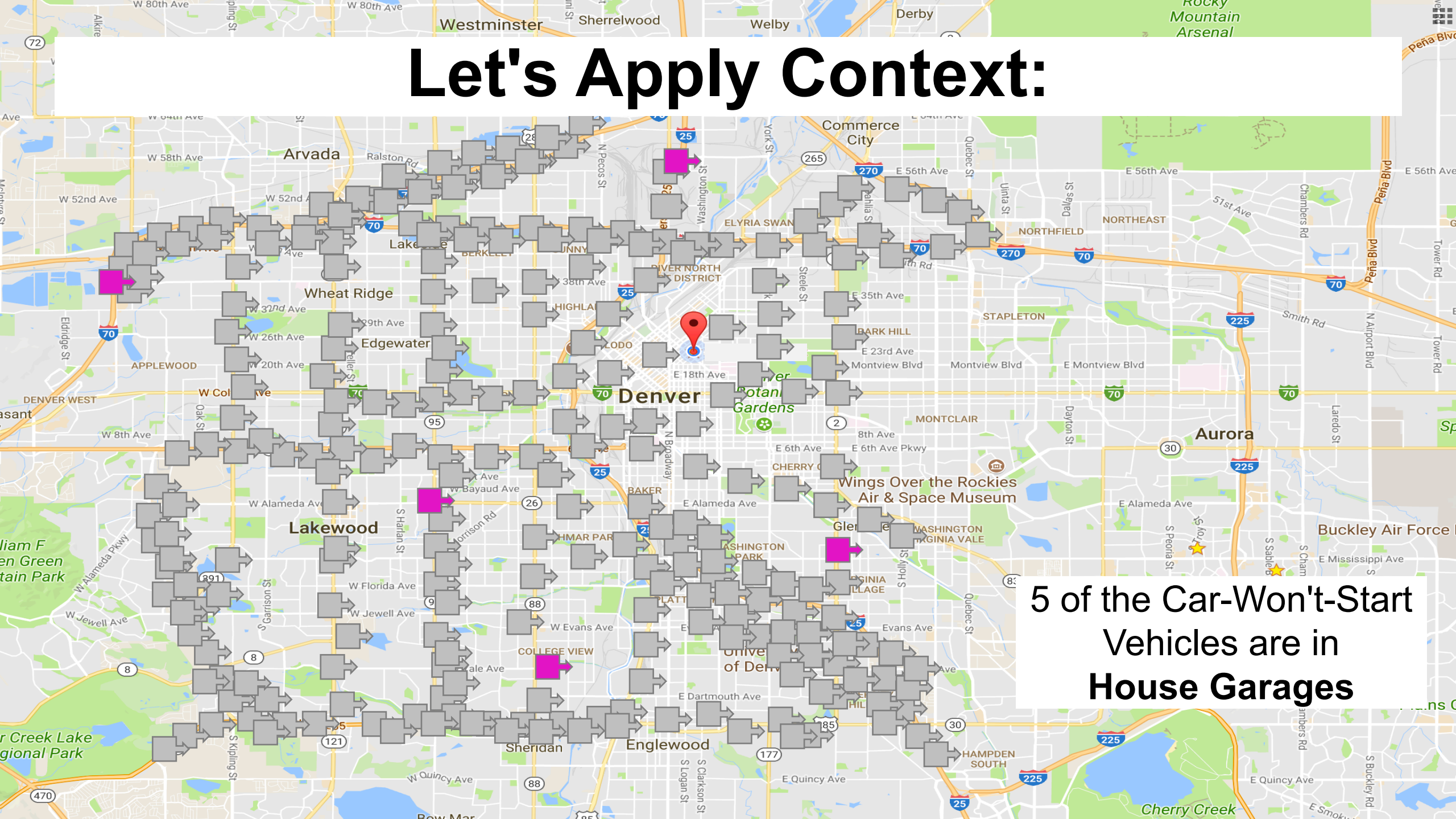
Machine Learning identifies a cluster!



Machine Learning identifies a cluster!



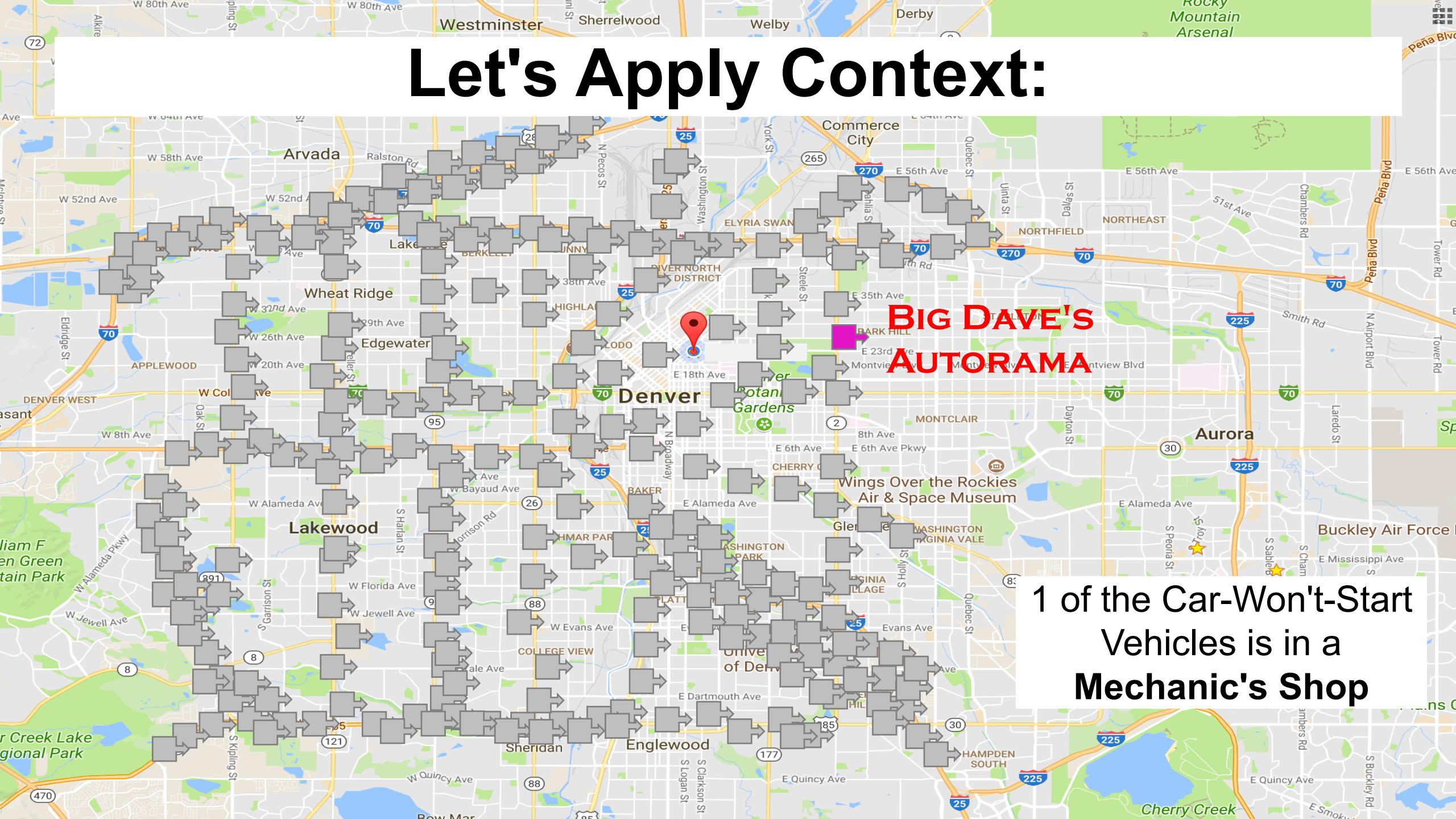
Let's Apply Context:



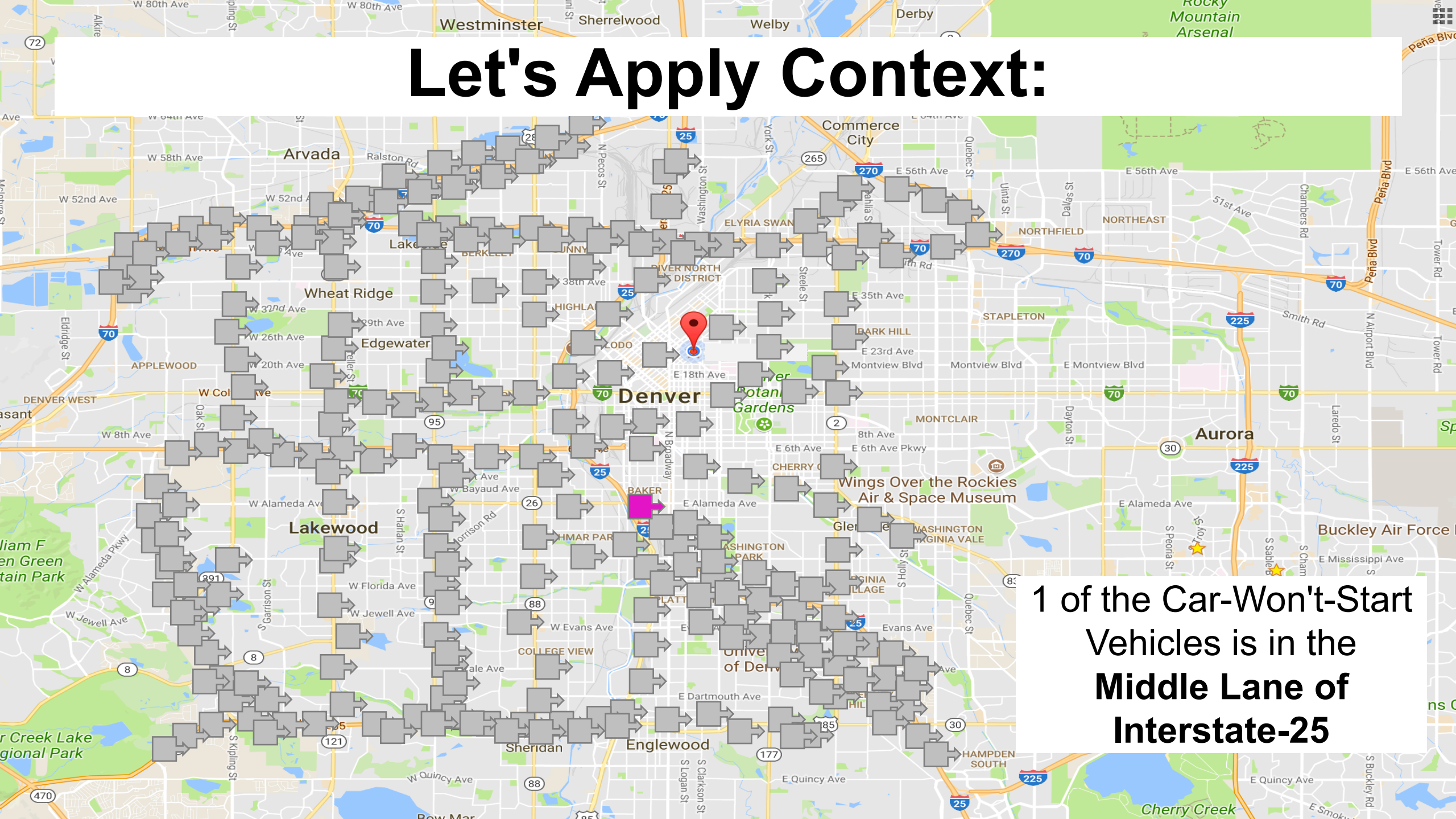
5 of the Car-Won't-Start Vehicles are in **House Garages**

Let's Apply Context:

Let's Apply Context:



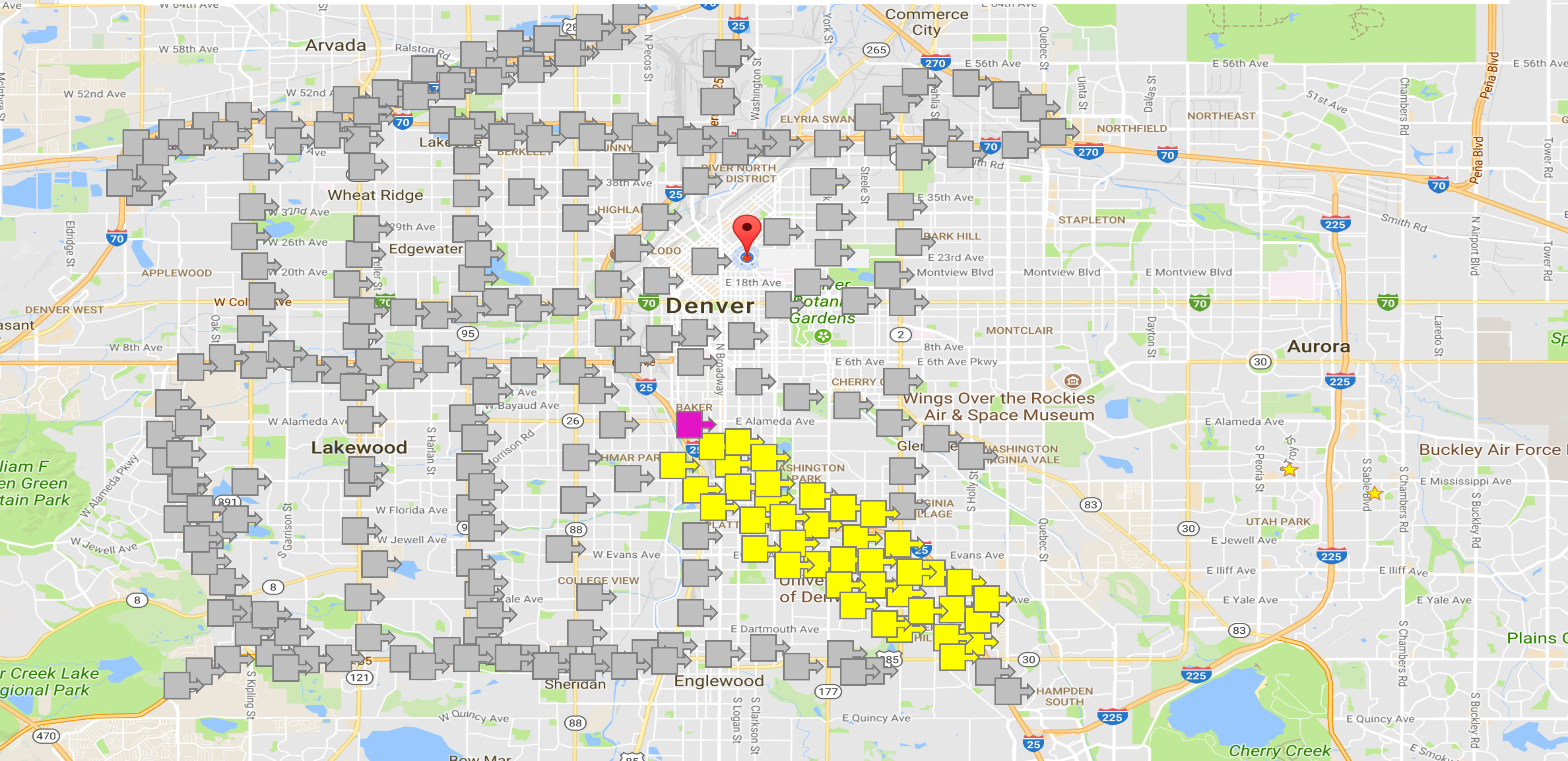
Let's Apply Context:



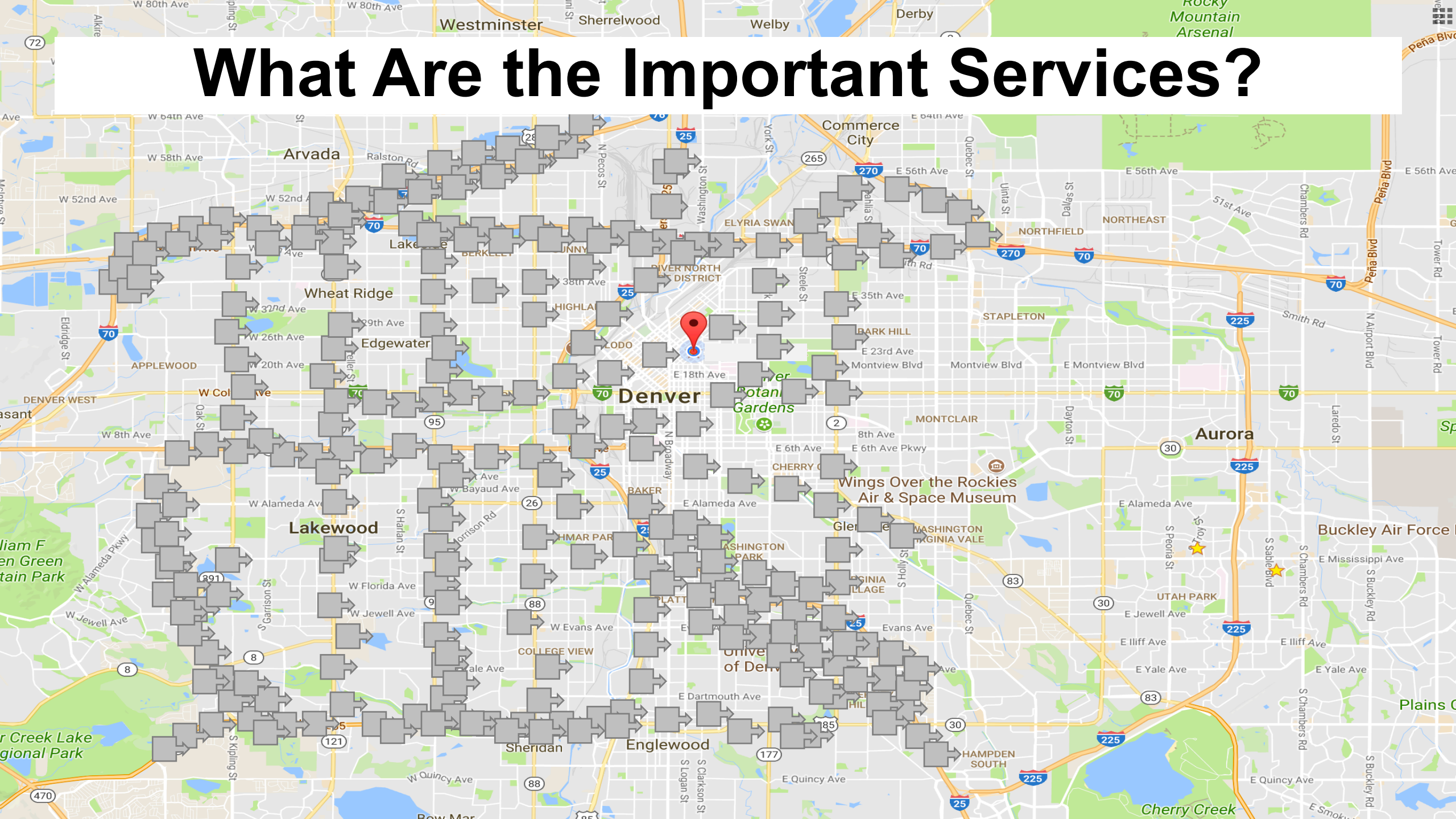
1 of the Car-Won't-Start Vehicles is in the **Middle Lane of Interstate-25**

Which One Should We Handle First?

