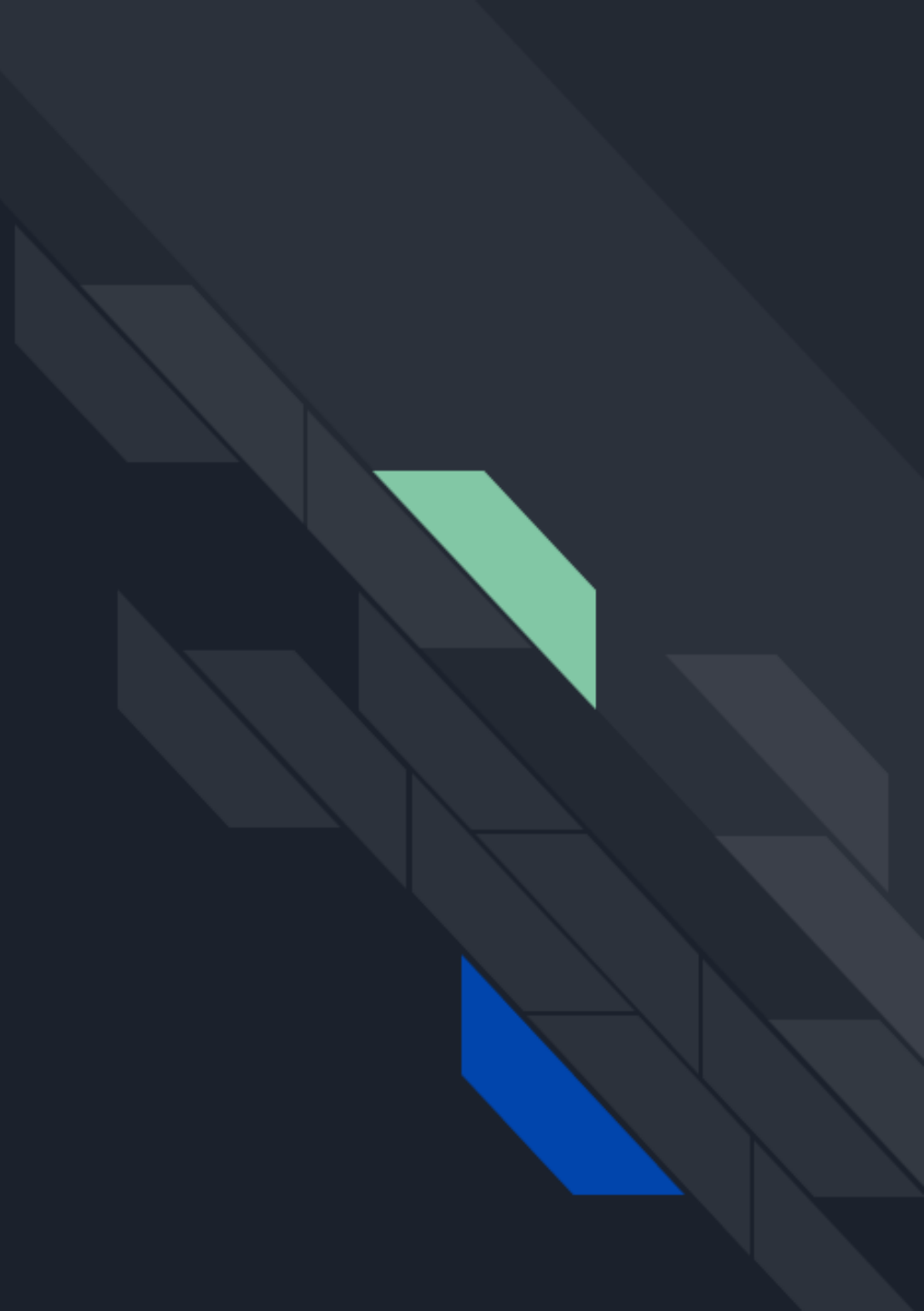


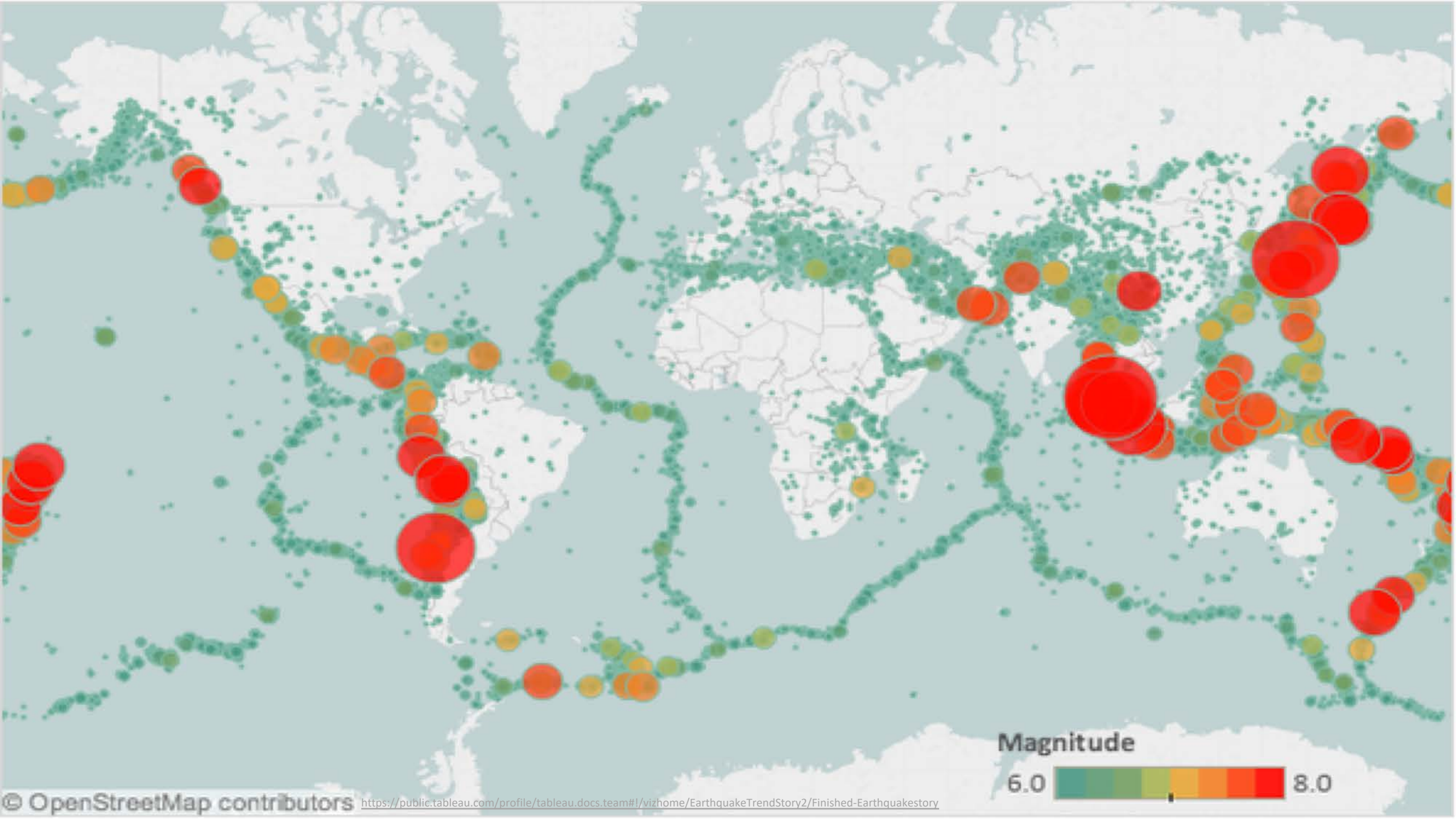
Red Alpha
www.red-alpha.com

Embedded Contextual Analytics

Put the Data at the Point of Need

Presented by Michael Deane



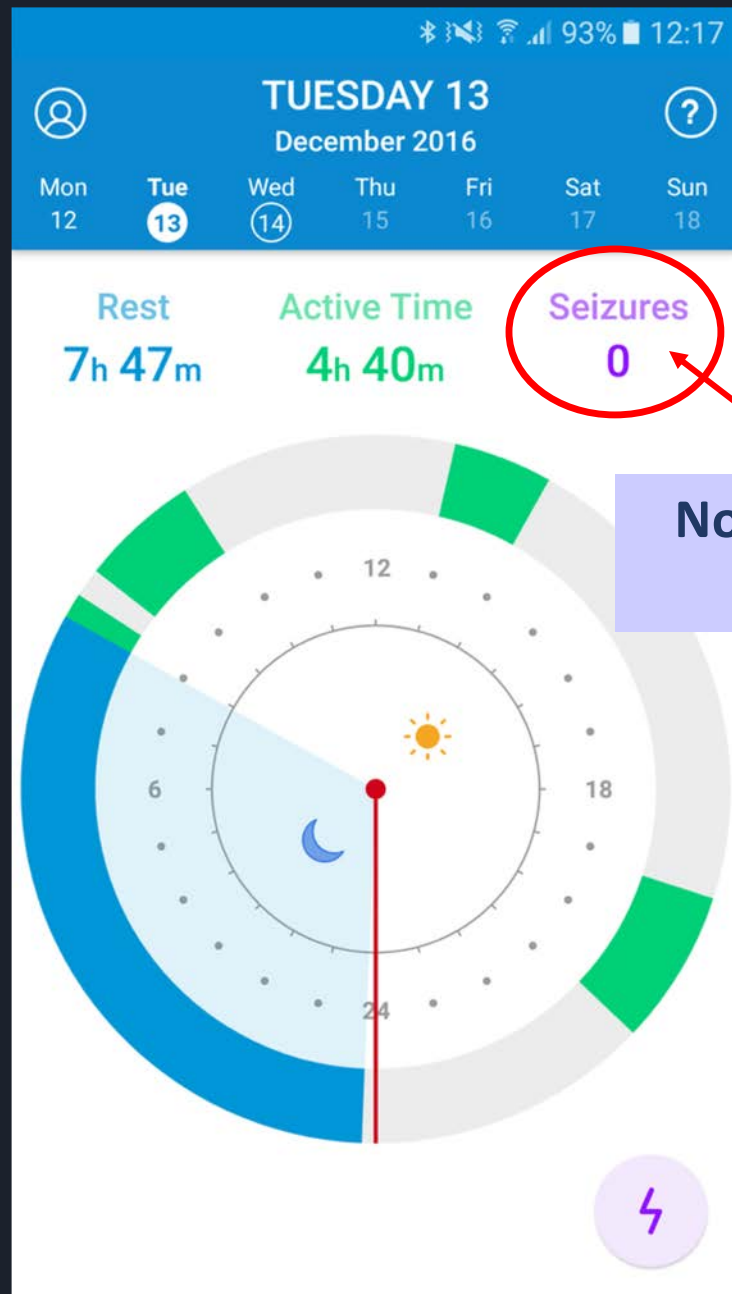


Magnitude

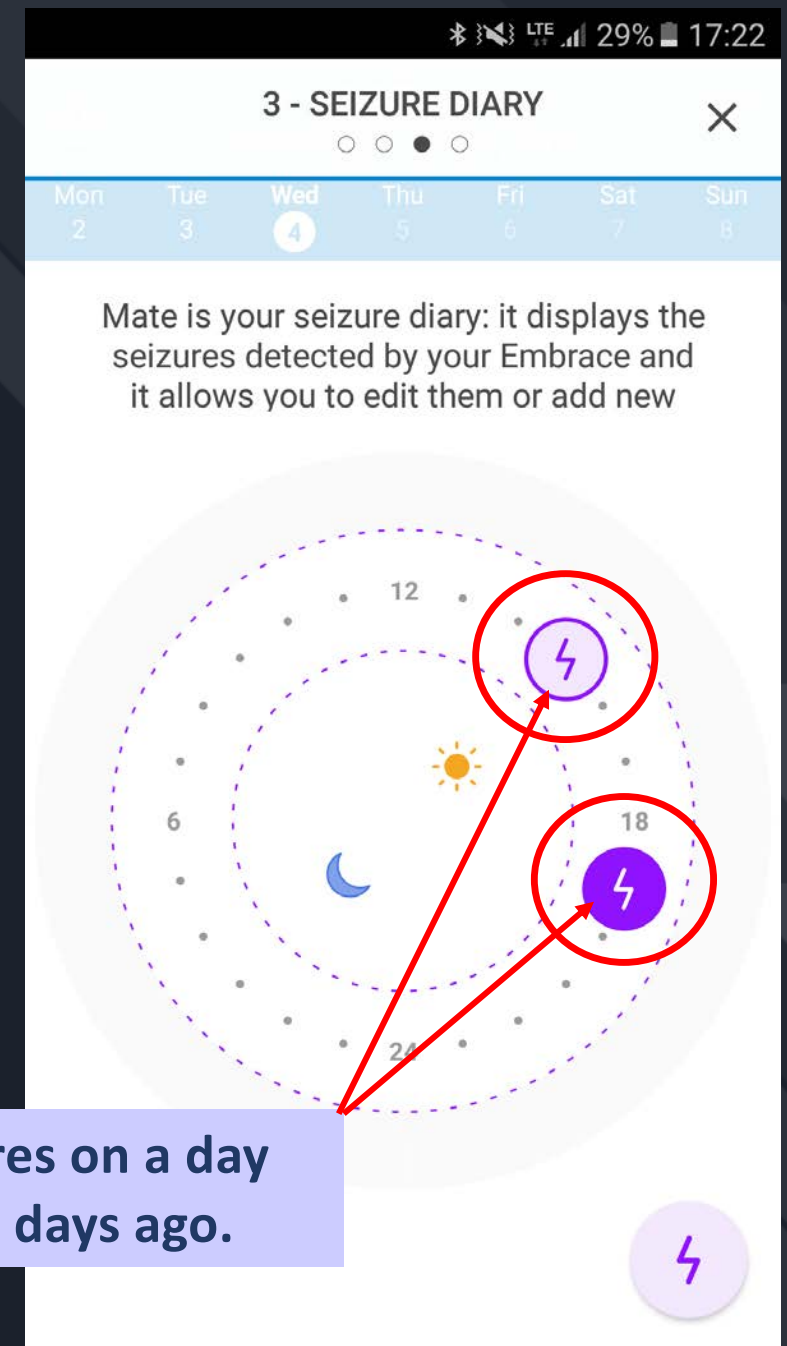
6.0



8.0



Is this contextual enough for you?

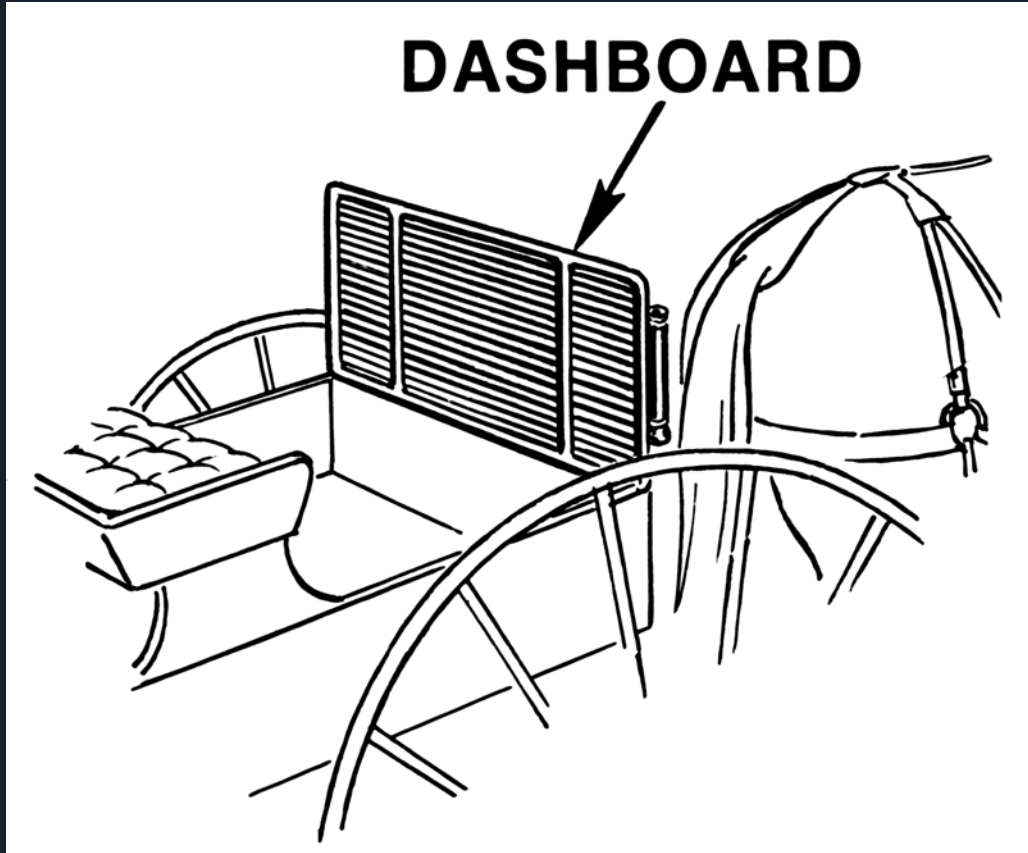




What are analytics?

What are embedded analytics?

What are contextual analytics?



<https://en.wikipedia.org/wiki/Dashboard>

Horse-drawn carriage

A *dashboard* protects the driver of a horse-drawn wagon from mud or debris *dashed* up by the horse's hooves.

No embedded data



Early days of the automobile

No embedded data

No speedometer for 25 years, until 1910

No gas gauge for 37 years, until 1922

<https://www.cargurus.com/Cars/1915-Ford-Model-T-Pictures-c21698#pictureId=41246673>



Modern day Automobile

Humans “tune out” when not given a task, the science of “human engagement” is evolving to address this risk.

Personalized seat, steering wheel, and mirrors adjustment

- Automatically adjust to individual pre-sets (prior human config, select your saved setting to use)

Parking assist, hands-off steering

- Pull into parking spot (choose to use, human has immediate override capability)
- Parallel parking (choose to use, human has immediate override capability)

Assisted driving, location aware (GPS)

- Lead driver to a destination (choose to use, human has immediate override capability)
- Adjust to speed limits (choose to use, human has immediate override capability)
- *Disengages assisted driving in location not “mapped” by the system*

