

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

But First, a Terminology Check

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

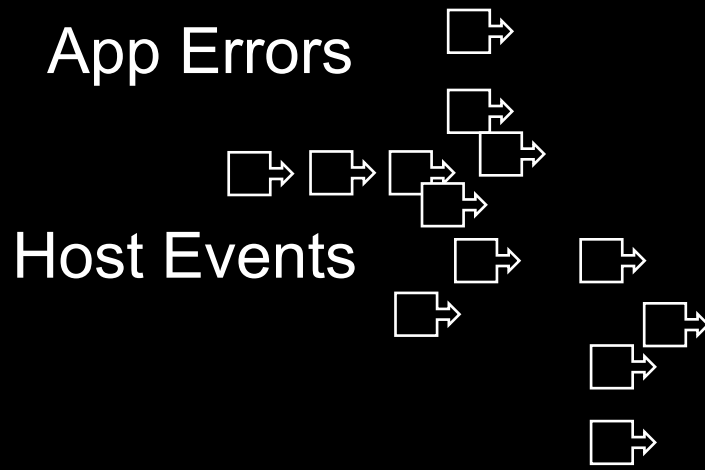




A Brief History of Event Management

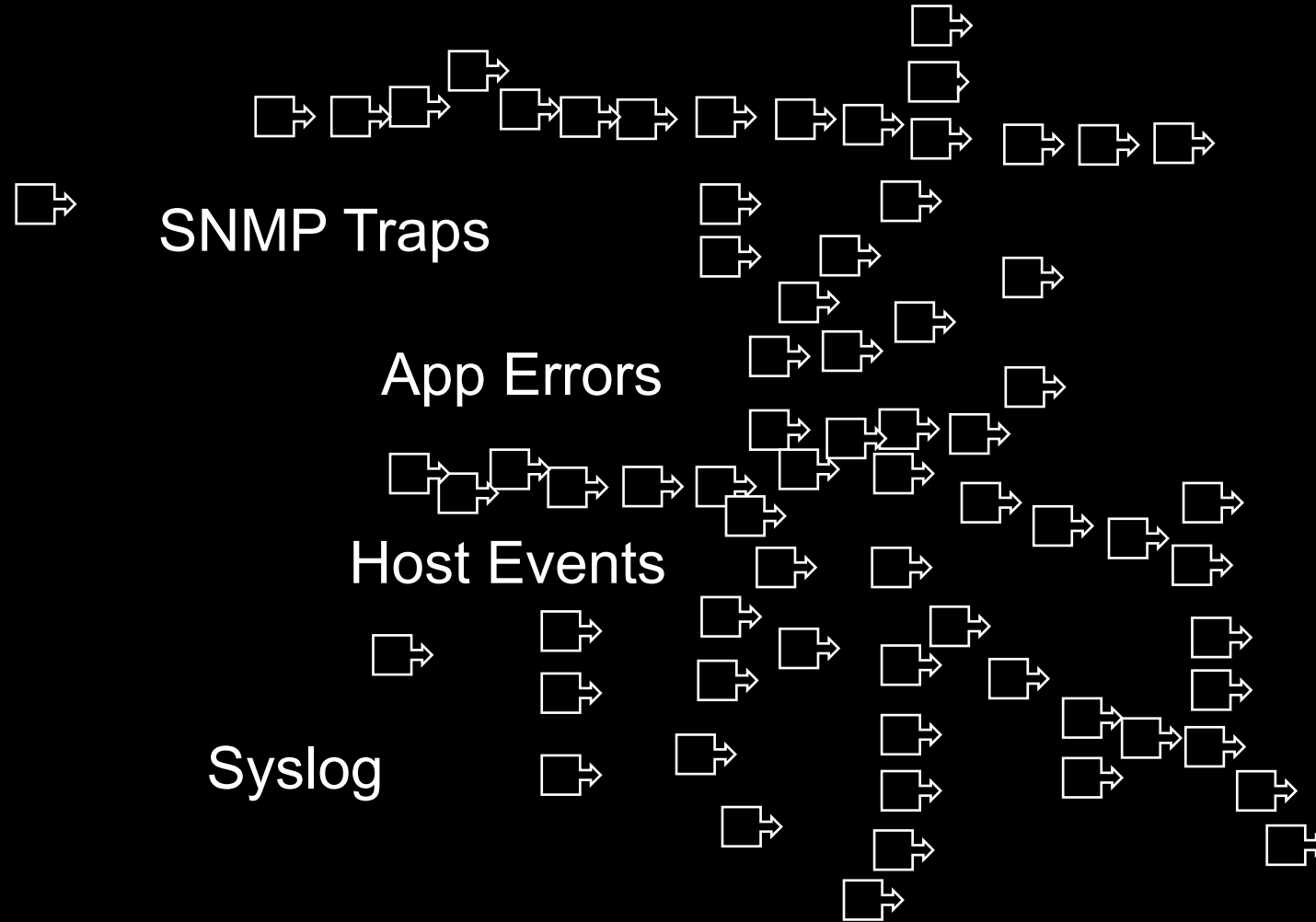
Remind Me: Why Are We Doing This?

But the Rate of Events Began Increasing



```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.2013.10; Linux x86_64; rv:15.0 Gecko/20100101 Firefox/15.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-20&product_id=K9-CU-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2; rv:42.0) Gecko/20100101 Firefox/42.0"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL7FF6ADFF9" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2; rv:42.0) Gecko/20100101 Firefox/42.0"
10.0.0.1 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 468 125.17.14.1 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&JSESSIONID=SD5SL9FF1ADFF3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2; rv:42.0) Gecko/20100101 Firefox/42.0"
10.0.0.1 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&JSESSIONID=SD5SL9FF1ADFF3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2; rv:42.0) Gecko/20100101 Firefox/42.0"
10.0.0.1 - - [07/Jan 18:10:55:108] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&JSESSIONID=SD5SL9FF1ADFF3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2; rv:42.0) Gecko/20100101 Firefox/42.0"
```

But the Rate of Events Began Increasing

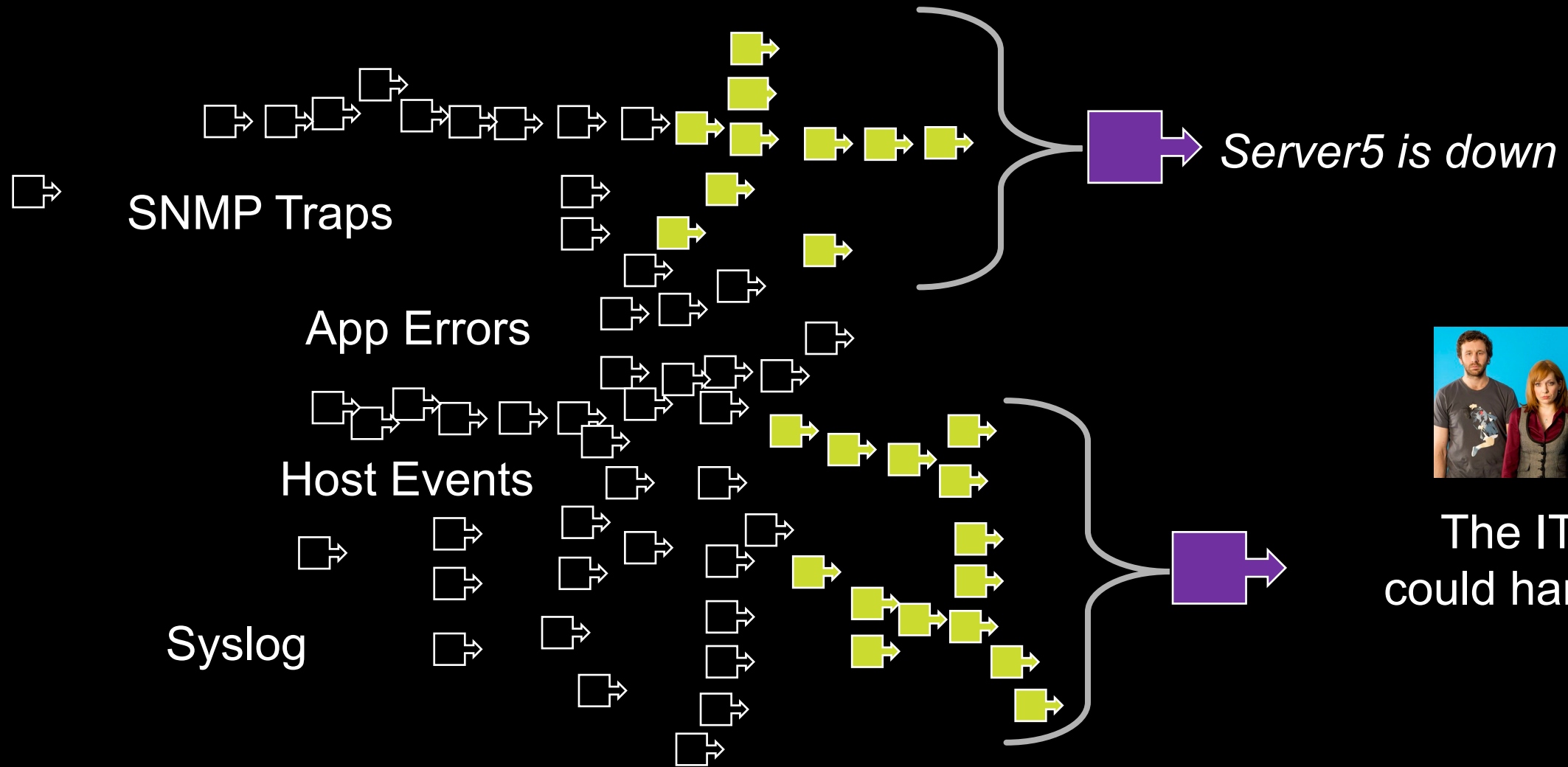


Until the IT folks
couldn't handle it

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD59L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/product.screen?product_id=FL-DSH-01&JSESSIONID=SD59L7FF6ADFF9"
5.1: SV1: - - [07/Jan 18:10:56:150] "GET /cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/product.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10"
j/action=purchase shopping_id=RP-LI-02" 468 125.17.14.101 "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF3"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD59L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/product.screen?product_id=FL-DSH-01&JSESSIONID=SD59L7FF6ADFF9"
5.1: SV1: - - [07/Jan 18:10:56:150] "GET /cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/product.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10"
j/action=purchase shopping_id=RP-LI-02" 468 125.17.14.101 "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF3"
  
```

The Event Manager is Born



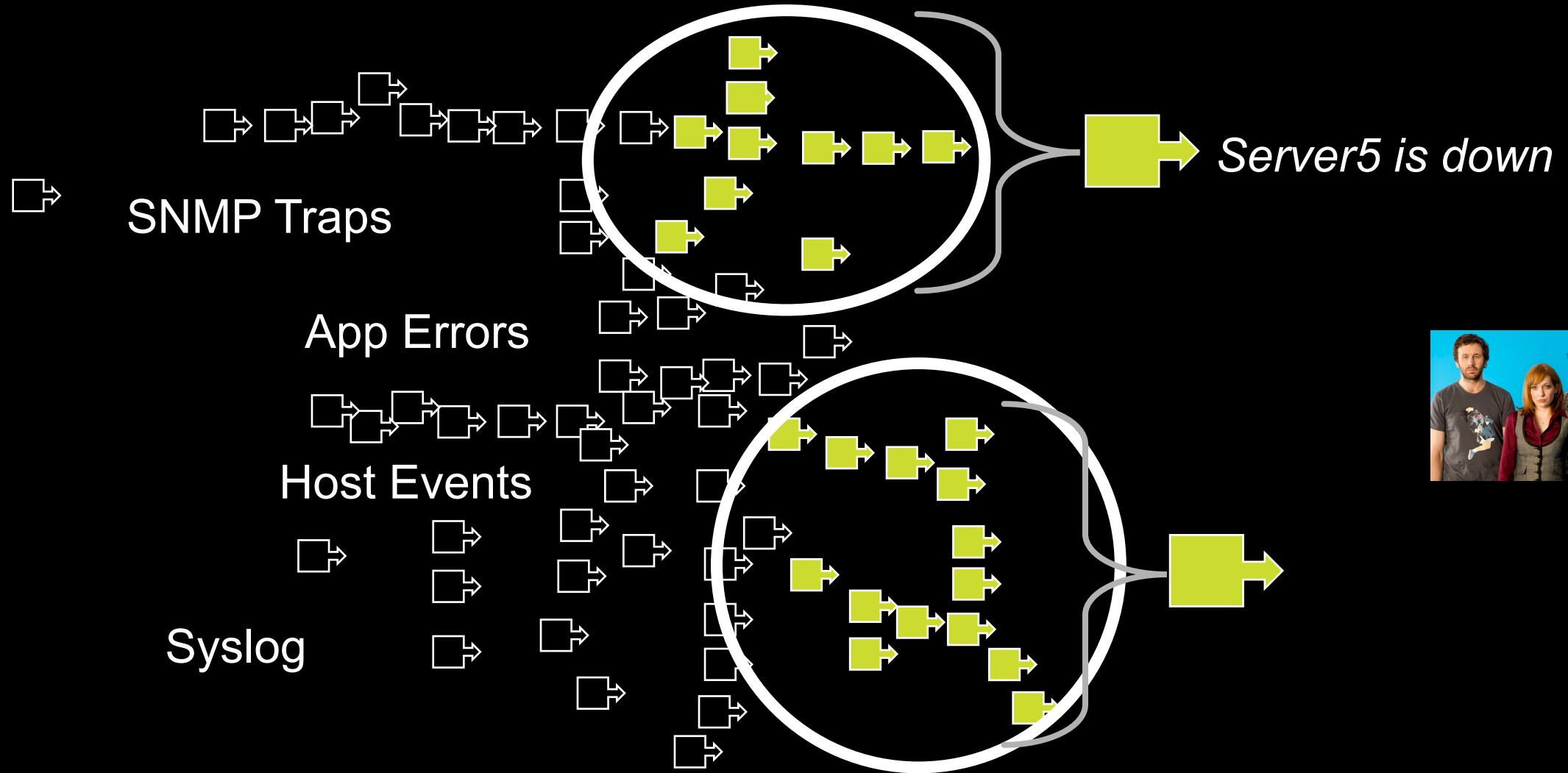
The IT Folks could handle it, again

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=K9-CU-01"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/changequantity?item_id=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SLBE12ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&item_id=EST-1"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=K9-CU-01"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/changequantity?item_id=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SLBE12ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&item_id=EST-1"

```

... along with the IT Silo!

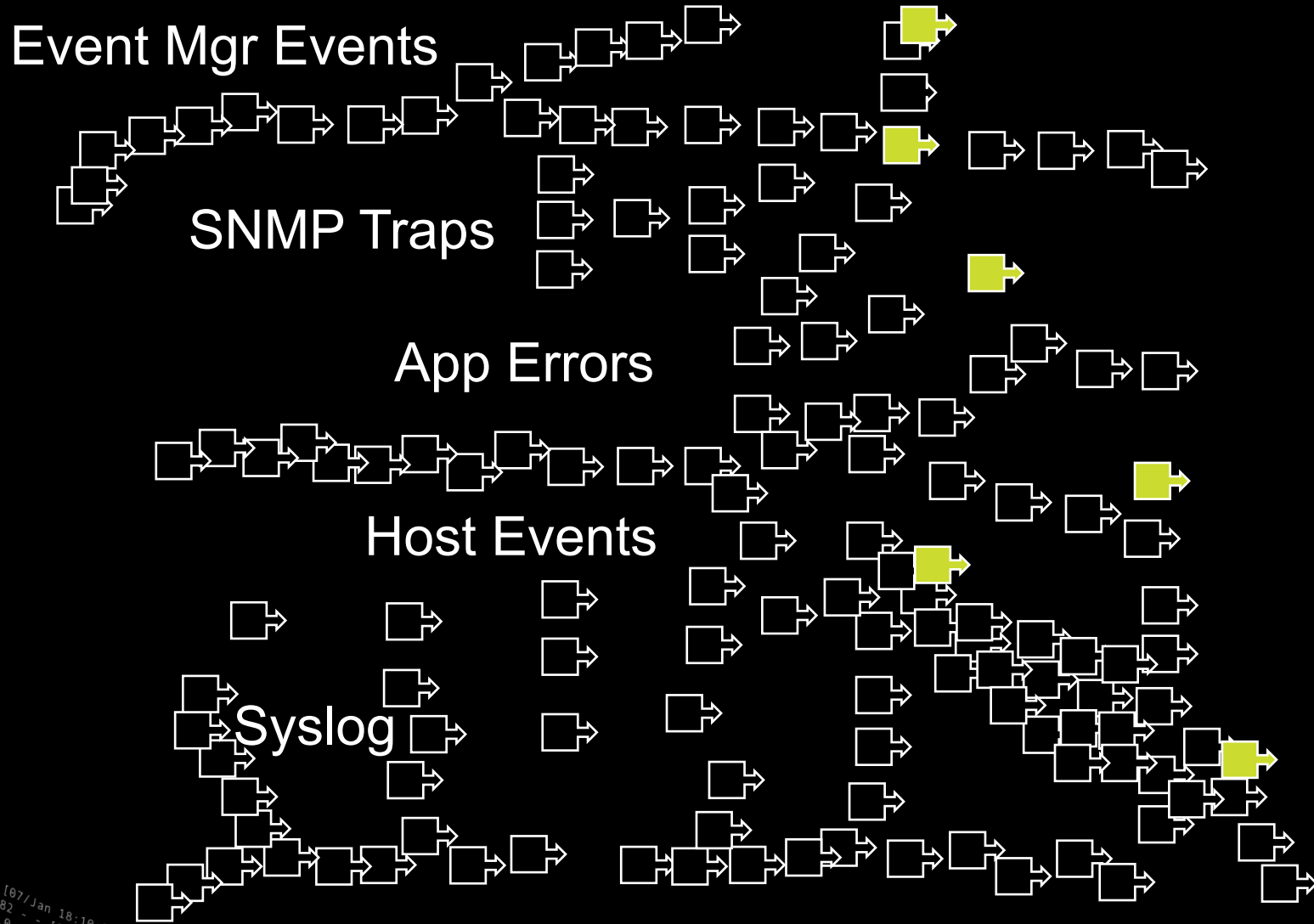


```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=K9-CU-01"
ows NT 27.160.0.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SLBE12ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/compare"
item_id=EST-16&product_id=RP-LI-02" 468 125.17.14.101:80 - - [07/Jan 18:10:56:189] "GET /cart.do?action=remove&item_id=EST-18&product_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/purchase"
http://buttercup-shopping.com/oldlink?item_id=EST-18&product_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/purchase"
http://buttercup-shopping.com/oldlink?item_id=EST-18&product_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/purchase"

```


But the Rate of Events Kept Going Up

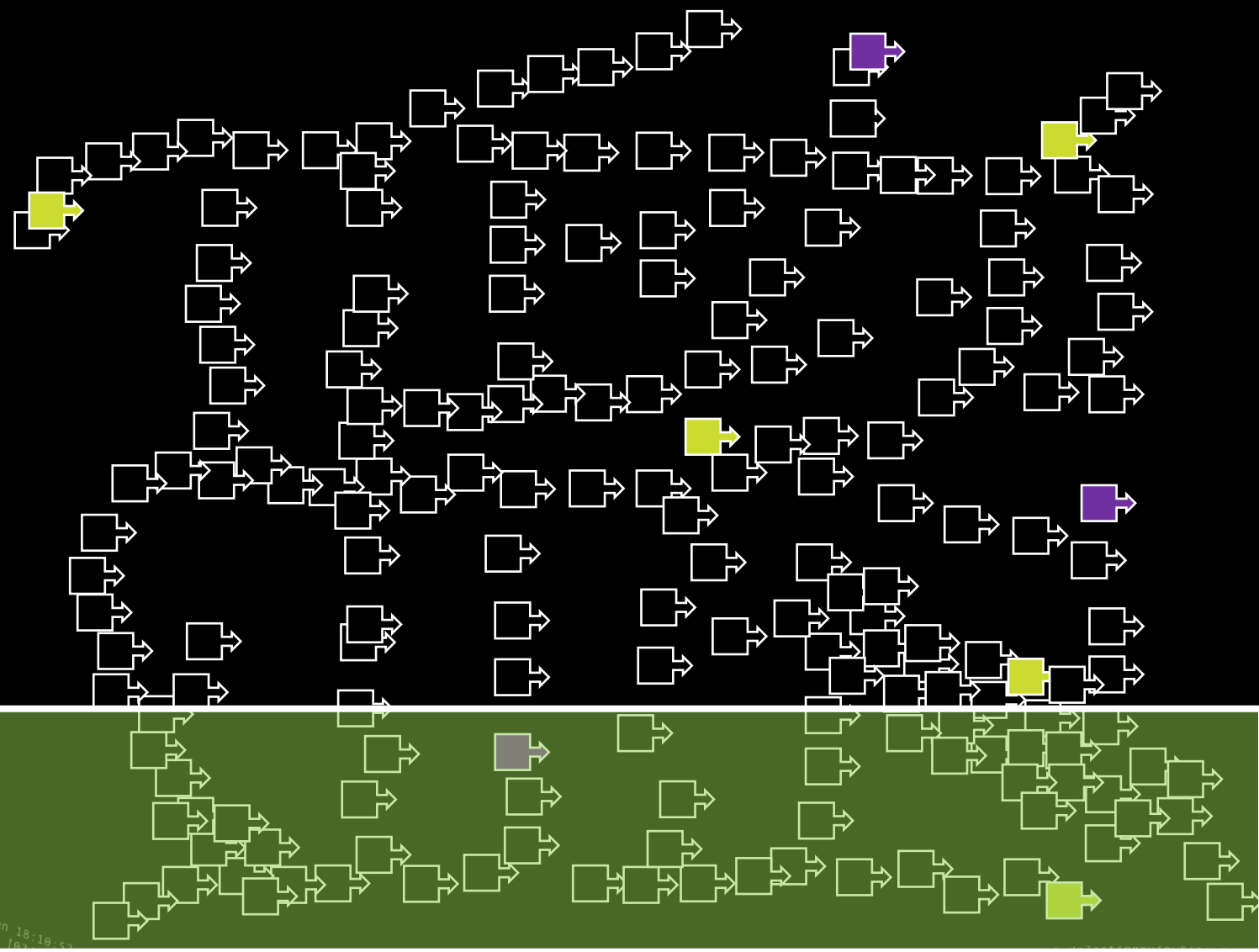


and **Event Managers**
Multiplied



```
130.60.4 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.2013.10; Linux x86_64; rv:15.0 Gecko/20100101 Firefox/15.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/compare.do?act=LI-02"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 468 125.17.14.101 "http://buttercup-shopping.com/purchase&itemId=EST-16&product_id=RP-LI-02" "Opera/9.80.2013.10; Linux x86_64; rv:15.0 Gecko/20100101 Firefox/15.0"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.2013.10; Linux x86_64; rv:15.0 Gecko/20100101 Firefox/15.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/compare.do?act=LI-02"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 468 125.17.14.101 "http://buttercup-shopping.com/purchase&itemId=EST-16&product_id=RP-LI-02" "Opera/9.80.2013.10; Linux x86_64; rv:15.0 Gecko/20100101 Firefox/15.0"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.2013.10; Linux x86_64; rv:15.0 Gecko/20100101 Firefox/15.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/compare.do?act=LI-02"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 468 125.17.14.101 "http://buttercup-shopping.com/purchase&itemId=EST-16&product_id=RP-LI-02" "Opera/9.80.2013.10; Linux x86_64; rv:15.0 Gecko/20100101 Firefox/15.0"
```