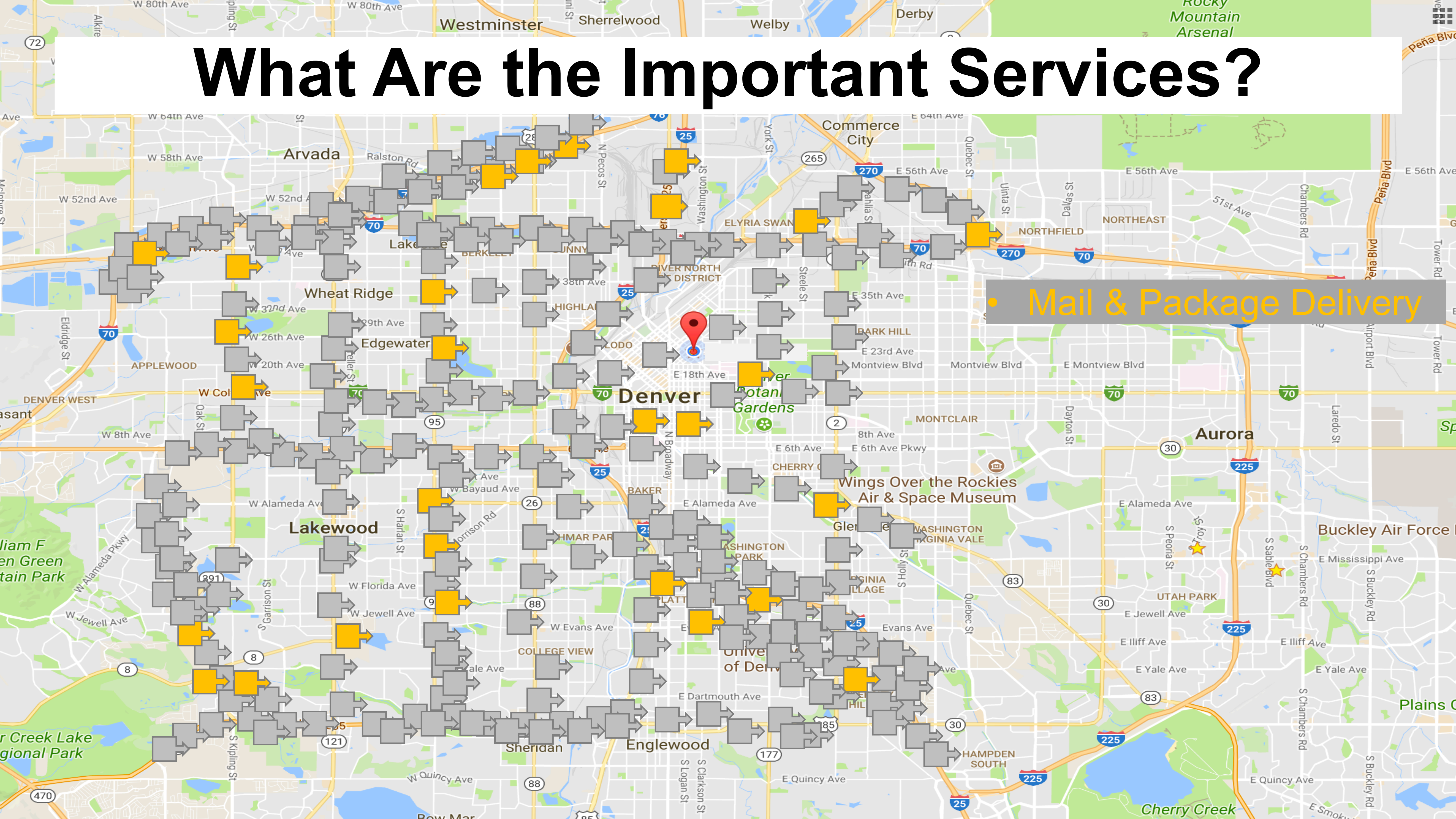
(Service) Context is Everything!



What Are the Important Services?

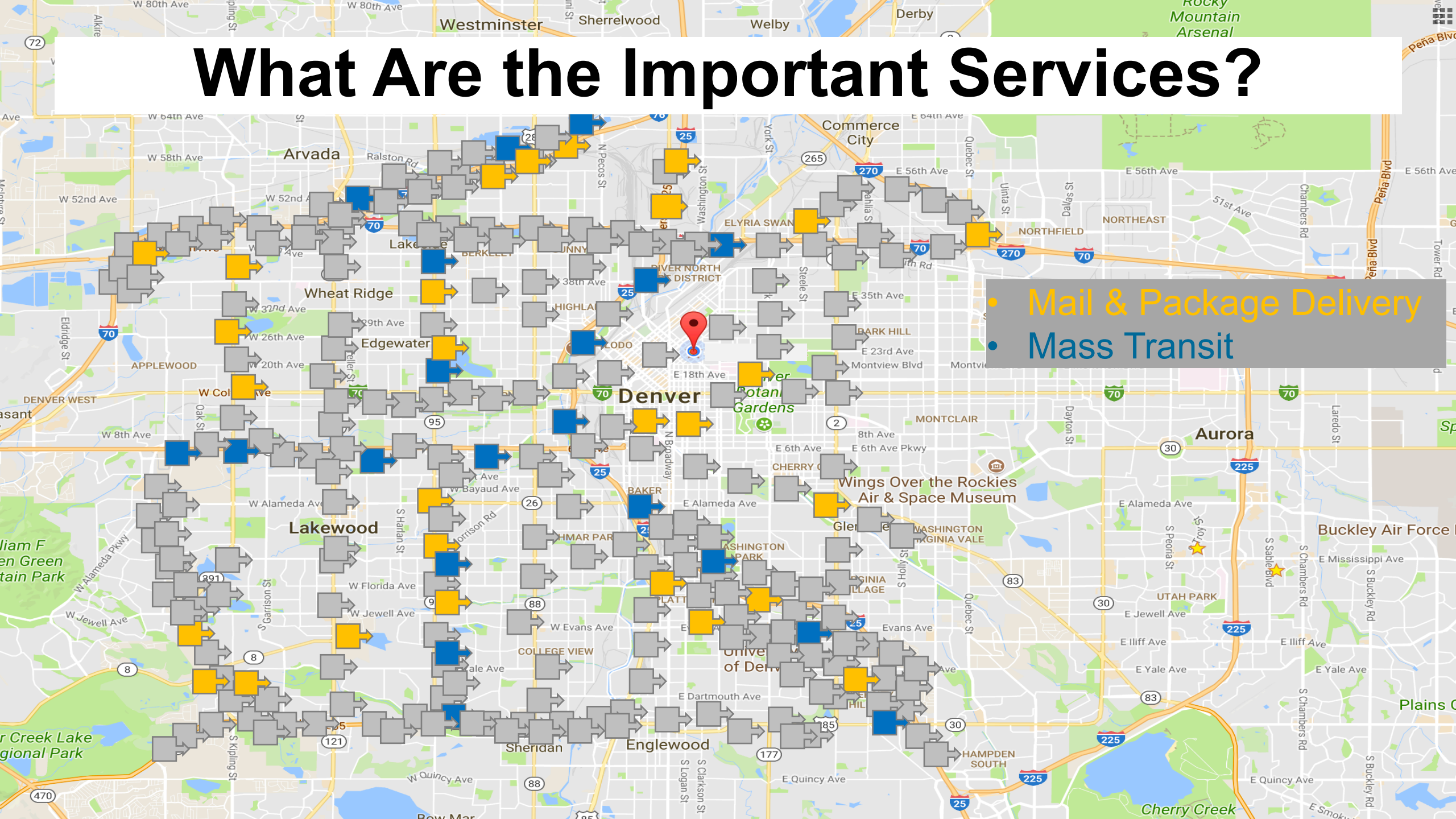


What Are the Important Services?

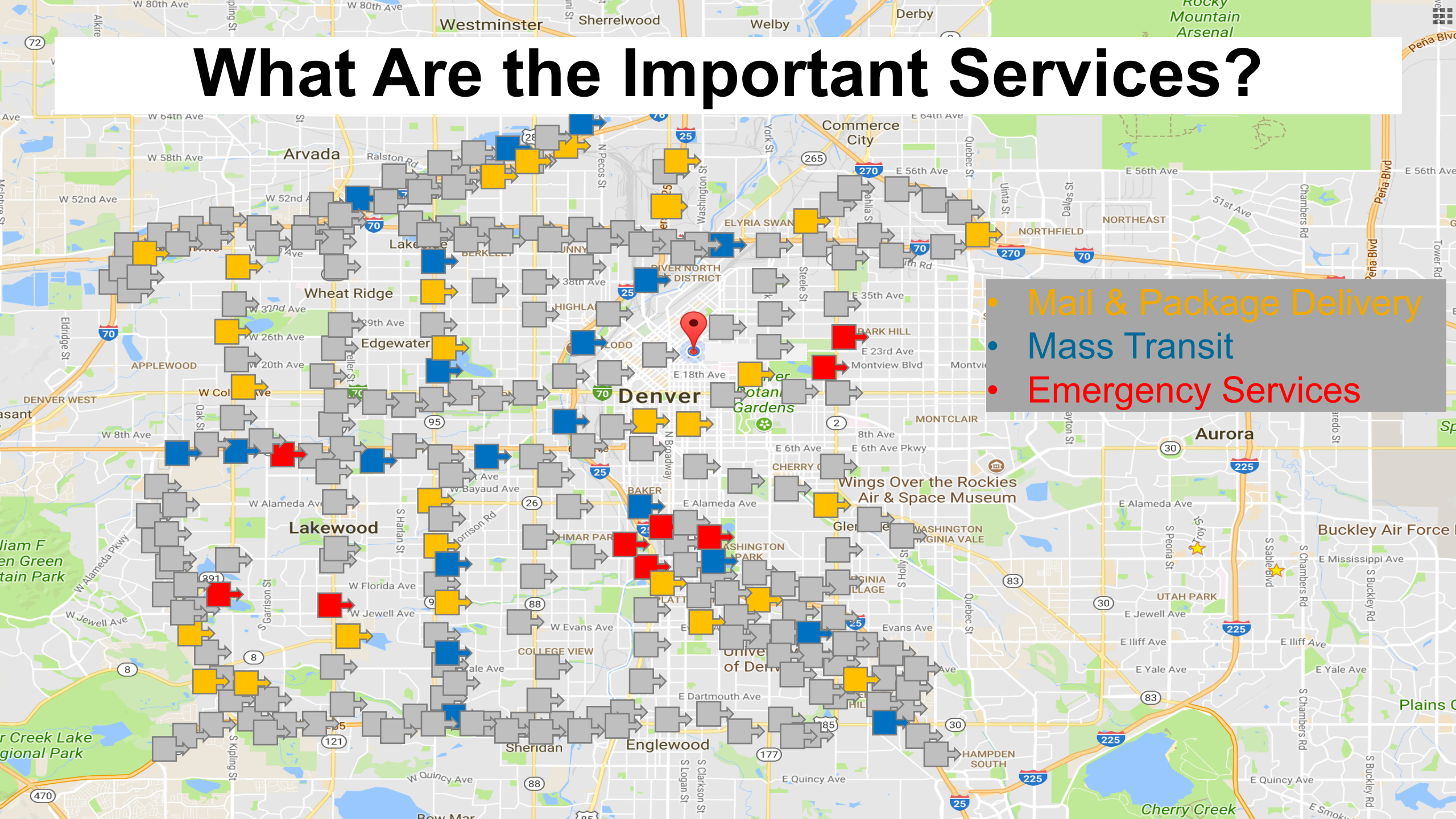


- Mail & Package Delivery

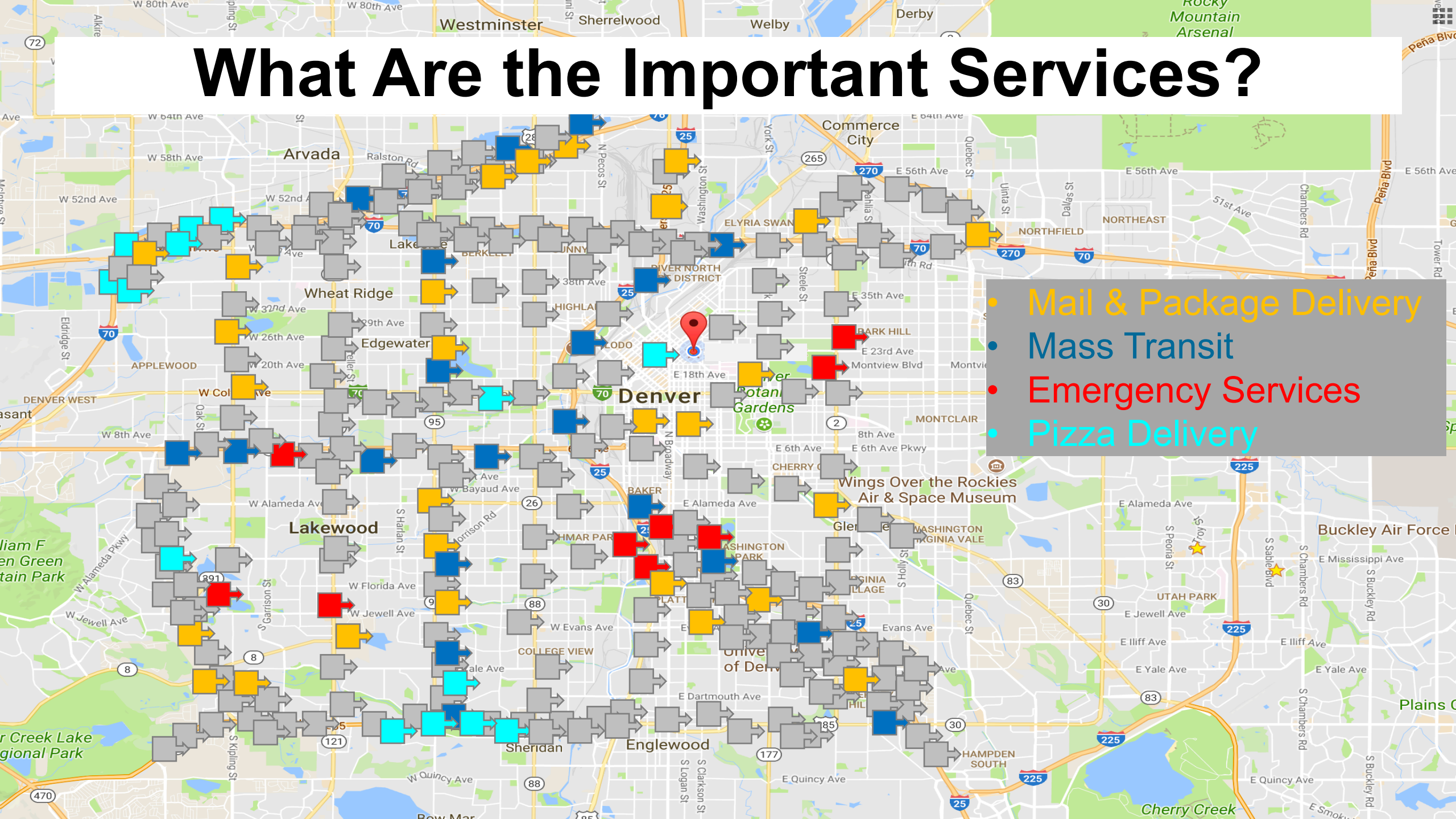
What Are the Important Services?