Assisted driving, forward-facing camera and radar

- Keep car centered between lanes
- Alert when making a lane departure (choose to use, human has immediate override capability)

Assisted collision avoidance, radar

- Maintain distance from car (prior human config, choose to use, human has immediate override capability)
- Rush hour traffic drivers love this feature

Assisted driving, camera tracking driver's eyes

- *Driver not alert?*
 - *Flashing lights on steering column*
 - *Audible alerting*
 - *Seat vibrations*



Future fully autonomous automated automobile

Attack surfaces of autonomous automated automobiles:

- Infrastructure signage
- Machine vision
- Global positioning system
- In-vehicle devices
- Acoustic sensors
- Radar
- Light detection and ranging
- Material/structure on which the vehicles drive
- In-vehicle sensors
- Odometric sensors
- Electronic devices
- Maps for longitudinal and lateral directions

The ability to take data—to be able to understand it, to process it, to extract value from it, to **visualize** it, to communicate it



**Who are the leaders in
embedded contextual
analytics?**

Firsttrade Navigator all-in-one screen

Connection Status: ● Real-time Quotes: ● Indicators: ●

+ Add widget

= Blain Personal (██████) ...

Filter by: Stocks Options Mutuals Other

VOO Vanguard S&P 500 ETF ⊖ ⊕
▲ \$31.50 (+0.38%) today 25

= Blain web ...

SYMBOL	CHG	LAST	BID	ASK
AAPL	+0.71	136.43	136.42	136.43
BABA	+1.03	101.55	101.54	101.55
FB	-0.11	133.42	133.42	133.42
GLD	-0.19	117.53	117.53	117.54
GOOGL	+4.66	851.21	851.00	851.25
TWTR	-0.24	16.38	16.38	16.39

= TSLA \$277.7480 +5.52 (+1.99) ...

