451 Research

Digital Transformation, Security and the Future of IT

Scott Crawford, Research Vice President

@s_crawford

Qualys

QSC20 San Francisco
RSA Conference USA 2020

451 Research is a leading IT research and advisory company

451 Research
Now a Part of
S&P Global
Market Intelligence

Founded in 2000, 451 Research is a technology research group within S&P Global Market Intelligence, providing enterprises, product vendors, service providers and investors with insight into market trends and drivers across multiple areas of focus

451 Research Channel Map

- Datacenter Services & Infrastructure
- Applied Infrastructure & DevOps
- Cloud Transformation
- Information Security
- Data, AI & Analytics
- Internet of Things
- Workforce Productivity & Collaboration
- Customer Experience & Commerce

4SIGHT

Universal Risk

Invisible Infrastructure

Pervasive Intelligence

Contextual Experience

Sweeping changes

Monolithic	→	Microservices
Standalone software	→	Integrated services
Self-contained	→	Service mesh
APIs	→	‘Functions as a Service’
Waterfall	→	Agile
IT	→	DevOps
Enterprise	→	IoT, OT, consumer
Networks	→	5G

Security’s incumbents and the ‘Innovator’s Dilemma’

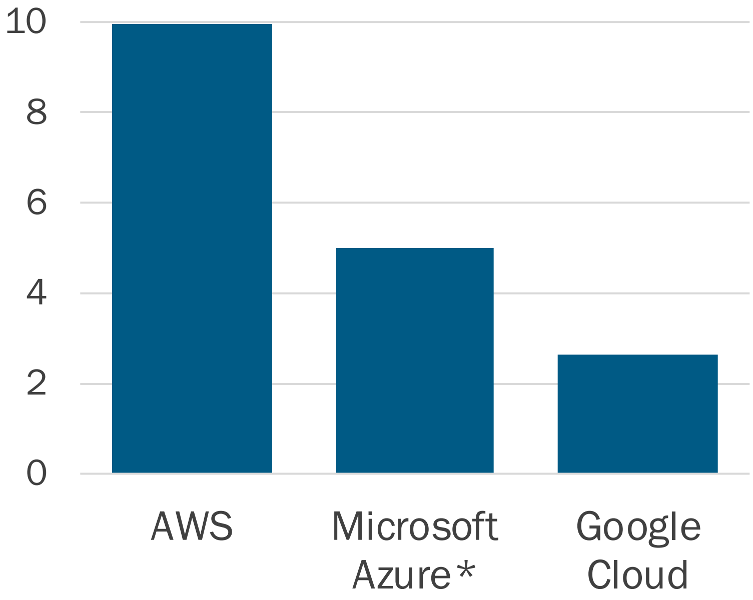
- Bet on the future, at the risk of under-investing in current traction?
- Or double down on current success – but risk missing out on tomorrow’s opportunities?

Clayton M. Christensen
1952-2020

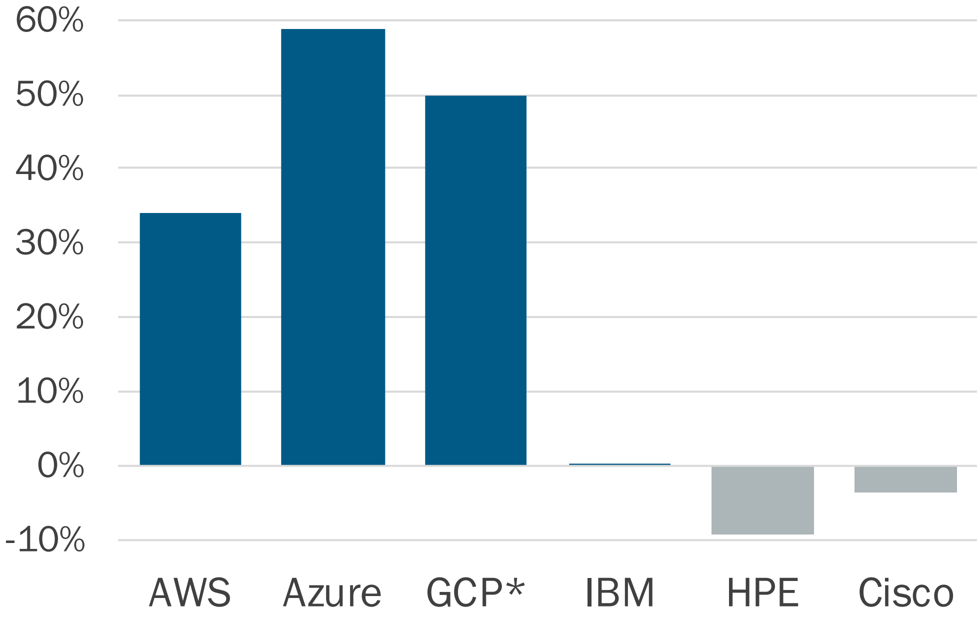
Here comes the **BOOM**!

How high is up?

Major cloud hyperscalers: Quarterly revenues ($ Billions)



YOY Growth



451

451RESEARCH.COM

Adapted from https://bernardgolden.com/amg-q419-numbers-how-high-can-they-go/

*Estimated

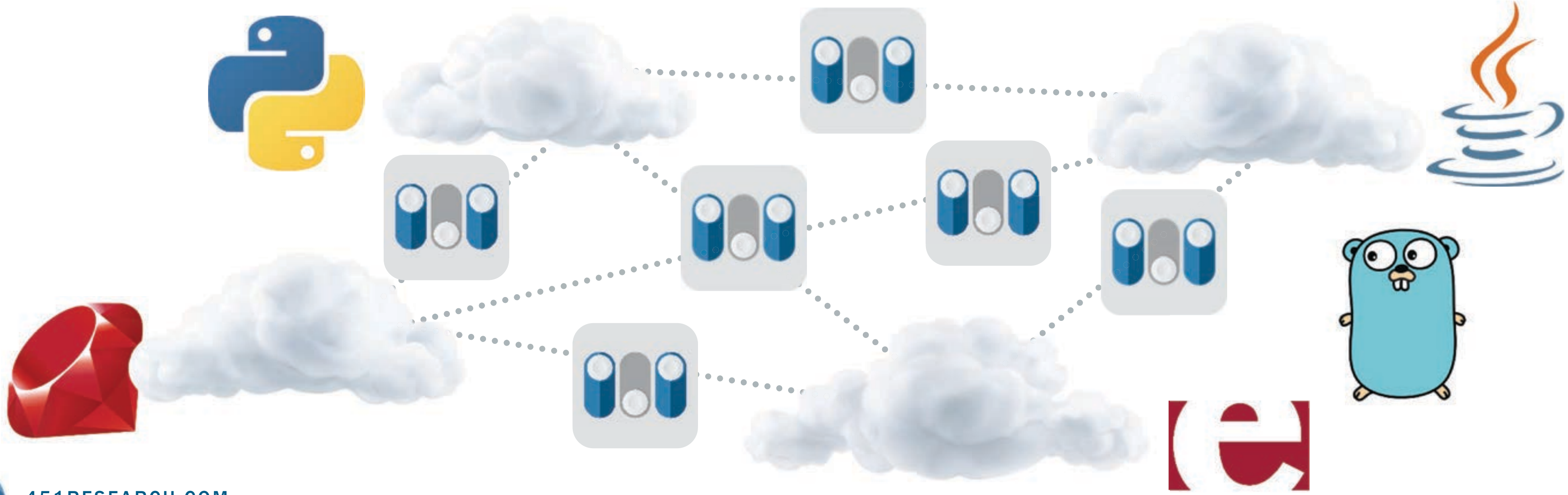
This is the way.