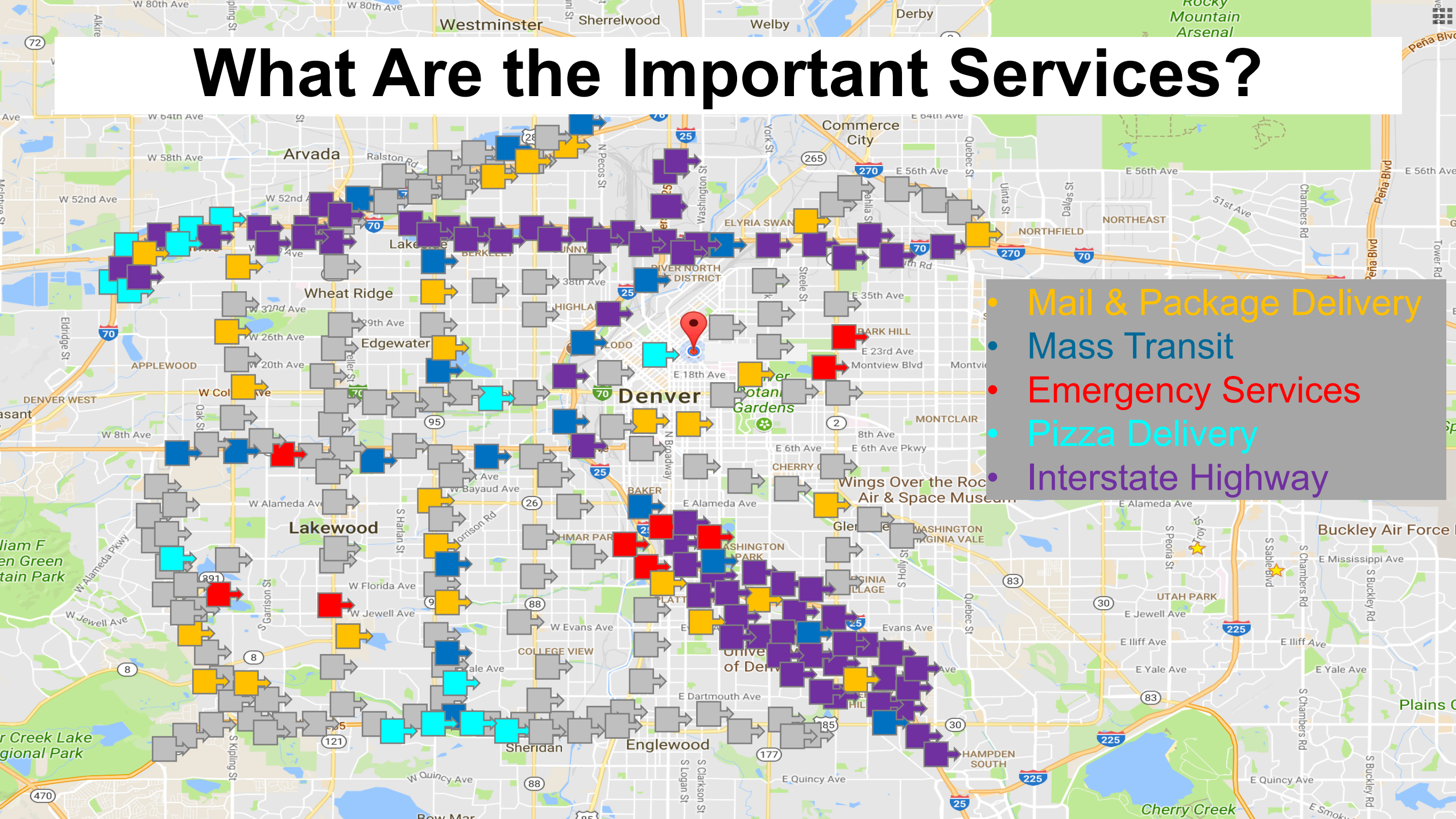
What Are the Important Services?



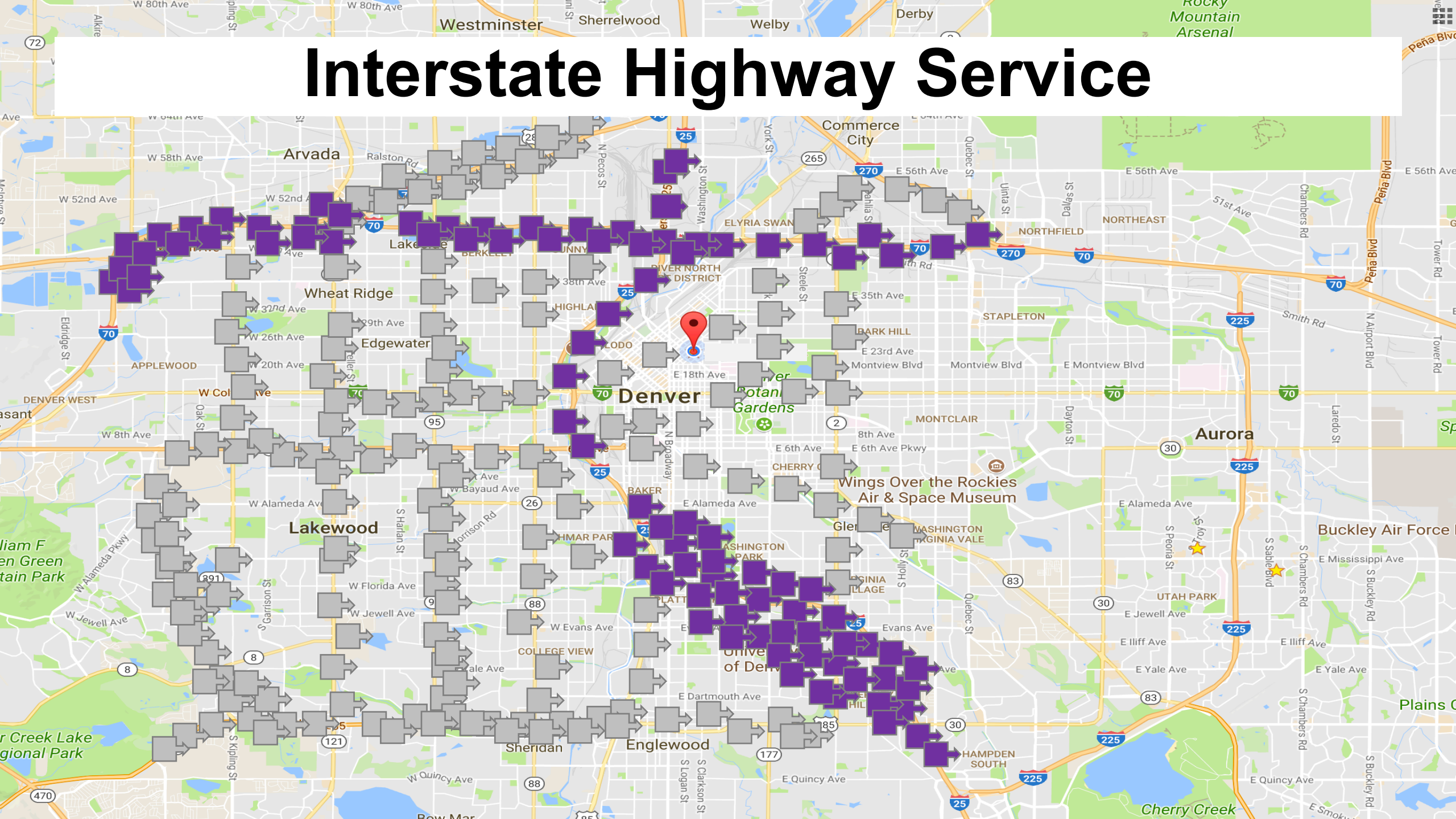
What Are the Important Services?



What Are the Important Services?



Interstate Highway Service



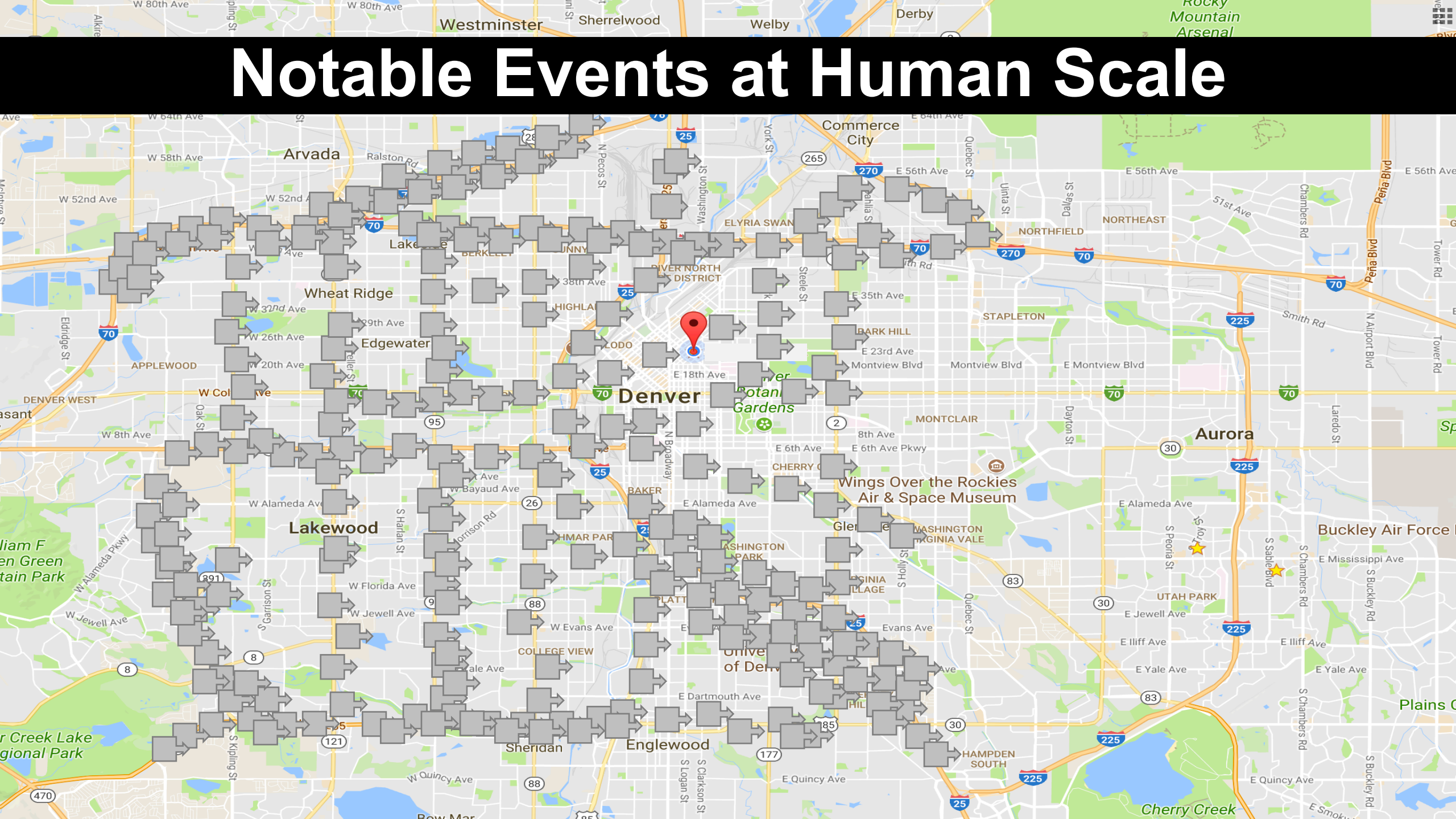
Events Aren't Enough

Metrics, Logged and Wire Data Fill In the Blind Spots

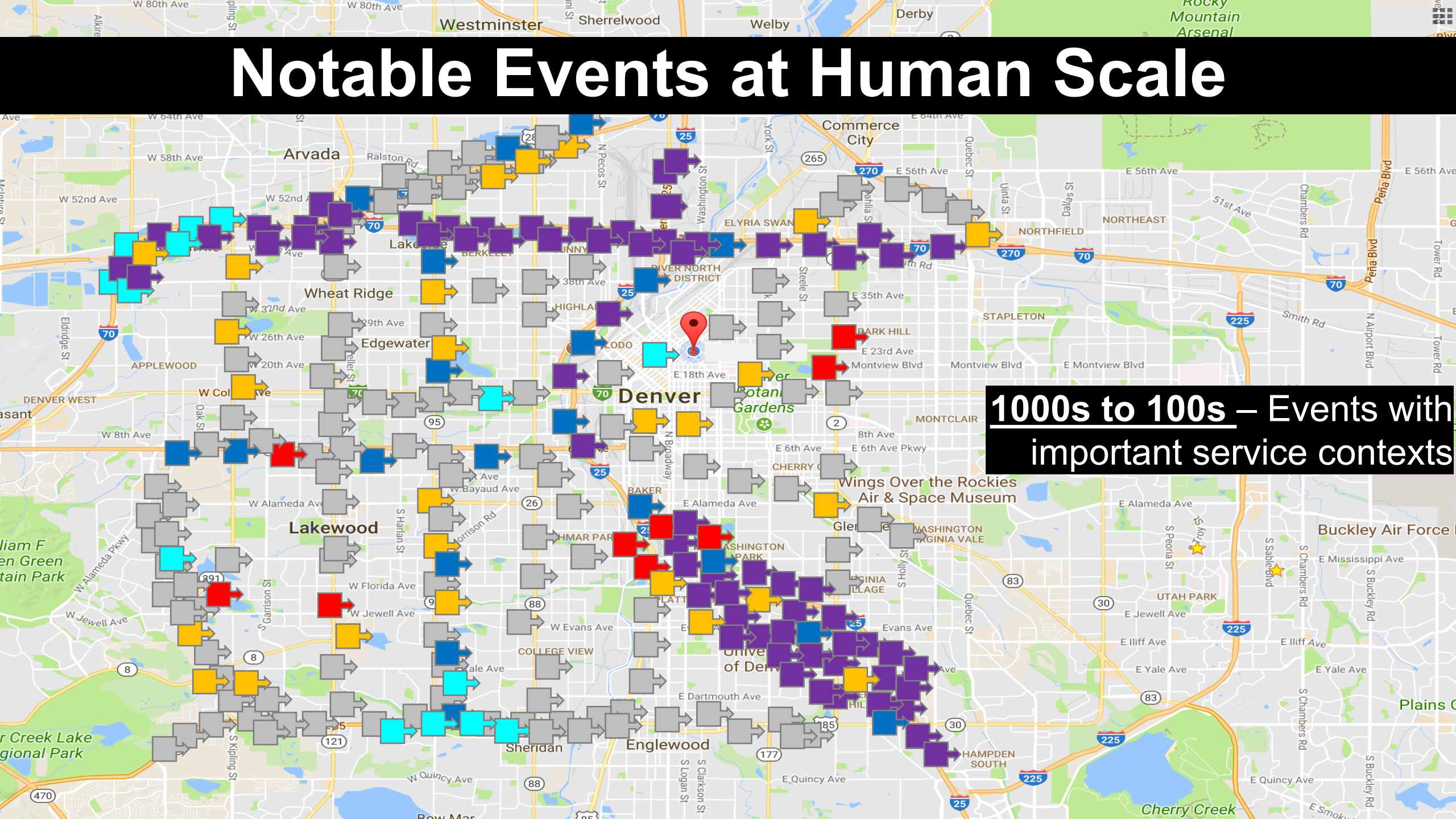
- Creative KPIs allow us to move beyond traditional events
  - KPI: Average vehicle speed (metric data)
  - KPI: Vehicle throughput (wire data)
  - KPI: Count of 911 calls tagged with "Interstate-25" (logged data)
- Machine Learning –based thresholding allows us to see "normal" vs "not normal"
  - Slower vehicle speeds during rush hour are normal