The Market in 5 Minutes
an hour ago [Benzinga]

Zacks Investment Ideas Feature highlights:
Tesla, Volatility Index and Global - Press
Releases
an hour ago [Zacks]

IHS Market Says China Will Continue to be
Largest Car Market for Foreseeable Future;
Raises 2017 China Auto Sales Forecast 1.9% to
28.6M Units

ORDERS

Open: 0
Executed: 0

GAIN
vs
LOSS

Gaining: 1
Losing: 0

CASH
vs
HOLDINGS

Cash:
\$155.93
Securities:
\$5,427.50

TOTAL EQUITY
\$5,583.03

TODAY'S P&L (%)
+\$31.50 (+0.56%)

Nasdaq 5,861 +22.56 (+0.38%) Dow Jones 20,739 +115.39 (+0.56%) S&P 500 2,364 +12.97 (+0.55%)

MARKET OVERVIEW

WATCHLIST

AAPL

Q

+ Add widget

AAPL Apple Inc. - Common Stock (NASDAQ)

\$136.4250 +0.71 (+0.52%) \$136.42 \$136.43 7 x 1 \$135.98 / \$136.62 8.75m

Updated 10:58 AM EDT

CHART NEWS CHAIN RESEARCH

1W 1D 30D

O 74.98 H 75.21 L 73.38 C 74.29

Volume (true, 20) 263,455M 420,738M

MA (50)

Candlestick charts
and indicators



STOCK ORDER

OPTION ORDER

ORDER STATUS

Transaction

Shares

SYMBOL

Buy

▼

AAPL

136.42 +0.71 (0.52%) BID: 136.4250 136.43
ASK: 136.4350

Price Type

Duration

Instructions

Market

▼

Day

▼

None

Margin Req: Long: +50%

Clear

Preview

Place Order

= % Gainers

EYEG	+48.79%	AOPW	+37.23%
\$2.44 +0.80		\$1.40 +0.38	
CLRW	+37.00%	CYH	+33.77%
\$6.2151 +0.08		\$6.23 +0.01	
DCTH	+32.78%	BLPH	+32.41%
\$0.2098 +0.08		\$1.67 +0.25	
TROX	+26.49%	SHLDW	+24.43%
\$18.34 +3.80		\$3.00 +0.08	
LL	+19.85%	VRML	+19.43%
\$18.4000 +1.08		\$2.00 +0.34	
PLK	+19.19%	NVFI	+19.05%
\$18.81 +1.00		\$1.70 +0.14	

Updated: 10:58 am EDT

= Most Actives

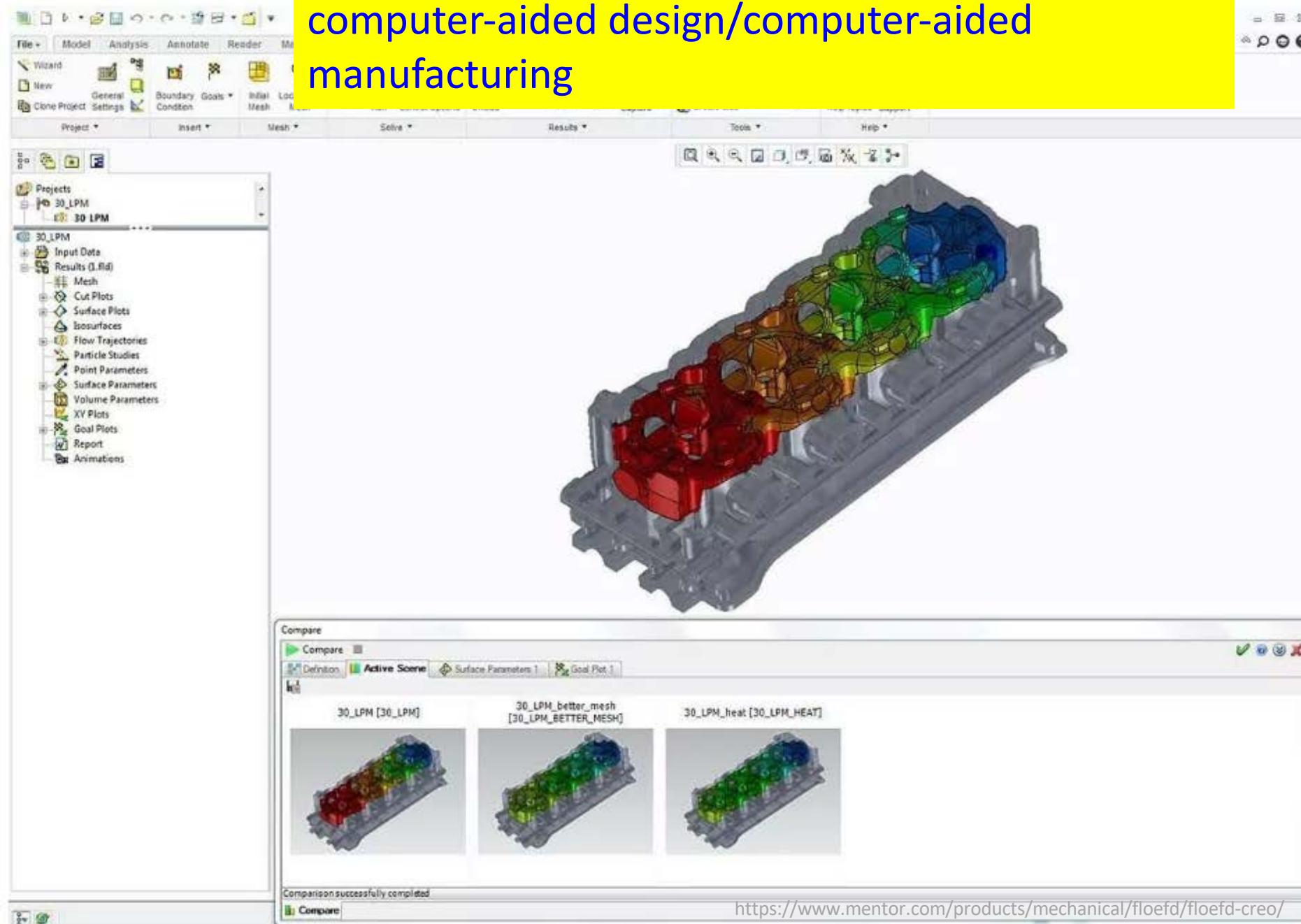
FOX	25.3m	BAC	24.7m
\$14.13 +0.39		\$24.7135 +0.39	
AMD	22.4m	DCTH	15.7m
\$13.22 +0.16		\$0.2098 +0.08	
DRYS	14.9m	RNVA	14.7m
\$3.25 +0.12		\$0.0750 +0.01	
VALE	14.6m	CHK	14.1m
\$11.43 +0.46		\$6.0250 +0.29	
CYH	12.0m	TEVA	11.9m
\$6.23 +0.01		\$06.87 +1.87	
AUY	10.5m	EYEG	10.2m
\$7.6050 +0.16		\$2.44 +0.80	

Updated: 10:58 am EDT

Users can add widgets
like watchlists.

CAD/CAM

computer-aided design/computer-aided manufacturing



FloEFD for PTC Creo is the most popular computational fluid dynamics (CFD) analysis tool that is **truly embedded into Pro/ENGINEER and Creo**.

It enables design engineers to frontload CFD by moving simulation early into the design process where it is more cost effective to identify and fix problems and enhance productivity by x2 to x40.

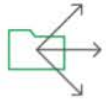
FloEFD is:

Embedded in Creo – one interface, one model

Intuitive and easy-to-use

Fast and has robust convergence criteria even for highly complex geometry

What do the prognosticators say?



- 1** Workloads – not just data – will be distributed



- 2** Multi-cloud, hybrid, and edge will form a continuum



- 3** Centralized data will be replaced by a single view of all data



- 4** Performance and scale will re-take center stage



- 5** Analytics embedded in the process will reshape the process



- 6** AI will make analytics more human, not less



- 7** Visualization, conversation, and presentation technologies will merge



- 8** Data literacy will become a KPI



- 9** External innovation will outpace internal innovation by 2X




- 10** Platforms will evolve into systems.

Analytics will be embedded:

- in dashboards
- in operational systems
- in business processes
- in websites & portals
- in mobile applications
- in end point applications

INTERNET OF THINGS



Passing data to a central data store, performing analytics, and returning the result of the analysis to the edge device is not realistic. **Analytics will be embedded into the edge devices.**



Workflow and automation, outside of manufacturing, has not been as successful as was originally envisioned.

Embedding analytic capabilities into the applications that end users spend most of their time in will build up their trust in the data. They will also be empowered by the ability to make data-driven and analytics-based decisions.

In time, the end users themselves will recommend that the most reliable data and analytics be used to drive automation of some processes.

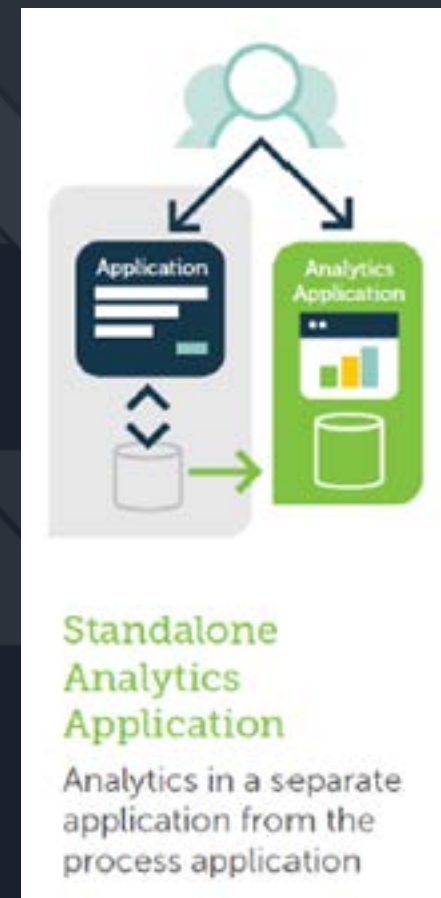


So...

What is the best way to get actionable, relevant, accurate, and timely information (derived from analysis of data) to these end users? ***The answer is not a dashboard in a separate software application.***

For too long, there has been a proliferation of incompatible software applications. Users have to repeatedly leave their current application to do a task only possible in another software application. Then, they return to the main application where they do most of their work. This process repeats itself over and over again everyday.

It is time for the end users to have the information they need inside the application where they are doing their work.





KEY TRENDS & INSIGHTS

- Occam's Razor (OR) organic traffic is down 15%.
- OR positions well in search engines for many keywords, but still has room to grow - especially in regard to Bing and Yahoo.
- OR engagement is healthy, but it's on a slight downward trend that needs to be reversed.
- OR RSS Feed Growth is up 26% despite the downturn in traffic and engagement.
- OR's \$5.16 Value per Acquisition is doing well, but this can improve by optimizing several site Goals.
- OR's 79% Surveyed Task Completion Rate is healthy.