But cloud is hardly the homogeneous, monolithic entity often portrayed

No single point of control

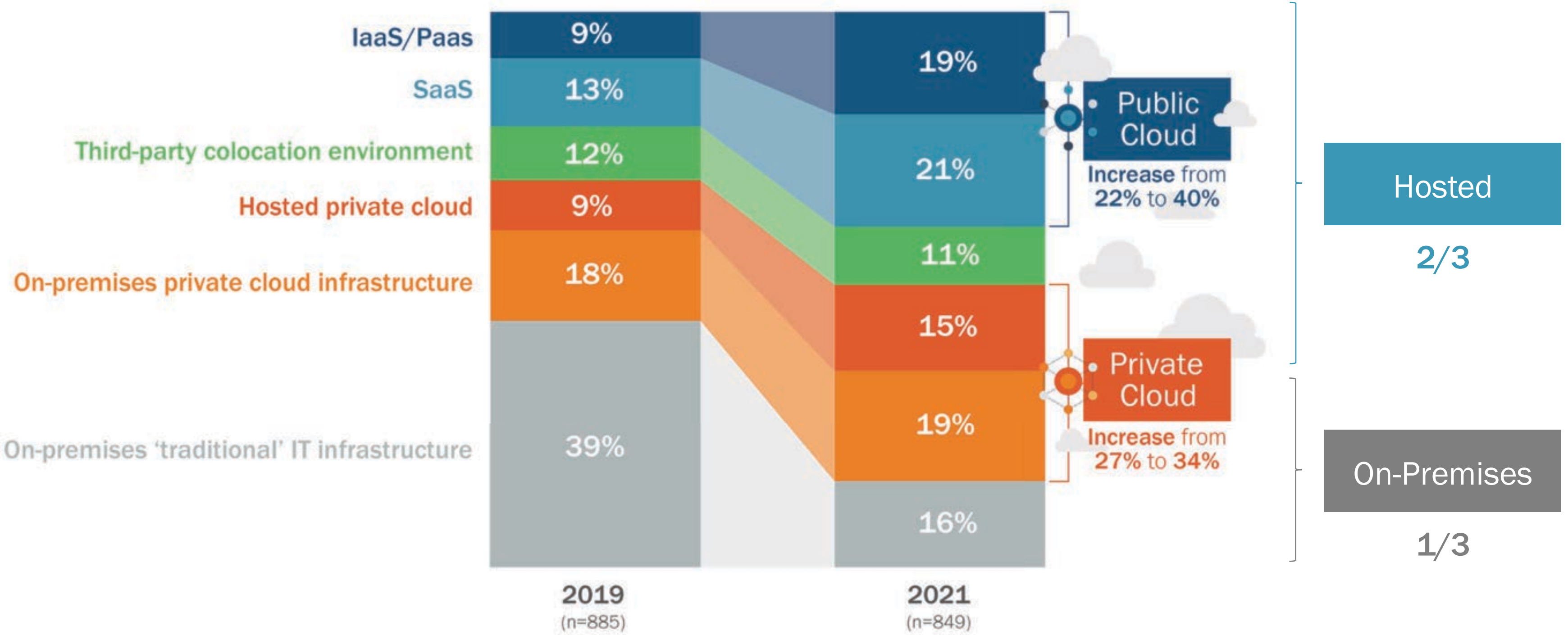
Polyglot applications

A lot of interconnections

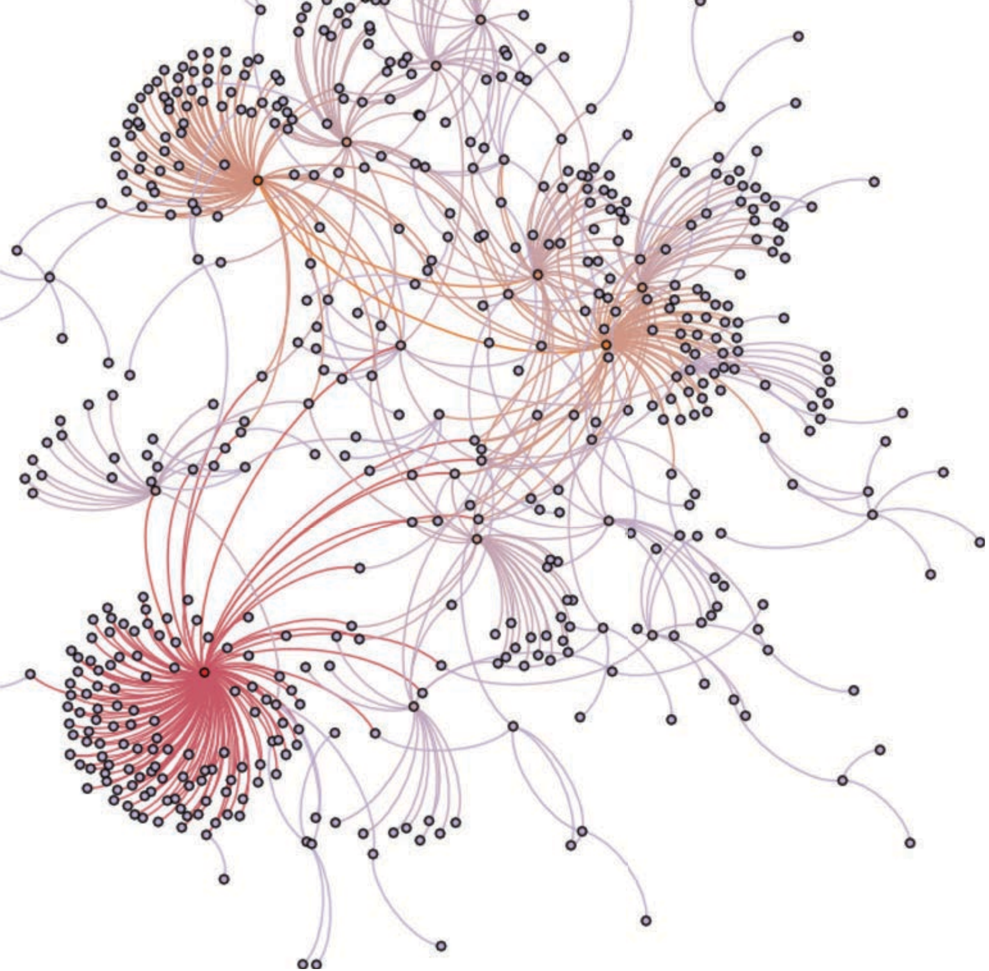


“It’s complicated…”