splunk> .conf2017

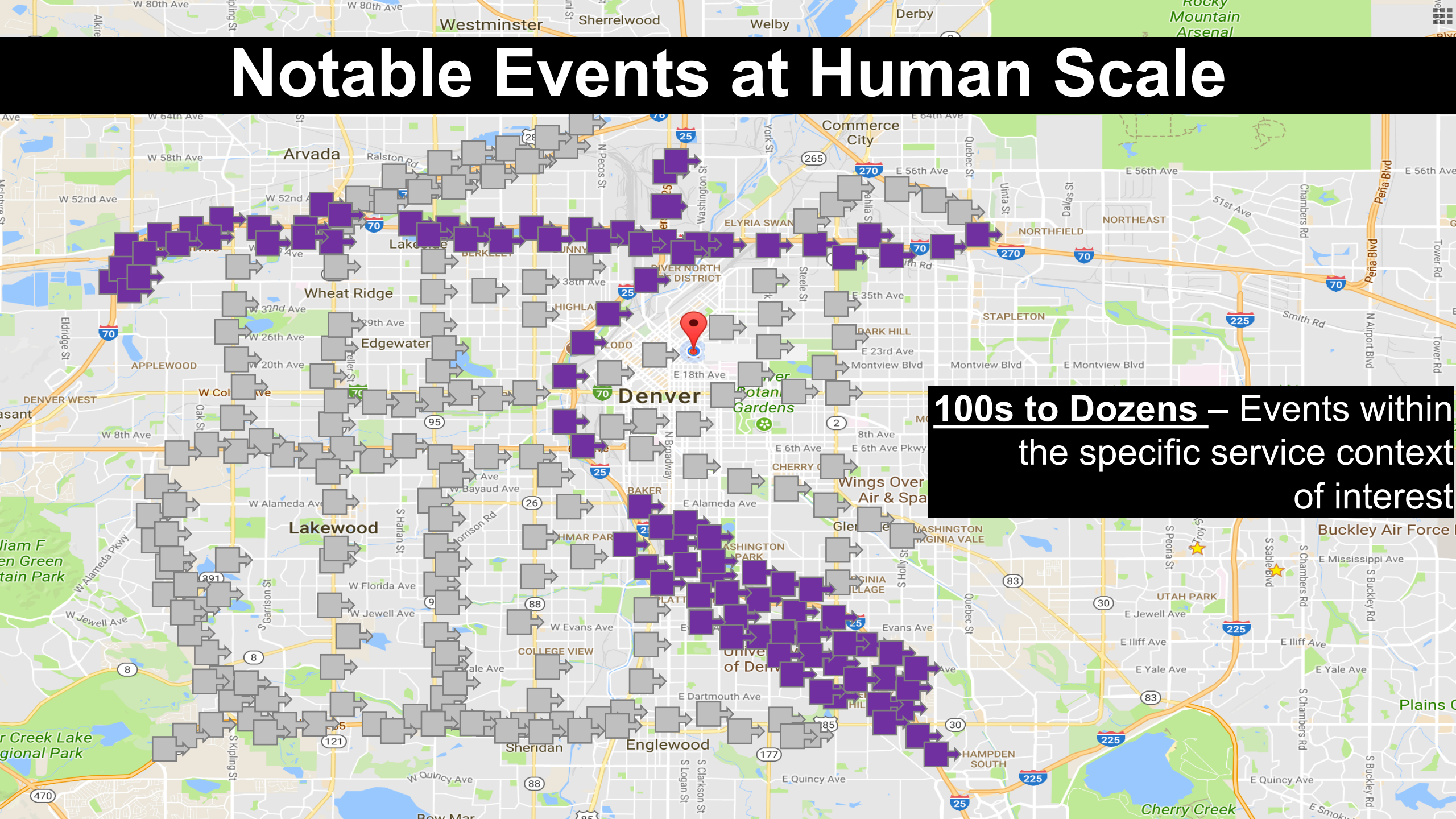
Notable Events at Human Scale



Notable Events at Human Scale

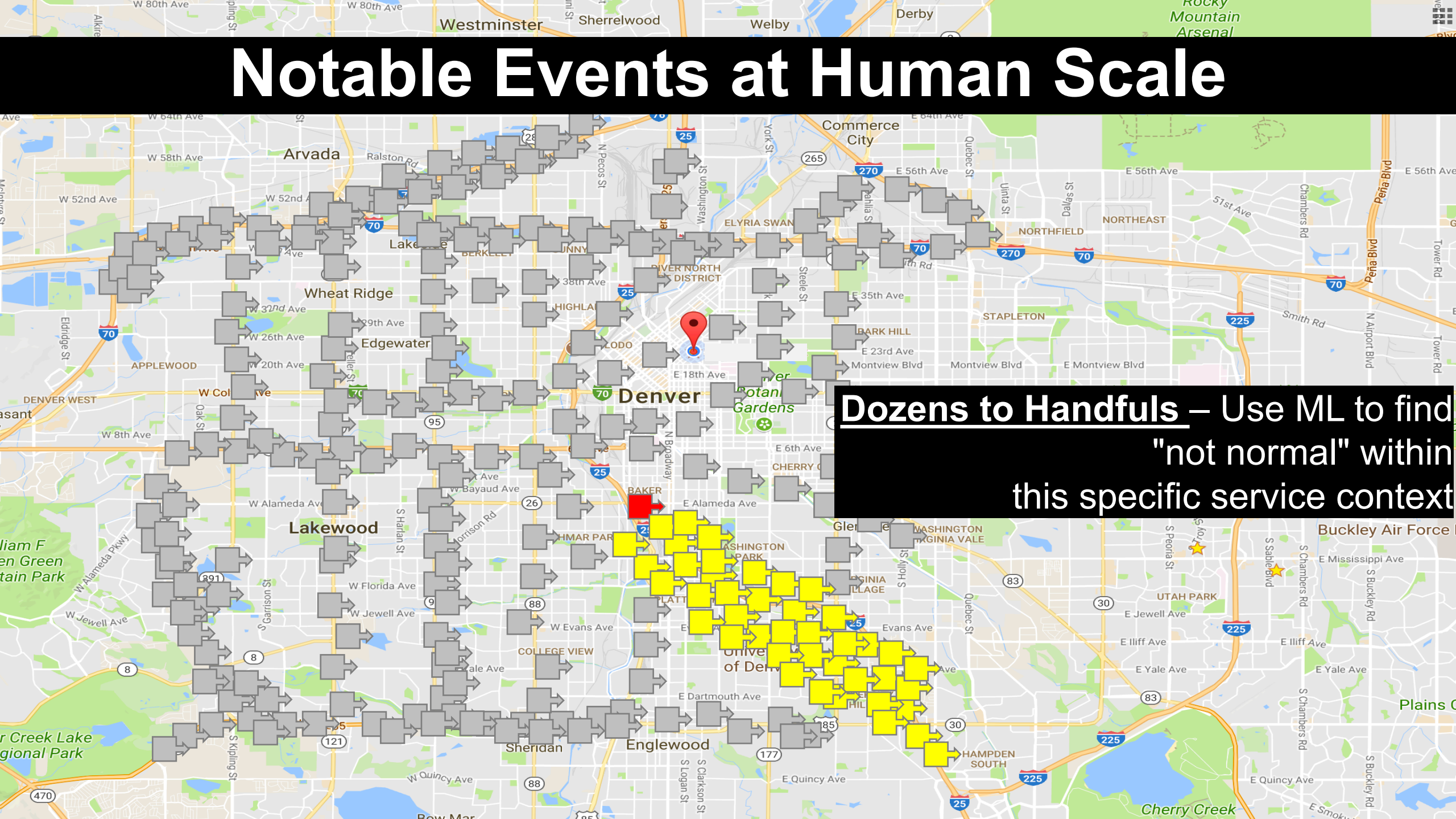


Notable Events at Human Scale

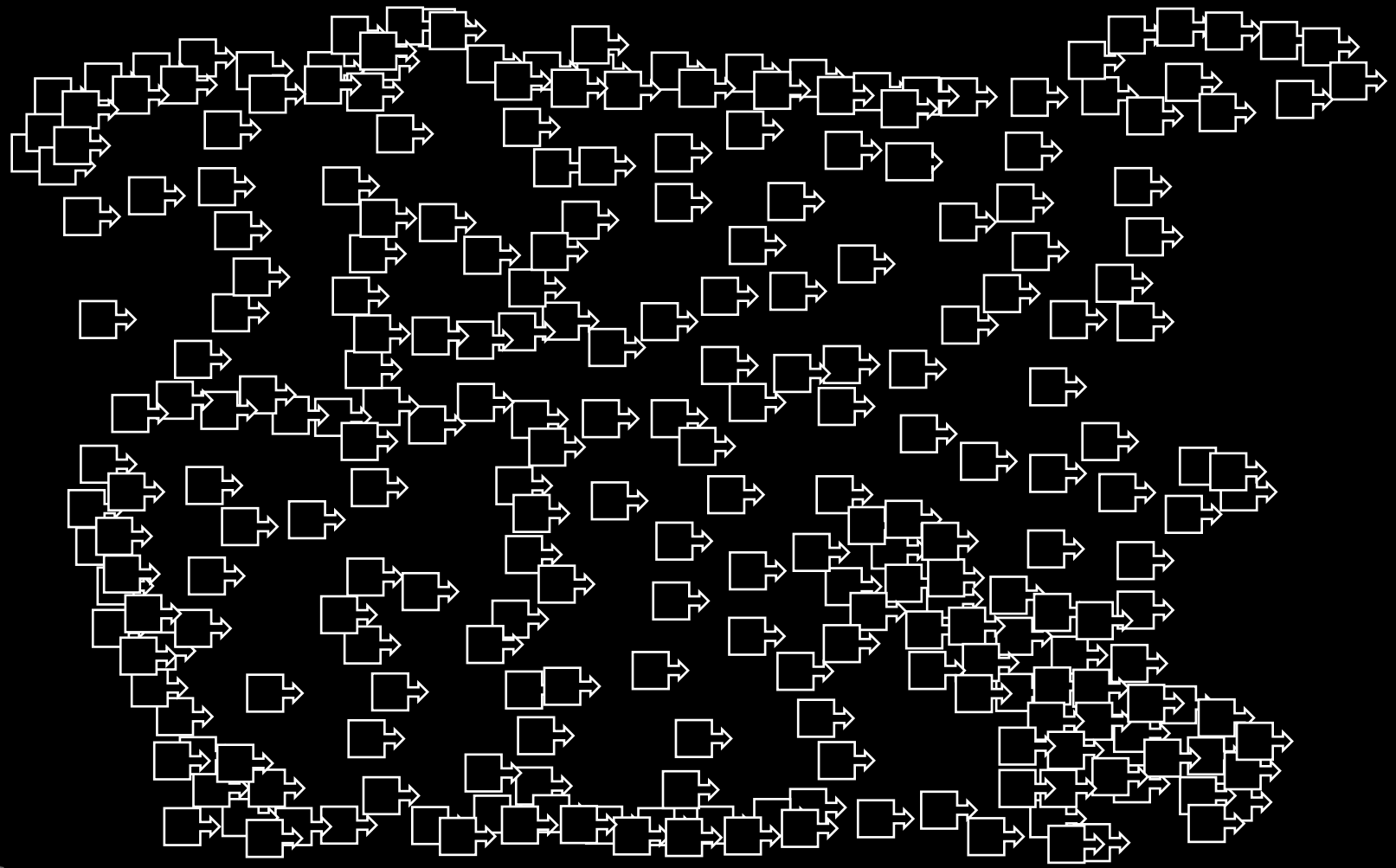


100s to Dozens – Events within the specific service context of interest

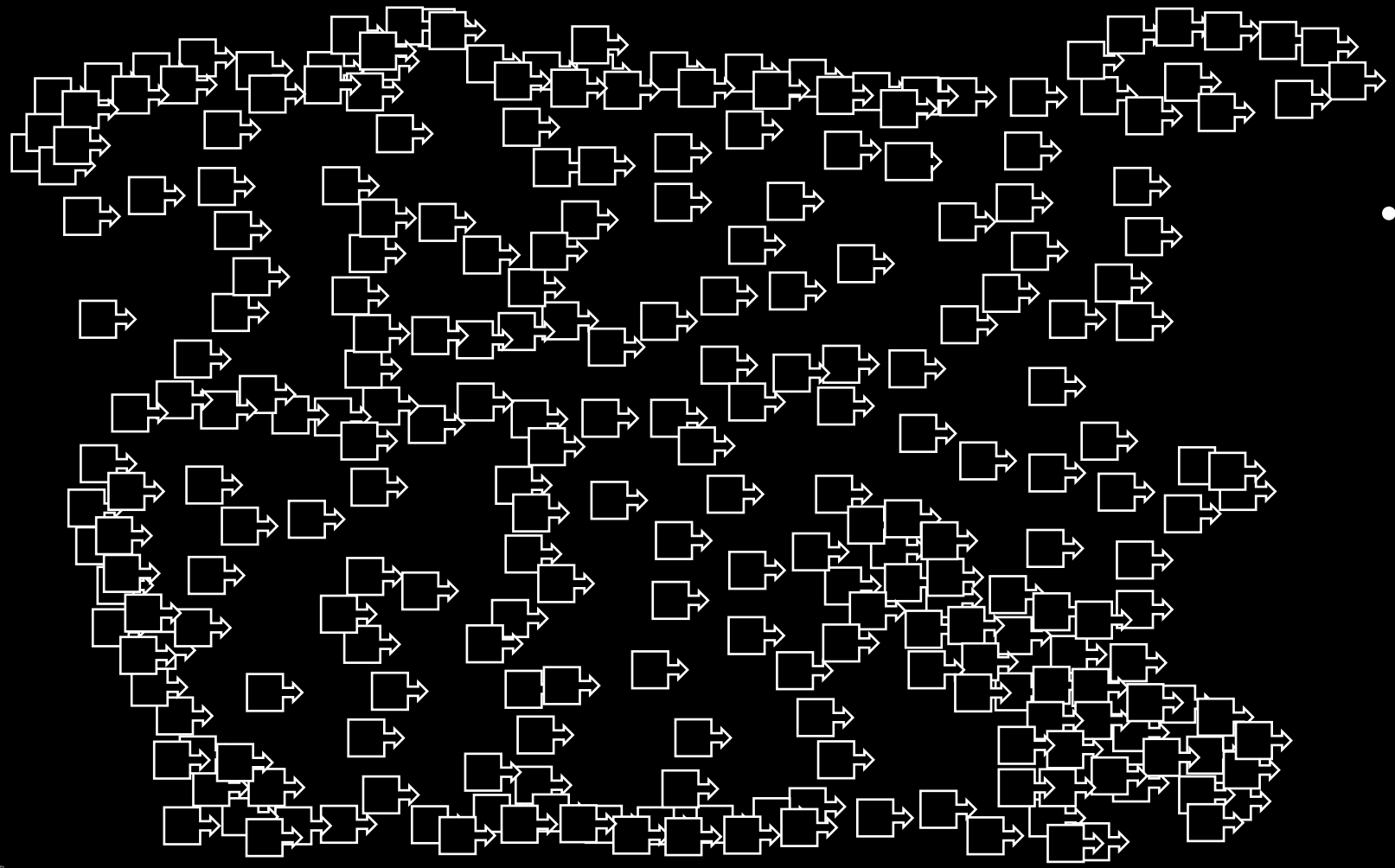
Notable Events at Human Scale



The Old IT Ways Don't Work Anymore

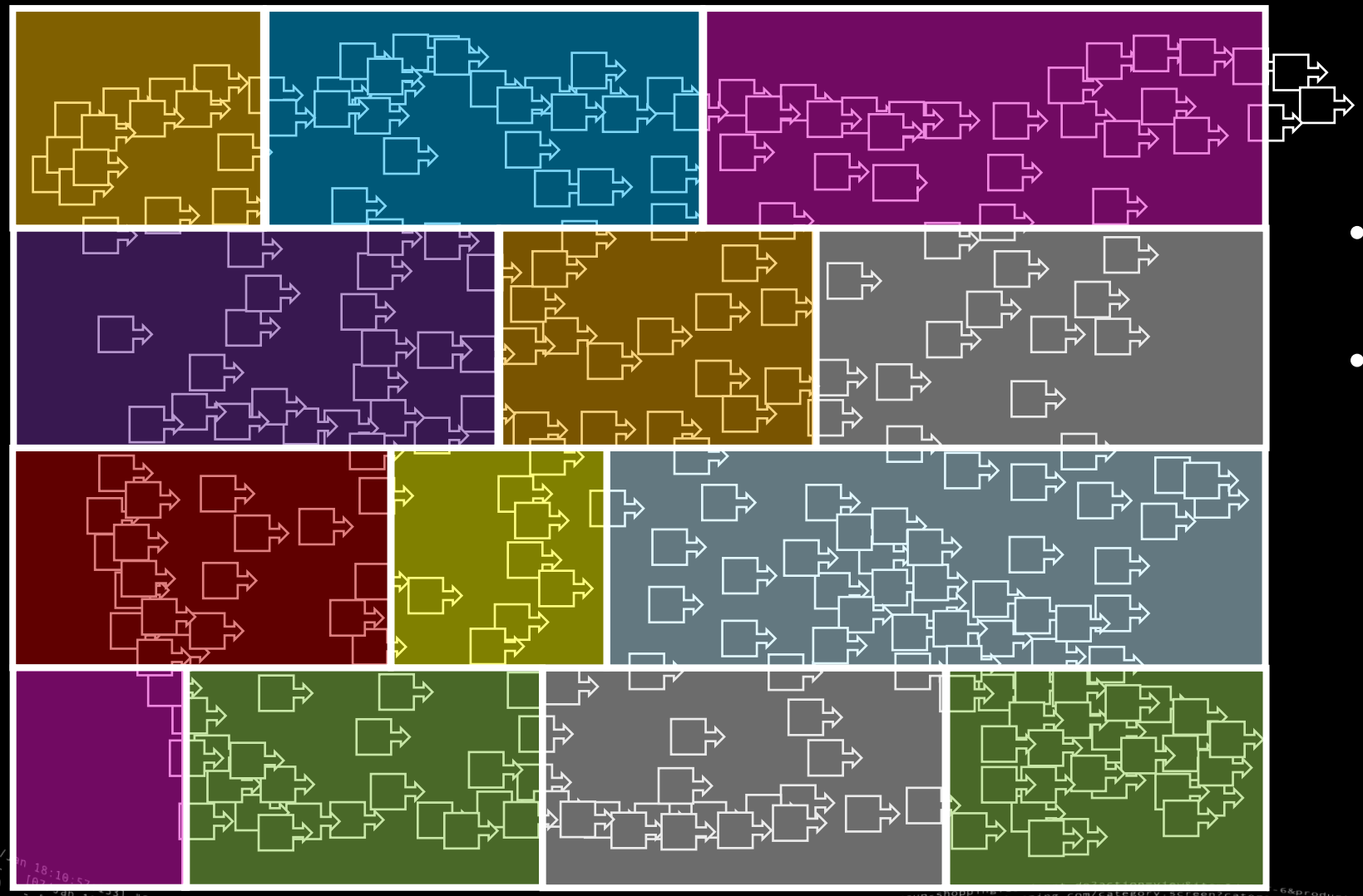


The Old IT Ways Don't Work Anymore



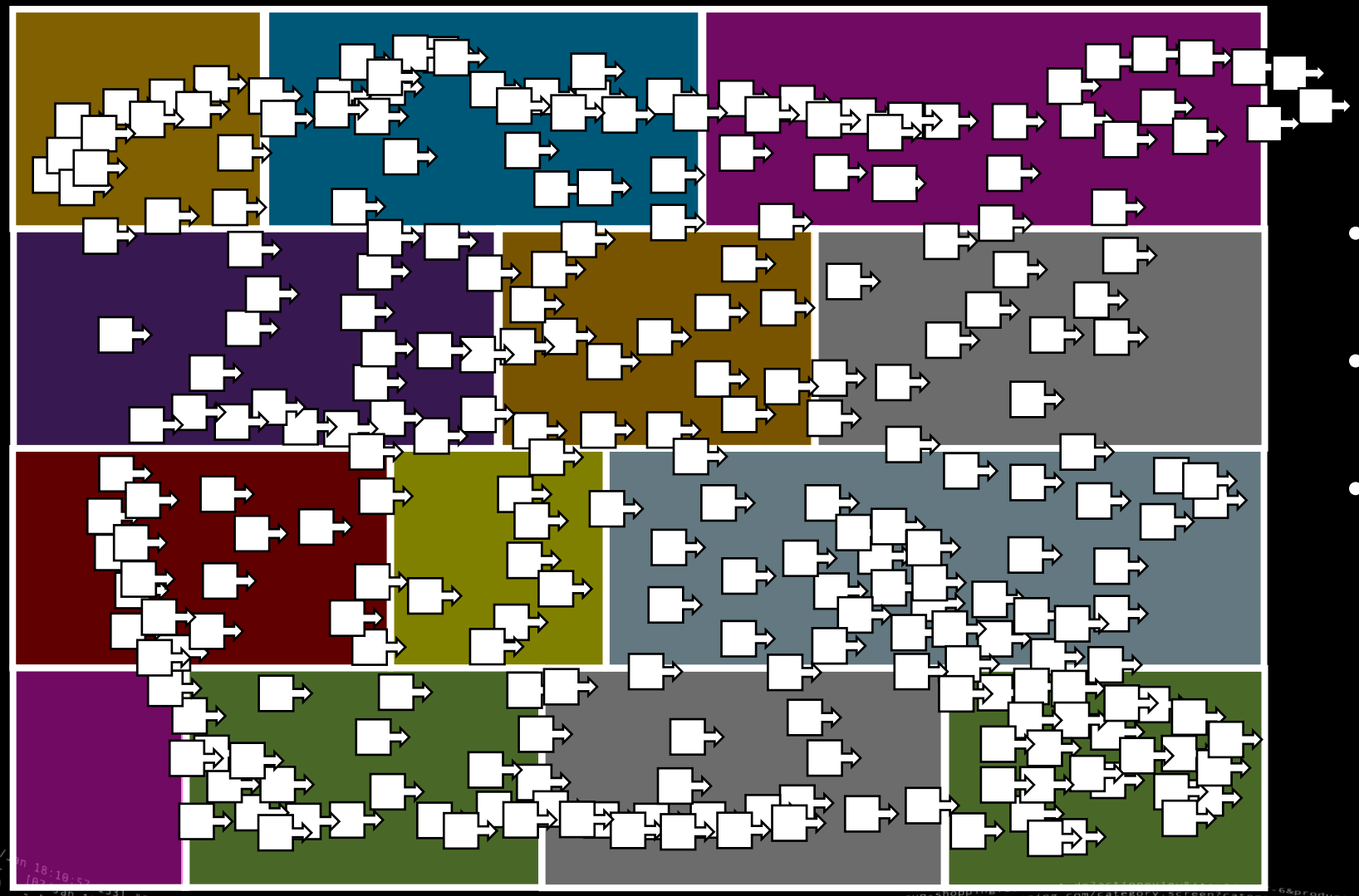
- Event Fatigue

The Old IT Ways Don't Work Anymore



- Event Fatigue
- Complex Environments

The Old IT Ways Don't Work Anymore



- Event Fatigue
- Complex Environments