RECOMMENDATIONS

- OR needs to work on SEO for several new and existing keywords to increase organic search.
- OR needs to encourage more engagement by means of modifying blog design to highlight important site Goals.
- OR needs to highlight RSS Feed subscription on site and on other web properties.
- OR needs to optimize Goal conversion for three highest value Goals.

IMPACT TO BUSINESS

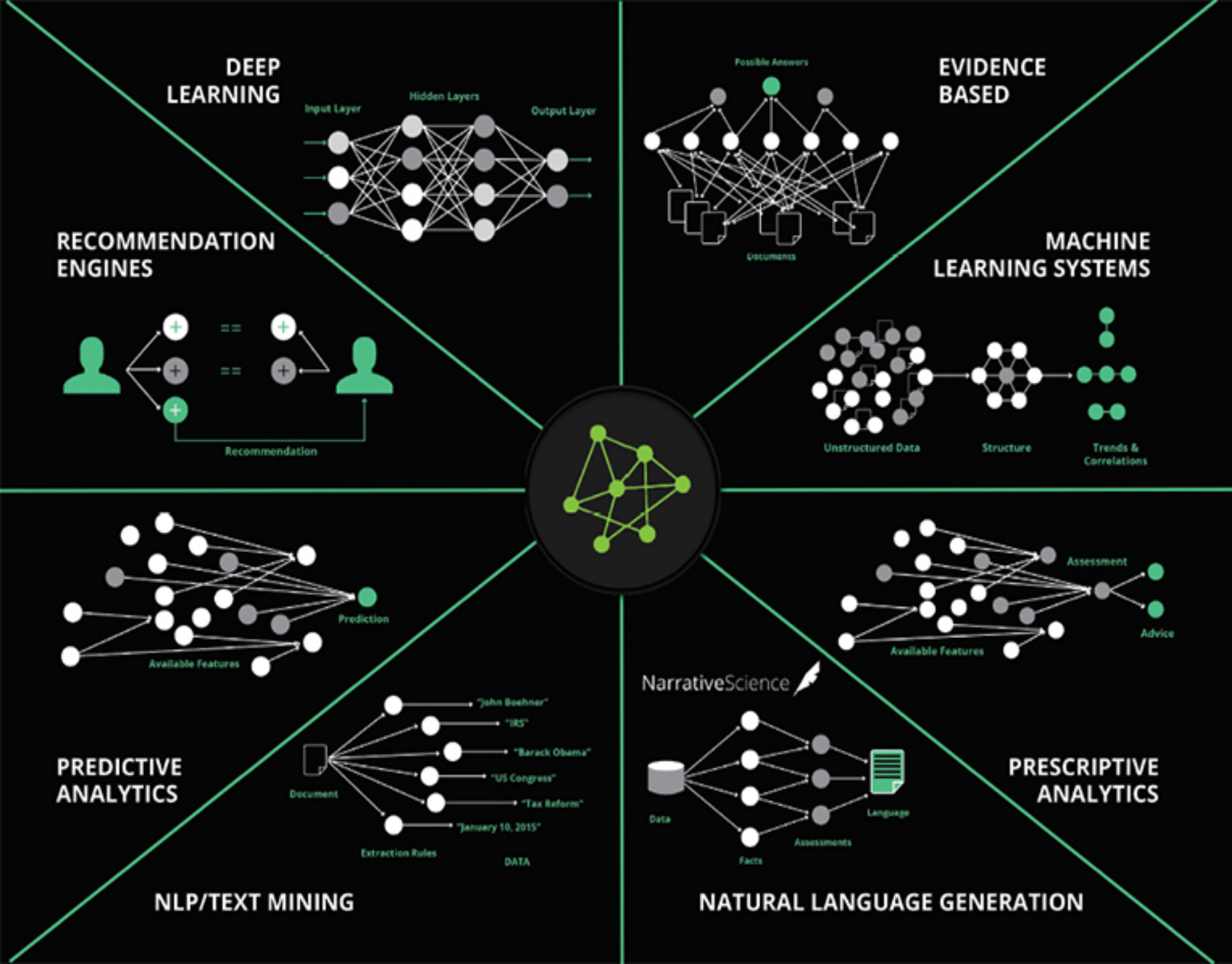
- Improving OR website Goal conversions has a positive 21.7% estimated economic value impact of \$362,000.
- Improving smaller OR website Goal conversions will have only an incremental economic impact on the site, but they will help the site grow its subscriber and social media base.



Maybe an exceptionally well executed dashboard is what a user in a certain role needs.



More often than not, a very small set of very specific metrics will suffice.



Will pursuing embedded contextual analytics impede my efforts in data science? **No.**

Consider where the output from these analytics will provide the most value.

If a certain role of end user in your application needs this data, then stream the updates directly into that user's primary interface.

Task the end users to validate the correctness and usefulness of the data.

Then automate!!!

Like electricity, **analytics will be a service that users and applications tap into.**

Embedded analytics transforms stand-alone products to on demand services.

By embedding analytics into operational processes, users gain a better understanding of the data and its business context, enabling them to not only spot and fix problems before they escalate out of control, but also identify and seize new opportunities before they vanish.

Embedded analytics remove the bottlenecks and delays of IT developing reports for you. Individual departments will no longer need to create their own shadow IT staffs and systems.

Data science and data analytics will deliver status metrics of key business processes, trigger alerts, inform workflows, and automate tasks to streamline processes and optimize performance.

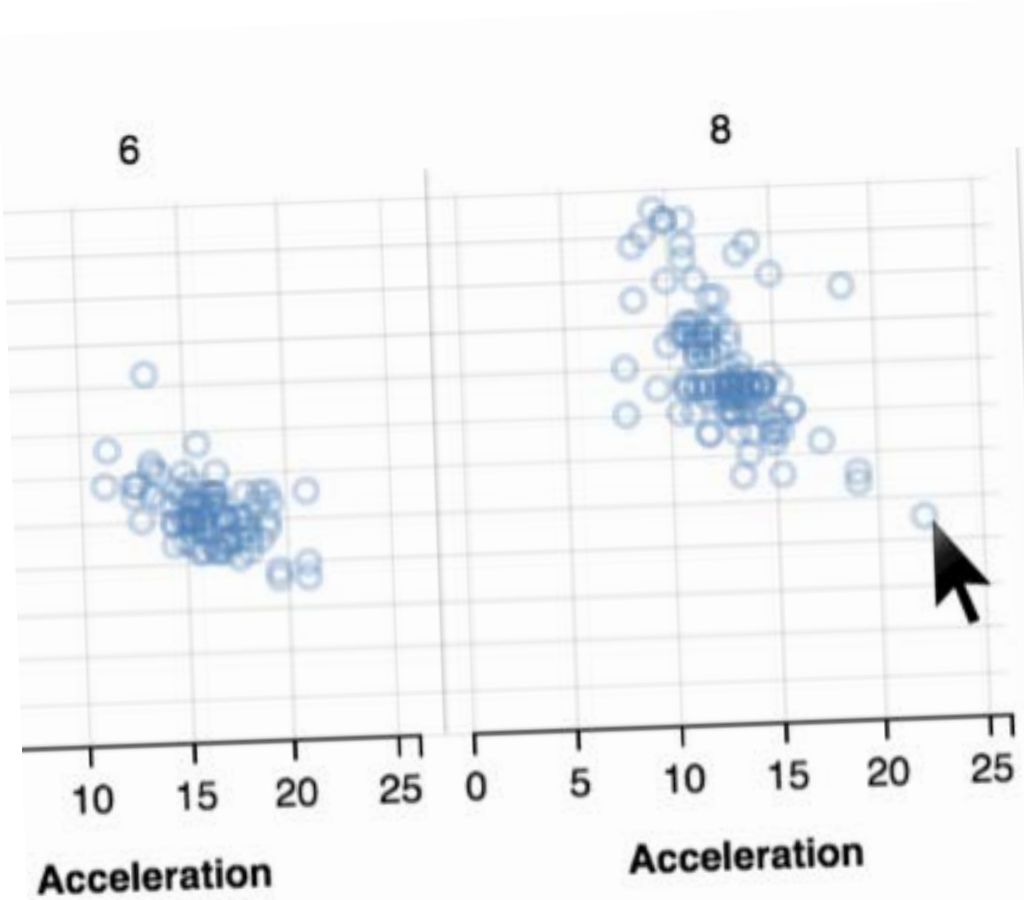


How difficult is it to embed contextual analytics?

If your applications are primarily web applications (HTML5, CSS3, JavaScript, and REST API), then you can introduce embedded contextual analytics this year.

1. A dashboard or chart can be inserted directly into an iFrame in your existing web application.
2. You can use JavaScript, a JavaScript Visualization Library and the REST API to dynamically paint charts into `<DIV></DIV>` tags in your existing web application.
3. API integration allows your application to interact, filter, and drill down into everything.