Environments Became More Complex

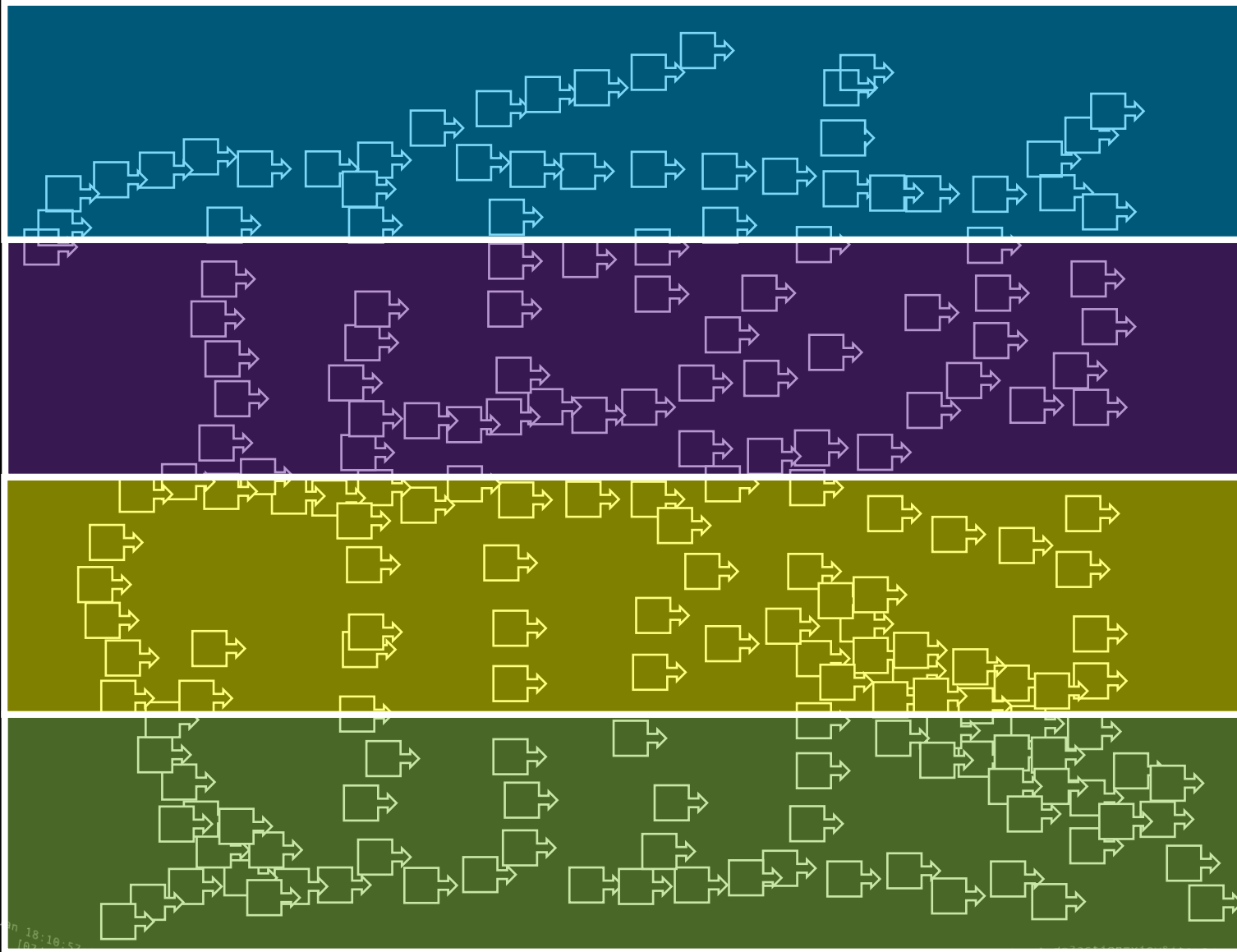


Network



```
130.60.4 - [07/Jan 18:10:57] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L9FF1ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GIFTS&product_id=FL-SW-01" "Opera/9.80.2017.10 Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 1.1.4322" 468 125.17.14 [id link?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3" "Mozilla/5.0 (Windows NT 6.0; rv:34.0) Gecko/20100801 Firefox/34.0" "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-20&product_id=K9-CU-01" "Opera/9.80.2017.10 Windows NT 6.0; rv:34.0" "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-18&product_id=AV-CB-01&JSESSIONID=SD105L9FF1ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-18&product_id=AV-CB-01&JSESSIONID=SD105L9FF1ADFF9" "Mozilla/5.0 (Windows NT 6.0; rv:34.0) Gecko/20100801 Firefox/34.0" "http://buttercup-shopping.com/cart.do?action=remove&item_id=EST-10&product_id=LI-02" "Opera/9.80.2017.10 Windows NT 6.0; rv:34.0" "http://buttercup-shopping.com/cart.do?action=remove&item_id=EST-10&product_id=LI-02" "Mozilla/5.0 (Windows NT 6.0; rv:34.0) Gecko/20100801 Firefox/34.0" "http://buttercup-shopping.com/cart.do?action=remove&item_id=EST-10&product_id=LI-02" "Opera/9.80.2017.10 Windows NT 6.0; rv:34.0" "http://buttercup-shopping.com/cart.do?action=remove&item_id=EST-10&product_id=LI-02" "Mozilla/5.0 (Windows NT 6.0; rv:34.0) Gecko/20100801 Firefox/34.0"
```


Environments Became More Complex



Cloud

Virtualization

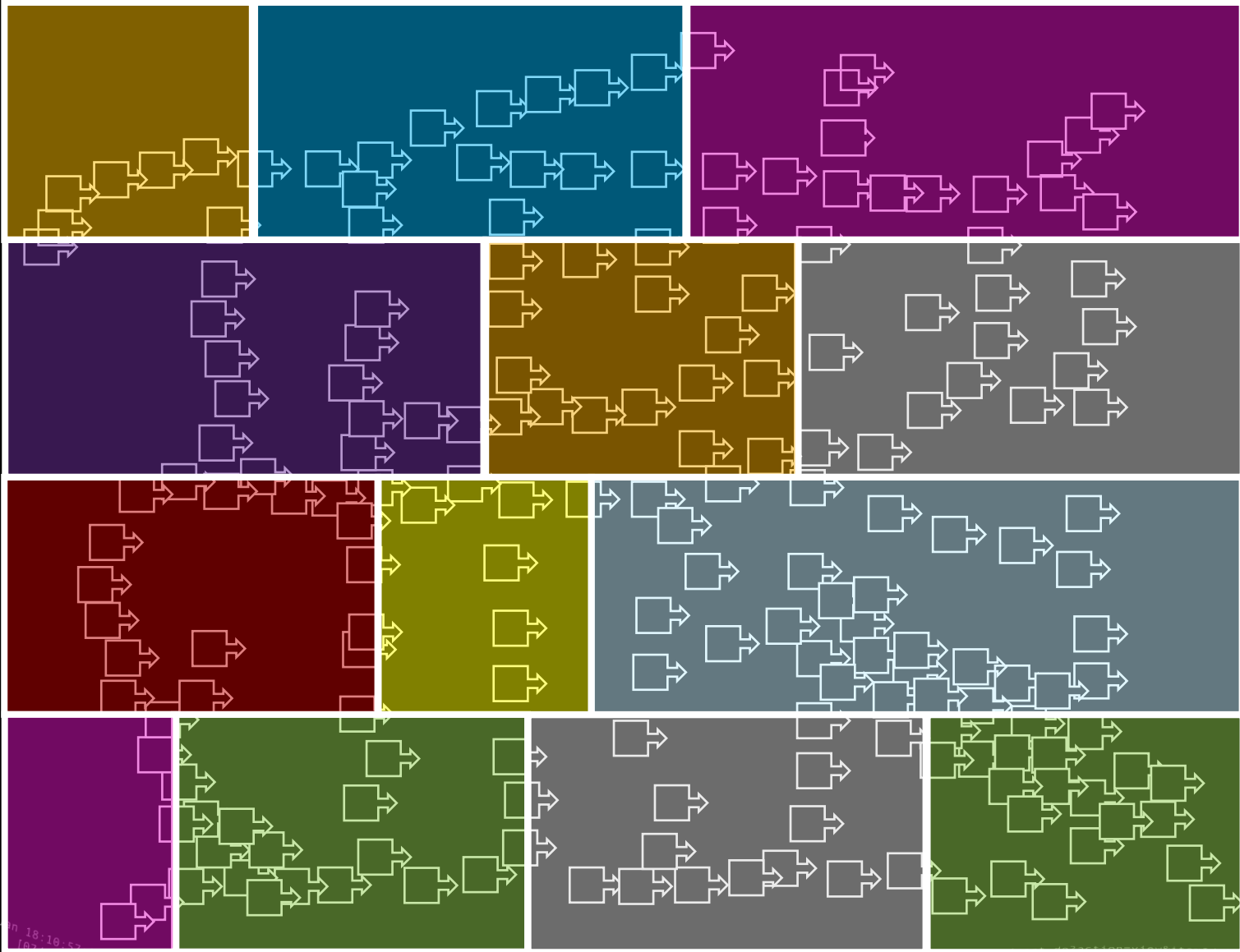
Storage

Network



```
130.60.4 - - [07/Jan 18:10:56:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GIFTS&product_id=FL-SW-01" "Opera/9.80.2011.220.82-beta1; Windows NT 5.1; SV1; .NET CLR 1.1.4322" 468 129.17.14 [10.0.2.15]
128.241.220.82 - - [07/Jan 18:10:56:150] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1310 "http://buttercup-shopping.com/product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3" "Opera/9.80.2011.220.82-beta1; Windows NT 5.1; SV1; .NET CLR 1.1.4322" 468 129.17.14 [10.0.2.15]
317.27.160.0 - - [07/Jan 18:10:56:189] "GET /cart.do?action=changequantity&item_id=EST-18&JSESSIONID=SD10SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-18&JSESSIONID=SD10SL9FF1ADFF3" "Opera/9.80.2011.220.82-beta1; Windows NT 5.1; SV1; .NET CLR 1.1.4322" 468 129.17.14 [10.0.2.15]
130.60.4 - - [07/Jan 18:10:56:198] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3" "Opera/9.80.2011.220.82-beta1; Windows NT 5.1; SV1; .NET CLR 1.1.4322" 468 129.17.14 [10.0.2.15]
```


Environments Became More Complex



* As a Service

Highly Available



On Demand

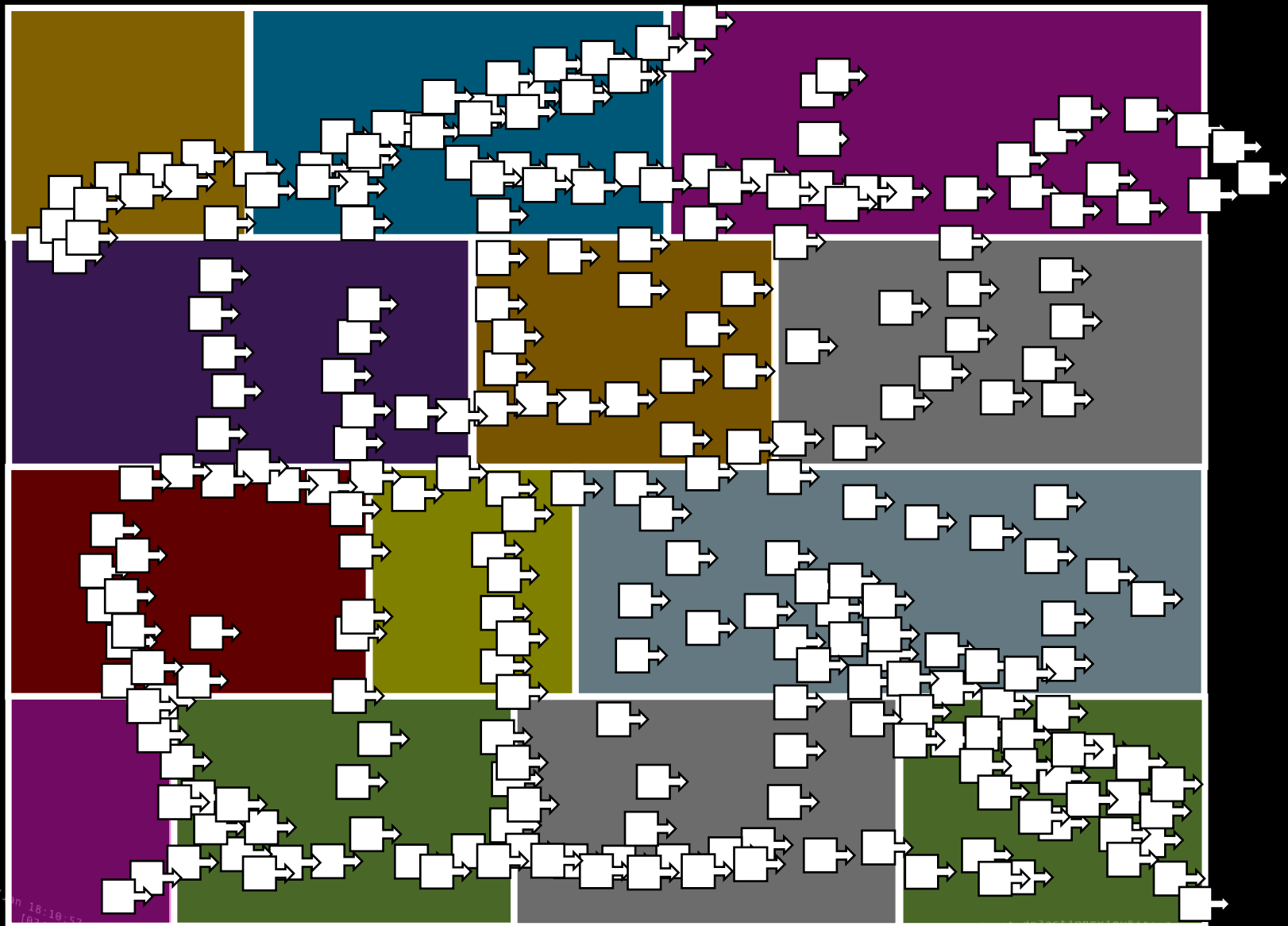
Software Defined

```

130.60.4 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L9FF1ADFF3 HTTP/1.1" 404 720
128.241.220.82 - - [07/Jan 18:10:56:150] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP/1.1" 404 3322
317.27.160.0 - - [07/Jan 18:10:55:187] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 1316
10.20.10.10 - - [07/Jan 18:10:55:108] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD55L7FF6ADFF9 HTTP/1.1" 200 3865

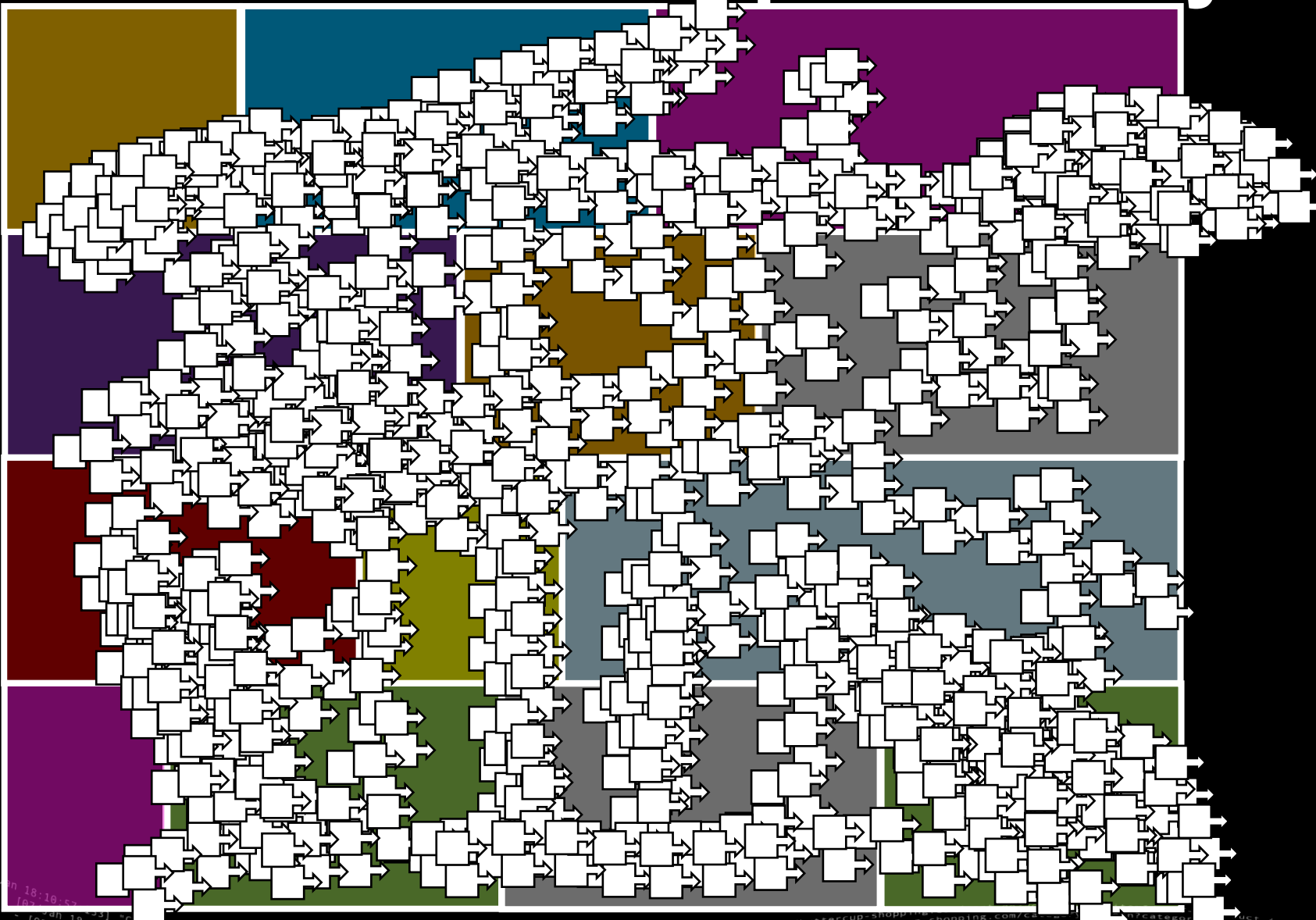
```

And the number of Events increased--



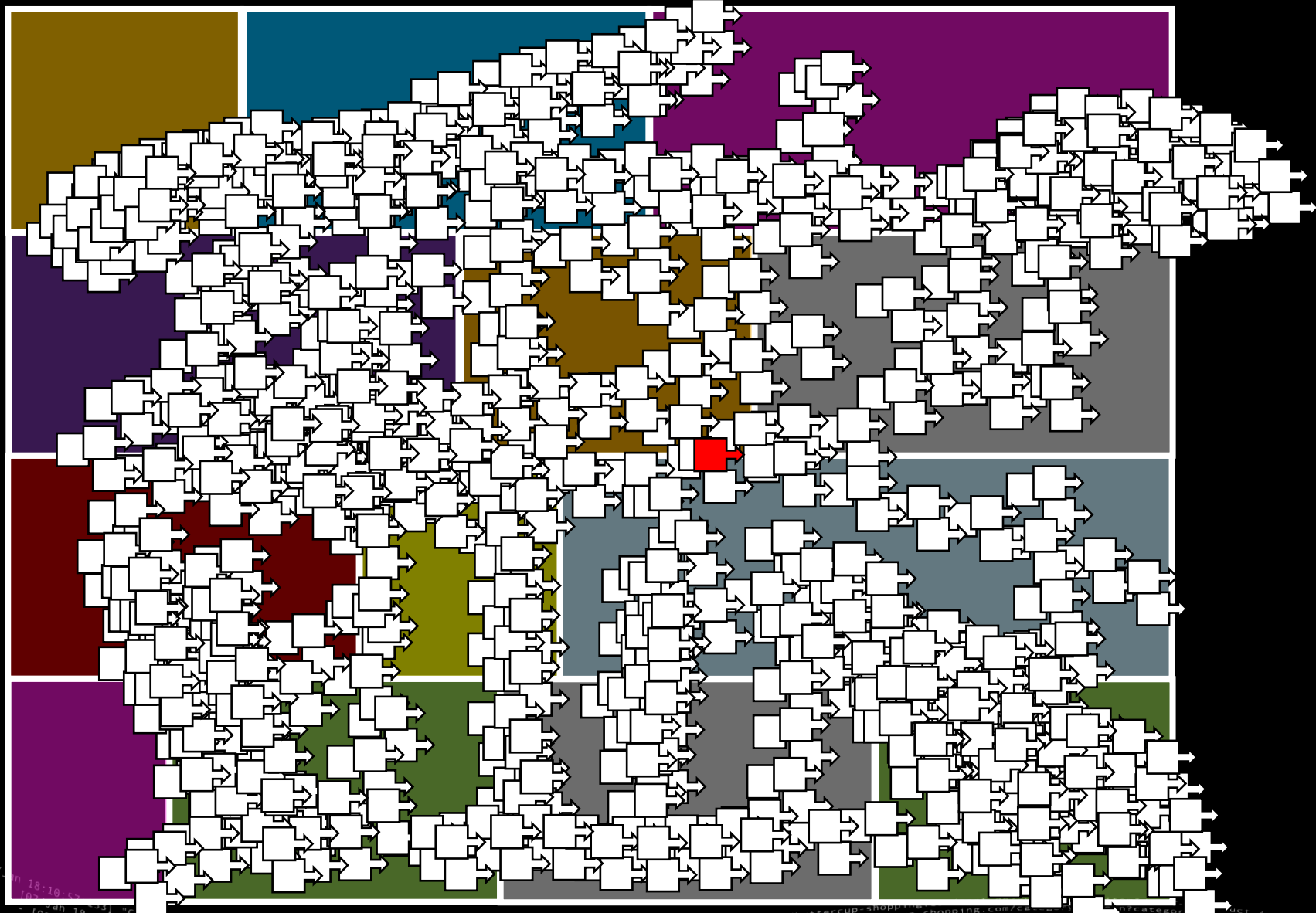
```
130.60.4 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GIFTS&product_id=FL-SW-01" "Opera/9.80.2017.12  
128.241.220.82 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-18&product_id=EST-20&product_id=K9-CU-01" "Compaq  
ows NT 5.1; SV1: 317 27.160.0.0 [07/Jan 18:10:55:189] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SLI0E2ADFF9 HTTP 1.1" 200 3865 "http://  
product_id=RP-LI-02" "Opera/9.80.2017.12; U.S. 317 27.160.0.0 [07/Jan 18:10:55:198] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&item_id=EST-1  
opping.com/purchase&item_id=EST-20&product_id=K9-CU-01" "Opera/9.80.2017.12; U.S. 317 27.160.0.0 [07/Jan 18:10:55:198] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&item_id=EST-1  
opping.com/purchase&item_id=EST-20&product_id=K9-CU-01" "Opera/9.80.2017.12; U.S. 317 27.160.0.0 [07/Jan 18:10:55:198] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&item_id=EST-1
```

... Exponentially



```
130.60.4 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 404 720 "http://buttercup-shopping.com/...?category_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&category_id=FI-SW-01"
... 317.27.160.0 0 "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/...?category_id=FI-SW-01"
... SVL: "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 468 125.17.14.10 "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/purchase-shopping_id=RP-LI-02"
... [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD55L9FF1ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/...?category_id=FI-SW-01"
... [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&category_id=FI-SW-01"
... [07/Jan 18:10:55:187] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 468 125.17.14.10 "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/purchase-shopping_id=RP-LI-02"
```

When a component fails in such an environment,



What does it even mean?