- Components multiply, Silos abound

Help!

- Which busted components should we focus on?
- When a component fails in such a complex environment, what does it even mean?
- What important services are impacted, if any?
- How do we identify those failures which are actually impacting the business-- customers, clients & revenue?

Machine Learning Won't Save Us

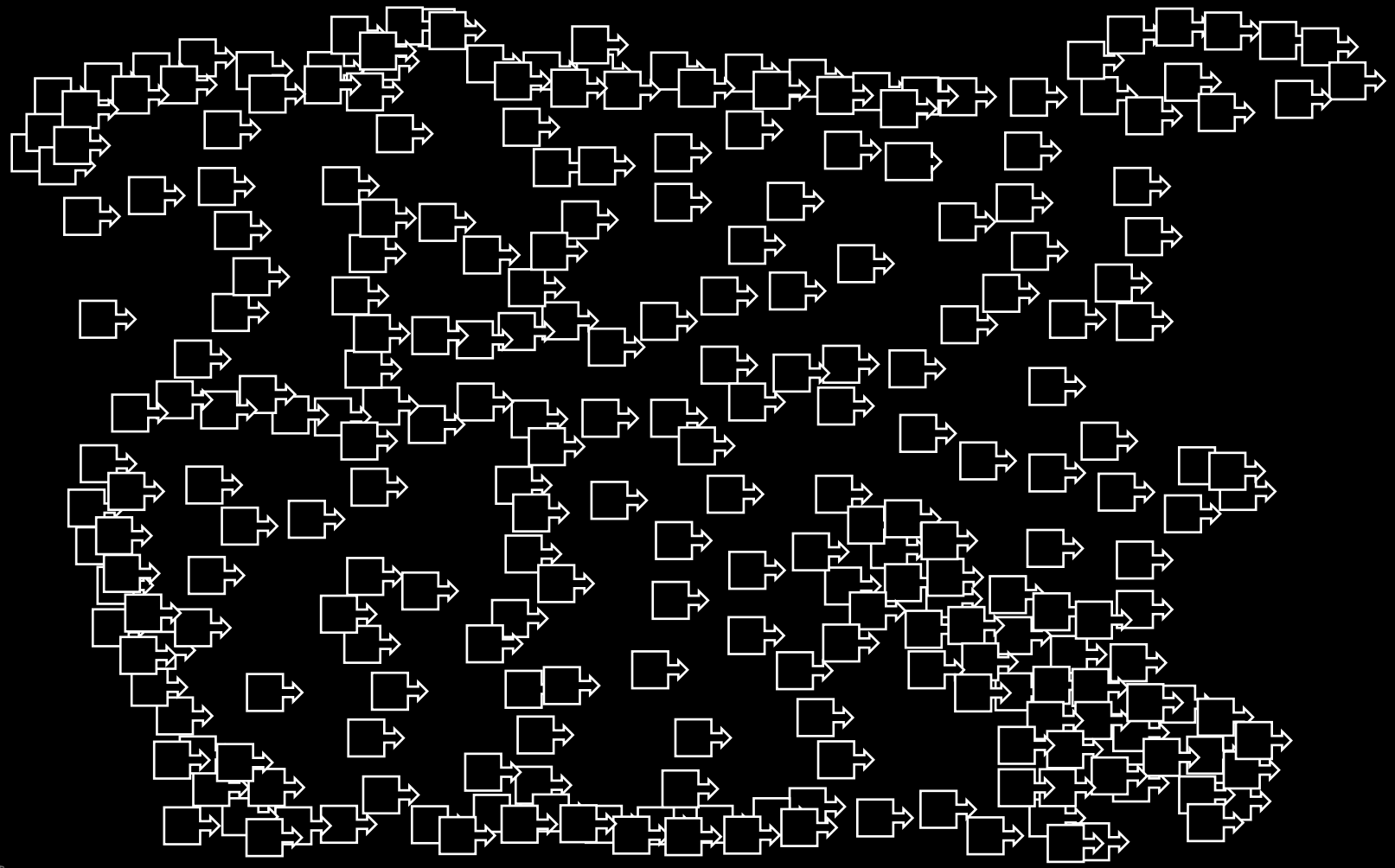
- ML is the latest approach to magically reduce the huge volume to find that "elusive root cause event"
- ML IS a powerful new capability which can be useful, but...
- ML alone will not solve our fundamental problems
- Without a service context, adding ML to the old deluge of events isn't enough