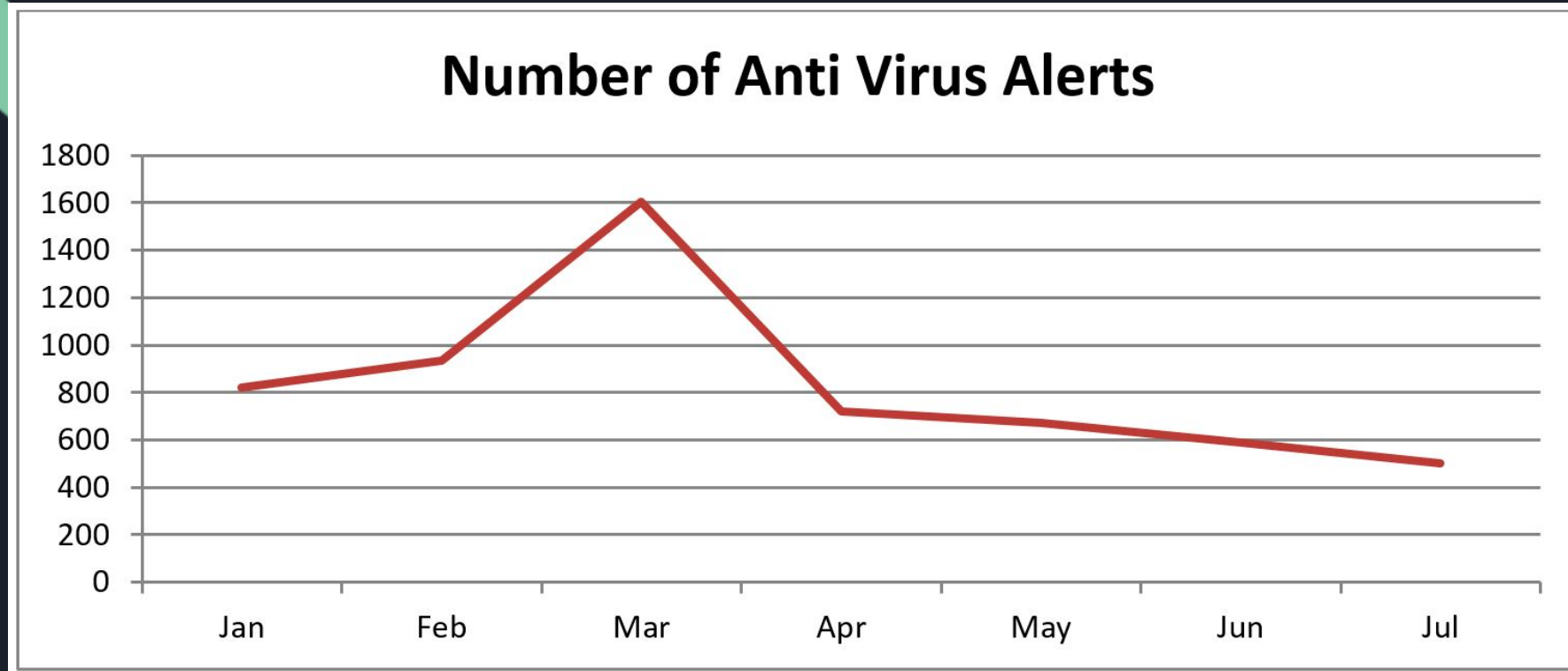
Developers



Name	oldsmobile cutlass salon
	brougham
Miles_per_Gallon	23.9
Cylinders	8
Displacement	260
Horsepower	90
Weight_in_lbs	3420
Acceleration	22.2
Year	1979-01-01
Origin	A

: An analyst hovers the mouse over an outlier to view details-on-demand.

Good or Bad? We don't know, without context.



<https://www.rsa.com/en-us/blog/2017-05/metrics-not-just-fun-facts>



1. White-Label

Standalone interactive visualizations with your branding

2. Lightweight Integrated

Lightweight iFrame- based integration with your app

3. Deeply Embedded

Deep SDK-based infusion into your app

4. Extended

Add custom visualizations and smart connectors

BUY: Remove product branding and replace with your own. Stand-alone business intelligence product suite.

Depth of integration

Developers

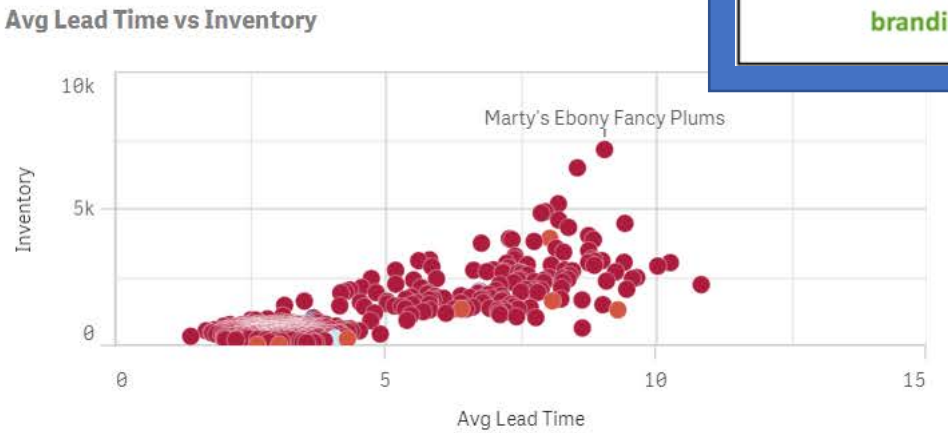
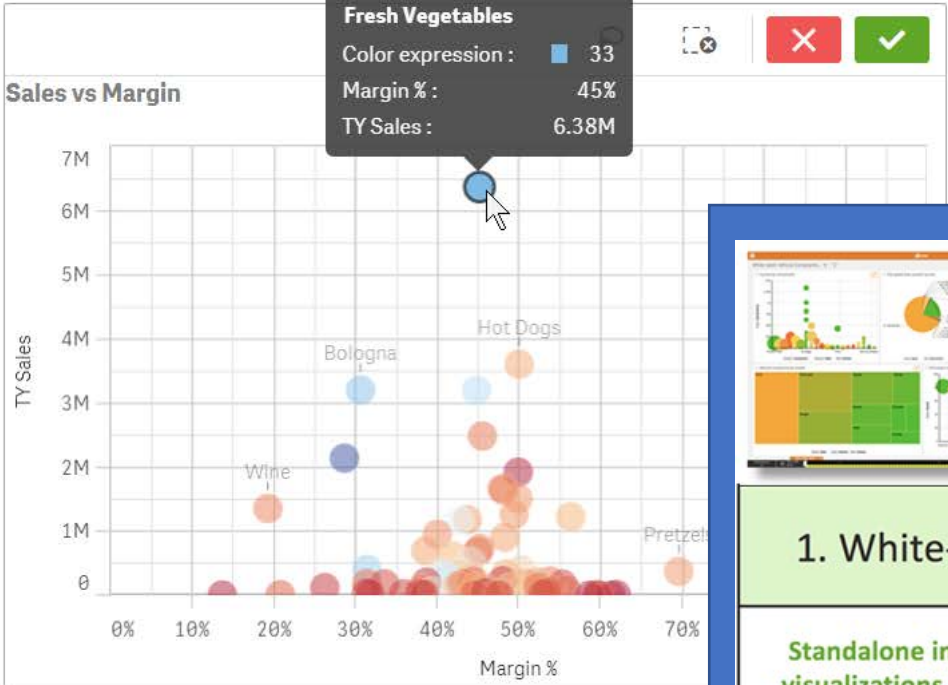
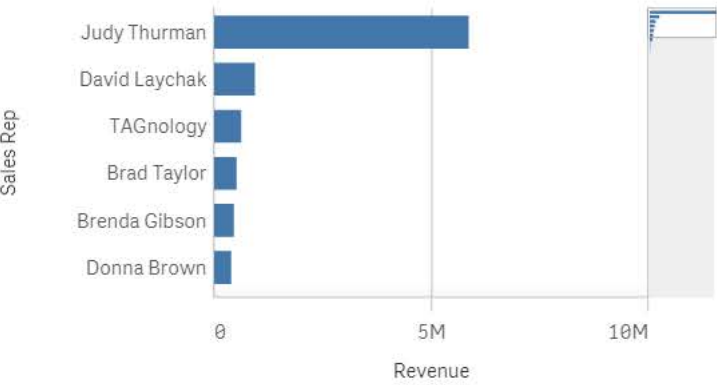
Developers

Sales Rep Performance

Sales Rep by Variance

Sales Rep	Sales Variance
Totals	-19.5%
Amalia Craig	-41.9%
Scott Powell	-41.8%
Janice Scott	-41.5%
Samantha Allen	-40.5%
Karen Clinton	-40.4%
John Greg	-39.7%
Cheryle Sincock	-39.0%
Craig Lary	-33.9%
Deborah Halmon	-29.1%
Sharon Carver	-27.1%
Ronald Golinski	-25.5%

Total Revenue = \$12,870,452



Sales Quantity by Sales Rep

colored by # of lost customers



1. White-Label

Standalone interactive visualizations with your branding

White Label, remains a separate application (no embedding).
Preconfigure or customize, then sell as your own brand of business intelligence tool.

iFrame

```
<div id="container">
  <p style="height:100px;"> </p>

  <div id="col1">
    <p> </p>
  </div>

  <div id="col2outer">

    <div id="col2mid">
      <p>
        <iframe src='http://localhost:4848/single/?
        appid=C%3A%5CUsers%5Clenovoflex5%5CDocuments%5CQlik%5CSense%5CApps%5CConsumer%20Sales.qvf&obj=MEAjCJ
        &opt=currsel&select=clearall' style='border:none;width:600px;height:400px;'></iframe>
      </p>
    </div>

    <div id="col2side">
      <p> </p>
    </div>

  </div>

</div>
```

<iframe></iframe>

- **Embed** finished product
 - Chart, table, map, or whatever visualization must already exist
 - Hosted somewhere else in a different web application



2. Lightweight Integrated

Lightweight iFrame- based integration with your app

Example shown,
using Qlik:



Sense™

iFrame

Your SaaS platform

Qlik Sense Server



2. Lightweight Integrated

Lightweight iFrame- based integration with your app



User logs in into your SaaS platform.

iFrame or DIV embeds charts



Your authentication module forwards identity to Qlik via a ticket



Your API based automation utility (Broker)

Stream Customer A



Sales app with customer A data

Stream Customer B



API calls create apps

Your software controls Qlik Sense via APIs.

Using these APIs you can automatically login your users and provision the apps.

Single sign on (via a ticket) ensures no double logins and automatically transfers authorizations from your platform to Qlik.

Example shown, using Qlik:



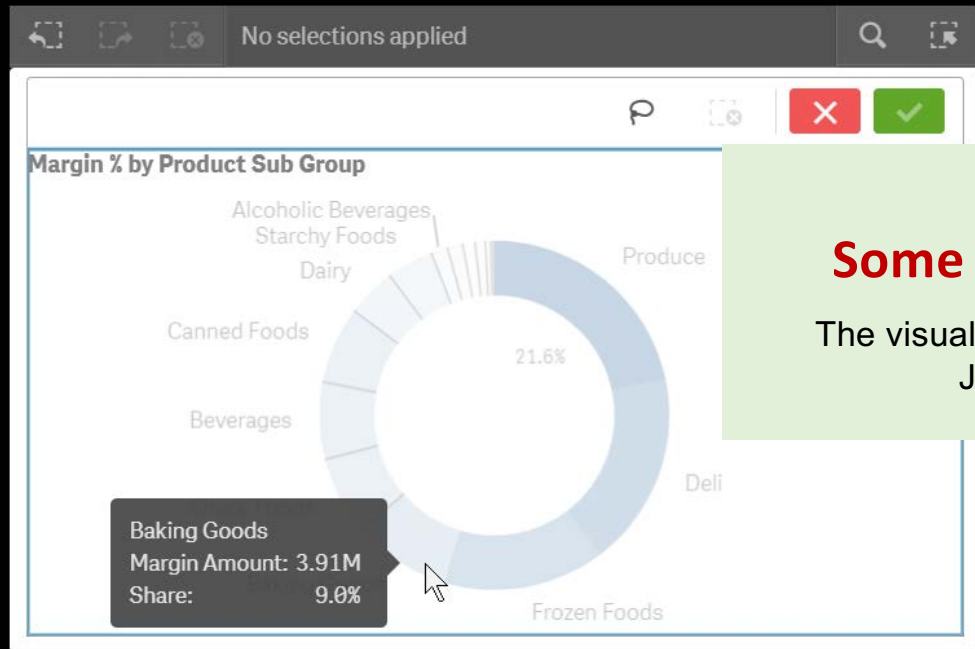
Sense

Is your application a SaaS, where you host and provision your services to many different customers?