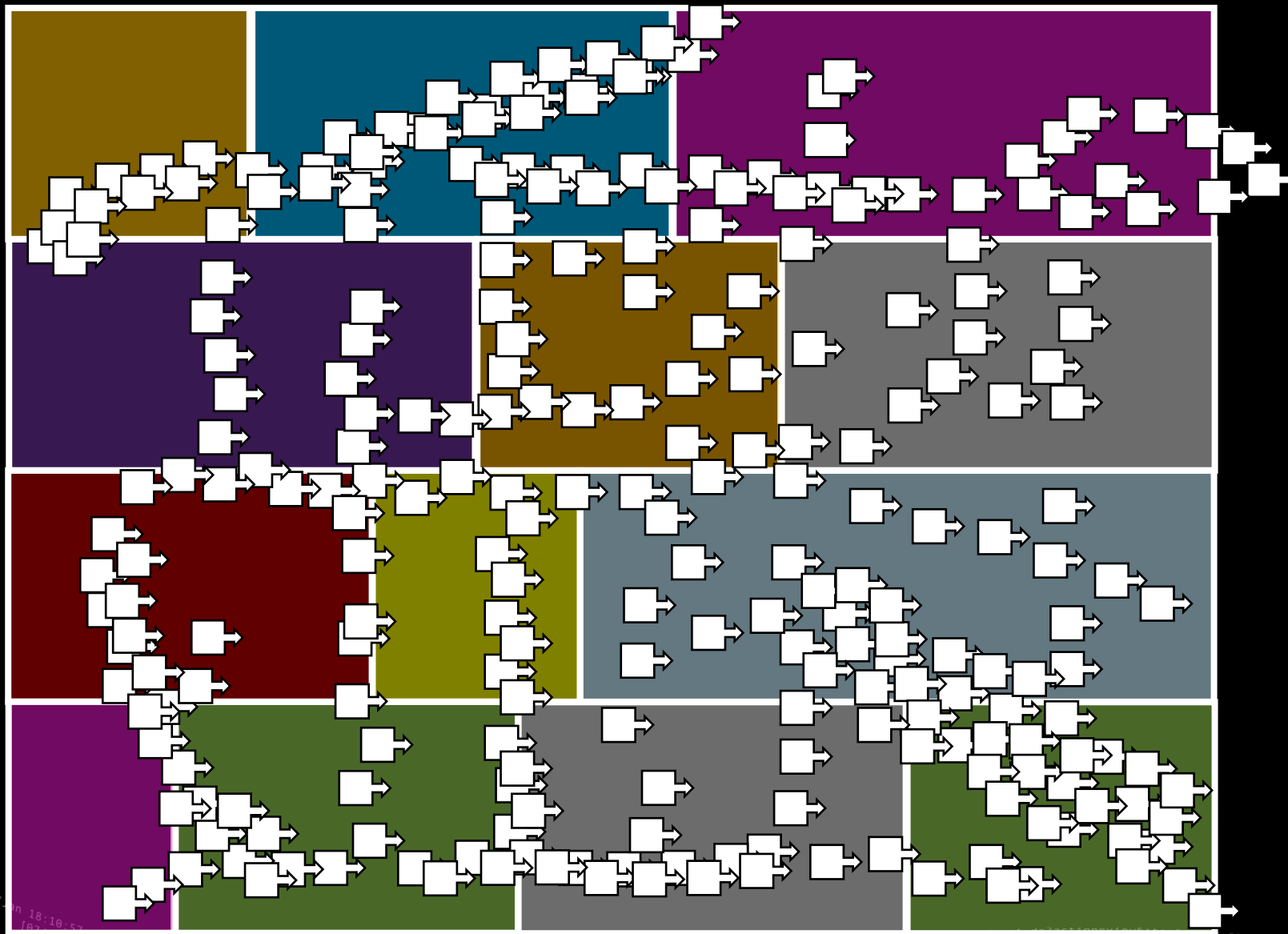


```
130.60.4 - - [07/Jan 18:10:57:123] "GET /category_screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-16&JSESSIONID=SD1SLAFF10ADFF10" 200 200  
128.241.220.82 - - [07/Jan 18:10:56:156] "GET /product_screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category_screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3" 200 1318  
... [07/Jan 18:10:56:189] "GET /cart.do?action=changequantity&item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 189 "GET /category_screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3" 200 1318  
... [07/Jan 18:10:56:198] "GET /category_screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "GET /category_screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3" 200 1318
```

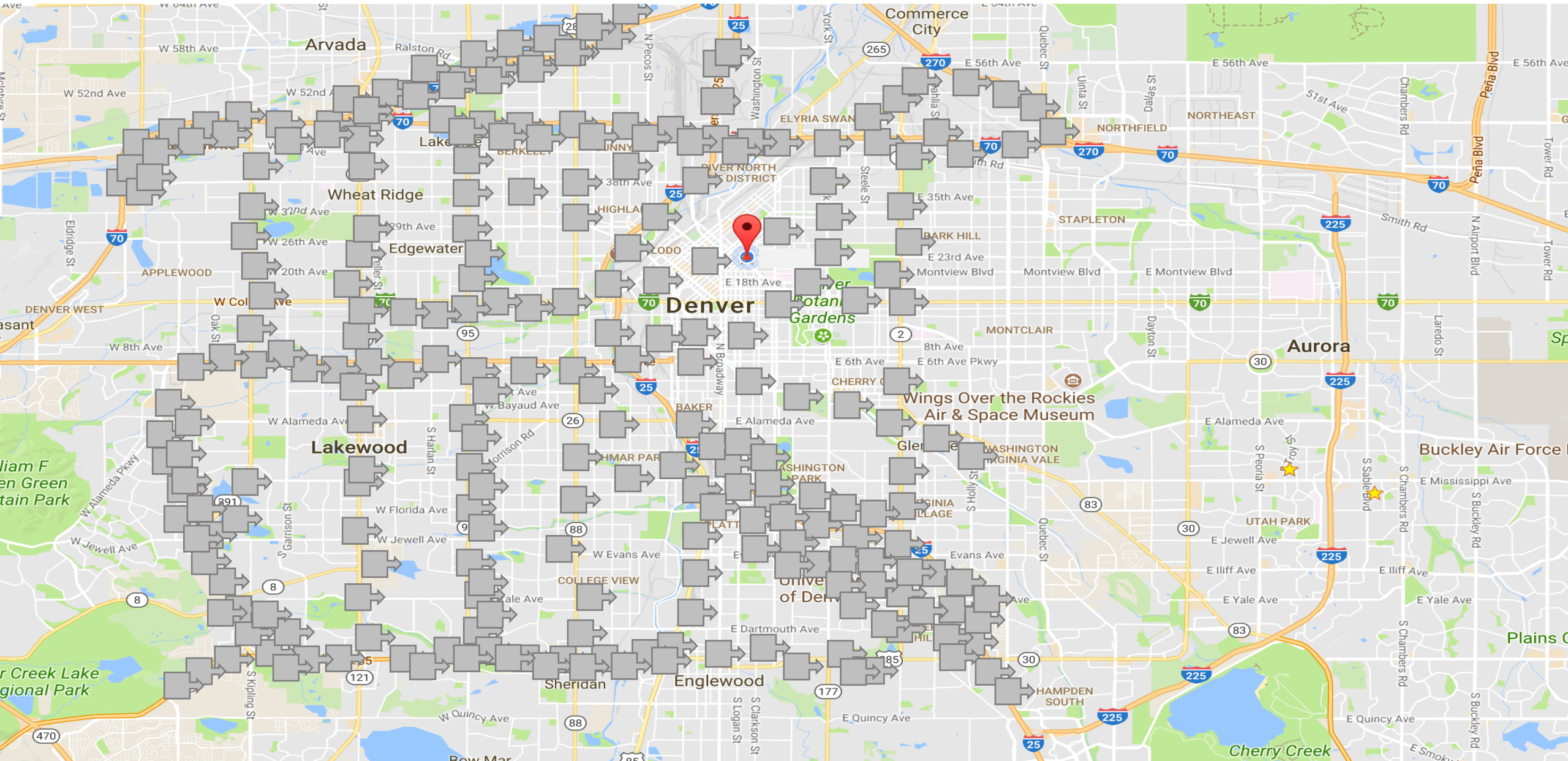



A Story about Denver Traffic

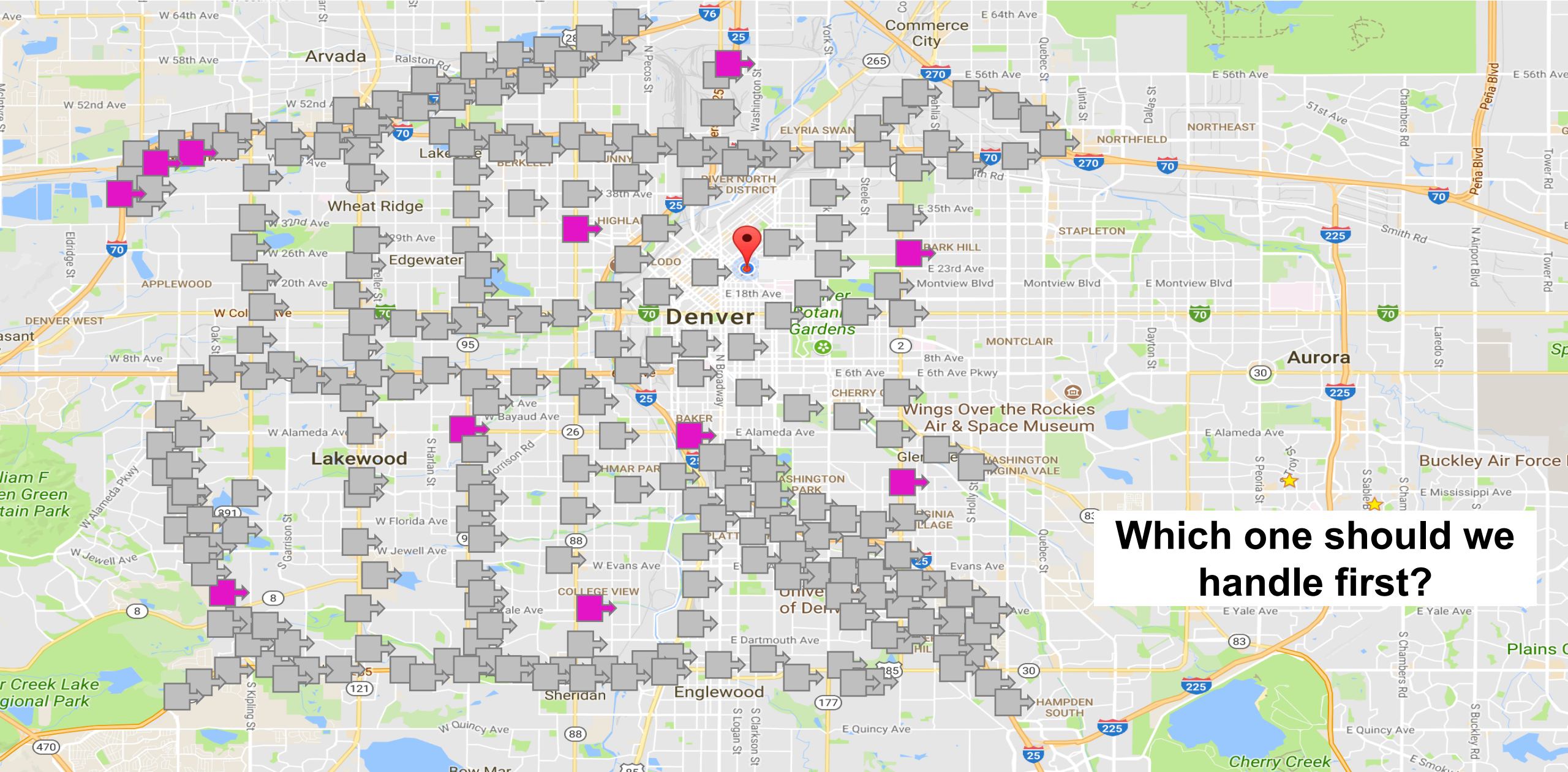
Managing Events is Lot Like Managing Vehicles



Welcome to the Vehicle Operations Center (VOC)

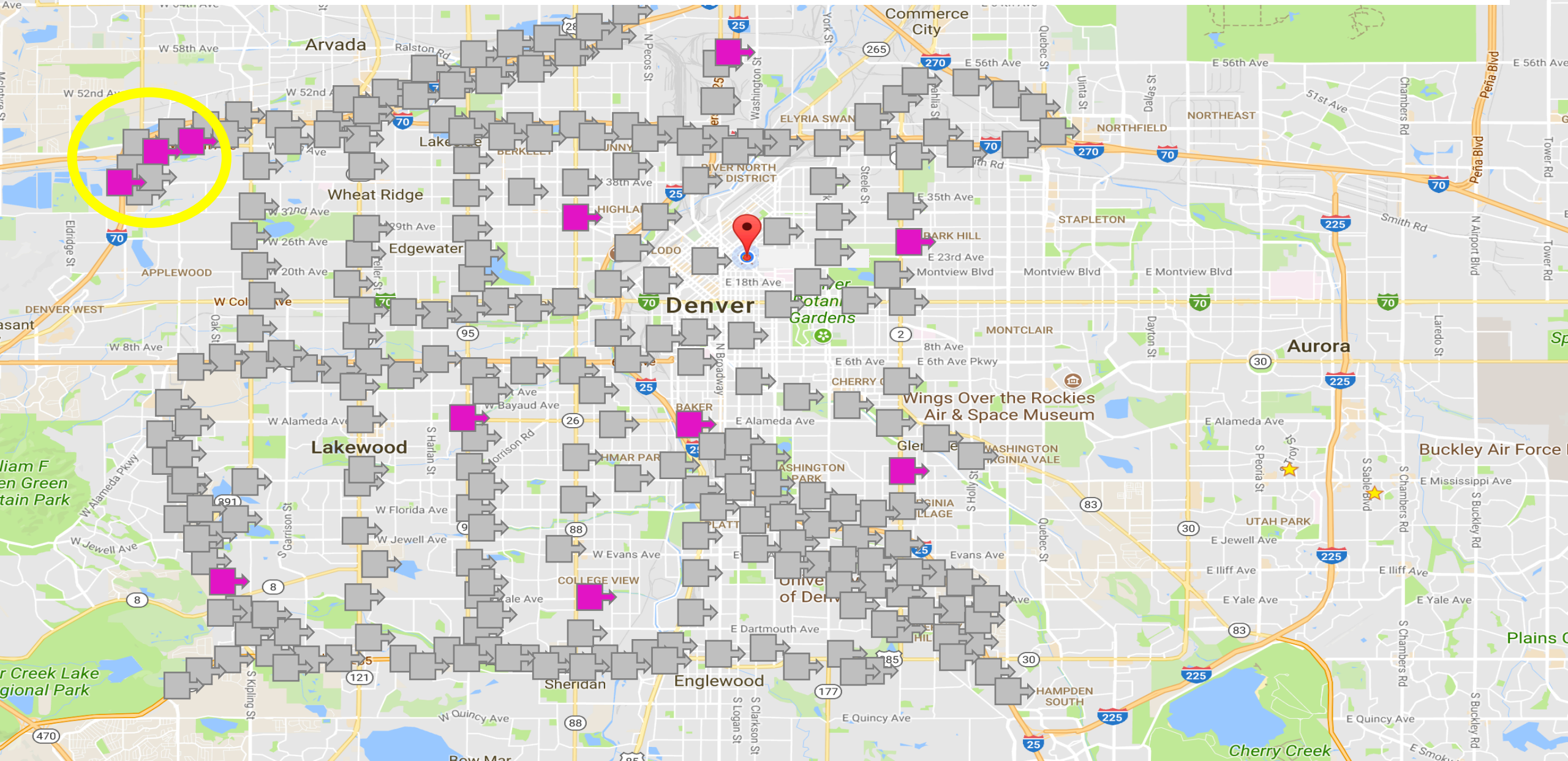


We Just Received 11 Car-Won't-Start events

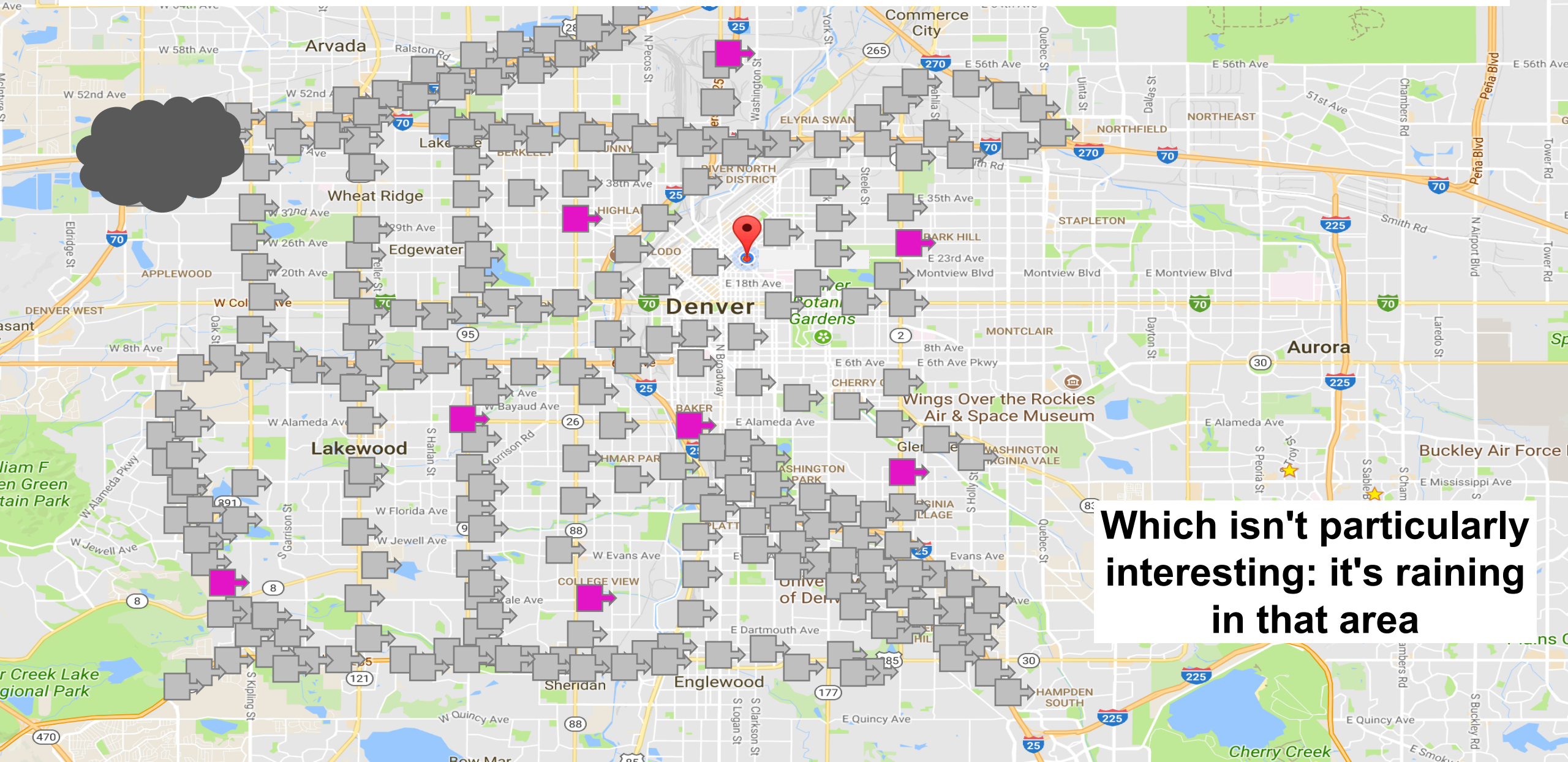


Which one should we handle first?

Machine Learning identifies a cluster!