Primary workload deployment venue

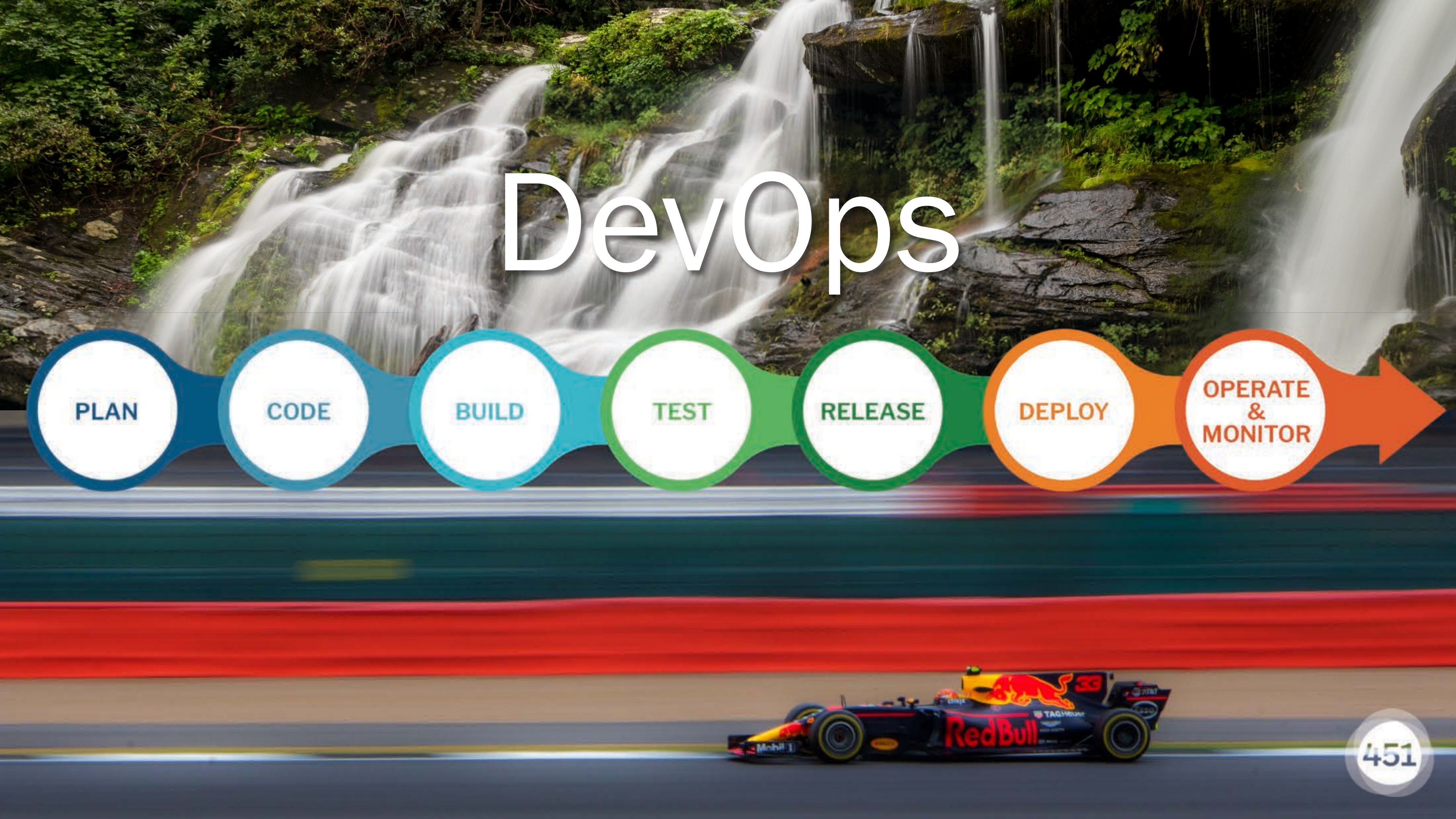


Q. Thinking about all of your organization’s workloads/applications, where are the majority of these currently deployed?
Q. And thinking about all of your organization’s workloads/applications, where will the majority of these be deployed two years from now?
Source: 451 Research’s Voice of the Enterprise: Digital Pulse, Workloads & Key Projects 2019



Maybe a little complexity

DevOps



PLAN

CODE

BUILD

TEST

RELEASE

DEPLOY

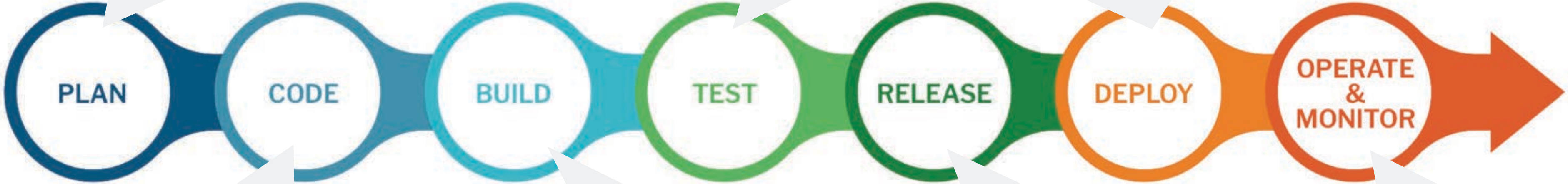
OPERATE & MONITOR

Security has lots of opportunities…

- Software composition analysis
- Developer training

- Dynamic app sec testing

- Operational container & platform security
- Secure orchestration
- Operational protections



- Static app sec testing
- Source security integrated with the IDE

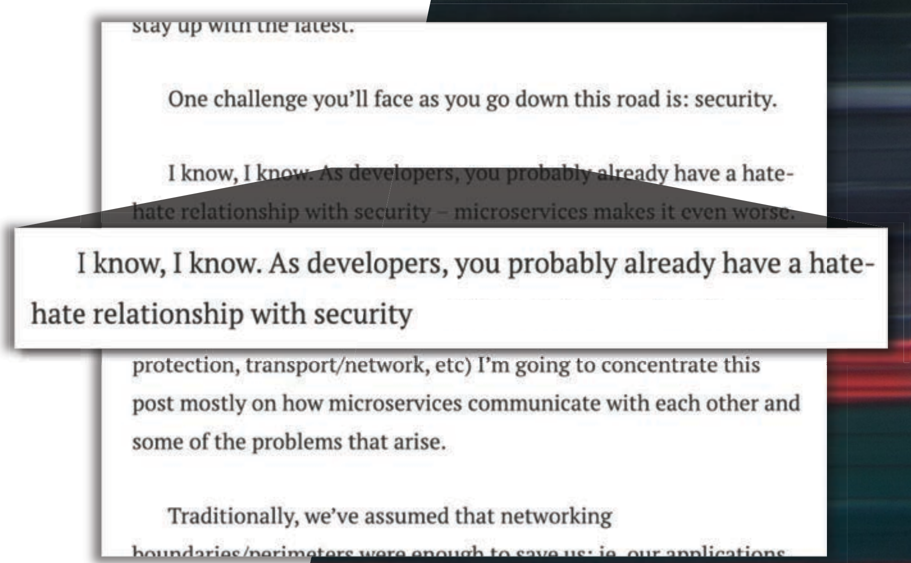
- Defining container security
- Runtime app sec built in

- Gating for security policy, compliance
- Vulnerability checks

- Vulnerability assessment
- Threat activity monitoring

But they don’t exactly love us…

- ▶ Pace
- ▶ Functional and business requirements *first*
- ▶ Toolchain integration
- ▶ ***Putting the developer <u>first</u>***



stay up with the latest.

One challenge you’ll face as you go down this road is: security.