A Better Way: Splunk ITSI for Event Analytics

splunk> .conf2017

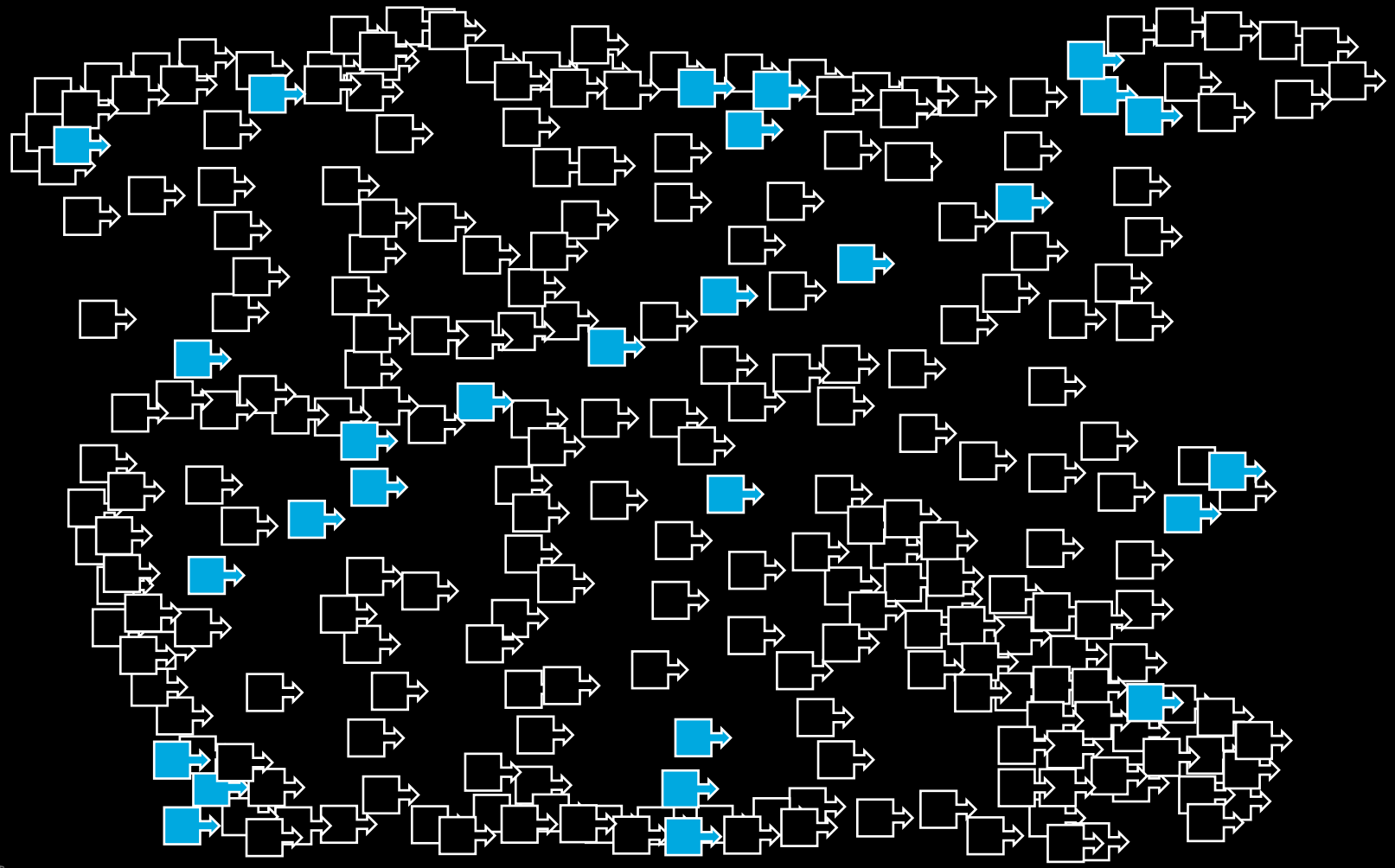
Apply a Flexible Service Context

Focusing on High Value Services



Apply a Flexible Service Context

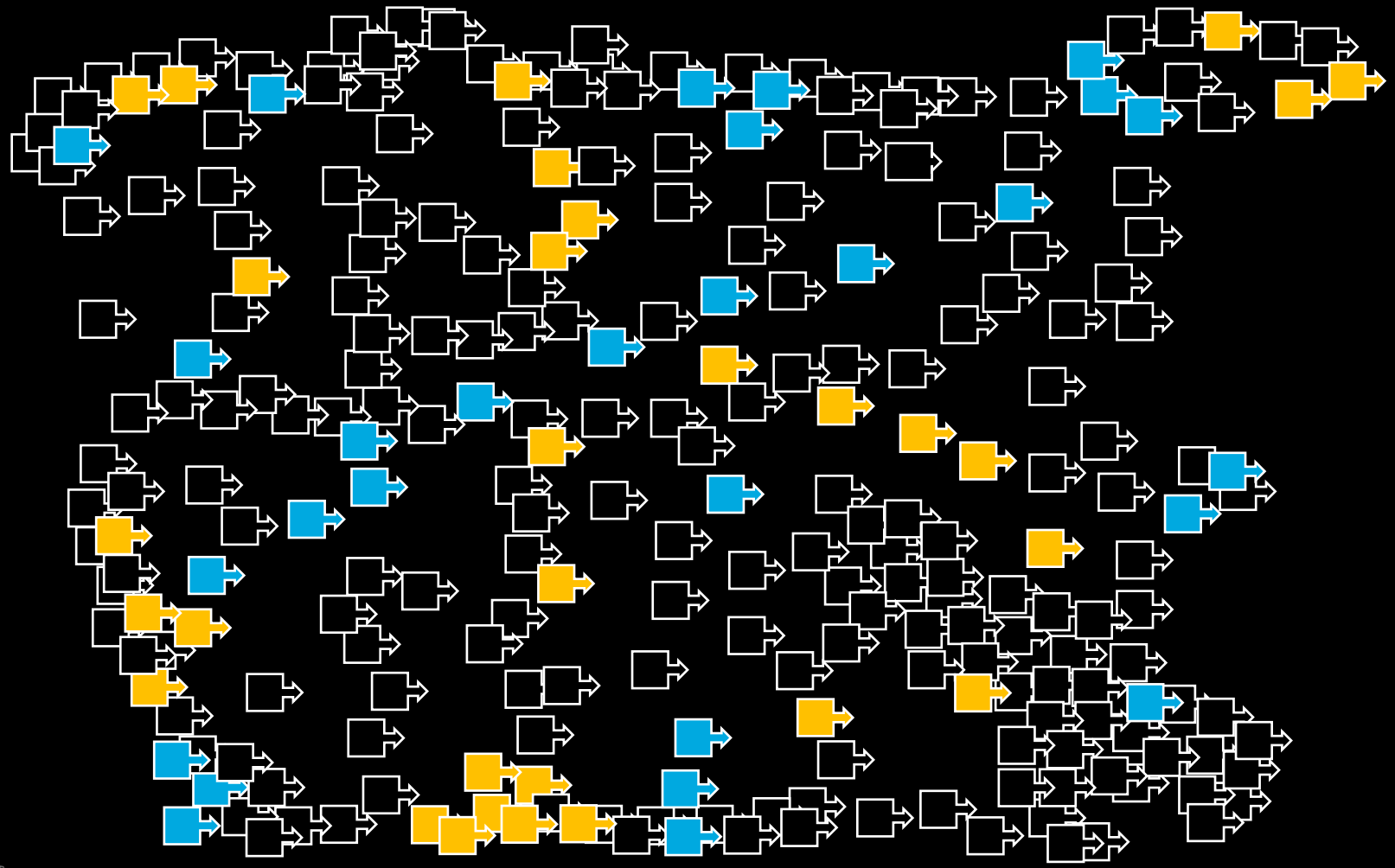
Focusing on High Value Services



- Customer Purchases

Apply a Flexible Service Context

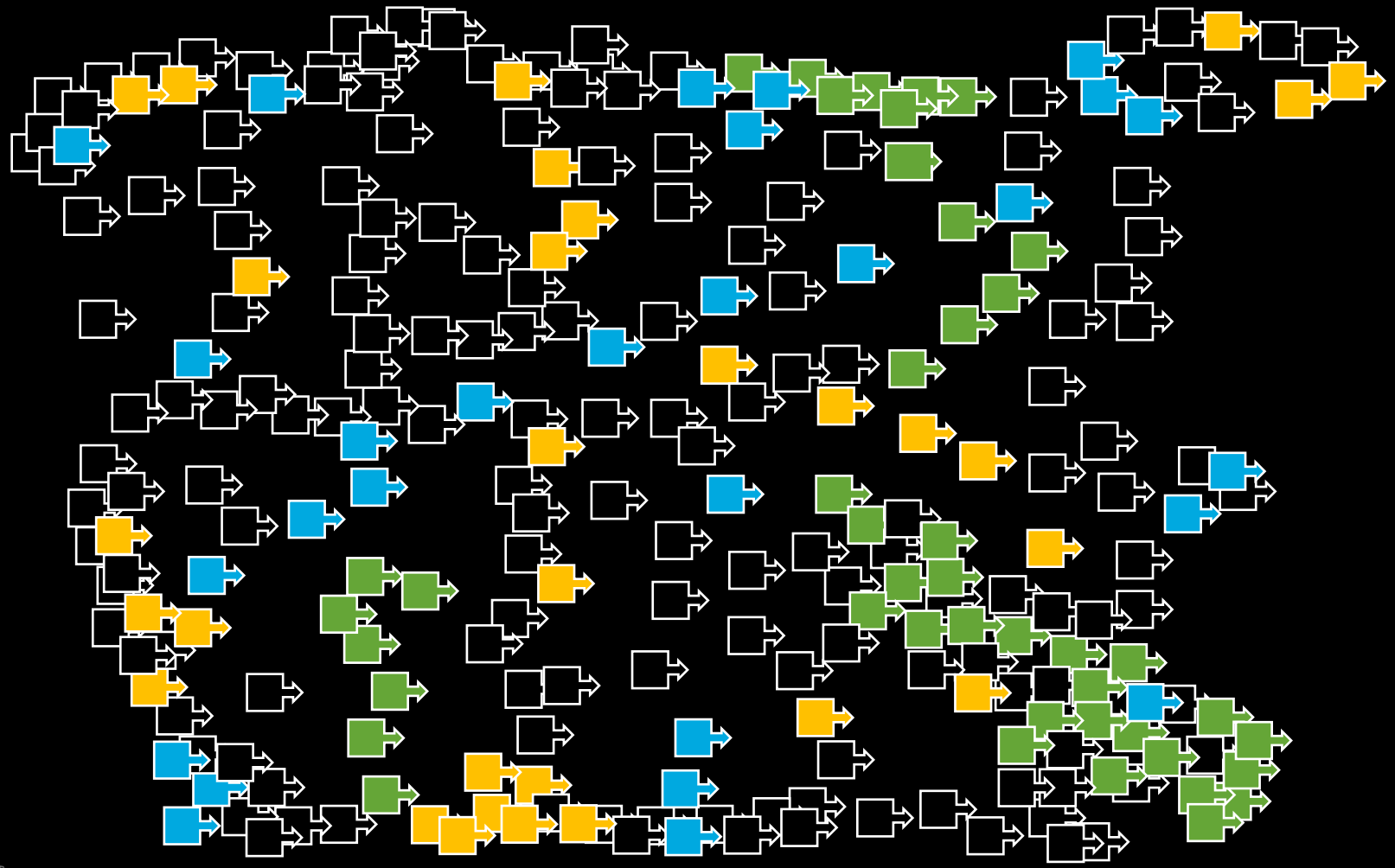
Focusing on High Value Services



- Customer Purchases
- Financial Transactions

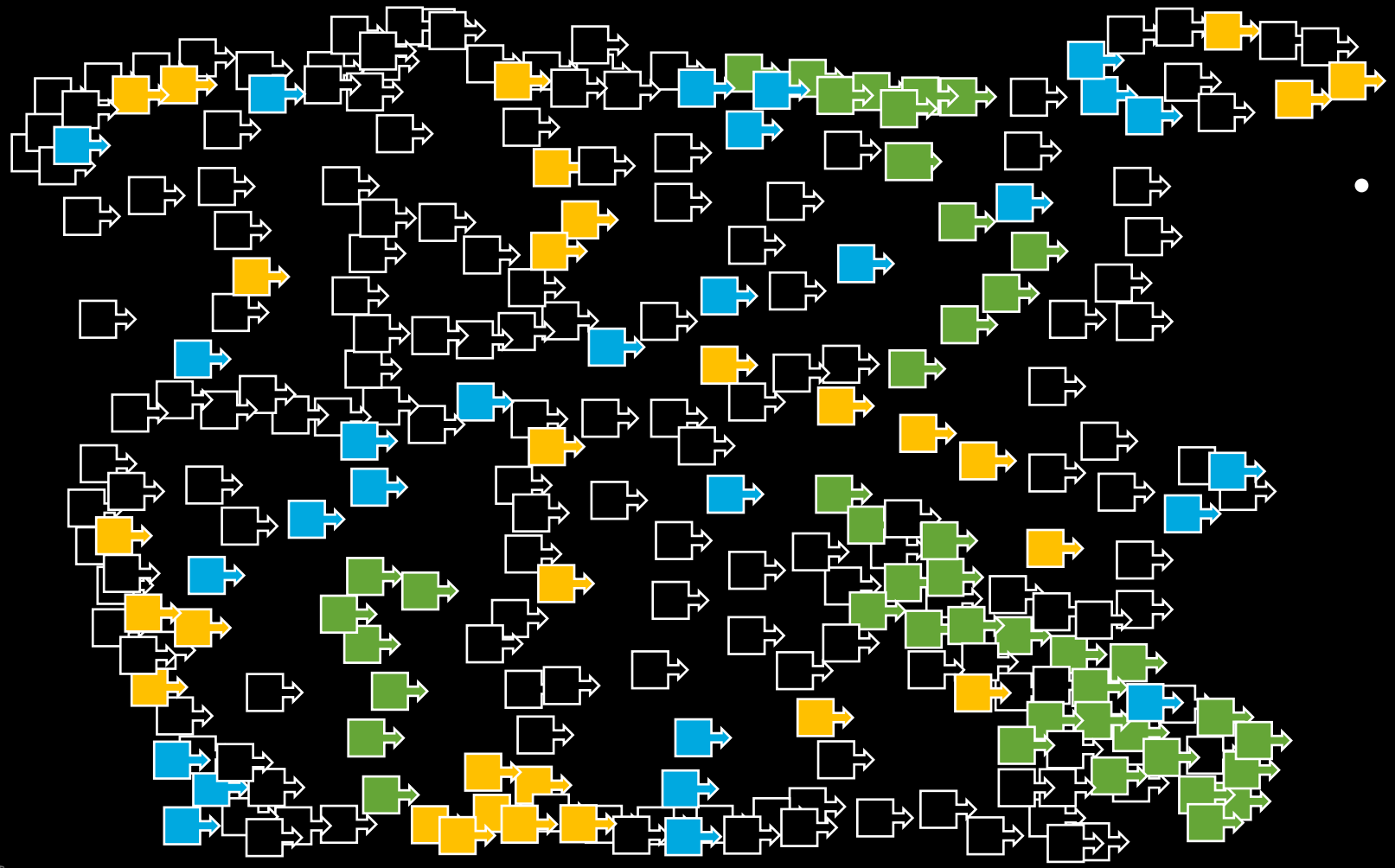
Apply a Flexible Service Context

Focusing on High Value Services



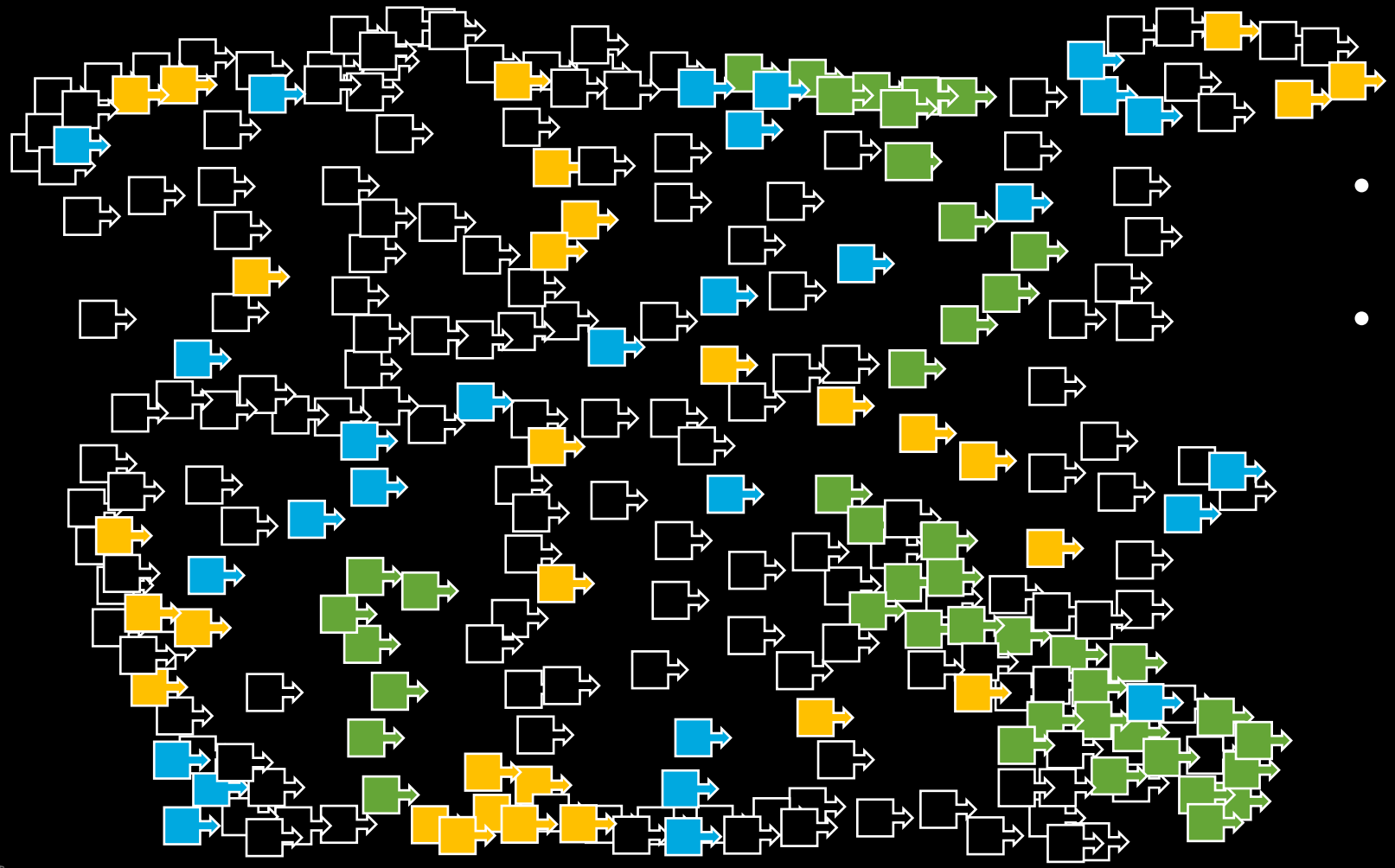
- Customer Purchases
- Financial Transactions
- Claims Processing

Use All the Data– At Scale



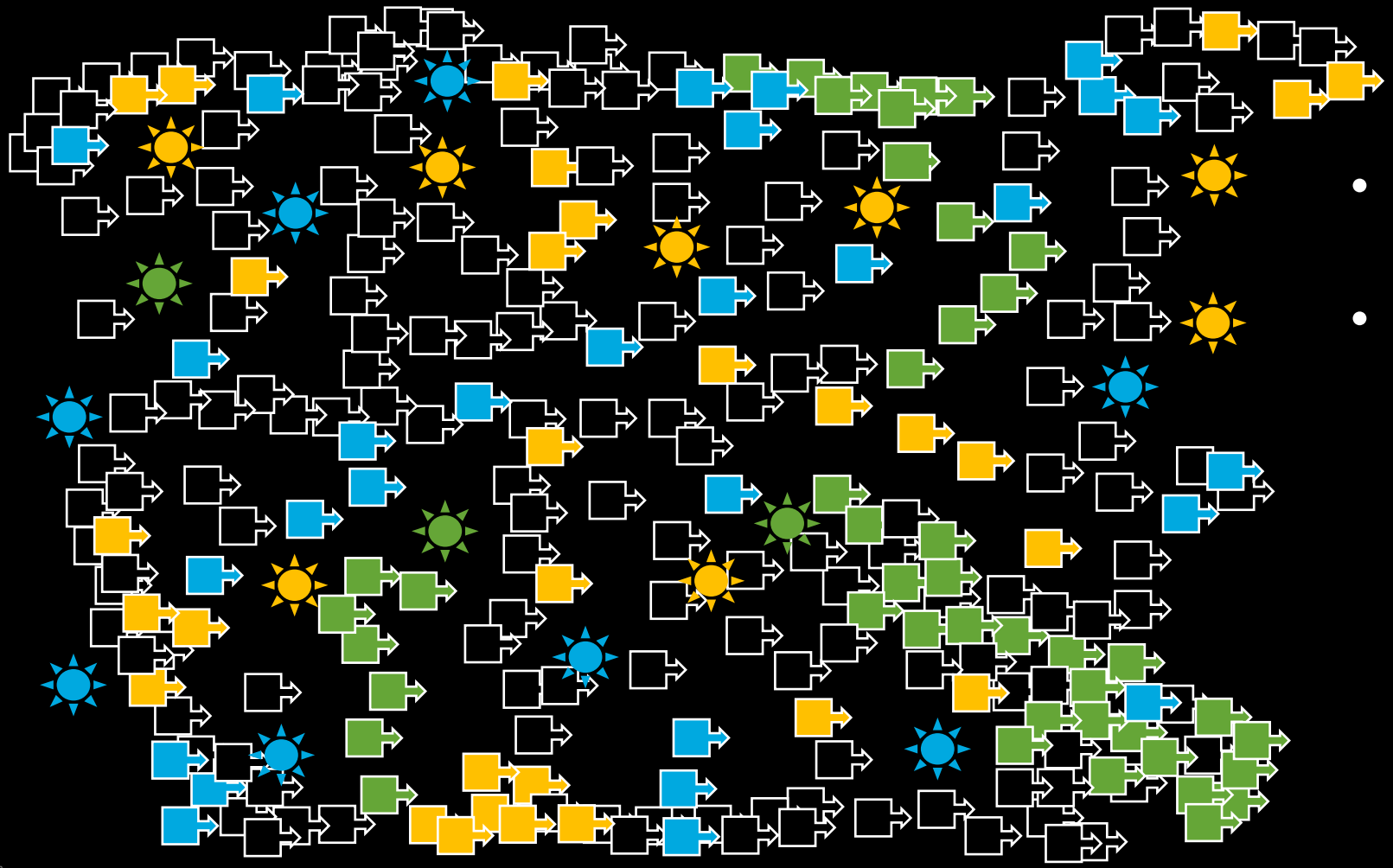
- No more filtering, reducing

Use All the Data– At Scale



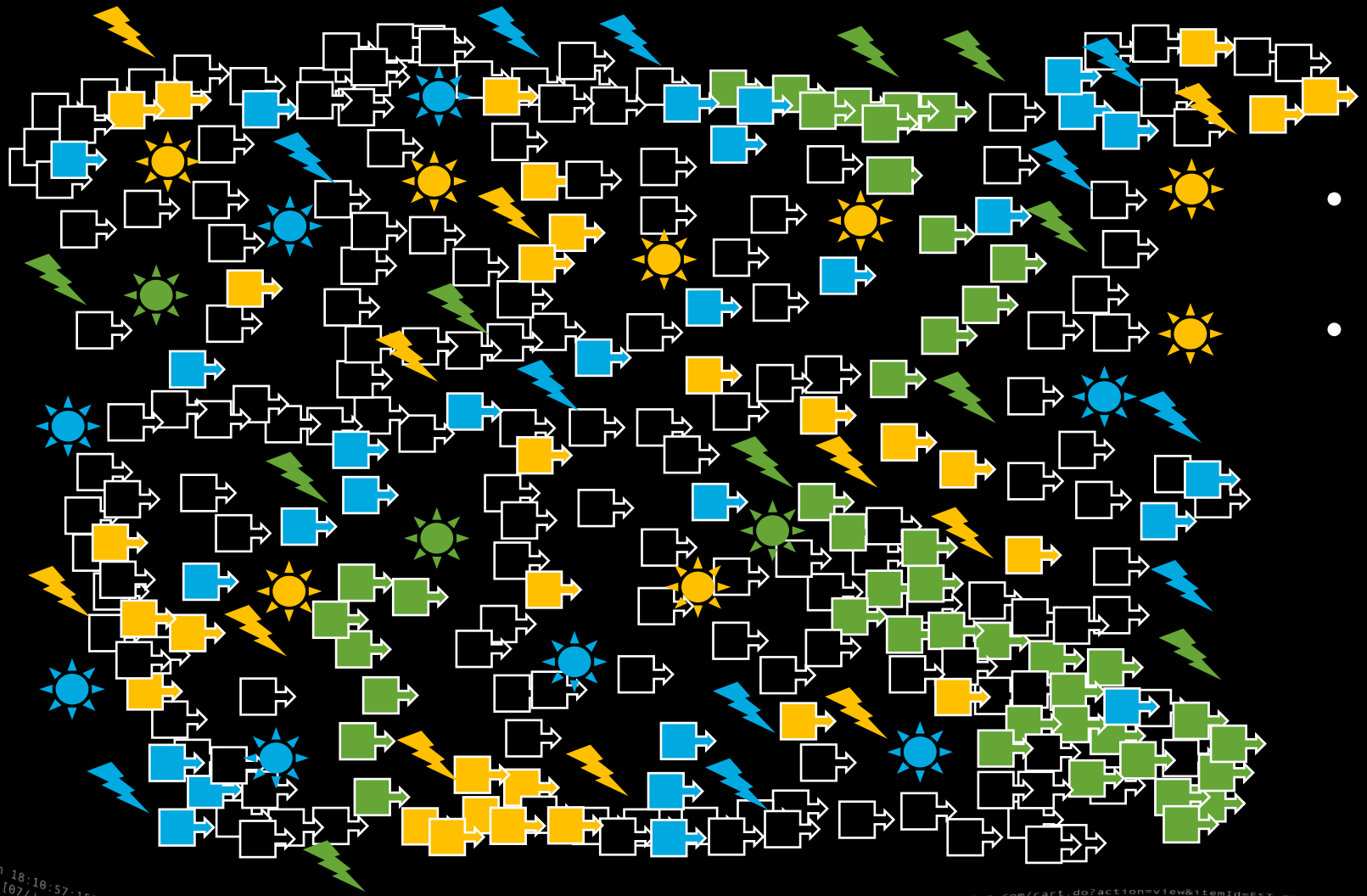
- No more filtering, reducing
- Use all types of data:
  - Traditional events