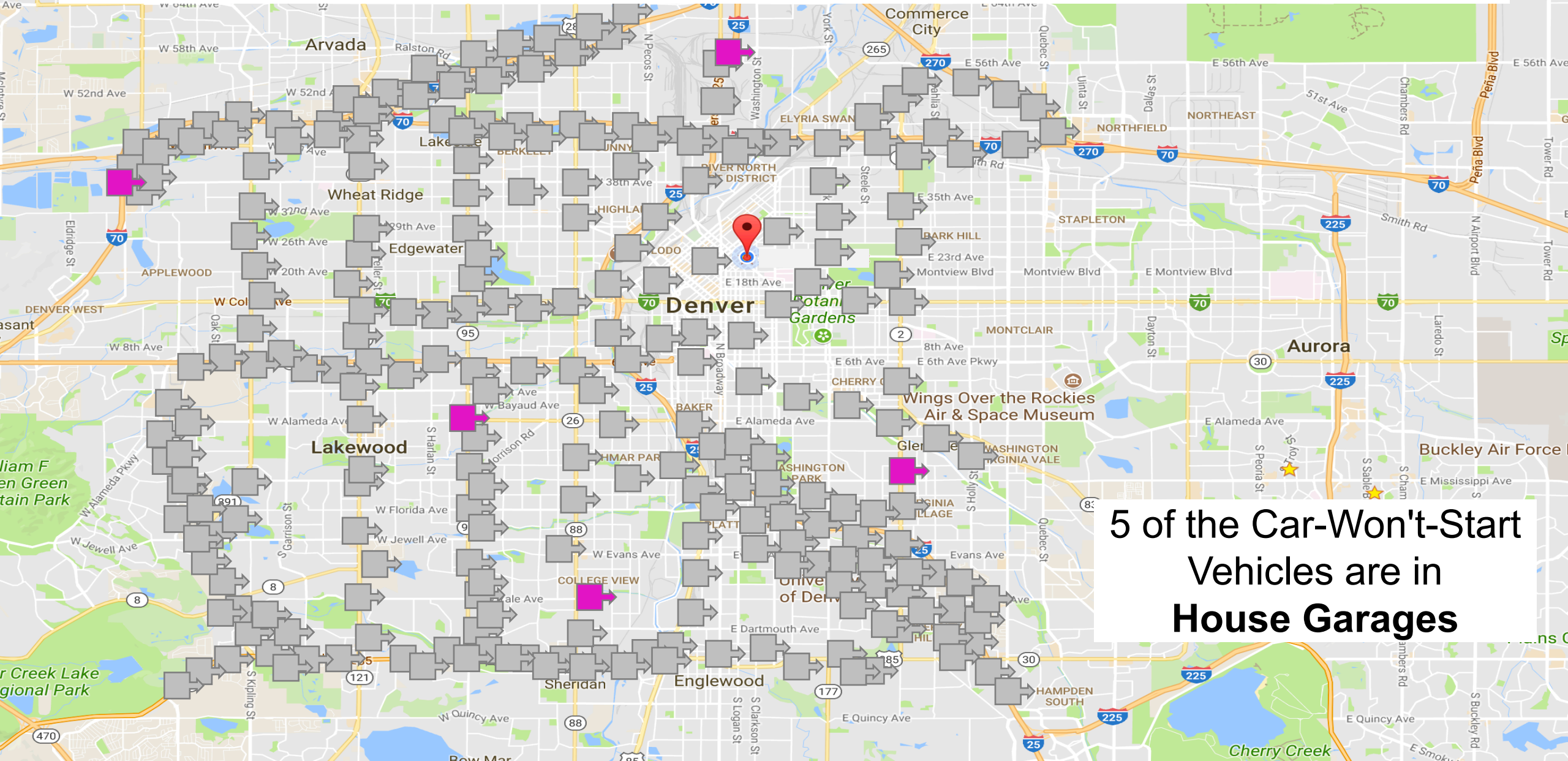


Machine Learning identifies a cluster!



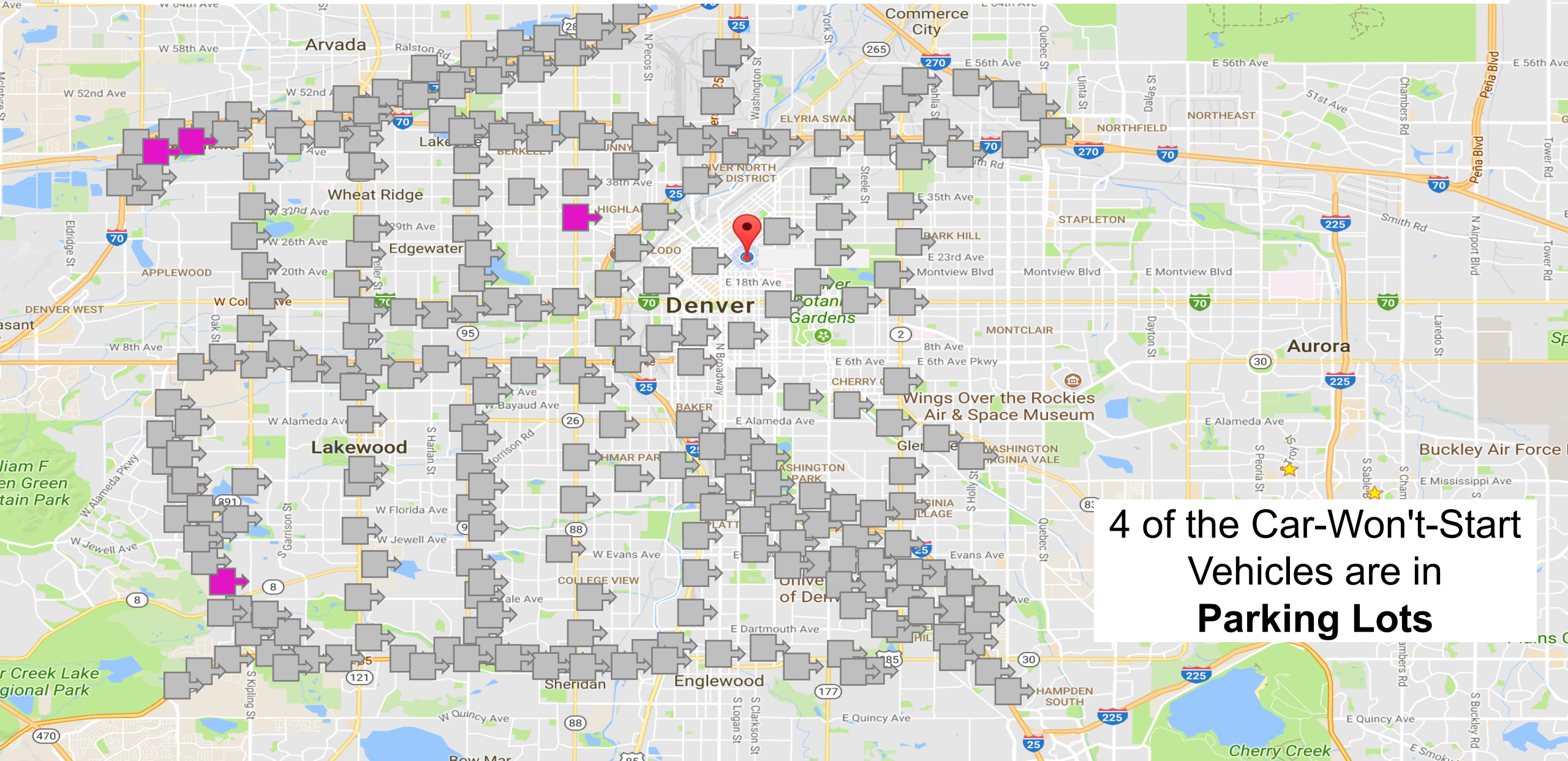
Which isn't particularly interesting: it's raining in that area

Let's Apply Context:



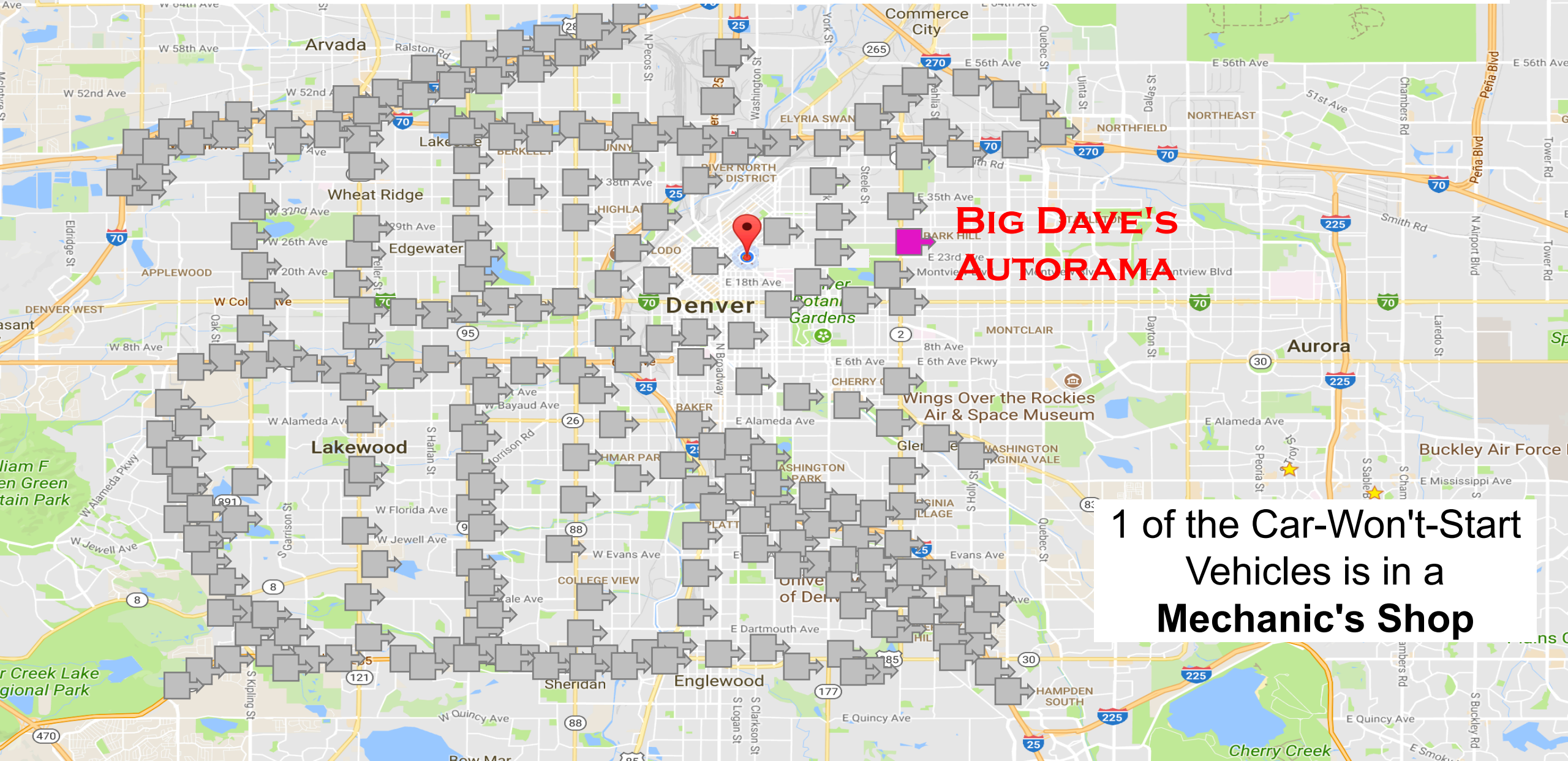
5 of the Car-Won't-Start Vehicles are in House Garages

Let's Apply Context:



4 of the Car-Won't-Start Vehicles are in Parking Lots

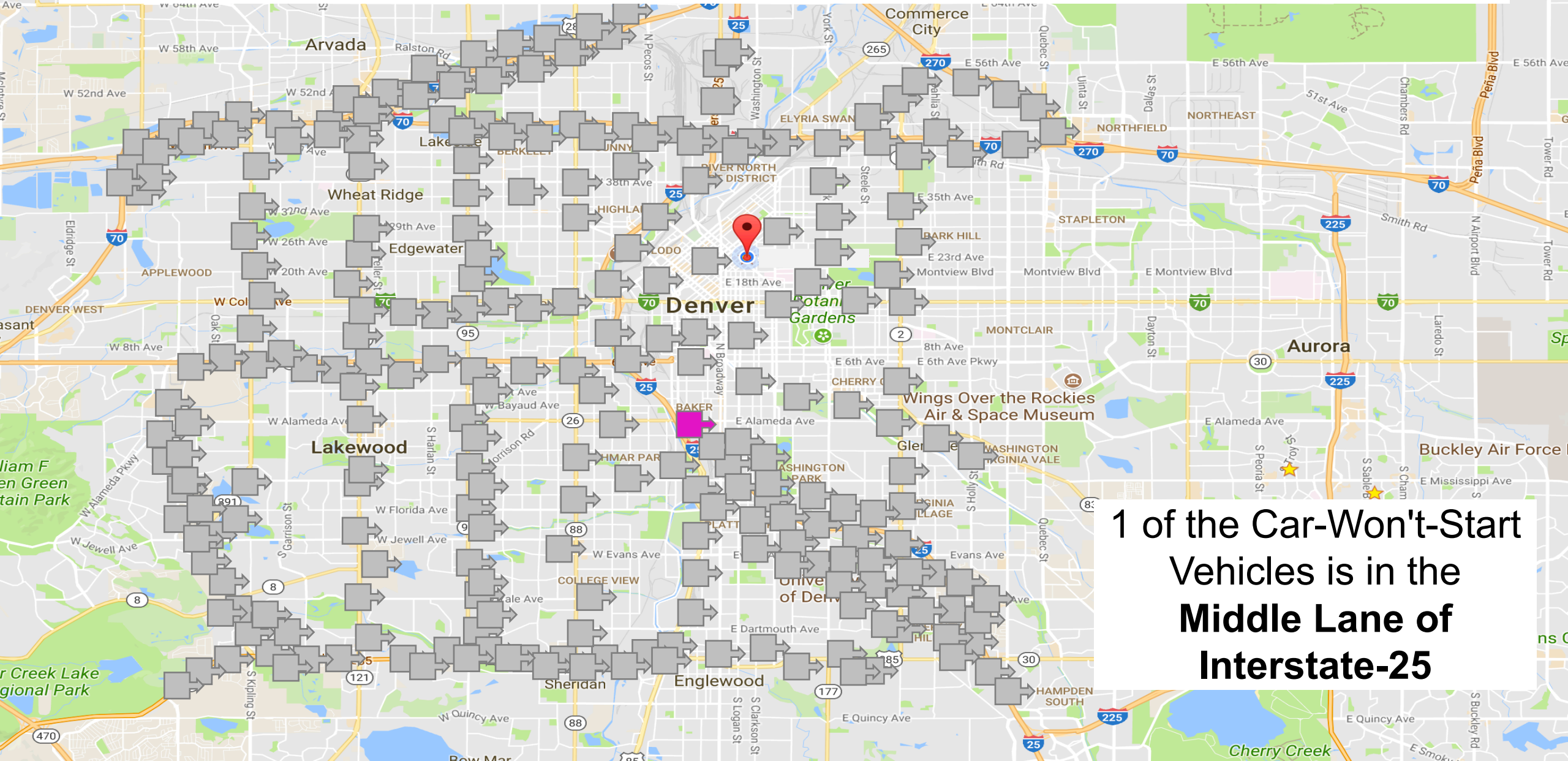
Let's Apply Context:



**BIG DAVE'S
AUTORAMA**

**1 of the Car-Won't-Start
Vehicles is in a
Mechanic's Shop**

Let's Apply Context:

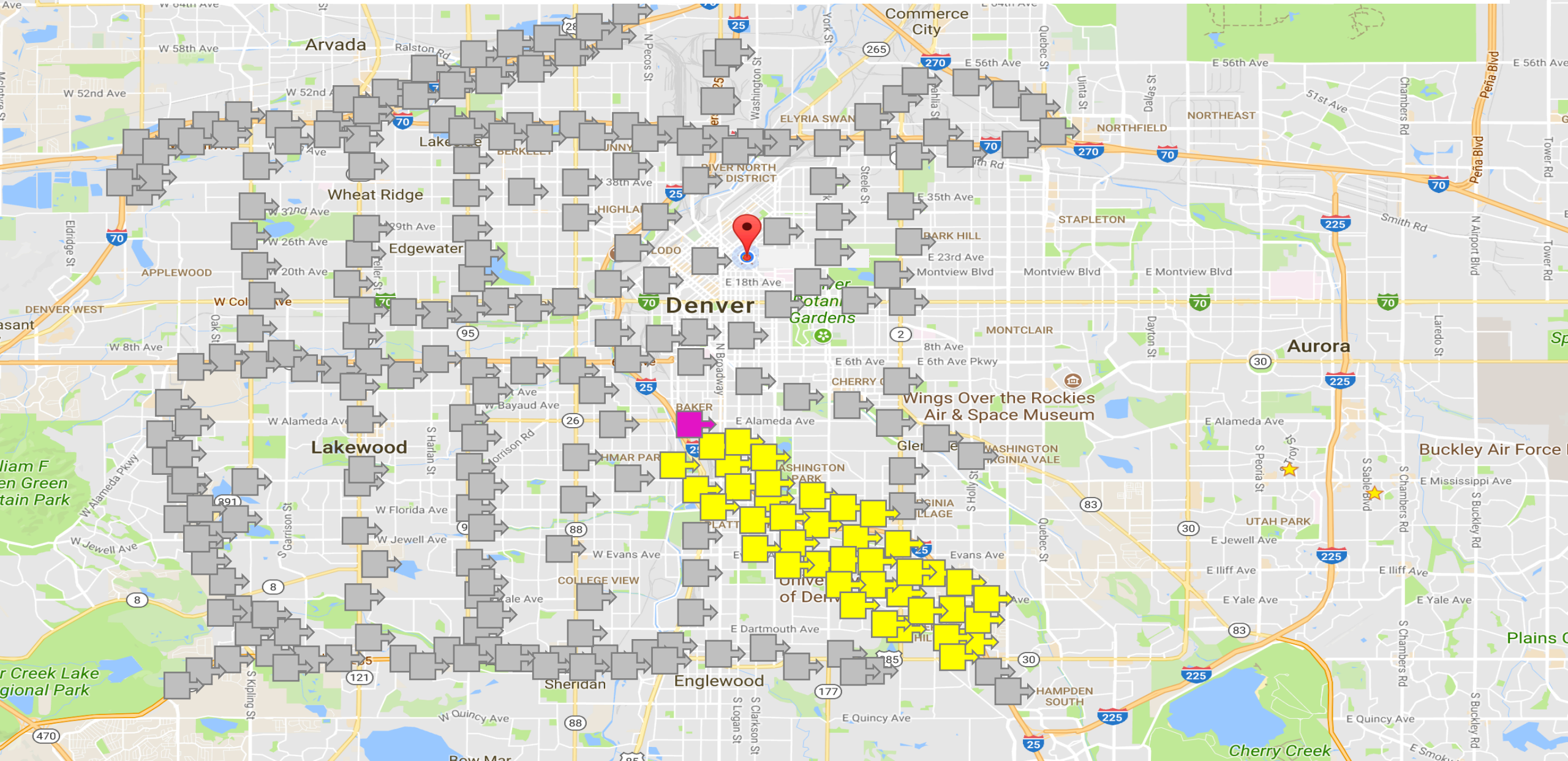


1 of the Car-Won't-Start Vehicles is in the Middle Lane of Interstate-25

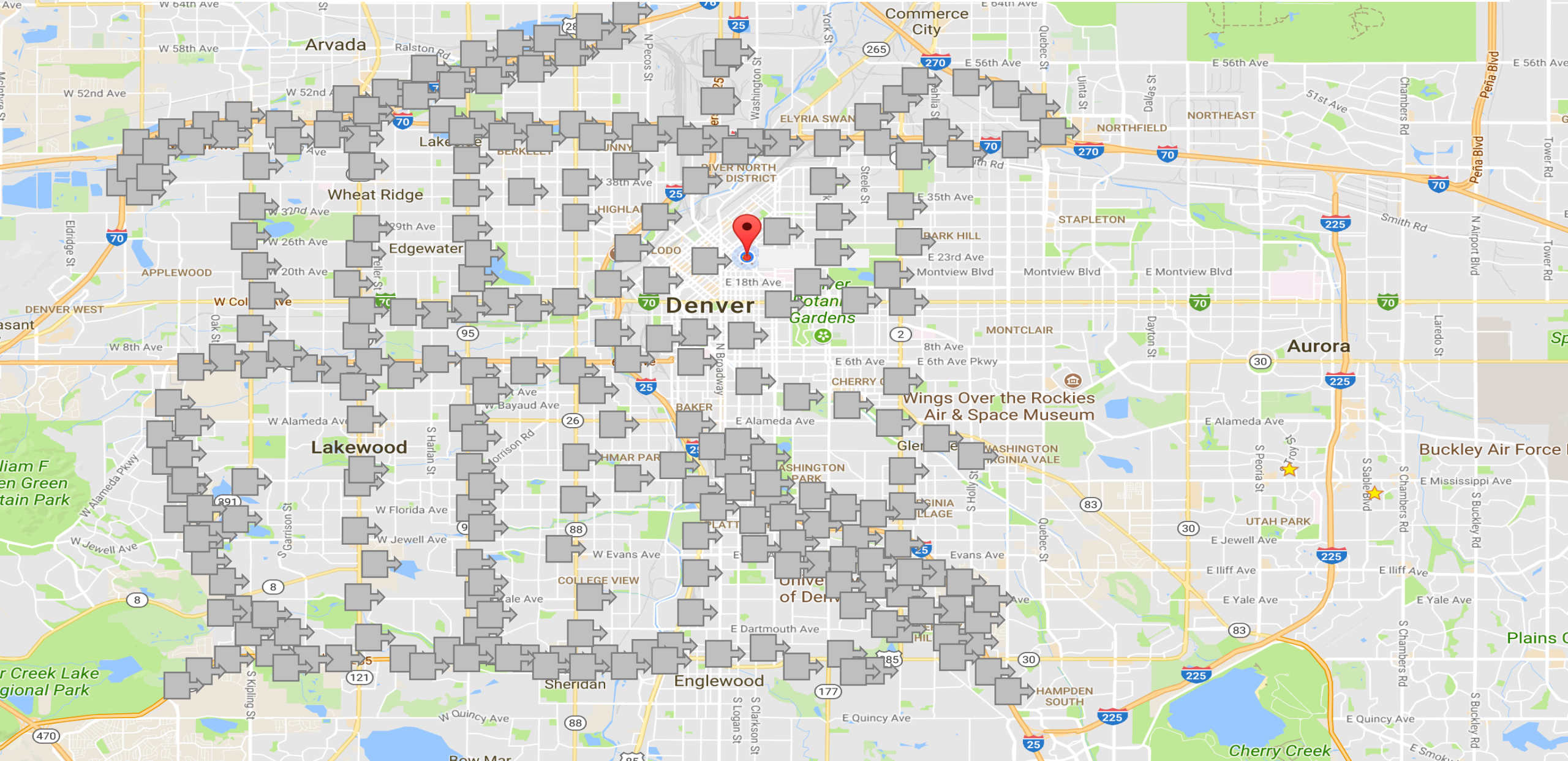
Which One Should We Handle First?