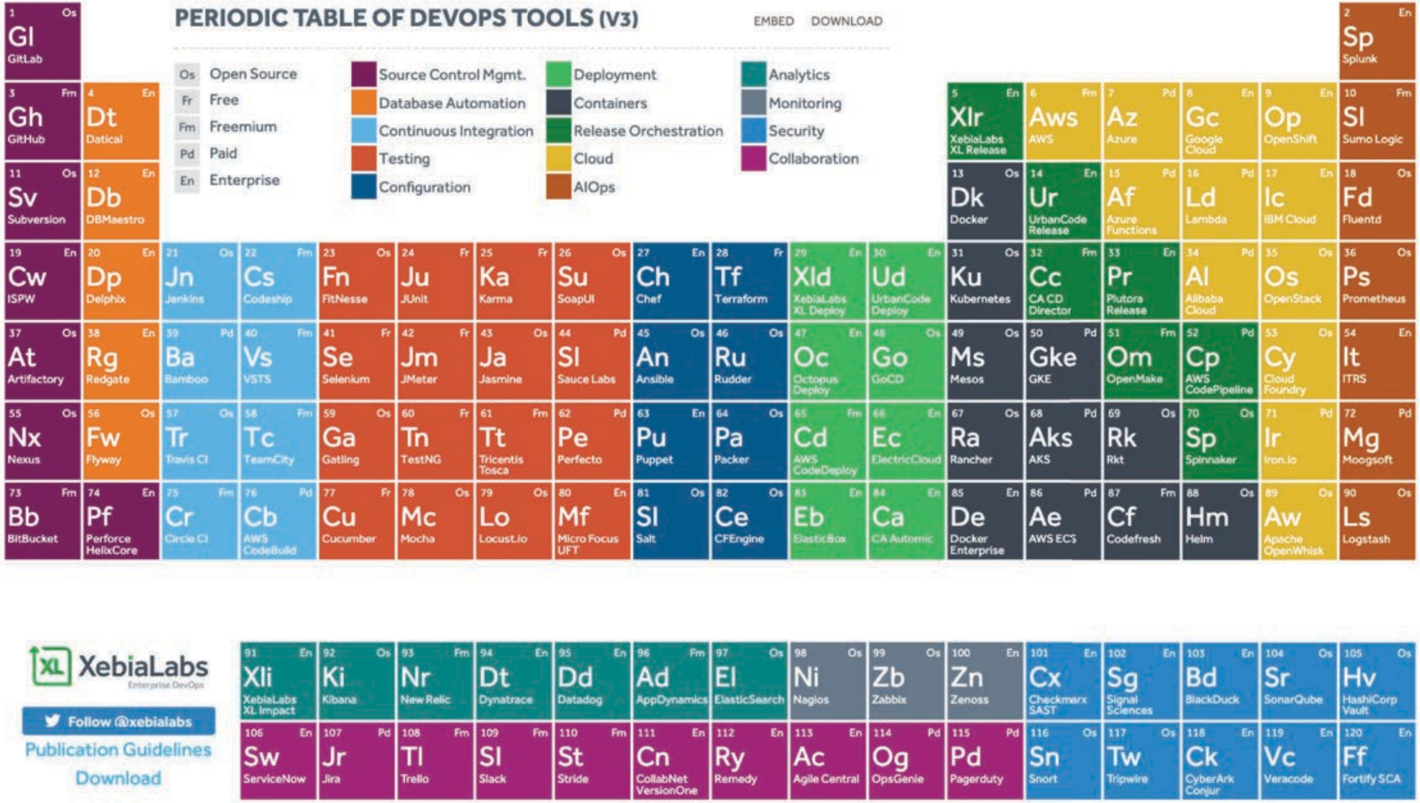
I know, I know. As developers, you probably already have a hate-hate relationship with security – microservices makes it even worse.

I know, I know. As developers, you probably already have a hate-hate relationship with security

protection, transport/network, etc) I’m going to concentrate this post mostly on how microservices communicate with each other and some of the problems that arise.

Traditionally, we’ve assumed that networking boundaries/perimeters were enough to save us; ie, our applications

And each shop has its own toolset preferences



PERIODIC TABLE OF DEVOPS TOOLS (V3)

EMBED DOWNLOAD

Os Open Source
Fr Free
Fm Freemium
Pd Paid
En Enterprise

Source Control Mgmt.
Database Automation
Continuous Integration
Testing
Configuration
Deployment
Containers
Release Orchestration
Cloud
AIOps
Analytics
Monitoring
Security
Collaboration

1	Os	Gl	GitLab
2	En	Sp	Splunk
3	Fm	Gh	GitHub
4	En	Dt	Datical
5	En	Xlr	XebiaLabs XL Release
6	Fm	Aws	AWS
7	Pd	Az	Azure
8	En	Gc	Google Cloud
9	En	Op	OpenShift
10	Fm	Sl	Sumo Logic
11	Os	Sv	Subversion
12	En	Db	DBMaestro
13	Os	Dk	Docker
14	En	Ur	UrbanCode Release
15	Pd	Af	Azure Functions
16	Pd	Ld	Lambda
17	En	Ic	IBM Cloud
18	Os	Fd	Fluentd
19	En	Cw	ISPW
20	En	Dp	Delphix
21	Os	Jn	Jenkins
22	Fm	Cs	Codeship
23	Os	Fn	FitNesse
24	Fr	Ju	JUnit
25	Fr	Ka	Karma
26	Os	Su	SoapUI
27	En	Ch	Chef
28	Fr	Tf	Terraform
29	En	Xld	XebiaLabs XL Deploy
30	En	Ud	UrbanCode Deploy
31	Os	Ku	Kubernetes
32	Fm	Cc	CA CD Director
33	En	Pr	Plutora Release
34	Pd	Al	Alibaba Cloud
35	Os	Os	OpenStack
36	Os	Ps	Prometheus
37	Os	At	Artifactory
38	En	Rg	Redgate
39	Pd	Ba	Bamboo
40	Fm	Vs	VSTS
41	Fr	Se	Selenium
42	Fr	Jm	JMeter
43	Os	Ja	Jasmine
44	Pd	Sl	Sauce Labs
45	Os	An	Ansible
46	Os	Ru	Rudder
47	En	Oc	Octopus Deploy
48	Os	Go	GoCD
49	Os	Ms	Mesos
50	Pd	Gke	GKE
51	Fm	Om	OpenMake
52	Pd	Cp	AWS CodePipeline
53	Os	Cy	Cloud Foundry
54	En	It	ITRS
55	Os	Nx	Nexus
56	Os	Fw	Flyway
57	Os	Tr	Travis CI
58	Fm	Tc	TeamCity
59	Os	Ga	Gatling
60	Fr	Tn	TestNG
61	Fm	Tt	Tricentis Tosca
62	Pd	Pe	Perfecto
63	En	Pu	Puppet
64	Os	Pa	Packer
65	Fm	Cd	AWS CodeDeploy
66	En	Ec	ElectricCloud
67	Os	Ra	Rancher
68	Pd	Aks	AKS
69	Os	Rk	Rkt
70	Os	Sp	Spinnaker
71	Pd	Ir	Iron.io
72	Pd	Mg	Moogsoft
73	Fm	Bb	BitBucket
74	En	Pf	Perforce HelixCore
75	Fm	Cr	Circle CI
76	Pd	Cb	AWS CodeBuild
77	Fr	Cu	Cucumber
78	Os	Mc	Mocha
79	Os	Lo	Locust.io
80	En	Mf	Micro Focus UFT
81	Os	Sl	Salt
82	Os	Ce	CFEngine
83	En	Eb	ElasticBox
84	En	Ca	CA Automic
85	En	De	Docker Enterprise
86	Pd	Ae	AWS ECS
87	Fm	Cf	Codefresh
88	Os	Hm	Helm
89	Os	Aw	Apache OpenWhisk
90	Os	Ls	Logstash
91	En	Xli	XebiaLabs XL Impact
92	Os	Ki	Kibana
93	Fm	Nr	New Relic
94	En	Dt	Dynatrace
95	En	Dd	Datadog
96	Fm	Ad	AppDynamics
97	Os	El	ElasticSearch
98	Os	Ni	Nagios
99	Os	Zb	Zabbix
100	En	Zn	Zenoss
101	En	Cx	Checkmarx SAST
102	En	Sg	Signal Sciences
103	En	Bd	BlackDuck
104	Os	Sr	SonarQube
105	Os	Hv	HashiCorp Vault
106	En	Sw	ServiceNow
107	Pd	Jr	Jira
108	Fm	Tl	Trello
109	Fm	Sl	Slack
110	Fm	St	Stride
111	En	Cn	CollabNet VersionOne
112	En	Ry	Remedy
113	En	Ac	Agile Central
114	Pd	Og	OpsGenie
115	Pd	Pd	Pagerduty
116	Os	Sn	Snort
117	Os	Tw	Tripwire
118	En	Ck	CyberArk Conjur
119	En	Vc	Veracode
120	En	Ff	Fortify SCA