Use All the Data– At Scale



- No more filtering, reducing
- Use all types of data:
  - Traditional events
  - Metrics

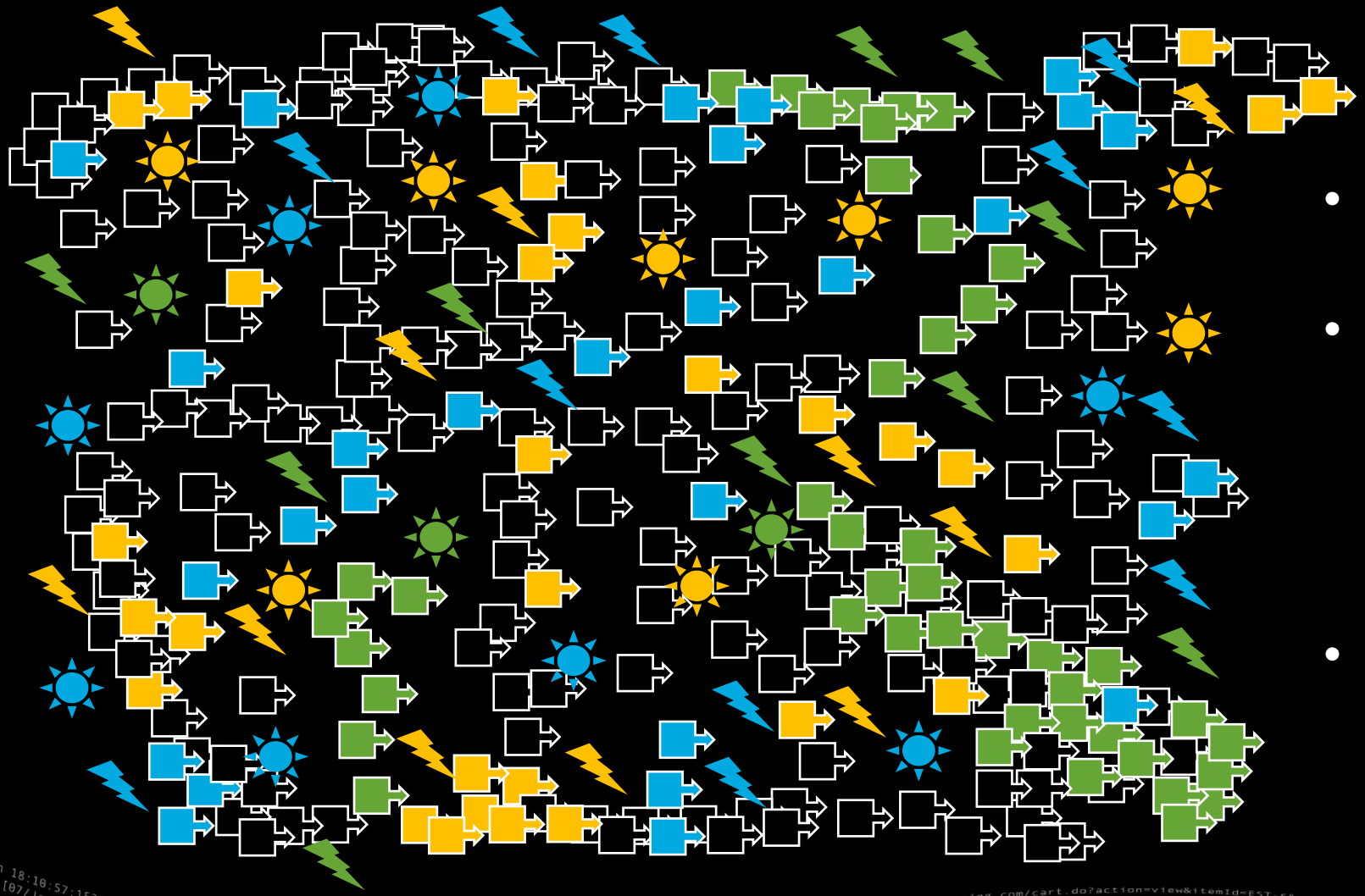
Use All the Data– At Scale



- No more filtering, reducing
- Use all types of data:
  - Traditional events
  - Metrics
  - Wire data

splunk> .conf2017

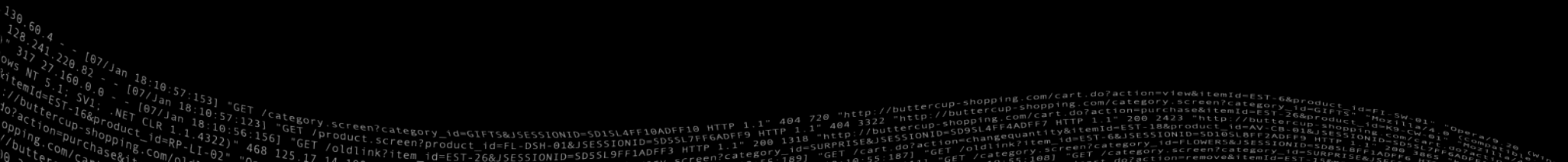
Use All the Data– At Scale



- No more filtering, reducing
- Use all types of data:
  - Traditional events
  - Metrics
  - Wire data
- "OK" & "Not OK" info

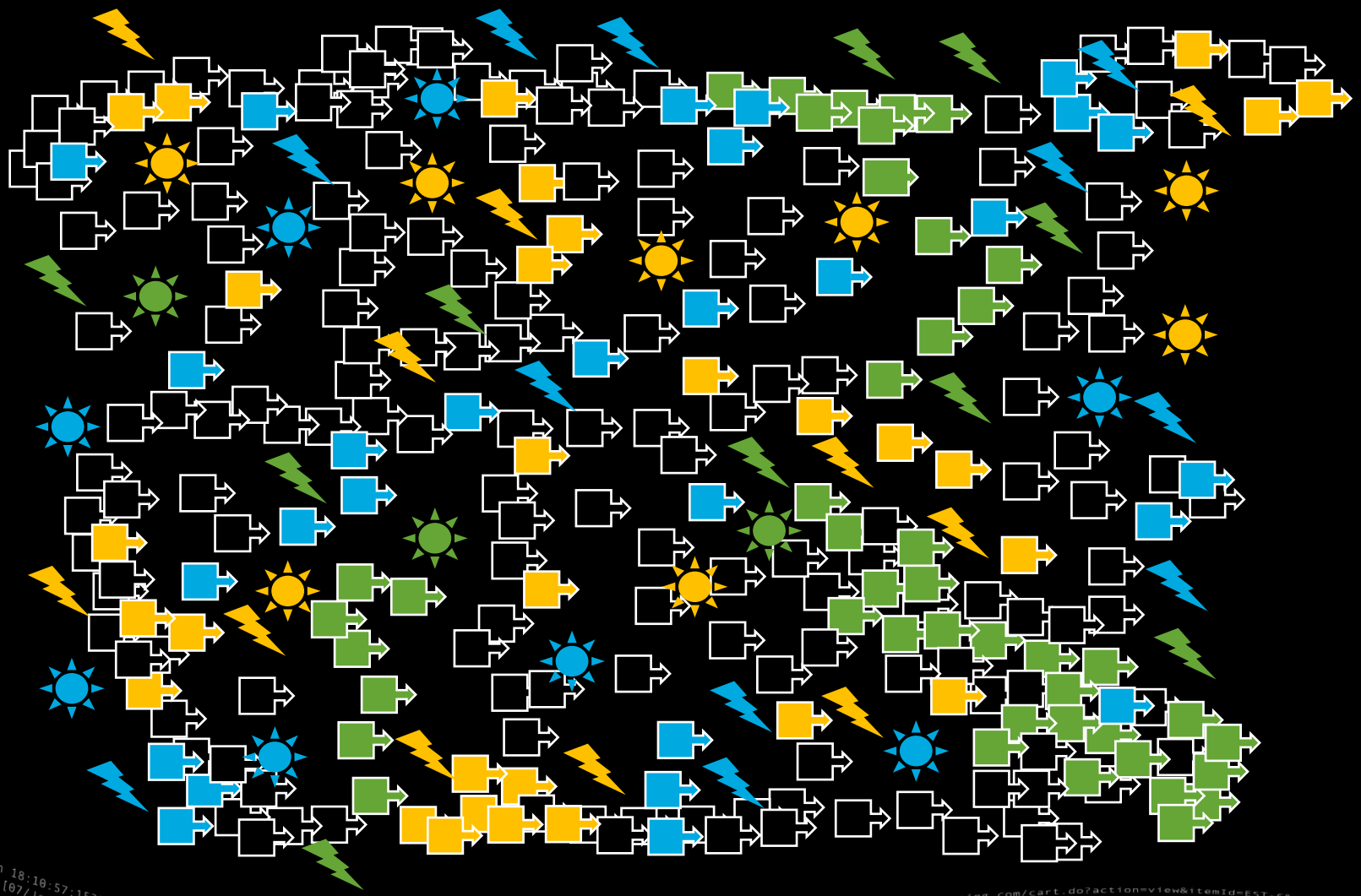
If You Can't Scale, You'll Fail

- Dealing with Gigabytes is easy
- Must be able to handle Terabytes
  and even Petabytes
  per day