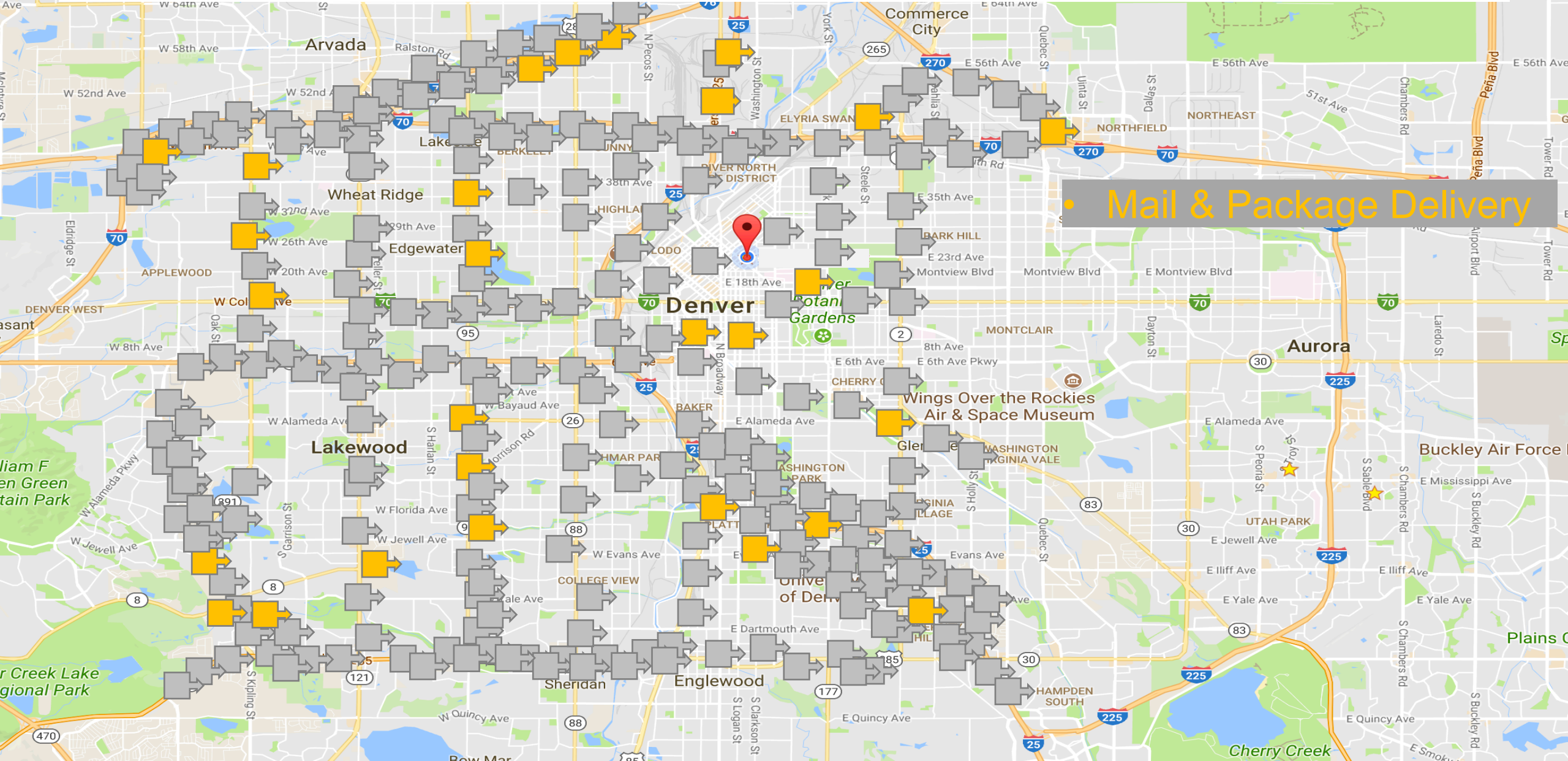
(Service) Context is Everything!



What Are the Important Services?

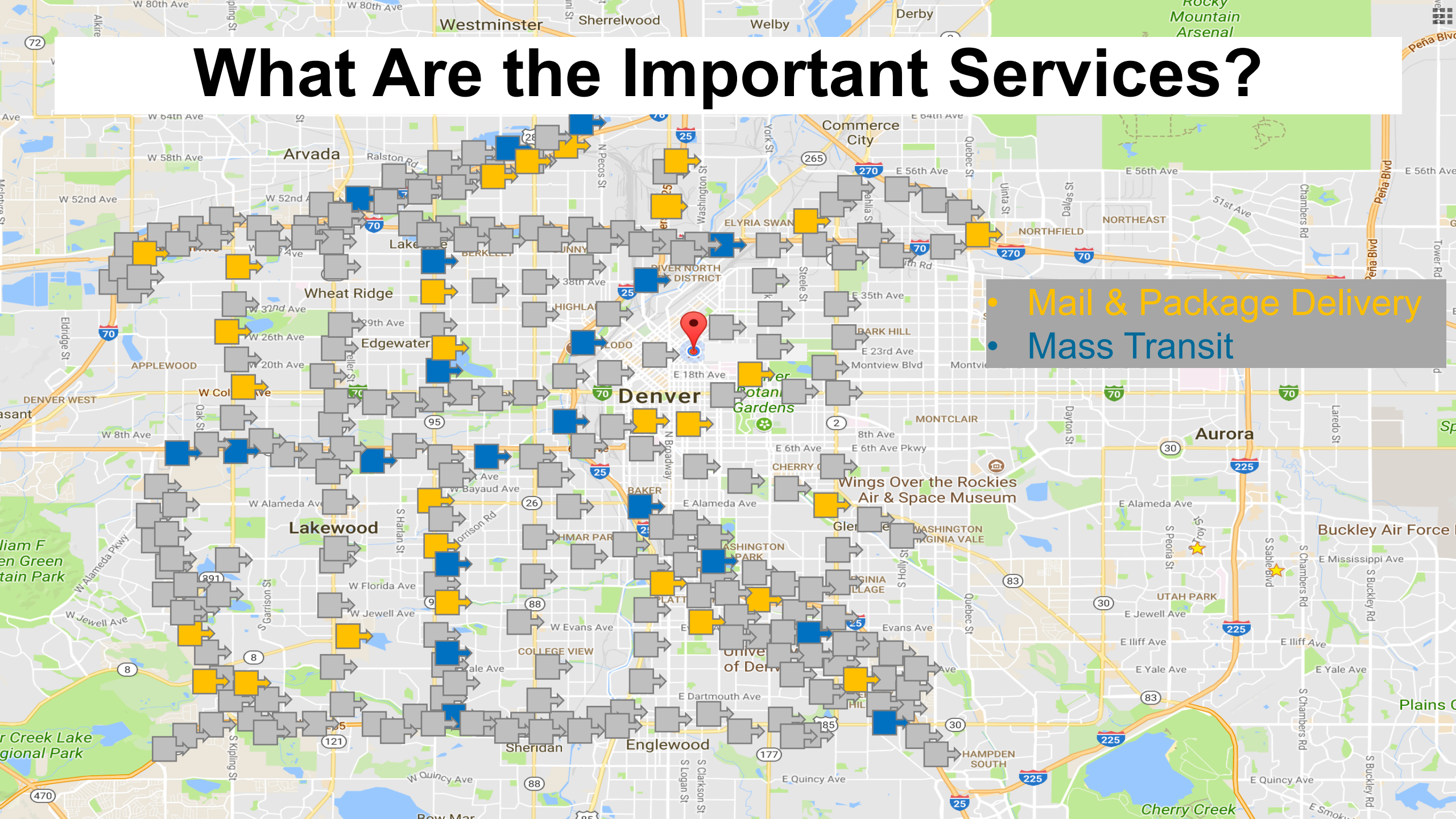


What Are the Important Services?



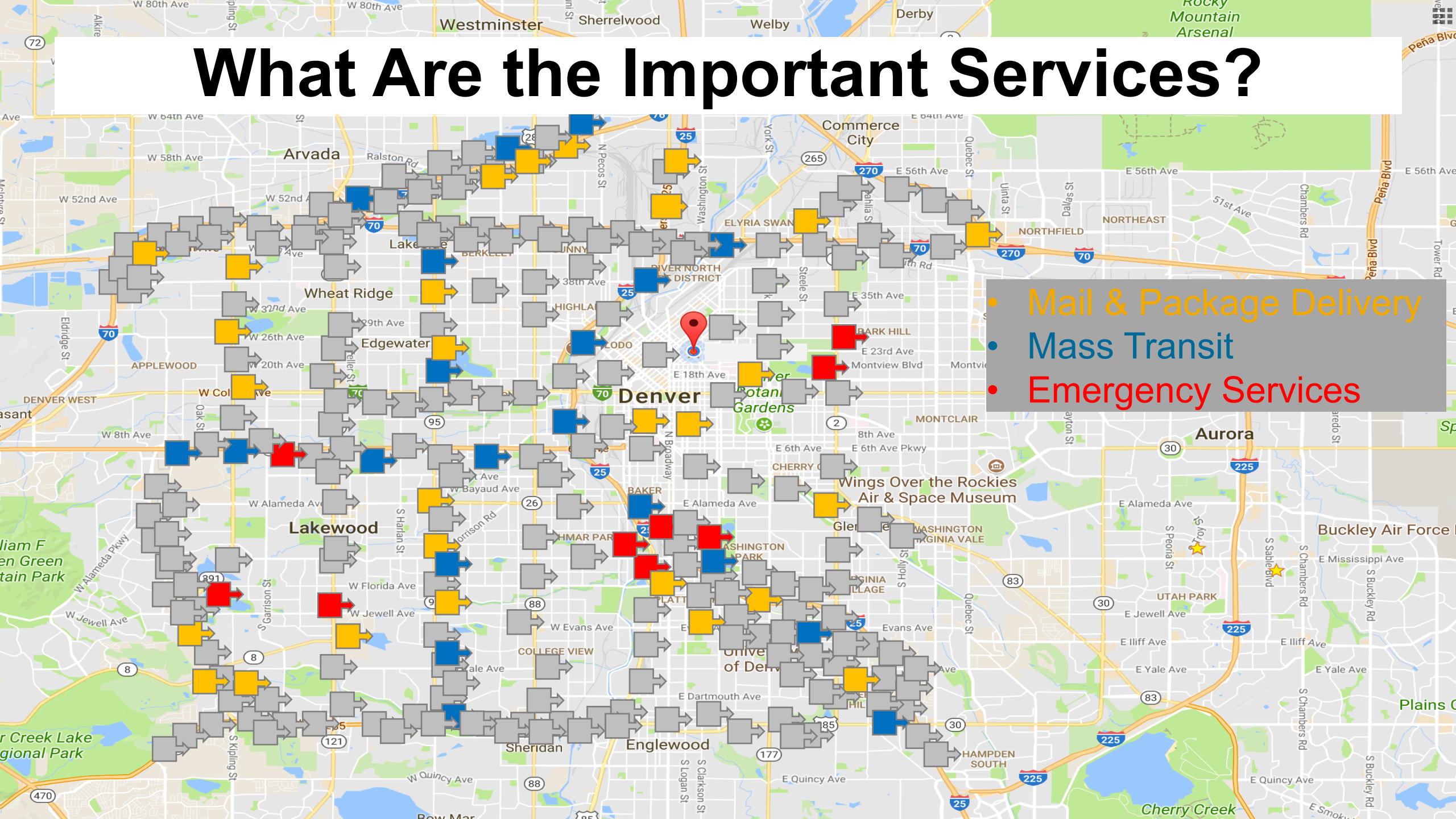
What Are the Important Services?

- Mail & Package Delivery
- Mass Transit



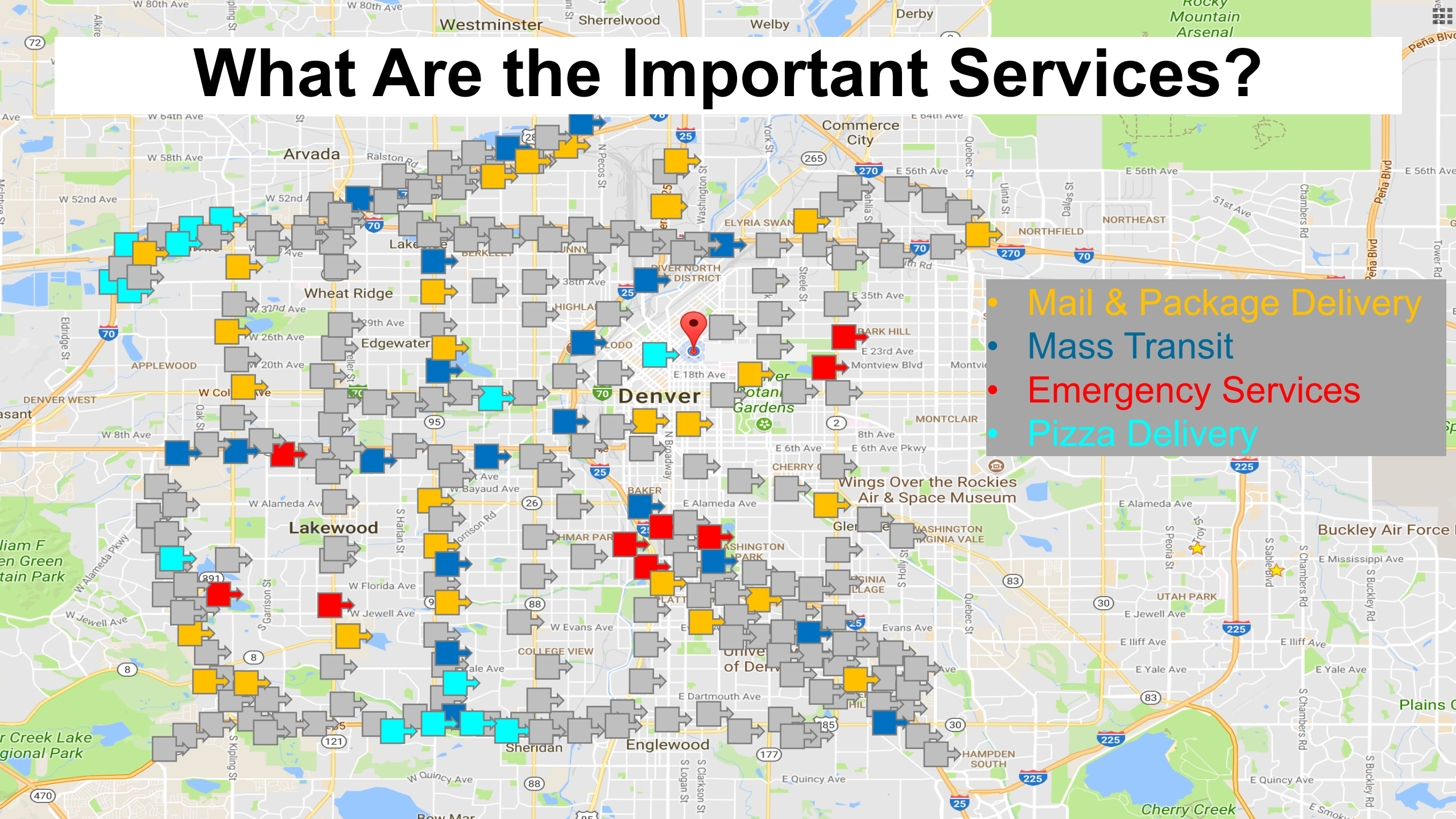
What Are the Important Services?

- Mail & Package Delivery
- Mass Transit
- Emergency Services

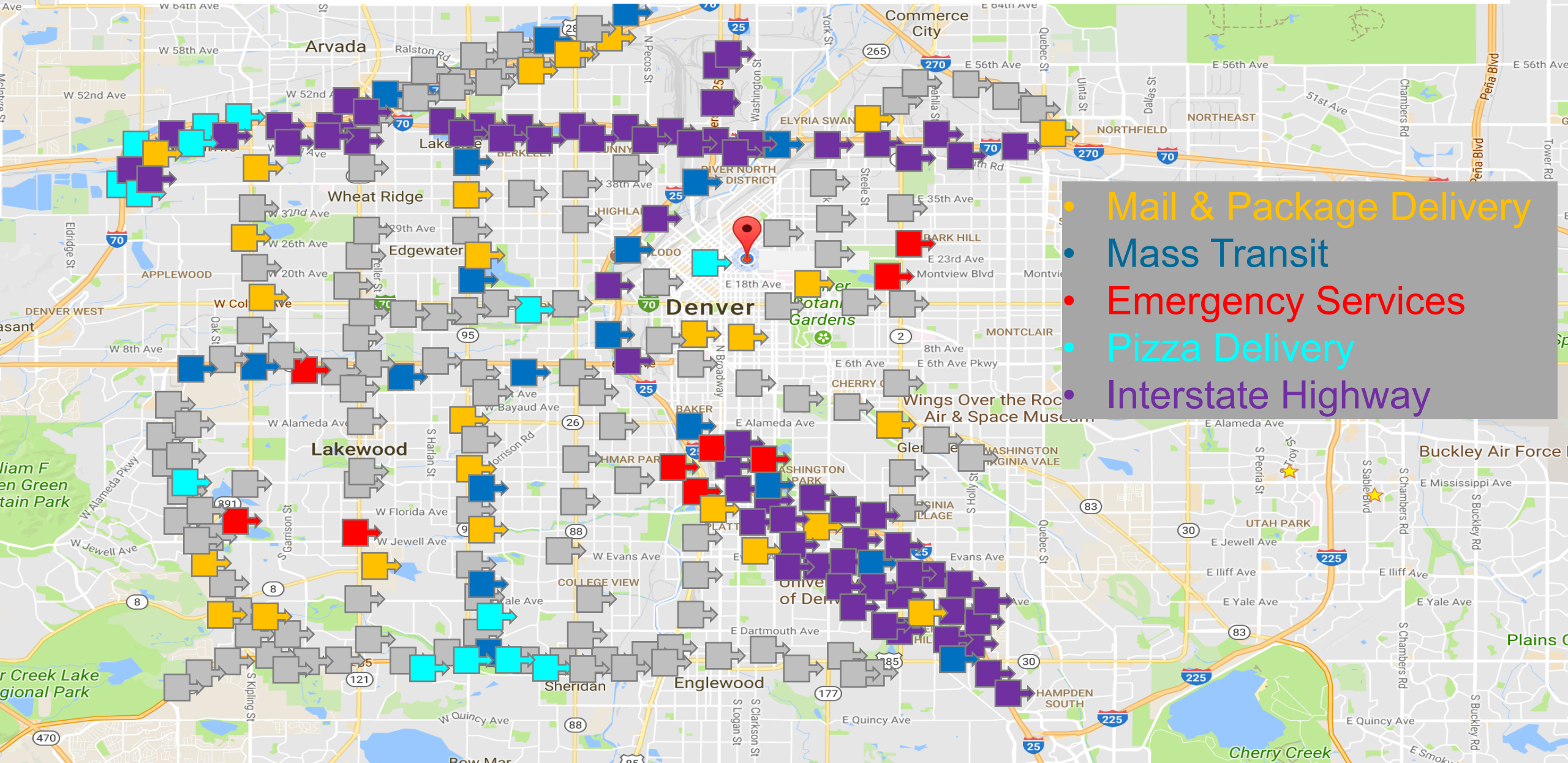


What Are the Important Services?

- Mail & Package Delivery
- Mass Transit
- Emergency Services
- Pizza Delivery

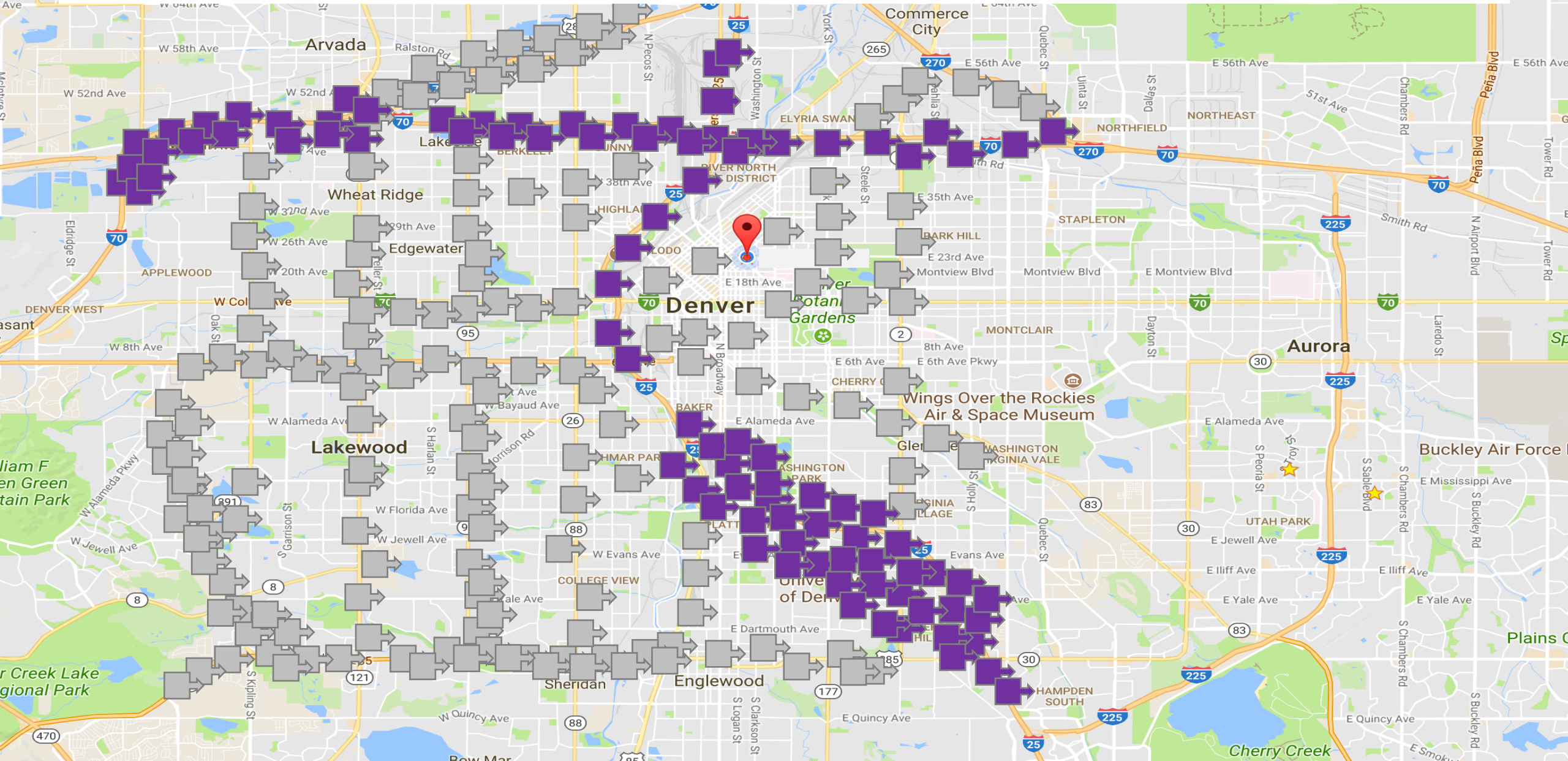


What Are the Important Services?