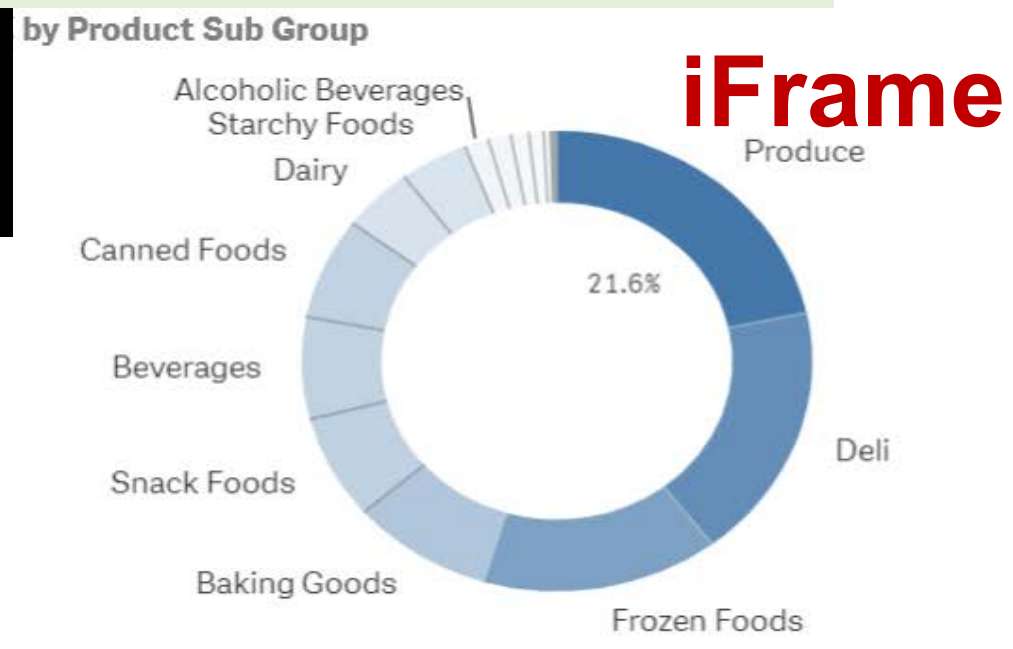
2. Lightweight Integrated

Lightweight iFrame- based integration with your app



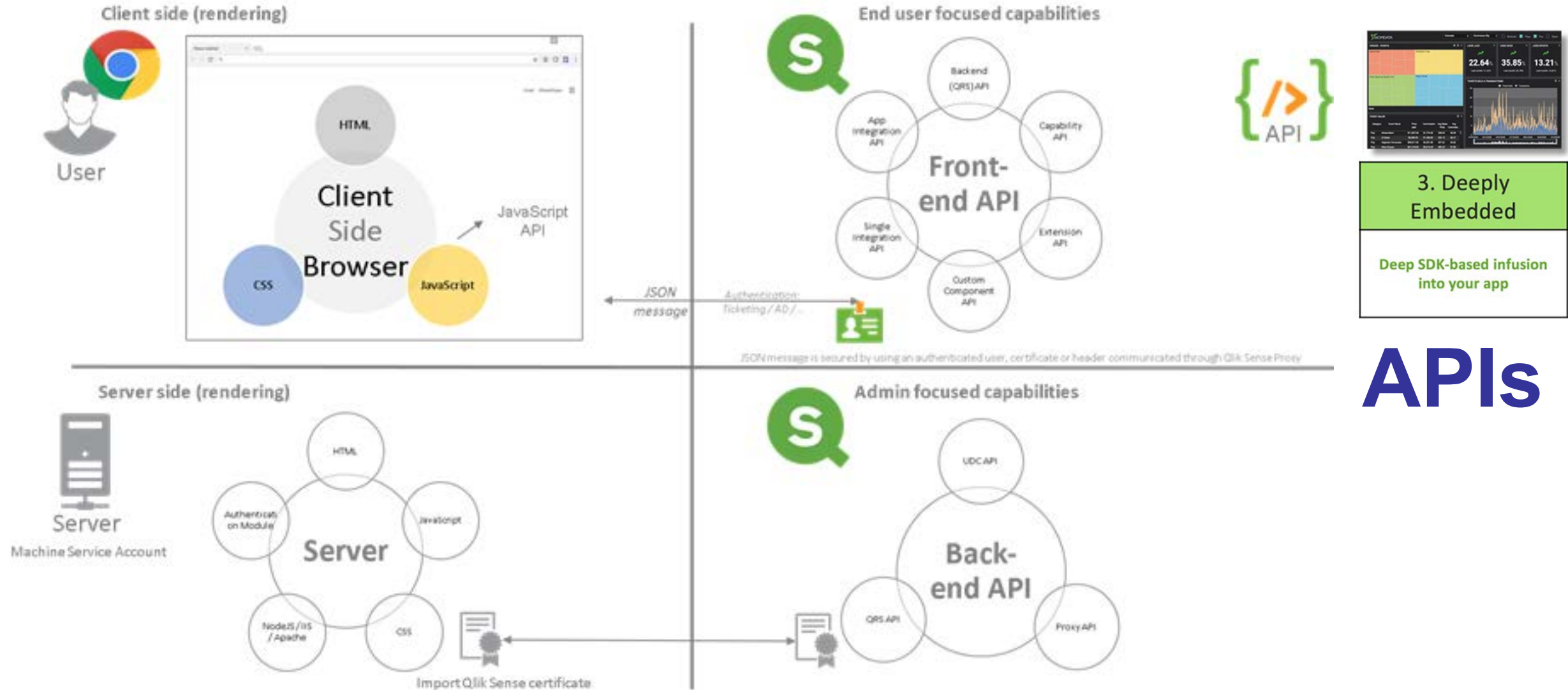
Some limited interactions supported.

The visual parts of Qlik Sense are based on web sockets, Javascript, CSS3, HTML5 and Angular.



Example shown, using Qlik:

Sense™



3. Deeply Embedded

Deep SDK-based infusion into your app

APIs

Example shown, using Qlik:

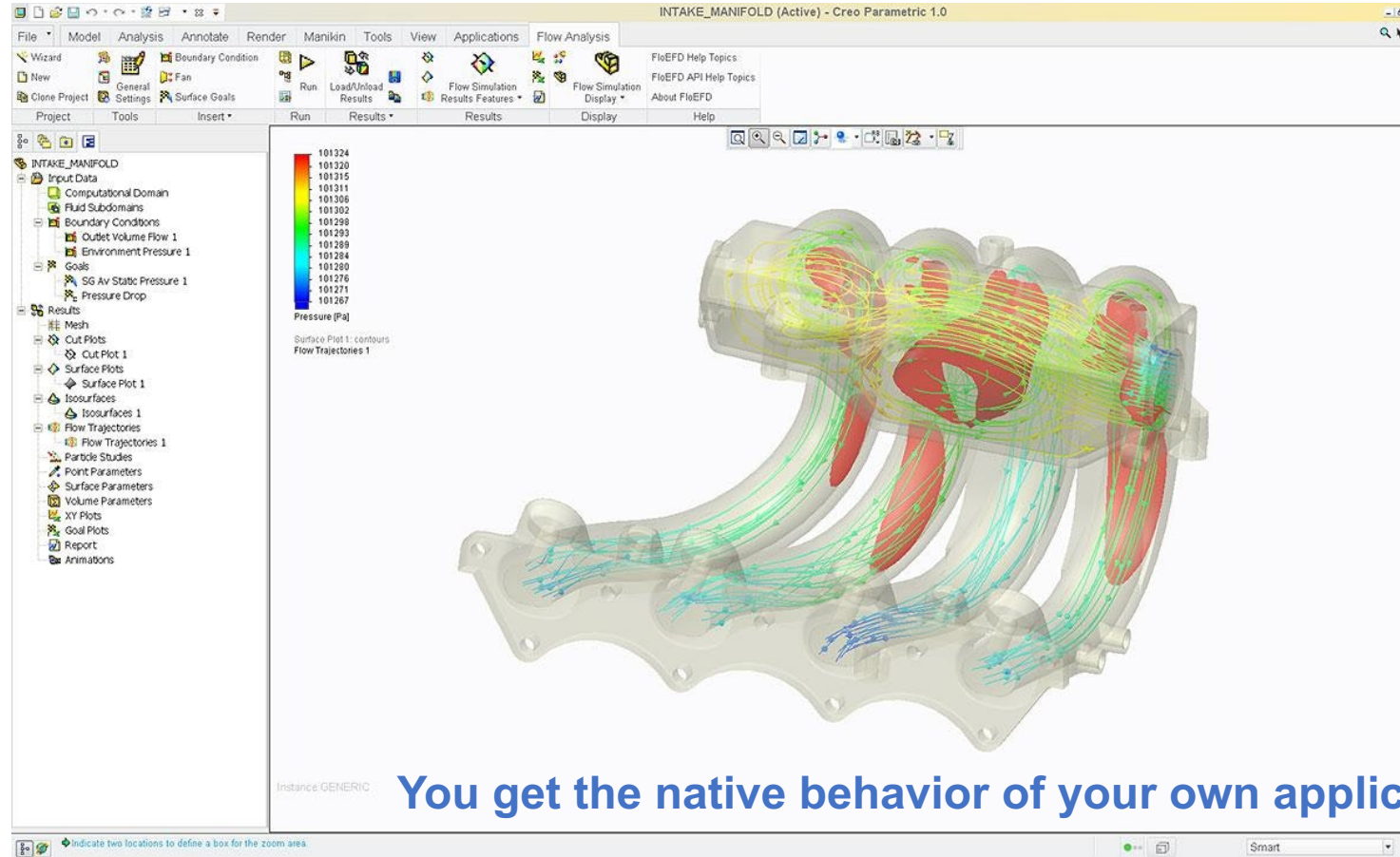
Use JavaScript APIs to embed objects in web pages (front end services) and APIs to communicate with backend services (an example would be the Qlik Engine API, which is a WebSocket protocol that uses JSON to pass information between the Qlik Associative

APIs provide seamless integration into your software applications and



3. Deeply Embedded

Deep SDK-based infusion into your app




You get the native behavior of your own application.