XL XebiaLabs
Enterprise DevOps

Follow @xebialabs

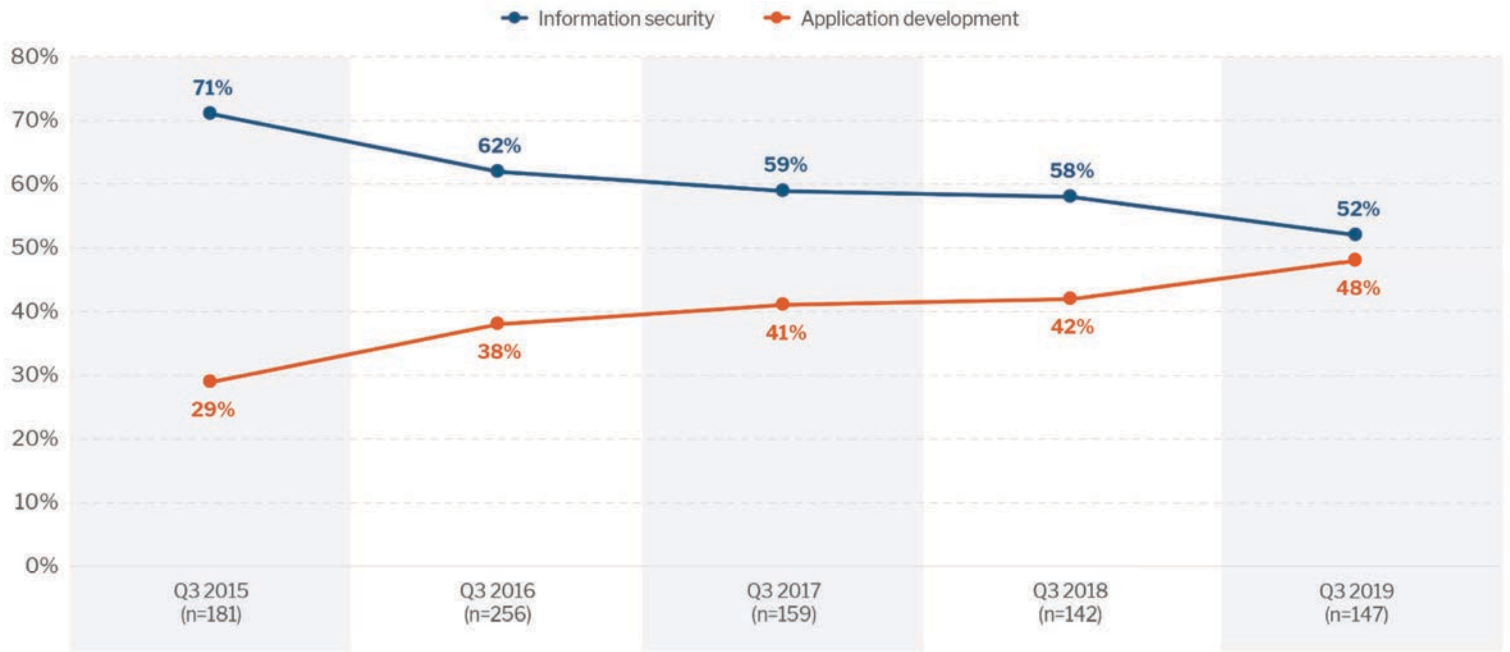
Publication Guidelines

Download

Source: https://xebialabs.com/periodic-table-of-devops-tools

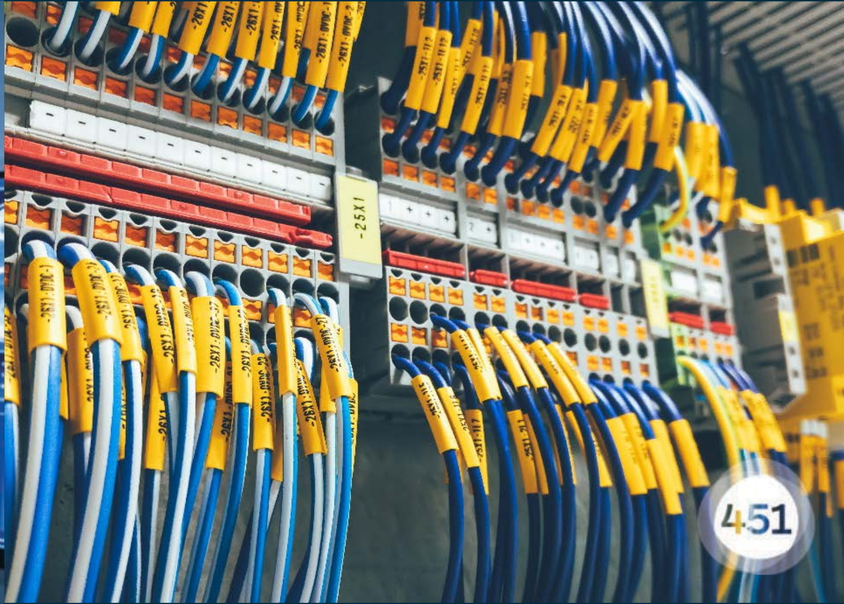
Security teams that don’t enable developers to use AST tools will soon be on the wrong side of a clearly identifiable trend

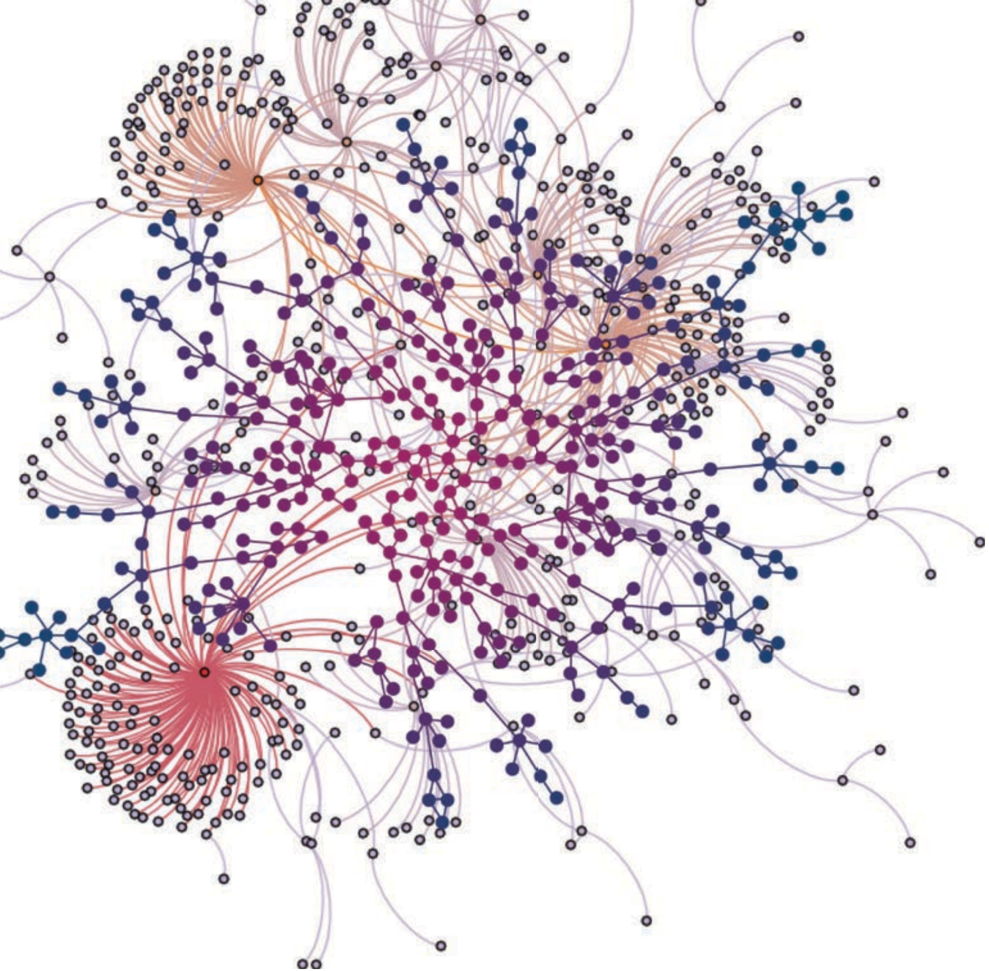
Application Security Tool Usage by Team



Q. How is the usage of application security tools allocated across the following two teams in your organization?
Base: Respondents currently using application security
Source: 451 Research’s Voice of the Enterprise: Information Security, Budgets & Outlook 2019

What about all the ‘things’?