- Mail & Package Delivery
- Mass Transit
- Emergency Services
- Pizza Delivery
- Interstate Highway

Interstate Highway Service

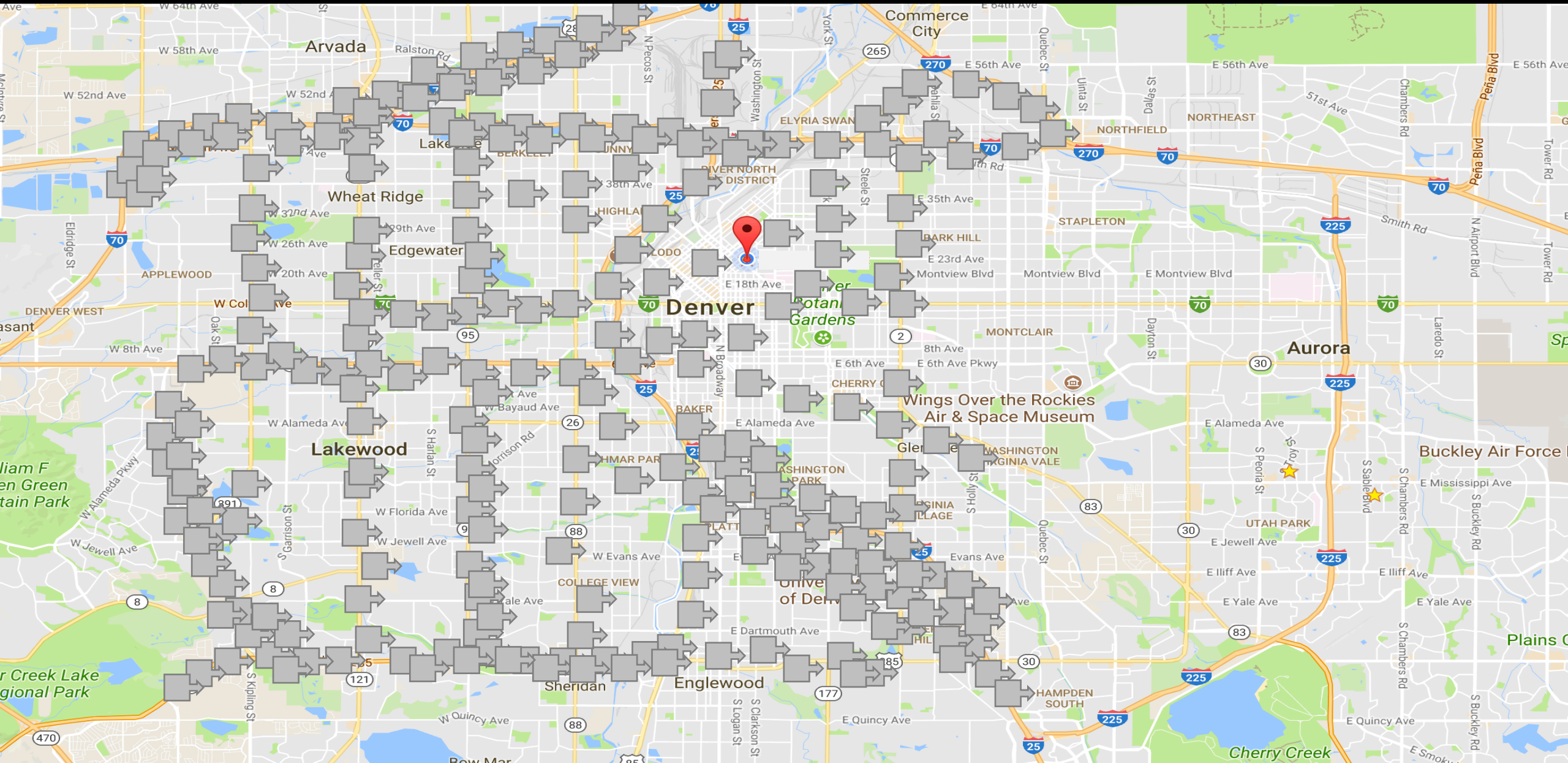


Events Aren't Enough

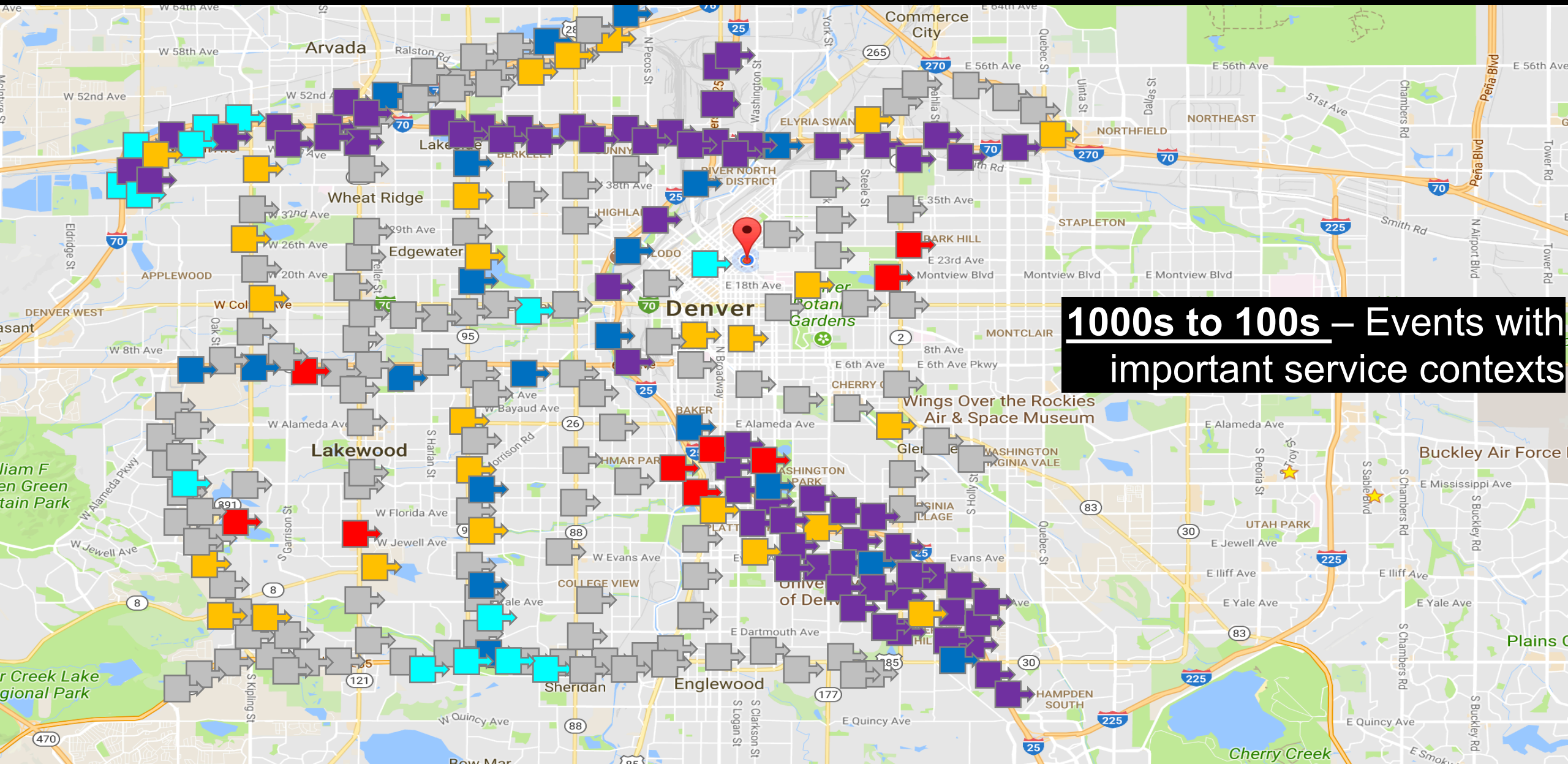
Metrics, Logged and Wire Data Fill In the Blind Spots

- ▶ 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

Notable Events at Human Scale

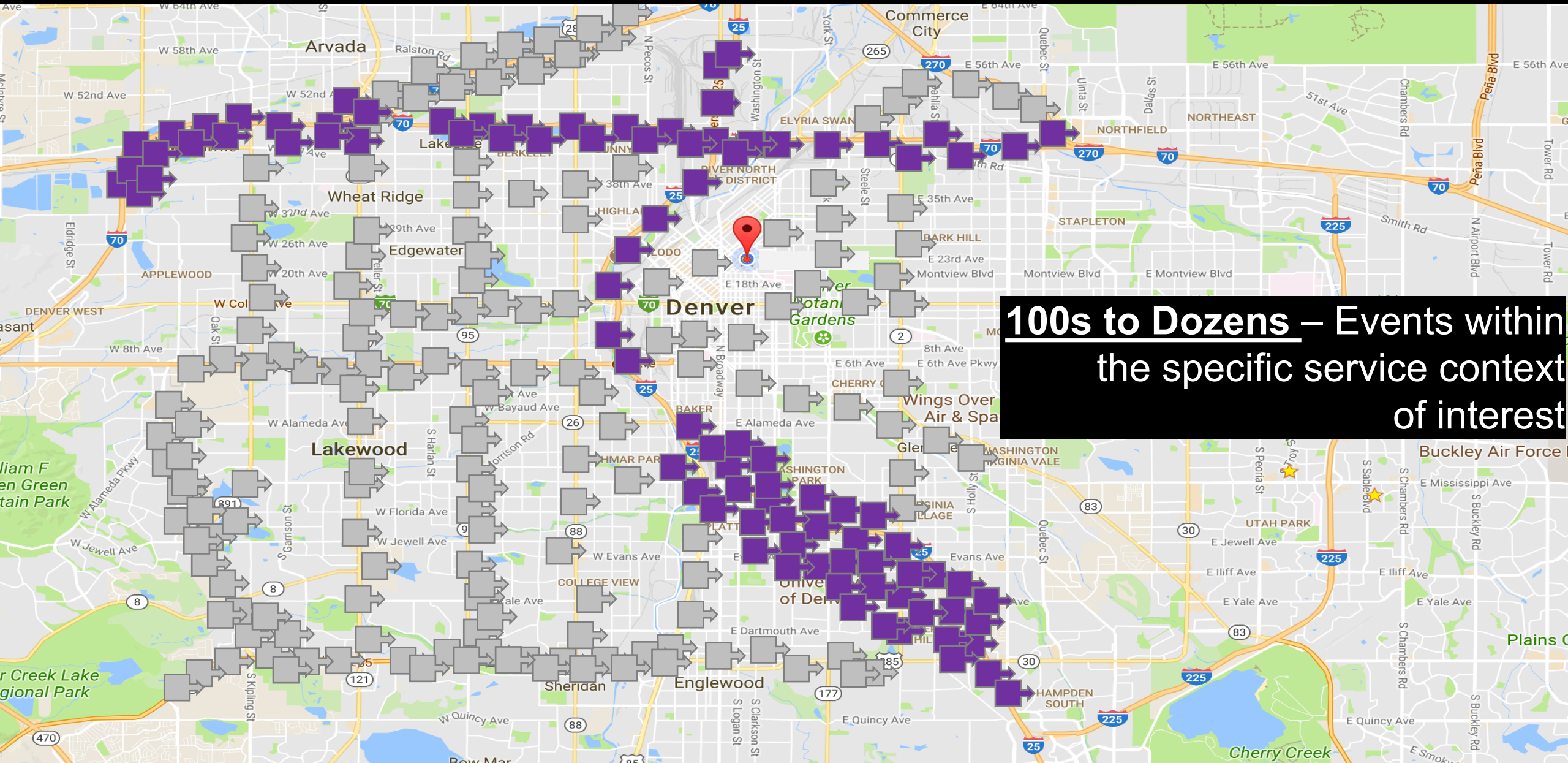


Notable Events at Human Scale



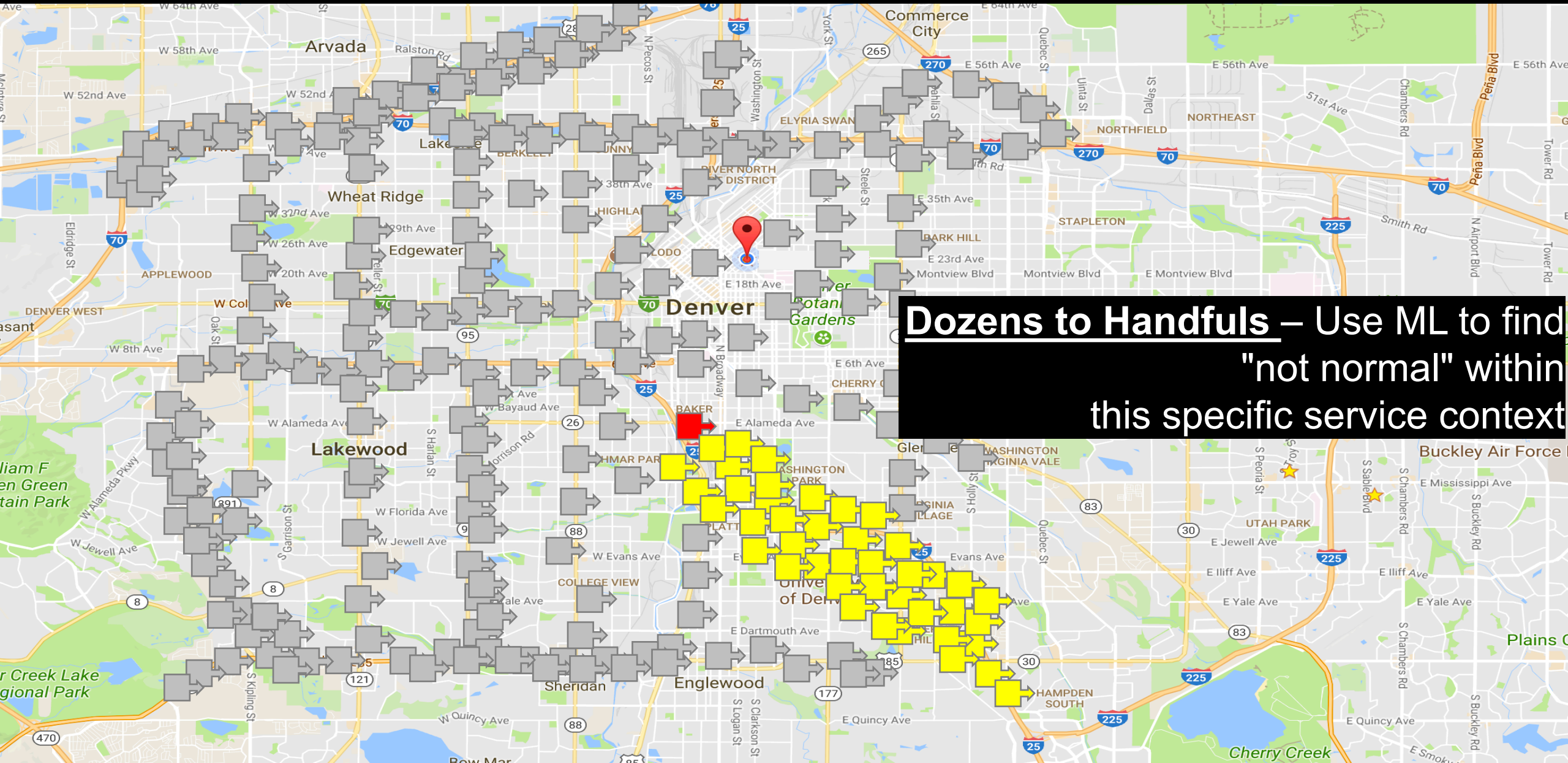
1000s to 100s – Events with important service contexts

Notable Events at Human Scale



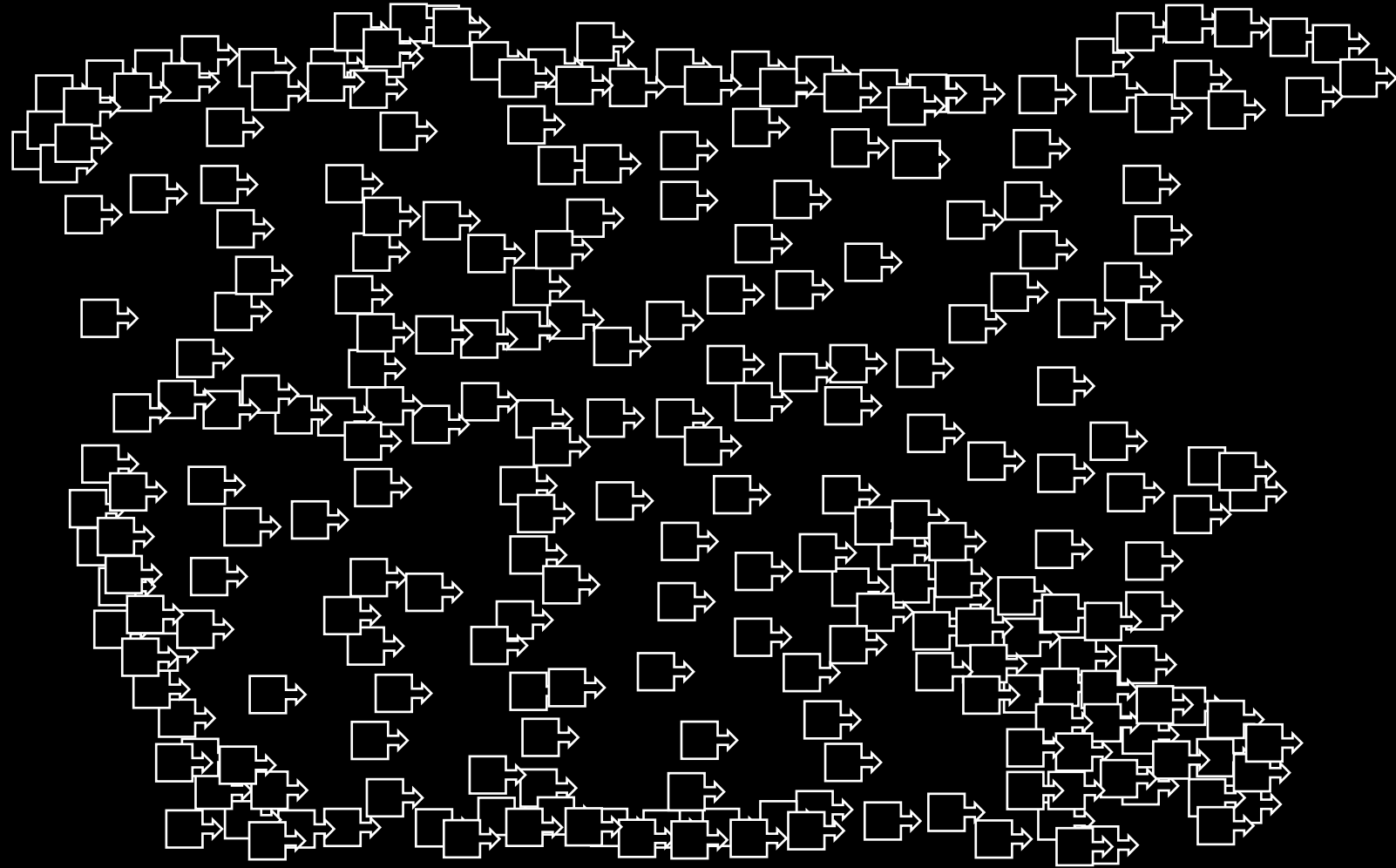
100s to Dozens – Events within the specific service context of interest

Notable Events at Human Scale



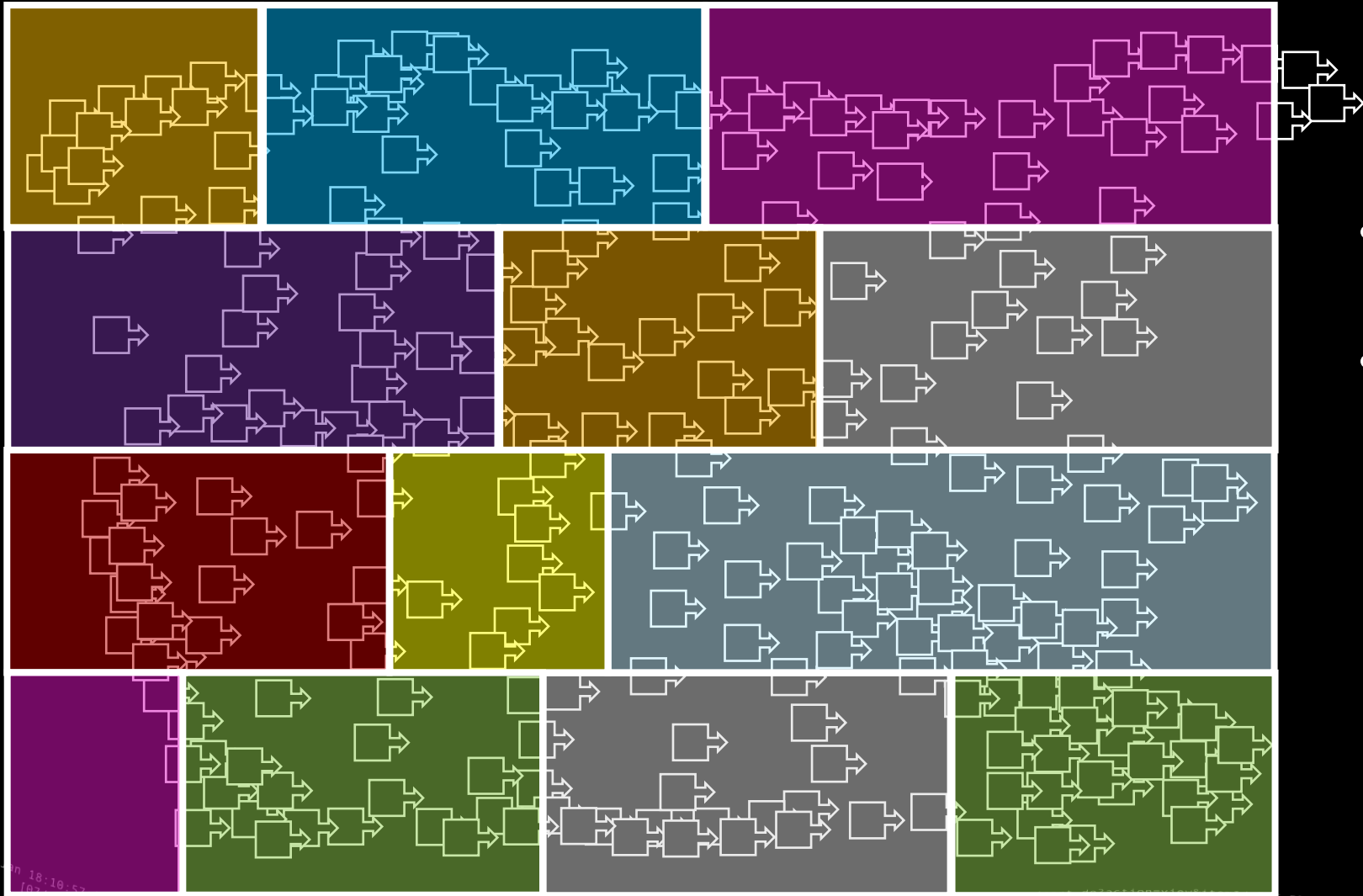
Dozens to Handfuls – Use ML to find "not normal" within this specific service context