The user should not need know that under the hood Qlik Sense is running

- no double logins
- no context switching
- no juggling multiple applications

Example shown,
using Qlik:



- 
- Buy?
 - Build?
 - **Buy *and* Build?**

Ridiculous number of embedded contextual analytic vendors to choose from...

<https://www.g2.com/categories/business-intelligence>

<https://insightplatforms.com/all-platform-categories>

<https://www.capterra.com/dashboard-software>

<https://bi-survey.com/>

Buy:

- qlik sense
- dundas
- envision
- sisense
- yellowfin
- pyramid analytics
- ms power bi
- tableau
- zoomdata

Build:

- bit+victoryEmbed
- geckoBoard
- matomoEmbed

- Buy?
- Build?
- ***Buy and Build?***

Ridiculous number of embedded contextual analytic vendors to choose from...

- <https://www.g2.com/categories/business-intelligence>
- <https://www.capterra.com/dashboard-software/>
- <https://insightplatforms.com/all-platform-categories/>
- <https://bi-survey.com/>

Buy:

- qlik sense
- dundas
- envision
- sisense
- yellowfin
- pyramid analytics
- ms power bi
- Tableau
- zoomdata

Build:

- bit+victoryEmbed
- GeckoBoard
- matomoEmbed

Scenarios

Data at the Point of Need

WALKOFF Playbook Execution

Device Manager

+ Add Device

- app Penetration Testing
- app STOP DOS DDOS
- app STOP Malware Viruses Worms Trojans
- app STOP Phishing
- app STOP Ransomware
- app STOP Website Attacks
- app Threat Hunting
- app UEBA User and Entity Behavior Analytics**
- app Vulnerability Scanning
- app Wifi Cracker
- wf Firewall Change
- wf Immediate Sandbox
- wf Known Malware Response

Add New Device

Name * **UEBA**

Description **Anomalies**

Associated App * **Walkoff**

Device Type *

Undo Changes and Close Add Device

Filter

Actions

SERVER		+	HOST DETAILS		ABILITY to GROW	
CPU	4			CPU		Rule
Memory	16GB		Memory		Terms	
Disk I/O	i	∞	Disk I/O			
Bandwidth	1GB	cloud	Bandwidth			

Scenario: Add a cloud-based application to your workflow.

WALKOFF Playbook Execution

Device Manager

+ Add Device

Name ~ App

Browse By

- All Applications
- All Workflows
- app Encryption Disk
- app IDS Intrusion Detection
- app Index for Search**
- app IPS Intrusion Prevention
- app Network Analysis
- app Packet Capture Analyzer Sniffer
- app Penetration Testing
- app STOP DOS DDOS
- app STOP Malware Viruses Worms Trojans
- app STOP Phishing

Add New Device

Name * **Index**

Description **Search**

Associated App * Walkoff

Device Type *

Undo Changes and Close Add Device

Filter

Actions

HOST DETAILS

CPU	
Memory	
Disk I/O	
Bandwidth	

ABILITY to GROW

Rule	Host ENV
Terms	

Scenario: Add a legacy application to your workflow.

WALKOFF Playbook Execution

Settings admin

Device Manager

+ Add Device

Name App

app Encryption Disk

app IDS Intrusion Detection

app Index for Search

app IPS Intrusion Prevention

app Network Analysis

app Packet Capture Analyzer Sniffer

app Penetration Testing

app STOP DOS DDOS

app STOP Malware Viruses Worms Trojans

app STOP Phishing

app STOP Ransomware

app STOP Website Attacks

app Threat Hunting

Add New Device

Name * **Denial of Svc**

Description **DOS DDOS**

Associated App * **Walkoff**

Device Type *

Undo Changes and Close Add Device

Filter

Actions

AVAILABLE ?		+ 80/200
Memory	40%	
Network I/O	30%	
Disk I/O	30%	
Swap	40%	

HOST DETAILS		ABILITY to GROW	
CPU		Rule Terms	Host ENV
Memory			
Disk I/O			
Bandwidth			

Scenario: Add an on-prem application to your workflow.

WALKOFF Playbook Execution

Settings admin

Device Manager

+ Add Device

Browse By

- All Applications
- All Workflows
- app Encryption Disk**
- app IDS Intrusion Detection
- app Index for Search
- app IPS Intrusion Prevention
- app Network Analysis
- app Packet Capture Analyzer Sniffer
- app Penetration Testing
- app STOP DOS DDOS
- app STOP Malware Viruses Worms Trojans
- app STOP Phishing

Add New Device

Name * **Disk Encrypt** Description **Files**

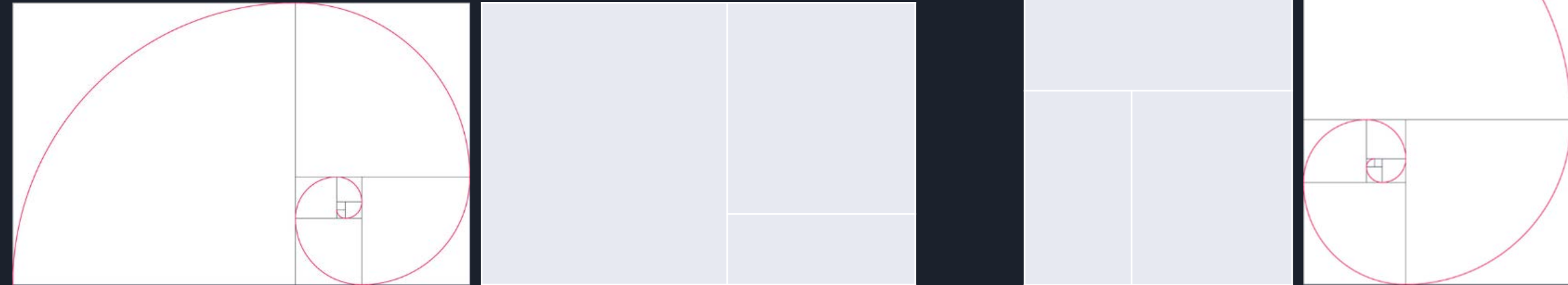
Associated App * **Walkoff** Device Type *

Undo Changes and Close Add Device

Filter Actions

SERVER		i	HOST DETAILS		ABILITY to GROW	
CPU	100%		CPU		Rule	Host ENV
Memory	100%	STOP	Memory			
Disk I/O	100%	📄	Disk I/O			
Bandwidth	1GB	🖨️	Bandwidth			

Scenario: Add an on-prem application to your workflow.



Golden Ratio: A traditional Golden Spiral is formed by the nesting of Golden Rectangles.



(In Progress)

create
empty
message

create text
message
component

create url
message
component



create text message component

NLG is a component that is included with present day business intelligence tools.

NL generation:

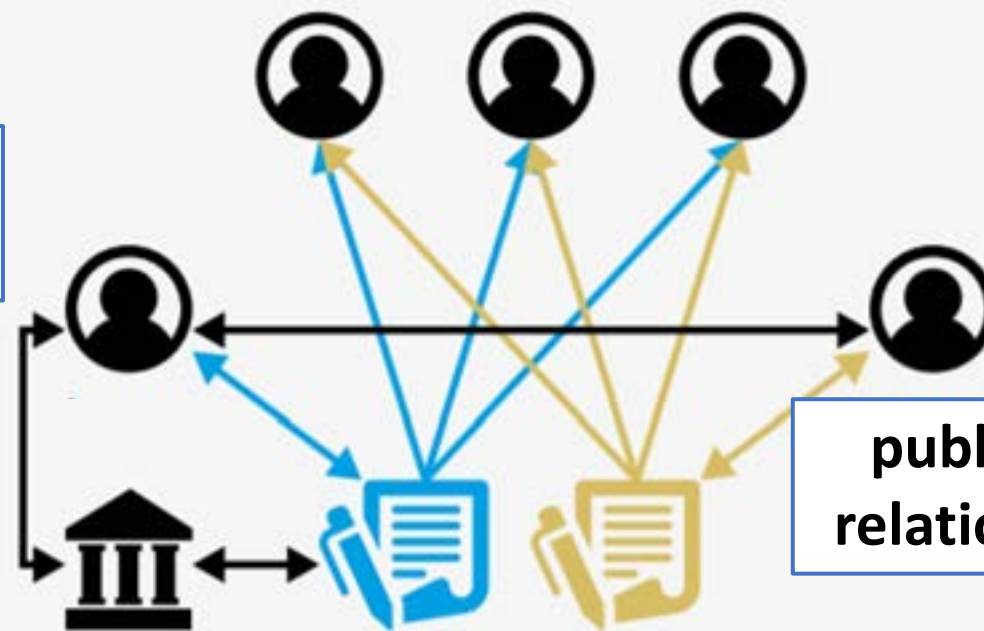
Machine learning widgets pull out relevant meta-data and make the content searchable. It can also extract highlights and summarize content from documents.

external
stakeholders

external
cyber orgs

leadership, legal,
security

public
relations





(In Progress)

create
empty
message

create text
message
component

create url
message
component



create text message component

Automated messaging can be built into the workflow.



NLG can assist in crafting the message to inform the organization. The NLG can also deliver a “recorded” oral message.

All network services are being blocked to the corporate subnetwork located at [...].

All individuals known to be present at that location will receive this same information via a telephone message, email, slack chat, and other personal and organization communication channels contacts (known to, on file with; HR).

The duration of this outage is not known at this time.

The message can be crafted to include detailed information:

- Compromised accounts
- Disrupted services
- Data and network affected by the incident
- Amount and type of damage done to the systems



(In Progress)

create
empty
message

create text
message
component

create url
message
component



create text message component

Automated messaging can be built into the workflow.

NLG can assist in crafting the message to the public (press release).

NL generation:

Machine learning widgets pull out relevant meta-data and make the content searchable. It can also extract highlights and summarize content from documents.




We have experienced a breach of our computer network.