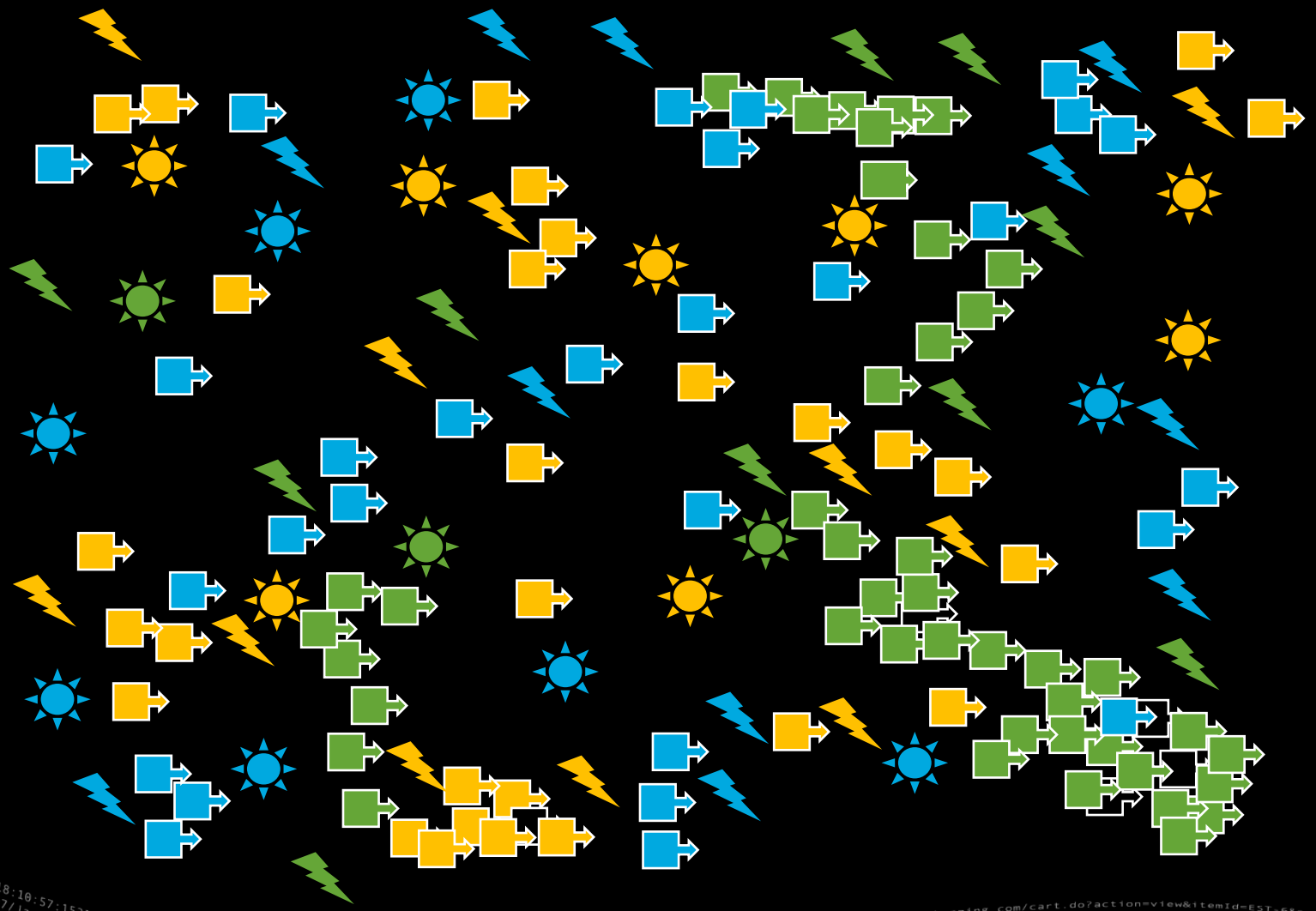
splunk> .conf2017

Use Machine Learning the Right Way



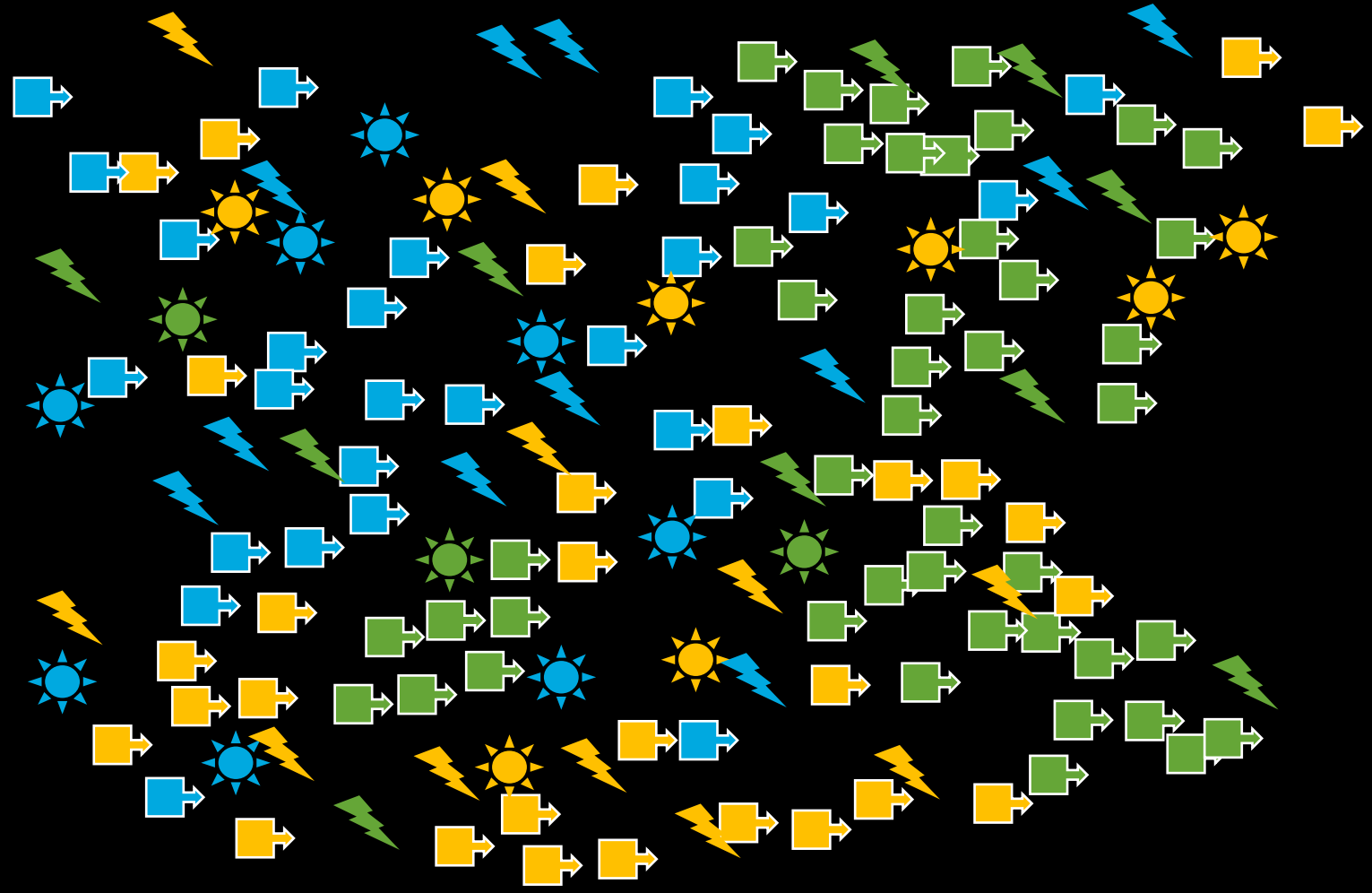
splunk> .conf2017

Use Machine Learning the Right Way



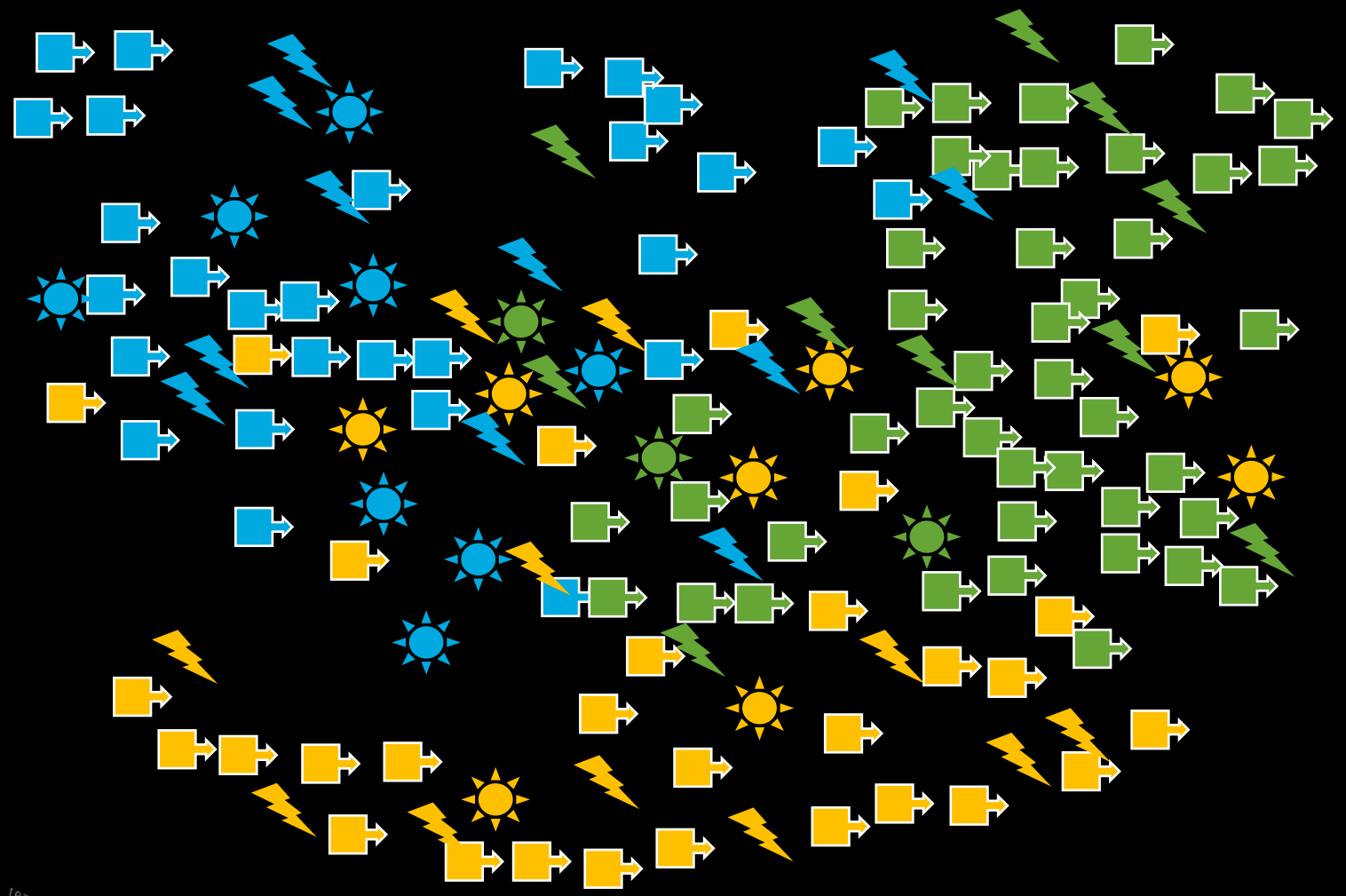
- At Every Step
- On All Types of Data

Use Machine Learning the Right Way



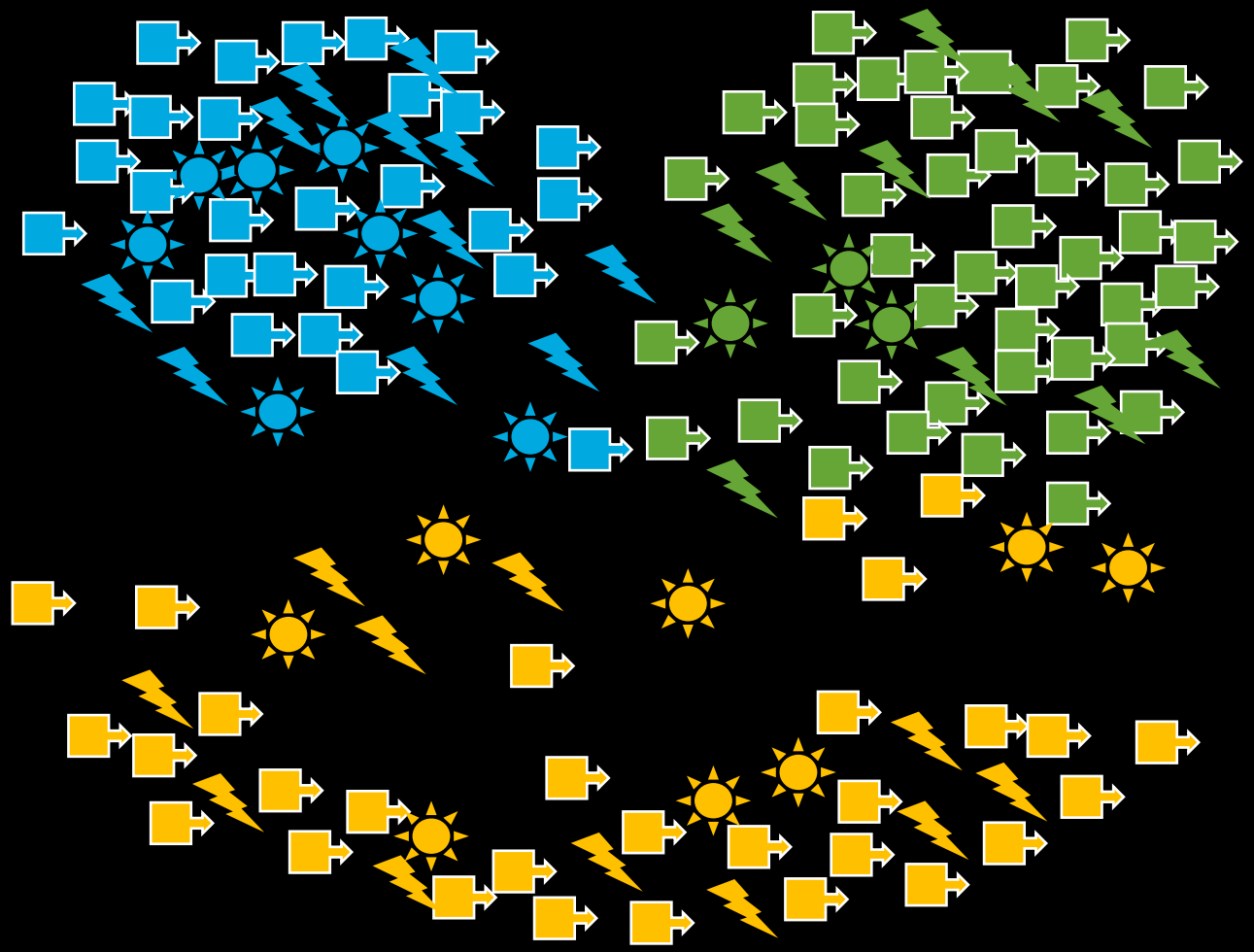
- At Every Step
- On All Types of Data
- From **High vs Low** to **Normal vs Not Normal**

Use Machine Learning the Right Way



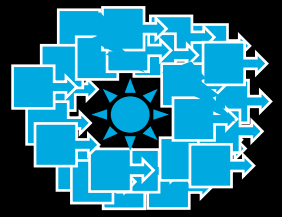
- At Every Step
- On All Types of Data
- From High vs Low to Normal vs Not Normal
- Move Beyond Alerts

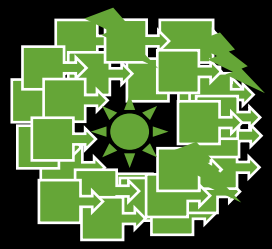
Use Machine Learning the Right Way

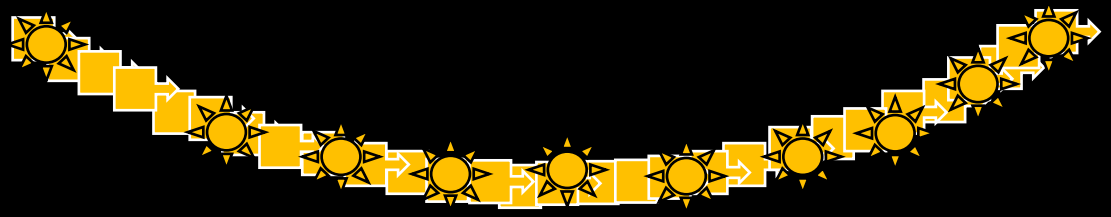


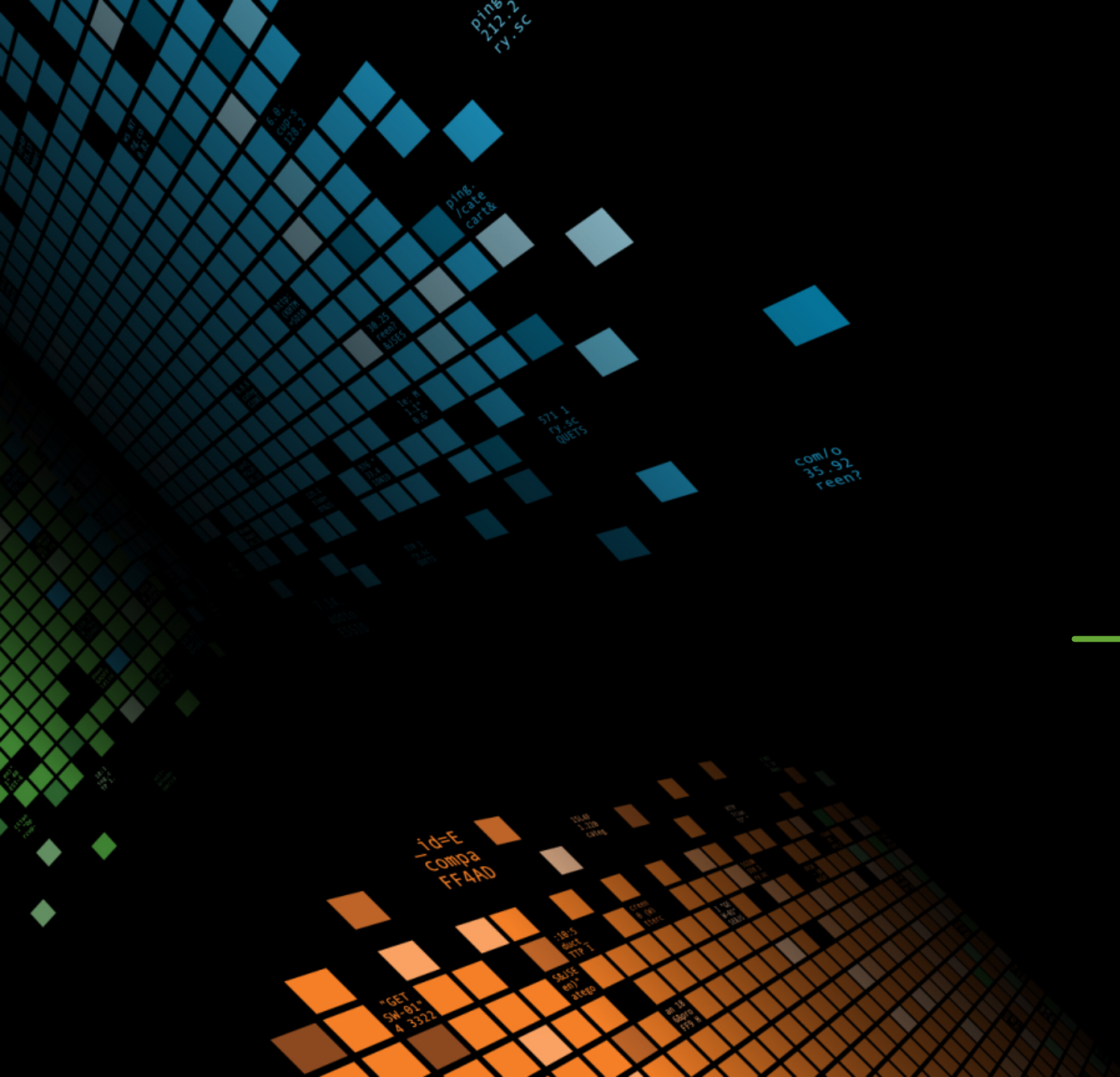
- At Every Step
- On All Types of Data
- From High vs Low to Normal vs Not Normal
- Move Beyond Alerts
- Get Proactive

Let's Drive!





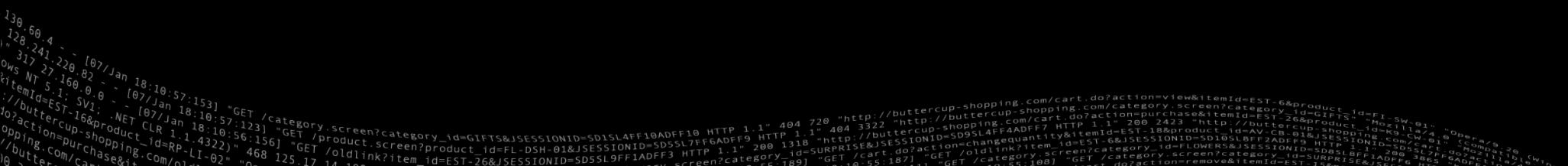




Demo

Life Gets Better for IT Ops

- Reduce complexity
- Produce Human-Scale, Prioritized, Actionable events
- Improve MTTR
- Simplify Operations

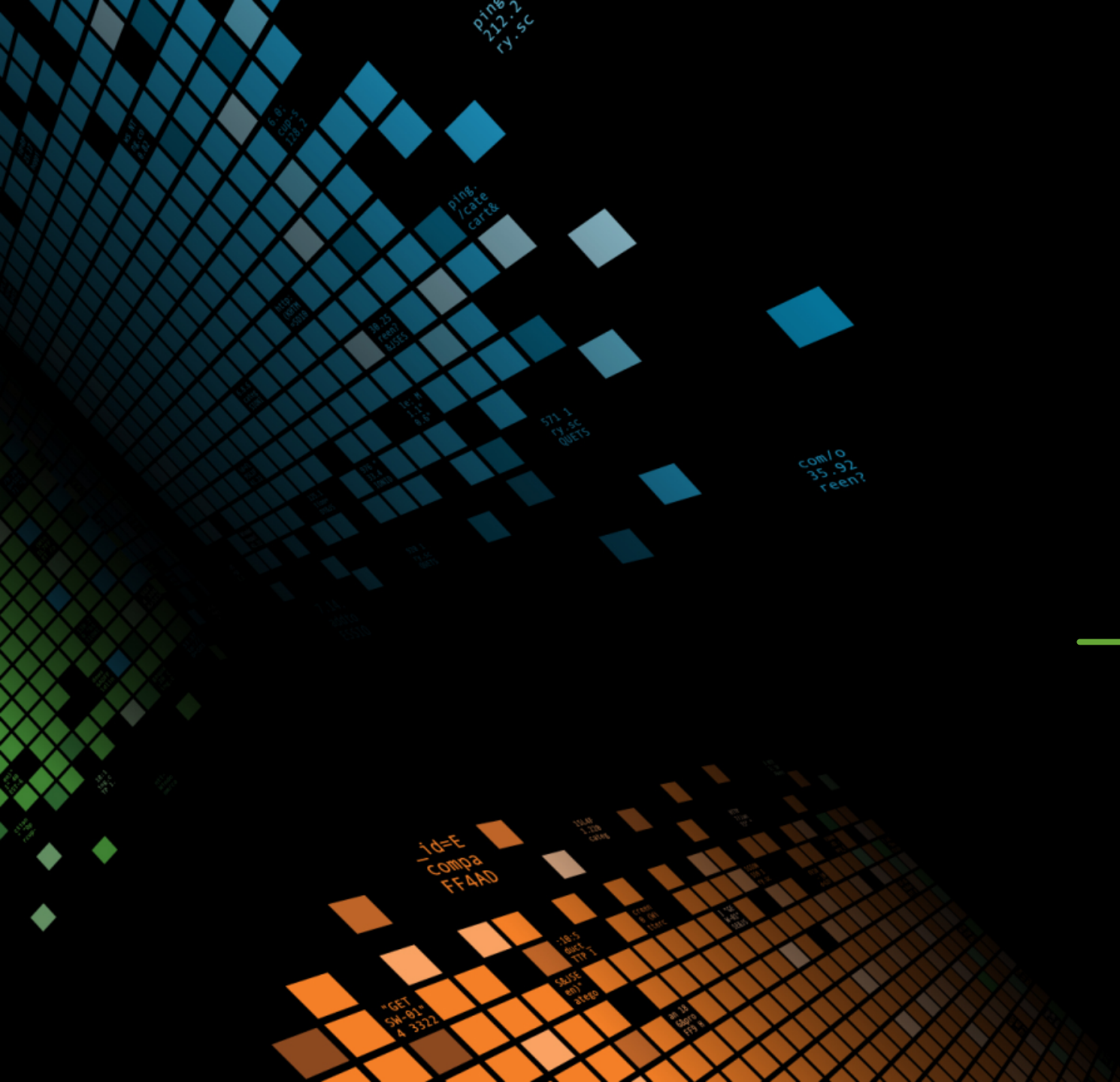


splunk> .conf2017

Empower IT Ops to

Find What's Broken, then Fix It

splunk> .conf2017



Q&A

Thank You

Don't forget to rate this session in the .conf2017 mobile app

David Millis | dmillis@splunk.com

splunk> .conf2017