The Old IT Ways Don't Work Anymore



```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.29  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS" "Maxillia/2.0 (compatible; http://www.maxillia.com)"  
ows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125 17 14 [d] "http://buttercup-shopping.com/product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-20&product_id=K9-CU-01" "CompuLink/1.0  
/buttercup-shopping-16&product_id=RP-LI-02" "Opera/9.80.29.11651; Windows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125 17 14 [d] "http://buttercup-shopping.com/product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-20&product_id=K9-CU-01"  
opping.com/purchase-16&product_id=RP-LI-02" "Opera/9.80.29.11651; Windows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125 17 14 [d] "http://buttercup-shopping.com/product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-20&product_id=K9-CU-01"  
/buttercup-shopping-16&product_id=RP-LI-02" "Opera/9.80.29.11651; Windows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125 17 14 [d] "http://buttercup-shopping.com/product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-20&product_id=K9-CU-01"  
/buttercup-shopping-16&product_id=RP-LI-02" "Opera/9.80.29.11651; Windows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125 17 14 [d] "http://buttercup-shopping.com/product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-20&product_id=K9-CU-01"
```

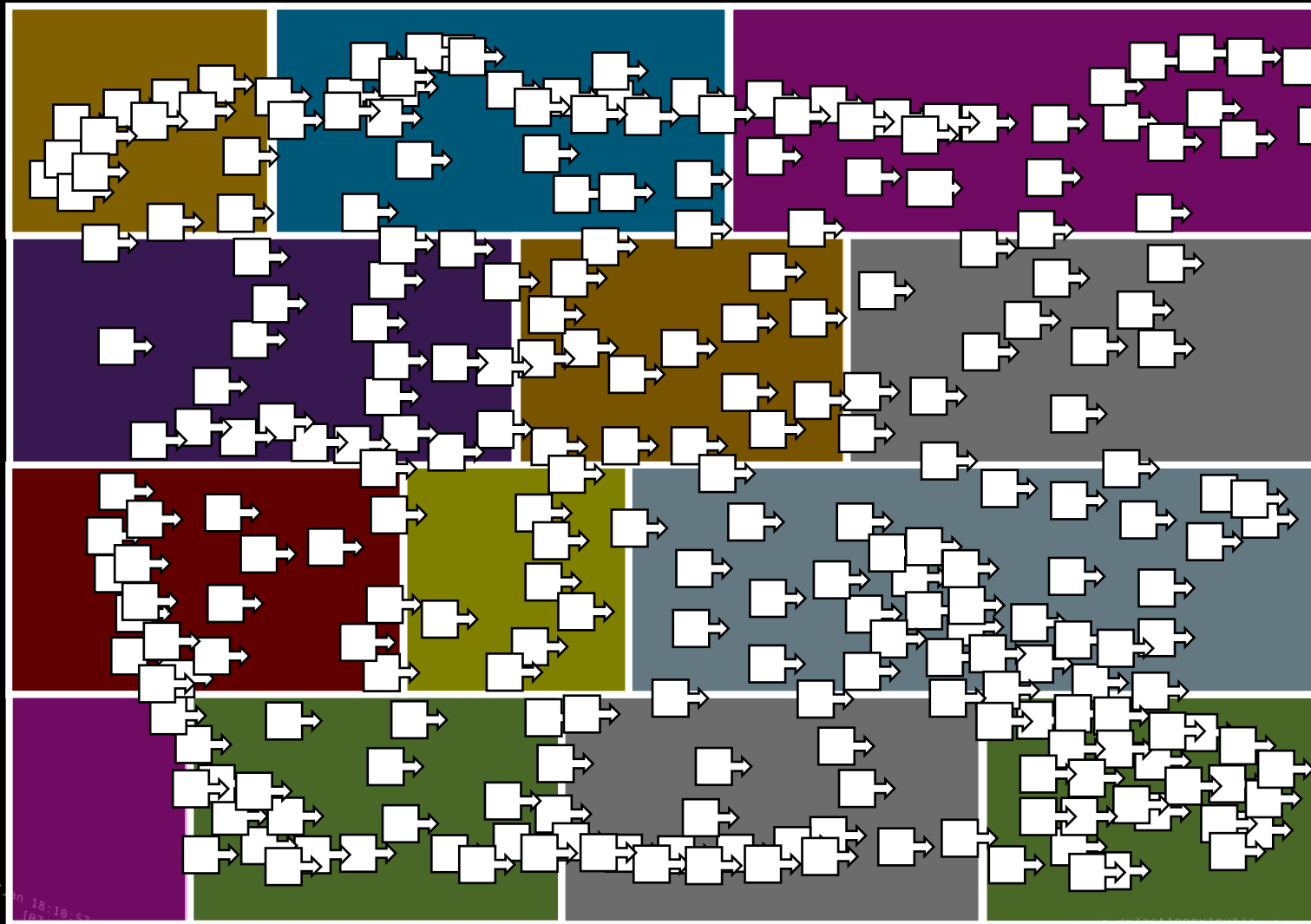

The Old IT Ways Don't Work Anymore



- Event Fatigue
- Complex Environments

```
130.60.4 - - [07/Jan 18:10:55:23] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GIFTS&product_id=FL-SW-01" Operate 20  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=FL-SW-01" Operate 20  
131.27.160.0 - - [07/Jan 18:10:56:150] "GET /product.screen?product_id=FL-DISH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF1ADFF3" Operate 20  
130.60.4 - - [07/Jan 18:10:55:23] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GIFTS&product_id=FL-SW-01" Operate 20  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=FL-SW-01" Operate 20  
131.27.160.0 - - [07/Jan 18:10:56:150] "GET /product.screen?product_id=FL-DISH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF1ADFF3" Operate 20  
130.60.4 - - [07/Jan 18:10:55:23] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GIFTS&product_id=FL-SW-01" Operate 20  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=FL-SW-01" Operate 20  
131.27.160.0 - - [07/Jan 18:10:56:150] "GET /product.screen?product_id=FL-DISH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF1ADFF3" Operate 20  
130.60.4 - - [07/Jan 18:10:55:23] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GIFTS&product_id=FL-SW-01" Operate 20  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=FL-SW-01" Operate 20  
131.27.160.0 - - [07/Jan 18:10:56:150] "GET /product.screen?product_id=FL-DISH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF1ADFF3" Operate 20
```

The Old IT Ways Don't Work Anymore



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

Machine Learning Won't Save Us

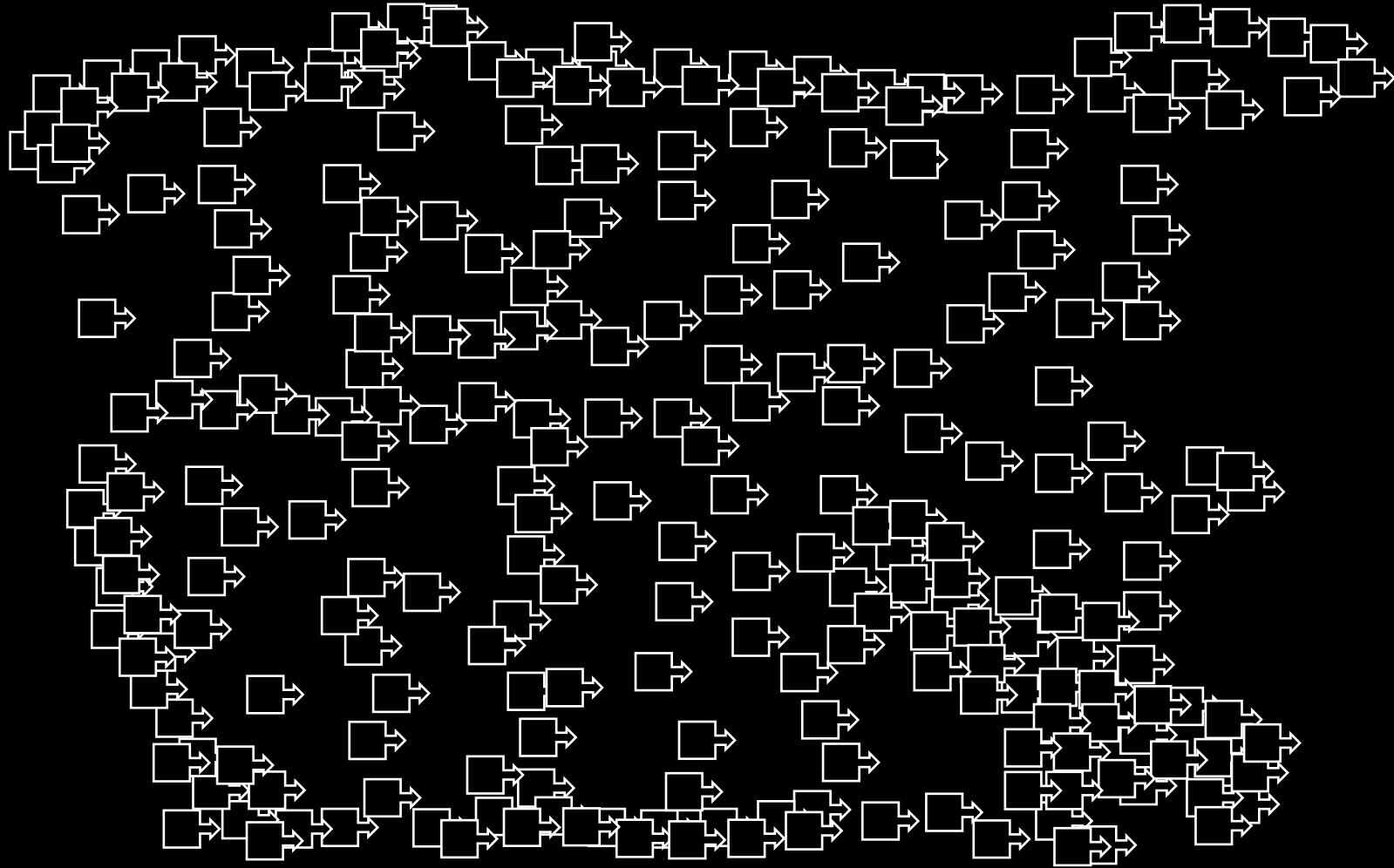
- ▶ ML is the latest approach to magically reduce the huge volume to find that "elusive root cause event"
- ▶ ML IS a powerful new capability which can be useful, but...
- ▶ ML alone will not solve our fundamental problems
- ▶ Without a service context, adding ML to the old deluge of events isn't enough

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=SD5LAFF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&item_id=EST-6&product_id=FL-SW-01" Opera/9.80.29
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5SL7FF6ADFF9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-20&product_id=K9-CU-01" Mozilla/5.0 (Windows NT 6.0; rv:2.0) Gecko/20100101 Firefox/4.0.1
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/changequantity?item_id=EST-18&product_id=AV-CB-01&SESSIONID=SD10SLBE12ADFF9 HTTP/1.1" 200 3367 "http://buttercup-shopping.com/oldlink?item_id=EST-16&product_id=RP-LI-02" Opera/9.80.29
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=SD5LAFF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&item_id=EST-6&product_id=FL-SW-01" Opera/9.80.29
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5SL7FF6ADFF9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-20&product_id=K9-CU-01" Mozilla/5.0 (Windows NT 6.0; rv:2.0) Gecko/20100101 Firefox/4.0.1
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/changequantity?item_id=EST-18&product_id=AV-CB-01&SESSIONID=SD10SLBE12ADFF9 HTTP/1.1" 200 3367 "http://buttercup-shopping.com/oldlink?item_id=EST-16&product_id=RP-LI-02" Opera/9.80.29
```

A Better Way: Splunk ITSI for Event Analytics

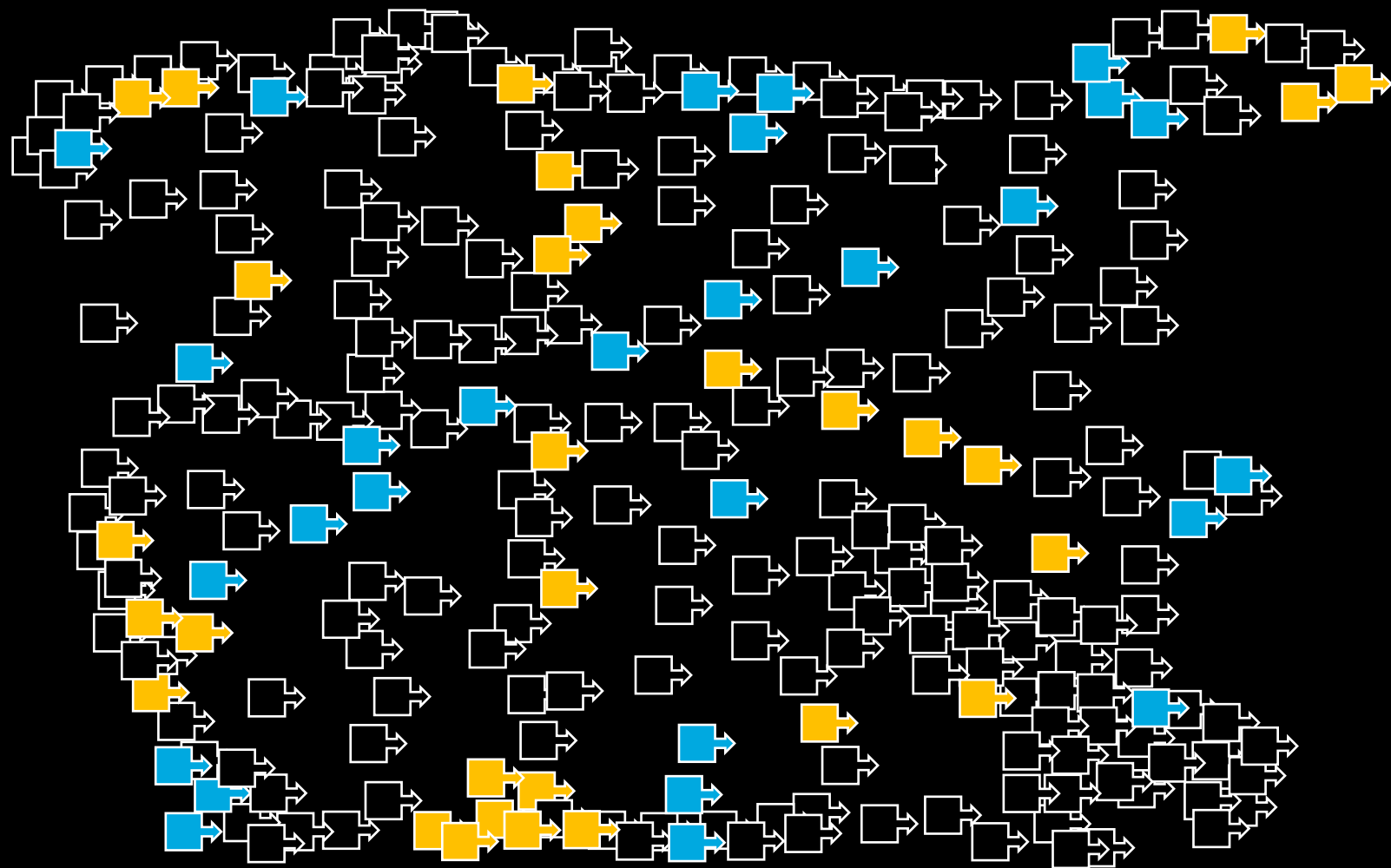
Apply a Flexible Service Context

Focusing on High Value Services



Apply a Flexible Service Context

Focusing on High Value Services



- Customer Purchases
- Financial Transactions

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" Operate 20  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?category_id=GIFTS&JSESSIONID=SD5SL7FF6ADFF9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS" Max 11/24 0  
ows NT 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01" Comput 20  
:/buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3" Comput 20  
:/buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3" Comput 20  
:/buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3" Comput 20  
:/buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3" Comput 20  
:/buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3" Comput 20  
:/buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3" Comput 20  
:/buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3" Comput 20  
:/buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3" Comput 20  
:/buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3" Comput 20
```

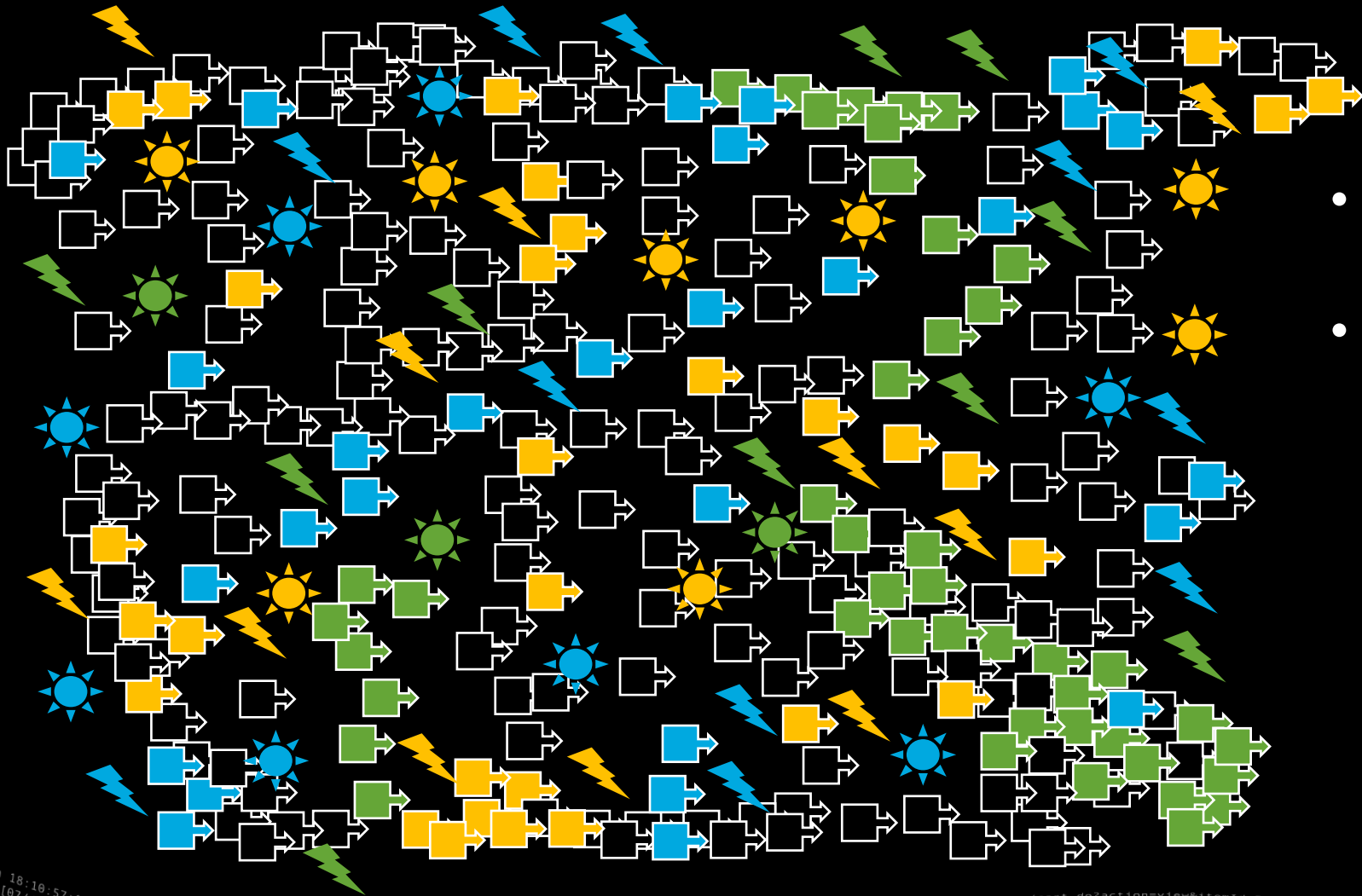

Use All the Data– At Scale



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

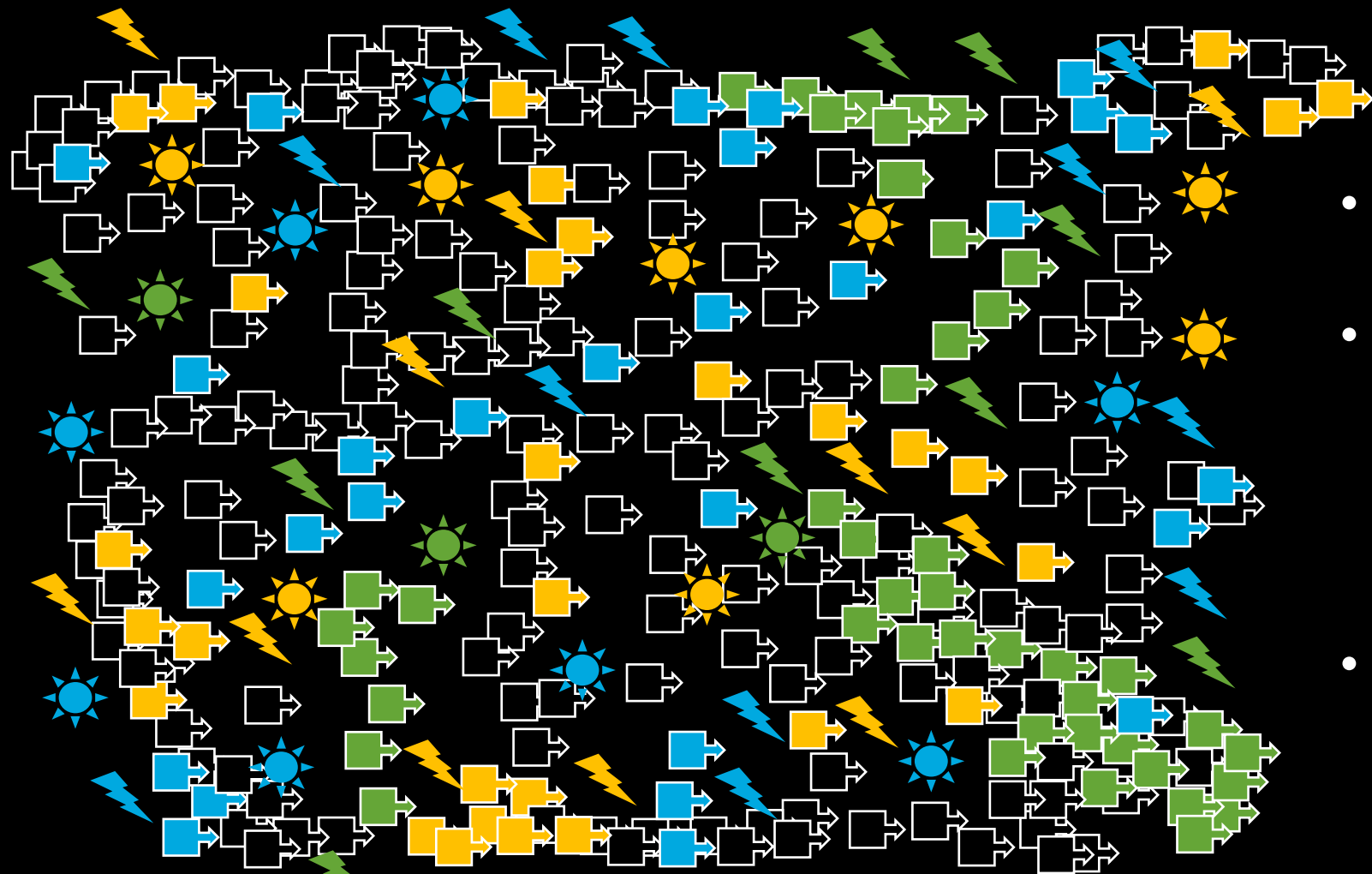
```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-5W-01" Opera/9.80.
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=Mx11474" Opera/9.80.
317.27.160.0.0 - - [07/Jan 18:10:56:150] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD105L9FF10ADFF10" Opera/9.80.
10.0.1.1:SV1: - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-5W-01" Opera/9.80.
10.0.1.1:SV1: - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-5W-01" Opera/9.80.
10.0.1.1:SV1: - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-5W-01" Opera/9.80.
10.0.1.1:SV1: - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-5W-01" Opera/9.80.
```