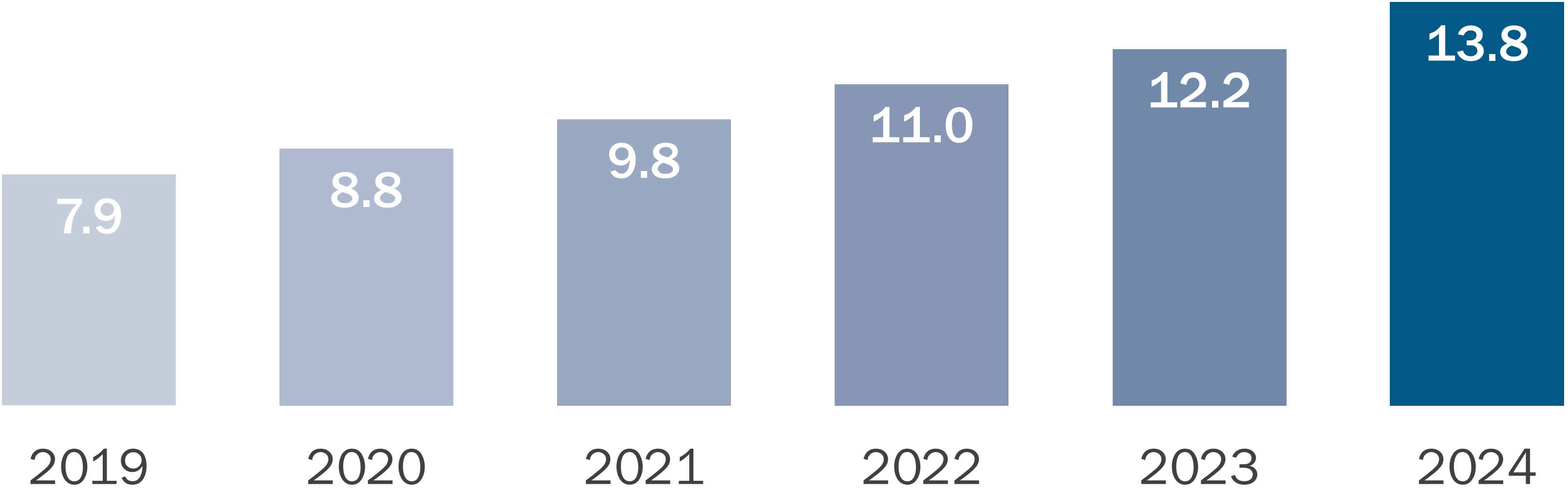




A bit more complexity

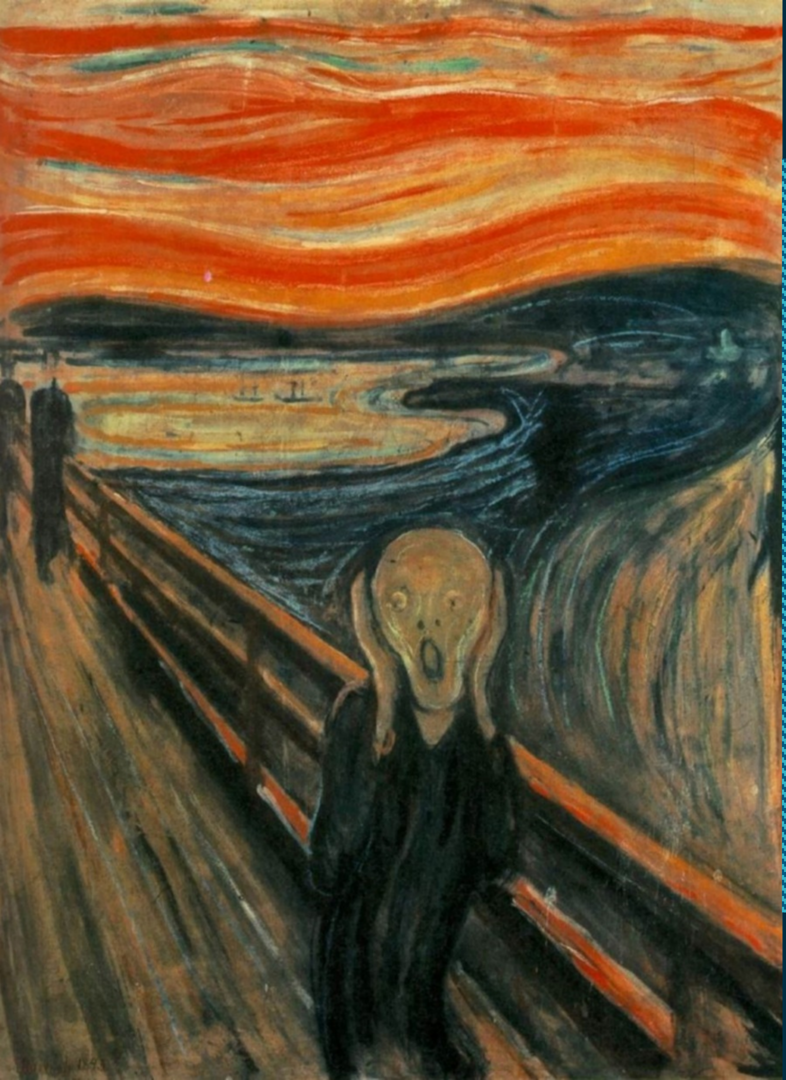
Okay, a **LOT** more complexity

In the enterprise*: Total connected IoT devices (in billions of units)



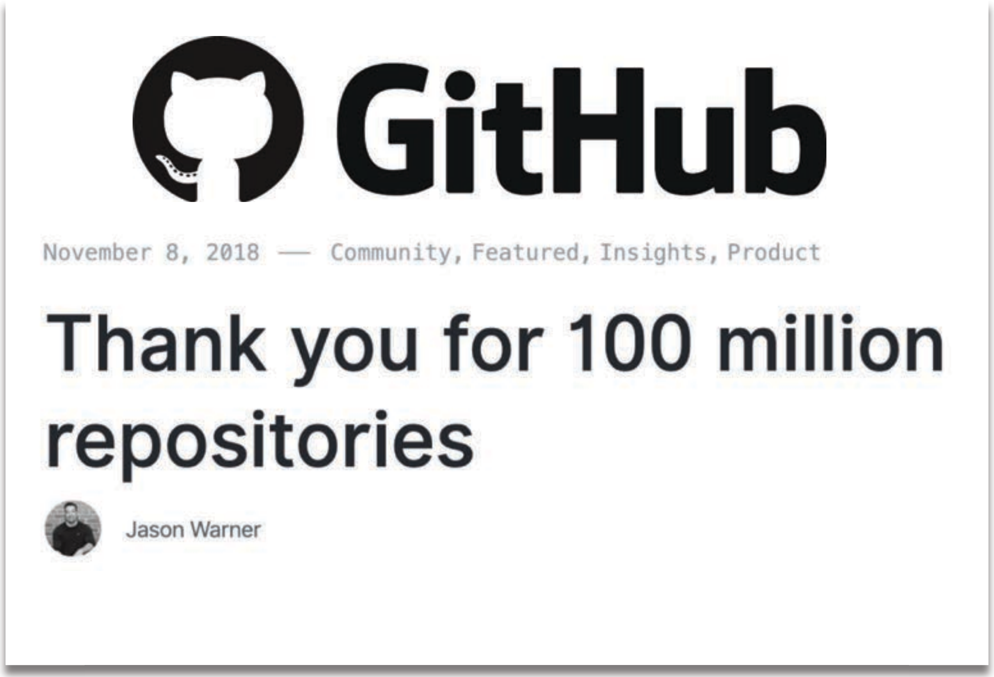
*Not including consumer devices (e.g., PCs, smart TVs, game consoles)

Source: 451 Research's IoT Market Monitor, June 2019



Where are we going to find the software to power all the things?