We do not have all the details at this time. As more information becomes available, we will inform the public and provide the appropriate details.

Any personal information breached will only be handled with direct communication to the affected person.

No information about individual persons will be shared with the general public. We have made arrangements to provide free identity protection service to each and every person impacted by this breach.



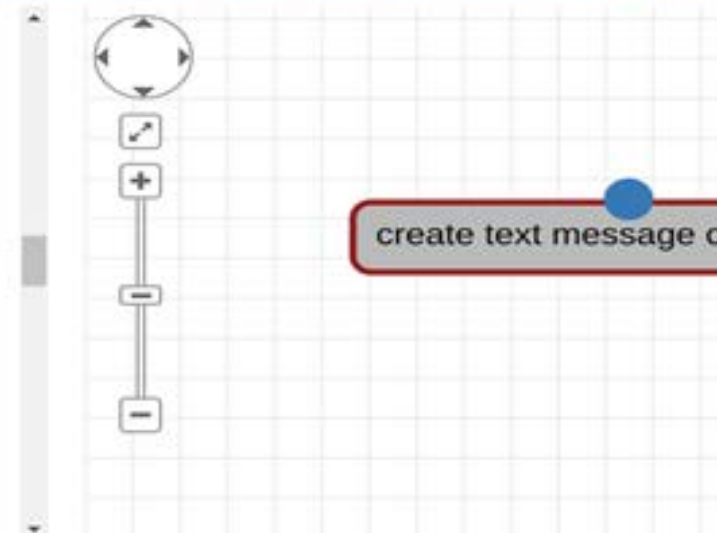


(In Progress)


create empty message

create text message component

create url message component




Automated messaging can be built into the workflow.



NLG can assist in crafting the messages to global Cyber Threat Intelligence operations and standards organizations.

NL generation:
Machine learning widgets pull out relevant meta-data and make the content searchable. It can also extract highlights and summarize content from documents.

- Craft messages specifically for:
- The Federal Bureau of Investigation (FBI)
 - The U.S. Secret Service (USSS)
 - The U.S. Immigration and Customs Enforcement (ICE)
 - The District Attorney
 - State and Local law enforcement
 - STIX-TAXII format → Automated Indicator Sharing (AIS)
 - Cyber Information Sharing and Collaboration Program (CISCP)
 - Information Sharing and Analysis Centers (ISACs)
 - National Cybersecurity and Communications Integration Center's (NCCIC)



“... information consumes the attention of its recipients.
Hence a wealth of information creates a poverty of attention.”

— Herbert Simon
Carnegie Mellon University

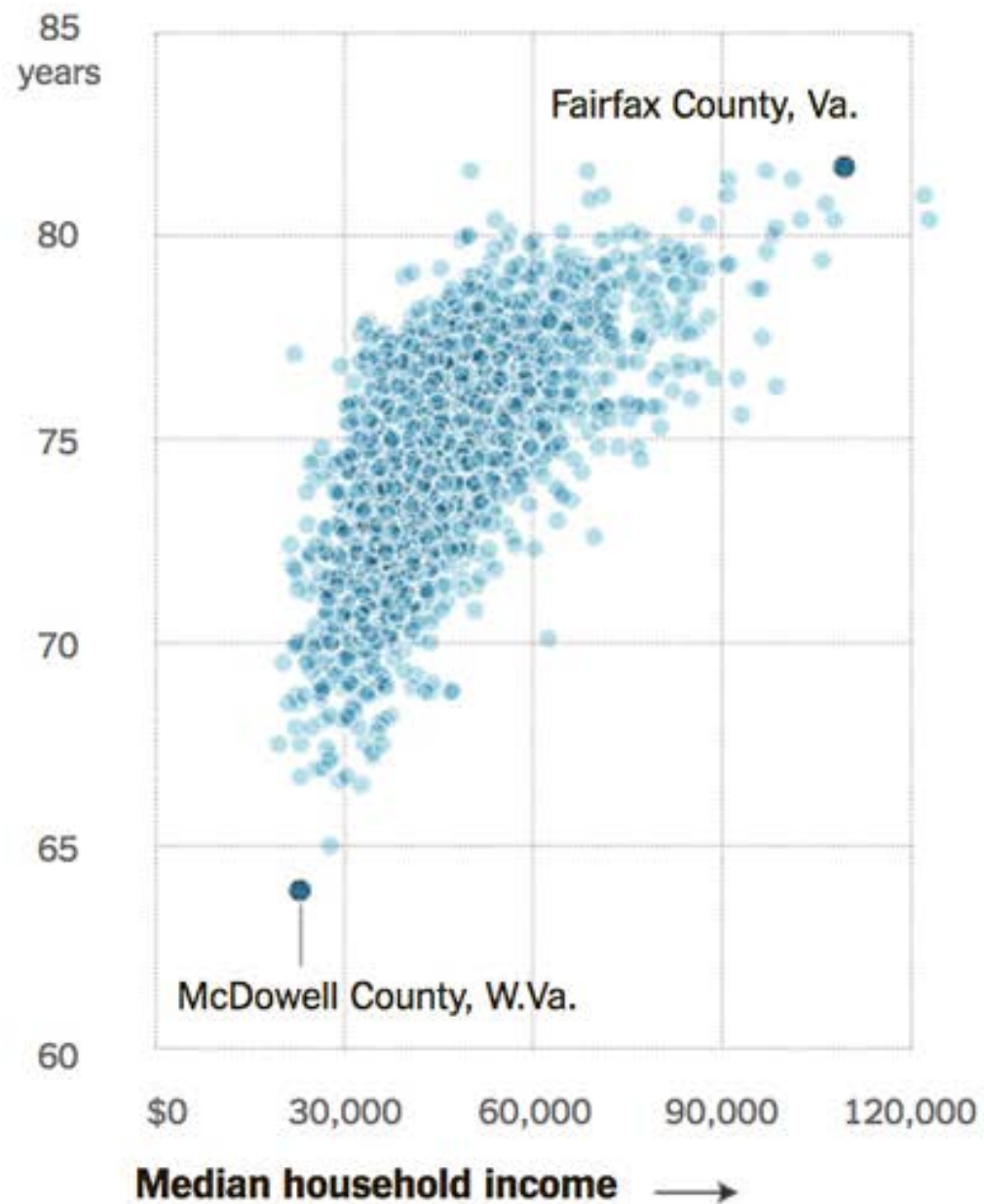
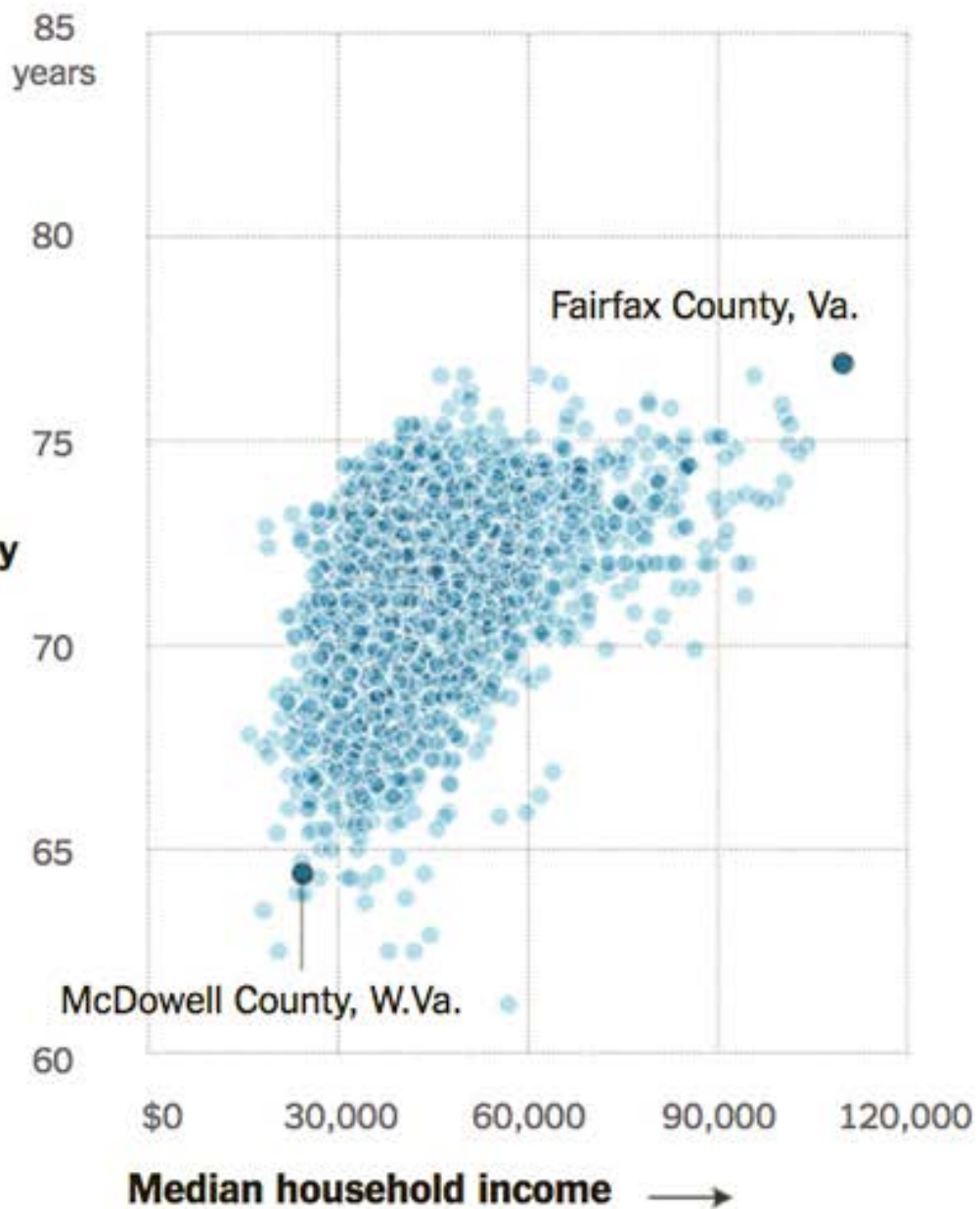
Herbert Alexander Simon was an American economist, political scientist and cognitive psychologist, whose primary research interest was decision-making within organizations and is best known for the theories of "bounded rationality" and "satisficing".

1990

Men

Today

↑
Life
expectancy



Thank you!



RED ALPHA

The best solutions for all your security needs.