Use All the Data– At Scale



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

Use All the Data– At Scale



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

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category_screen?category_id=GIFTS&JSESSIONID=SD15L4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product_screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-2&product_id=K9-CU-01"
317.27.160.0.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/category_screen?category_id=FLOWERS&JSESSIONID=SD19SL8FF2ADFF9 HTTP 1.1"
...
10.55.187] "GET /category_screen?category_id=EST-10&JSESSIONID=SD19SL8FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/category_screen?category_id=FLOWERS&JSESSIONID=SD19SL8FF2ADFF9 HTTP 1.1"
10.55.198] "GET /category_remove?itemId=EST-10&JSESSIONID=SD19SL8FF2ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/category_remove?itemId=EST-10&JSESSIONID=SD19SL8FF2ADFF9 HTTP 1.1"
```

If You Can't Scale, You'll Fail

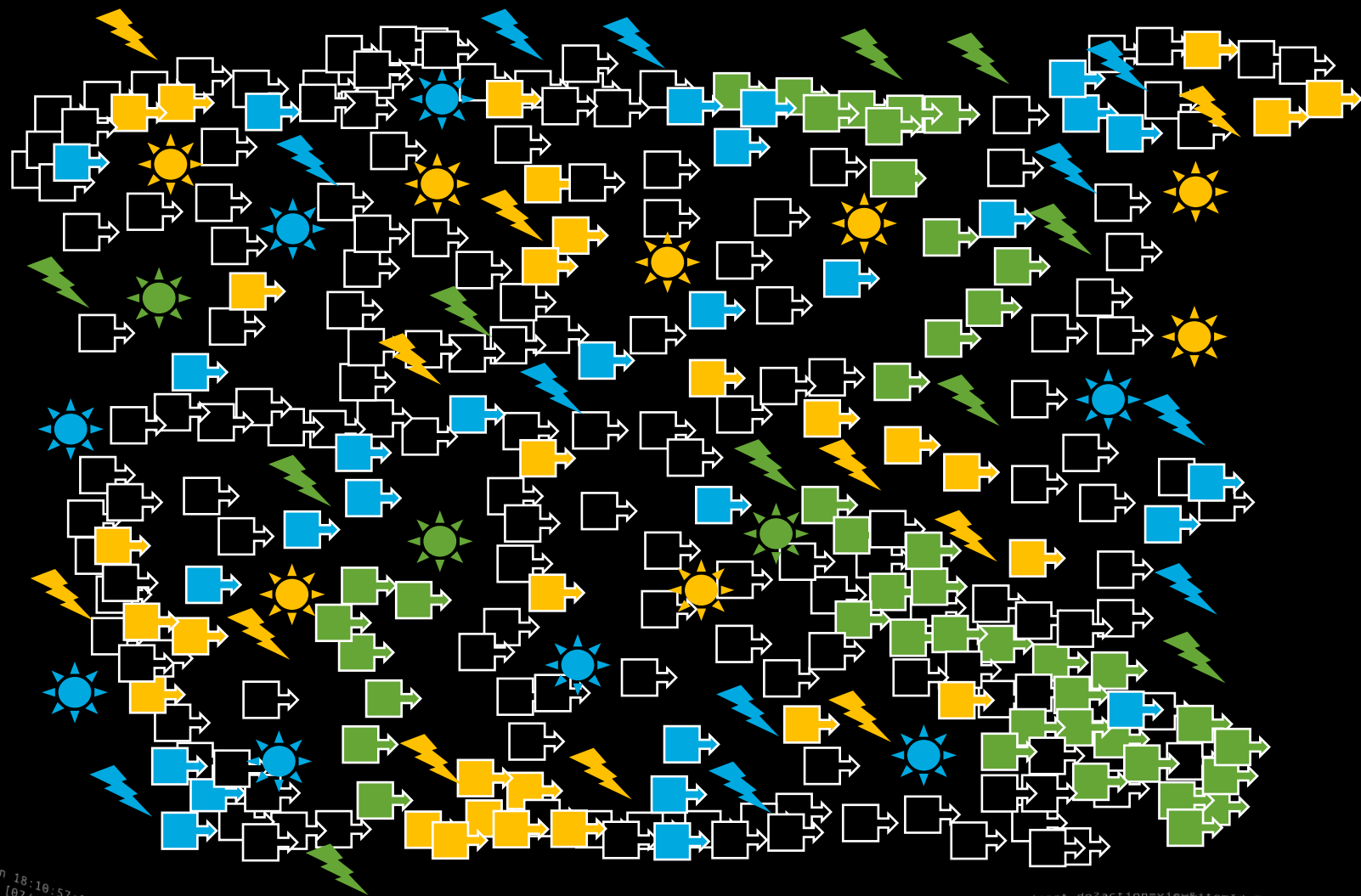
- ▶ Dealing with Gigabytes is easy
- ▶ Must be able to handle Terabytes and even Petabytes per day

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3"
...
http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01"
http://buttercup-shopping.com/cart.do?action=update&itemId=EST-26&product_id=AV-CB-01&JSESSIONID=SD10SL0FE2ADF9 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=update&itemId=EST-26&product_id=AV-CB-01&JSESSIONID=SD10SL0FE2ADF9"
http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9"
http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&JSESSIONID=SD5SL9FF1ADFF3"

```


Use Machine Learning the Right Way



```
130.60.4 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GIFTS&product_id=FL-SW-01" "Opera/9.80.2017.12  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=K9-CU-01" "Comput  
ows NT 5.1; SV1: - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-188&product_id=AV-CB-01&JSESSIONID=SD10SL  
item_id=EST-16&product_id=RP-LI-02" 468 125.17.14.105 [07/Jan 18:10:56:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD55L7FF6ADFF9 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/purchase.com/ol  
shopping.com/purchase.com/ol  
buttercup-shopping.com/ol
```

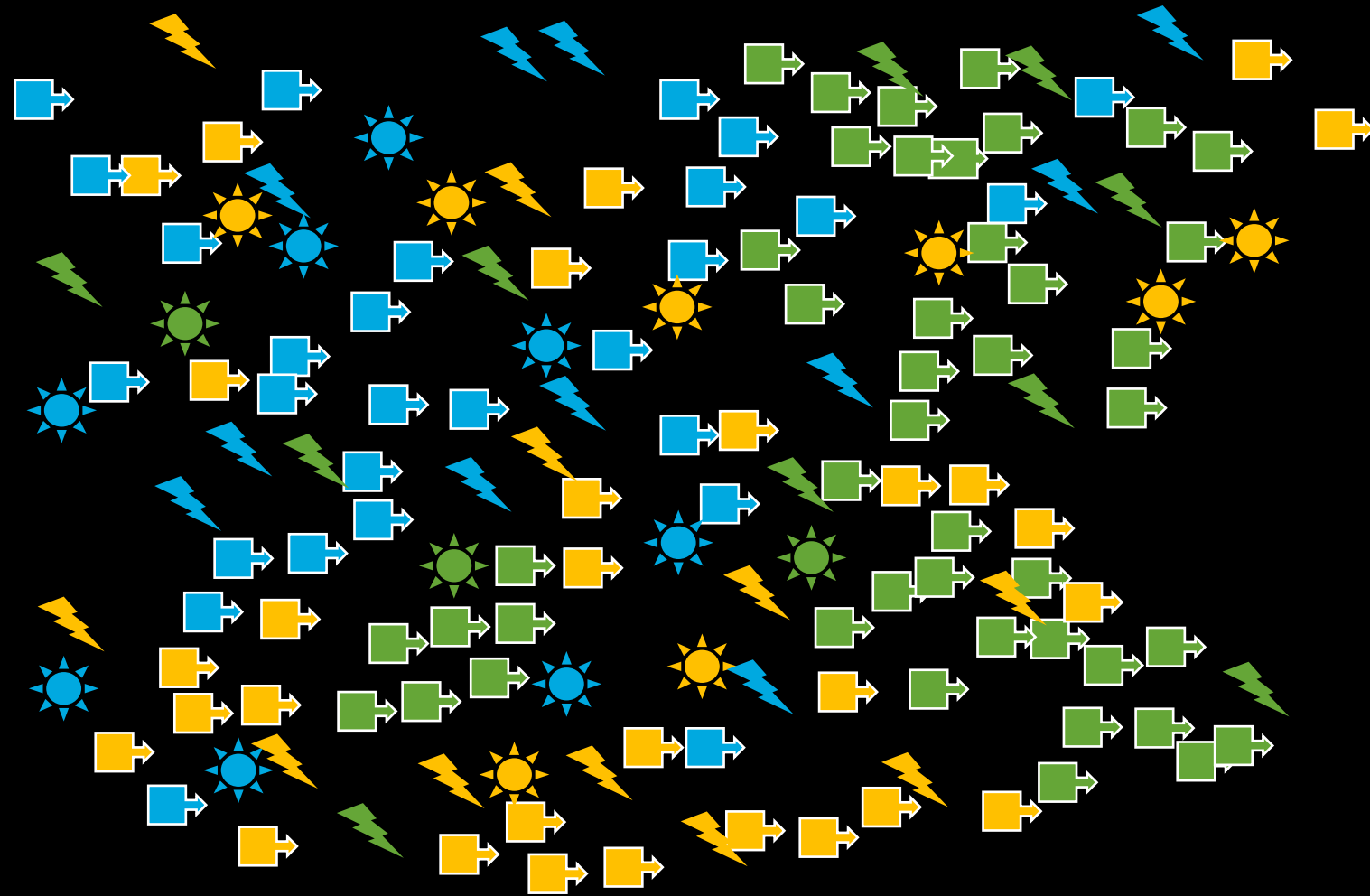
Use Machine Learning the Right Way

- At Every Step
- On All Types of Data



```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.2013.11beta Windows NT 5.1; SV1; .NET CLR 1.1.4322)"  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5; rv:41.0) Gecko/20100801 Firefox/41.0" "Opera/9.80.2013.11beta Windows NT 5.1; SV1; .NET CLR 1.1.4322)"  
10.0.2.1 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL01E2ADFF3 HTTP 1.1" "Opera/9.80.2013.11beta Windows NT 5.1; SV1; .NET CLR 1.1.4322)"  
10.0.2.1 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 468 125.17.14.10 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL01E2ADFF3 HTTP 1.1" "Opera/9.80.2013.11beta Windows NT 5.1; SV1; .NET CLR 1.1.4322)"  
10.0.2.1 - - [07/Jan 18:10:56:189] "GET /cart.do?action=changequantity&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.2013.11beta Windows NT 5.1; SV1; .NET CLR 1.1.4322)"  
10.0.2.1 - - [07/Jan 18:10:56:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-26&product_id=K9-CU-01" "Opera/9.80.2013.11beta Windows NT 5.1; SV1; .NET CLR 1.1.4322)"
```

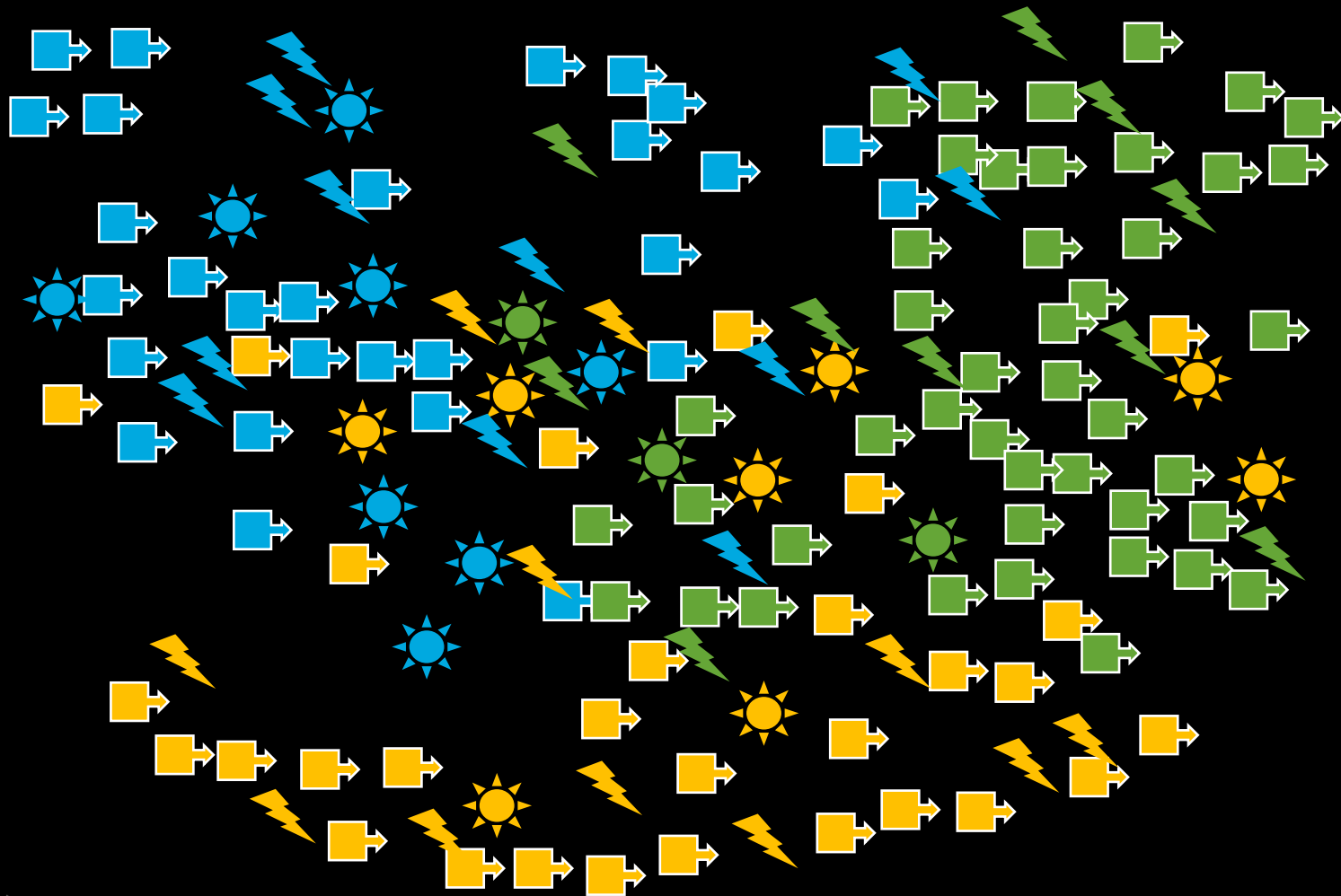
Use Machine Learning the Right Way



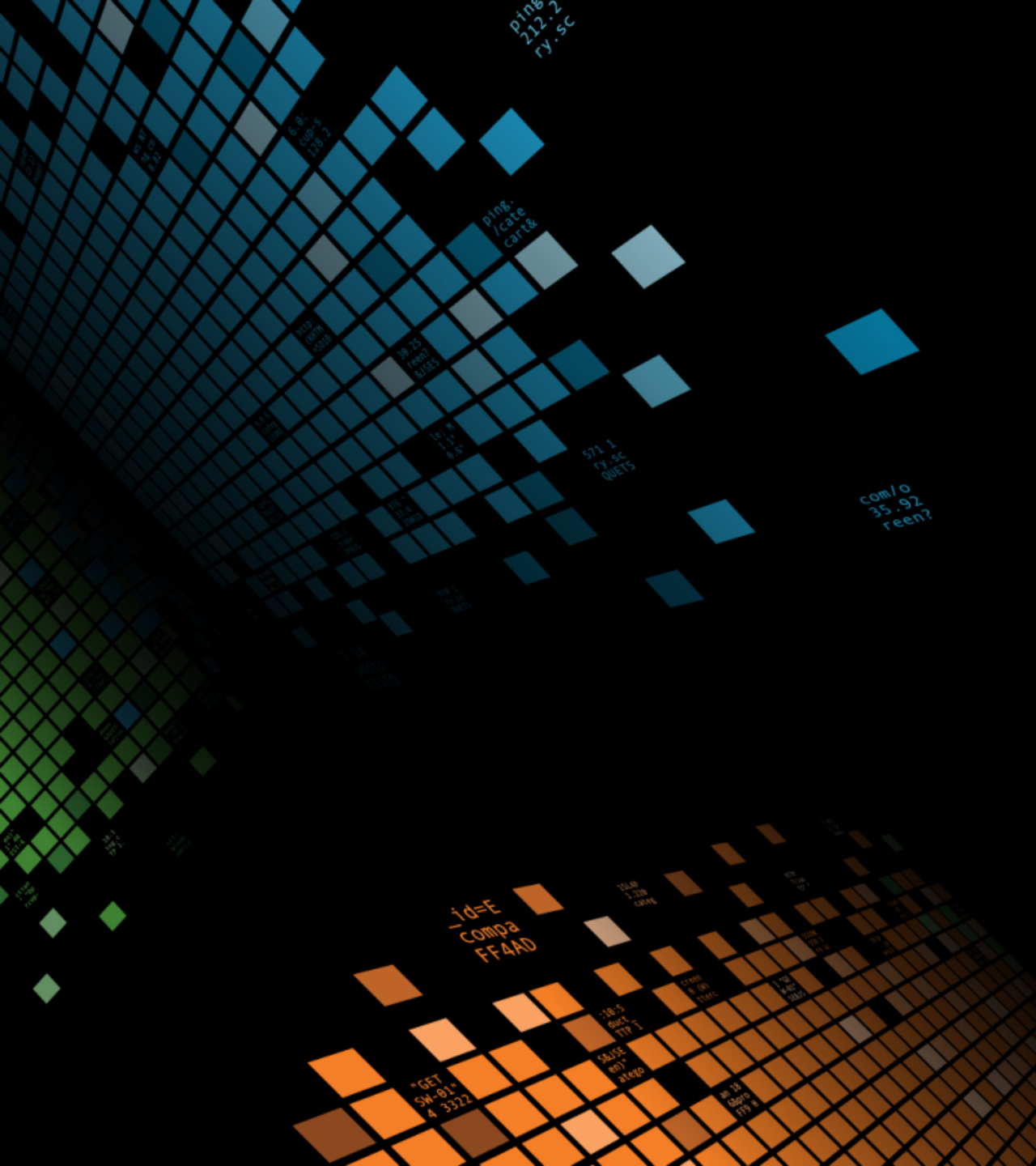
- At Every Step
- On All Types of Data
- From High vs Low to Normal vs Not Normal

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.2013.0 (Windows NT 6.0; U; en; rv:1.9.2.13) Gecko/20100308 Firefox/3.6"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DISH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-20&product_id=K9-CU-01" "Computers 2016.9.13 (Windows NT 6.0; rv:51.0) Firefox/51.0"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9F2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.2013.0 (Windows NT 6.0; U; en; rv:1.9.2.13) Gecko/20100308 Firefox/3.6"
468.125.17.14 [oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 404 1220 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-20&product_id=K9-CU-01" "Computers 2016.9.13 (Windows NT 6.0; rv:51.0) Firefox/51.0"
130.60.4 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DISH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-20&product_id=K9-CU-01" "Computers 2016.9.13 (Windows NT 6.0; rv:51.0) Firefox/51.0"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.2013.0 (Windows NT 6.0; U; en; rv:1.9.2.13) Gecko/20100308 Firefox/3.6"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DISH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-20&product_id=K9-CU-01" "Computers 2016.9.13 (Windows NT 6.0; rv:51.0) Firefox/51.0"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9F2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.2013.0 (Windows NT 6.0; U; en; rv:1.9.2.13) Gecko/20100308 Firefox/3.6"
468.125.17.14 [oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 404 1220 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-20&product_id=K9-CU-01" "Computers 2016.9.13 (Windows NT 6.0; rv:51.0) Firefox/51.0"
```

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



Demo

Life Gets Better for IT Ops

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

130.60.4 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.20
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=0IFTS" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14 [http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9IE2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&JSESSIONID=SD18FF1ADFF3" 3865
buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD55L9FF1ADFF3" 3865
buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD55L9FF1ADFF3" 3865
buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD55L9FF1ADFF3" 3865

Empower IT Ops to

Find What's Broken, then Fix It

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L4FF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.2013.1041; rv:1.9.2.1041; Gecko/20100101; Firefox/35.108"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD105L9FF2ADFF9 HTTP/1.1" "Opera/9.80.2013.1041; rv:1.9.2.1041; Gecko/20100101; Firefox/35.108"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 189 "GET /cart.do?action=remove&itemId=EST-1&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" "Opera/9.80.2013.1041; rv:1.9.2.1041; Gecko/20100101; Firefox/35.108"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L4FF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.2013.1041; rv:1.9.2.1041; Gecko/20100101; Firefox/35.108"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD105L9FF2ADFF9 HTTP/1.1" "Opera/9.80.2013.1041; rv:1.9.2.1041; Gecko/20100101; Firefox/35.108"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 189 "GET /cart.do?action=remove&itemId=EST-1&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" "Opera/9.80.2013.1041; rv:1.9.2.1041; Gecko/20100101; Firefox/35.108"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L4FF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.2013.1041; rv:1.9.2.1041; Gecko/20100101; Firefox/35.108"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD105L9FF2ADFF9 HTTP/1.1" "Opera/9.80.2013.1041; rv:1.9.2.1041; Gecko/20100101; Firefox/35.108"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 189 "GET /cart.do?action=remove&itemId=EST-1&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" "Opera/9.80.2013.1041; rv:1.9.2.1041; Gecko/20100101; Firefox/35.108"
```

Q&A

Thank You

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

David Millis | dmillis@splunk.com

splunk> **.conf2017**