Oh.



GitHub

November 8, 2018 — Community, Featured, Insights, Product

Thank you for 100 million repositories

Jason Warner

Microsoft to acquire GitHub for $7.5 billion

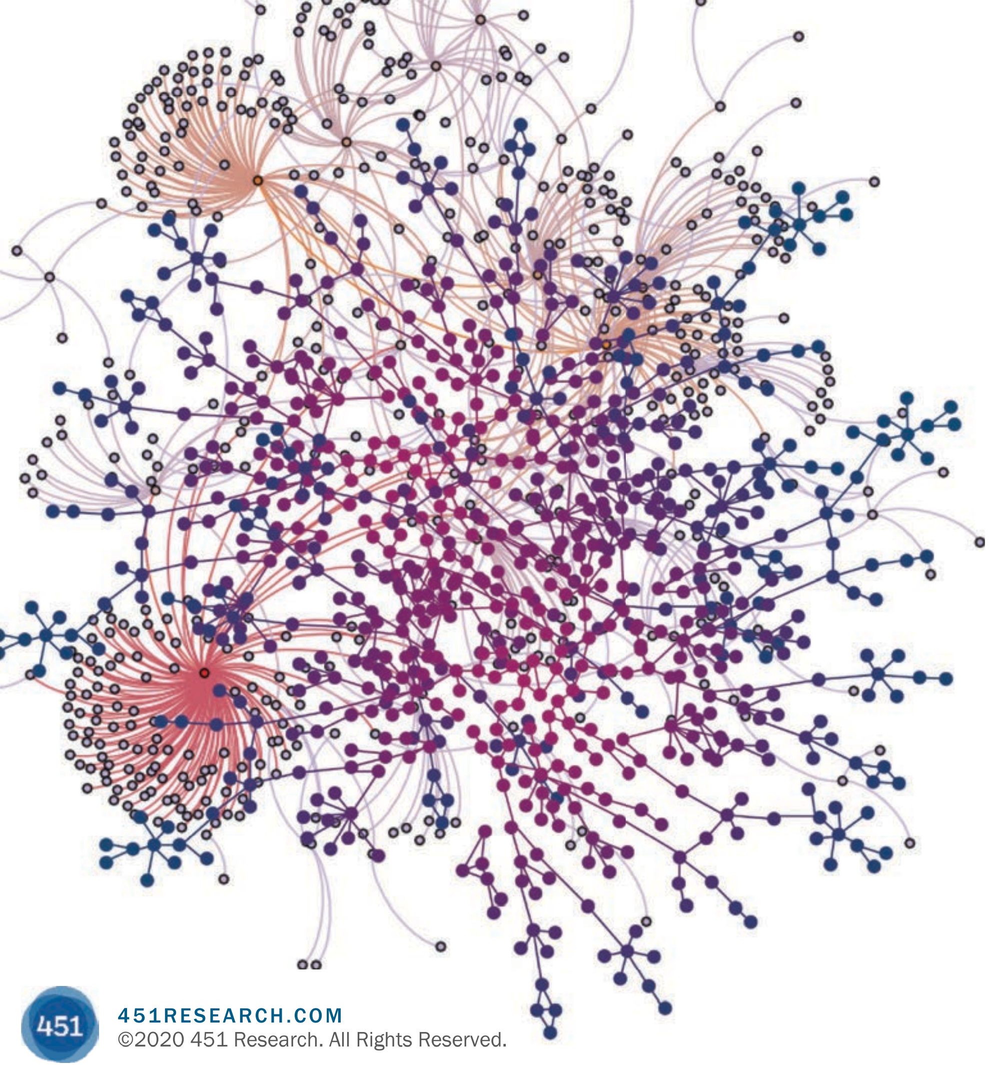
June 4, 2018 | Microsoft News Center

Sources: https://github.blog/2018-11-08-100m-repos/, https://news.microsoft.com/2018/06/04/microsoft-to-acquire-github-for-7-5-billion/

Vulnerability remediation and the ‘Russian doll’ of open source

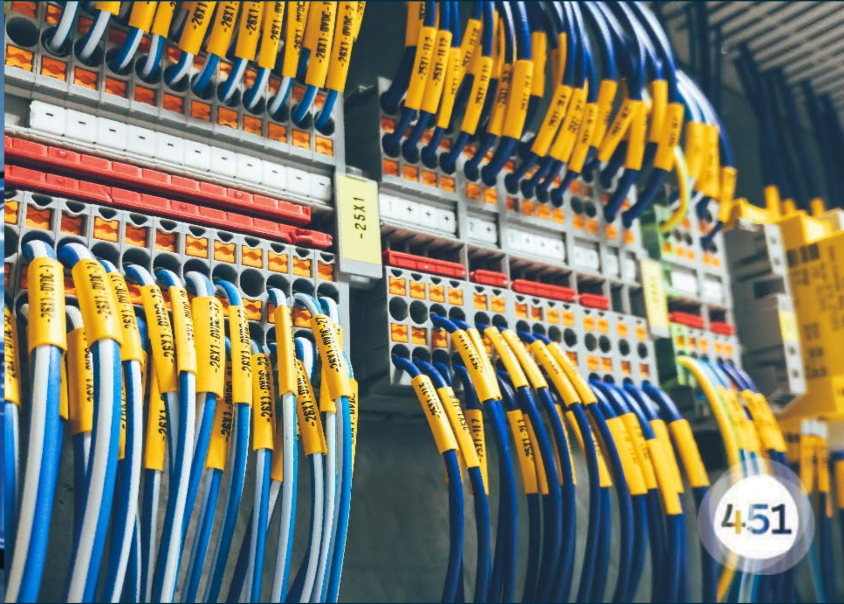
Example: Struts 2 vulnerability

- ...which extends the Java Servlet API
- ...had a vulnerability in OGNL (remote code execution exposure)
- ...which is incorporated in Jakarta
- ...which was part of Apache



Still more complexity

Let’s get ’em all on the network!



How many people?

What's trust got to do with it?

It’s all about *proof*

Who seeks access?

Enterprise users

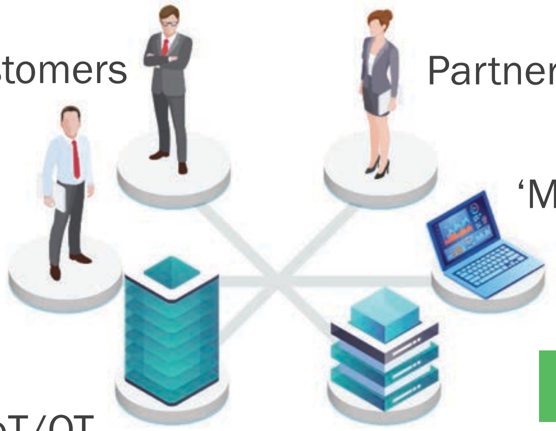
Customers

Partners

‘M2M’

IoT/OT

Traditional IT endpoints



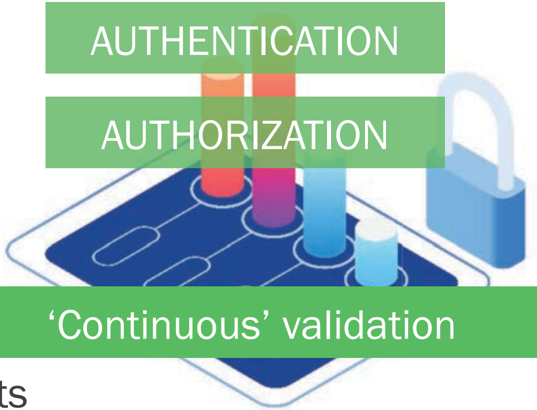
Under ***what*** conditions?

Decision-making: AI/ML-enabled

AUTHENTICATION

AUTHORIZATION

‘Continuous’ validation



To ***which*** targets?

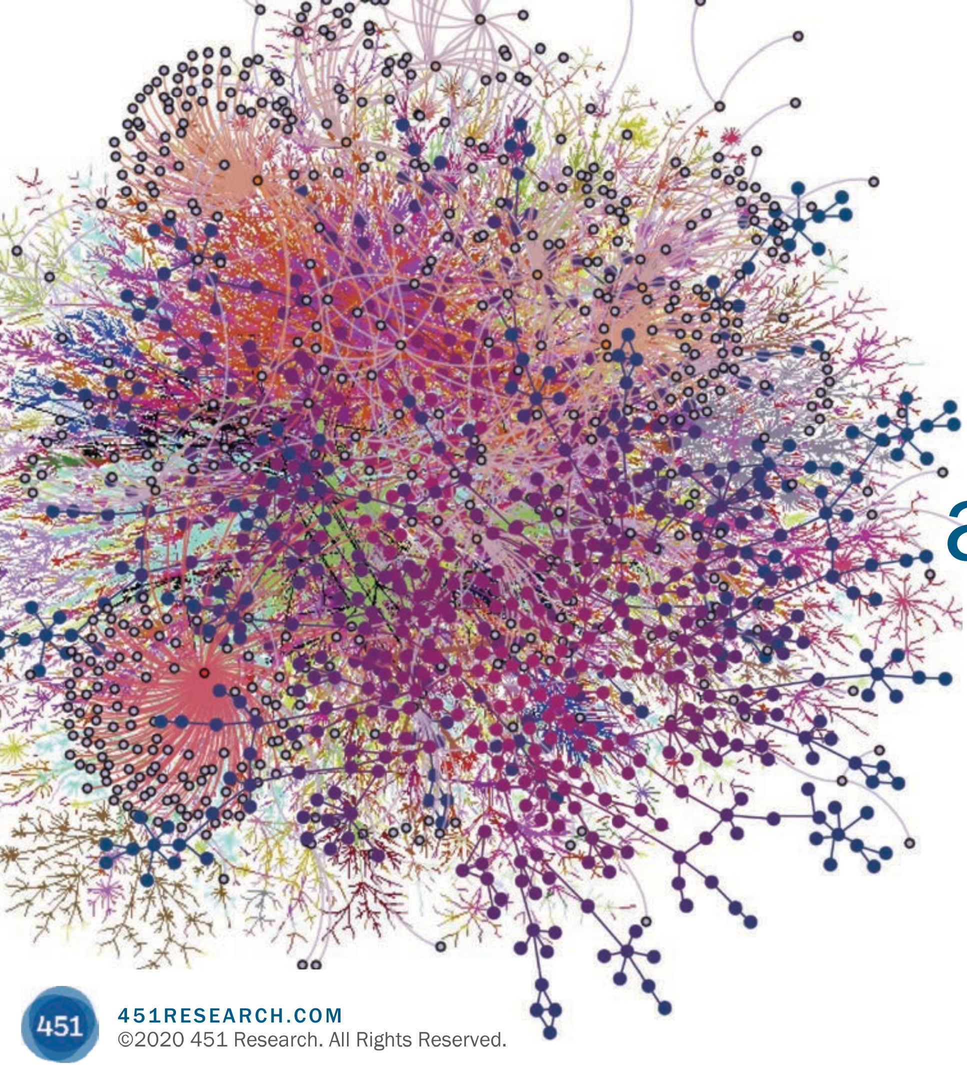
Fine-grained access control

Applications, cloud resources, APIs, SaaS, etc.

*...and, oh yeah, **DATA***

WITH SECURITY FOR DATA THROUGHOUT

451RESEARCH.COM



Now, multiply each decision on a scale of billions.

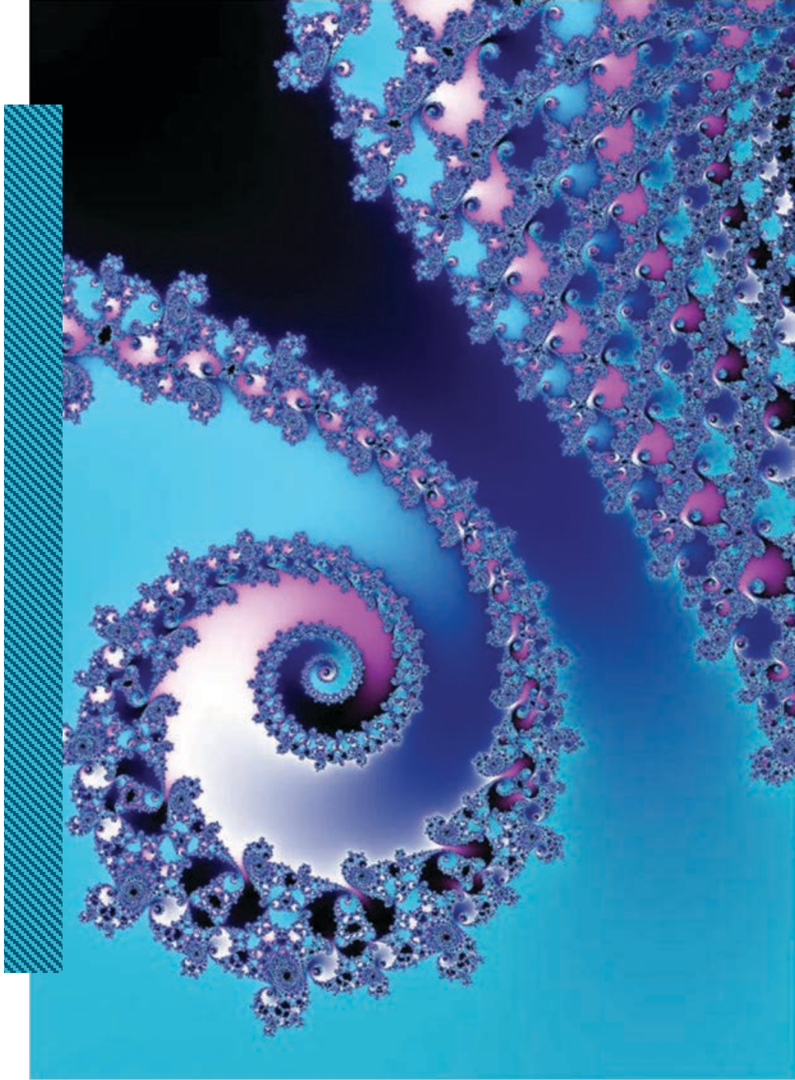
Continuously.

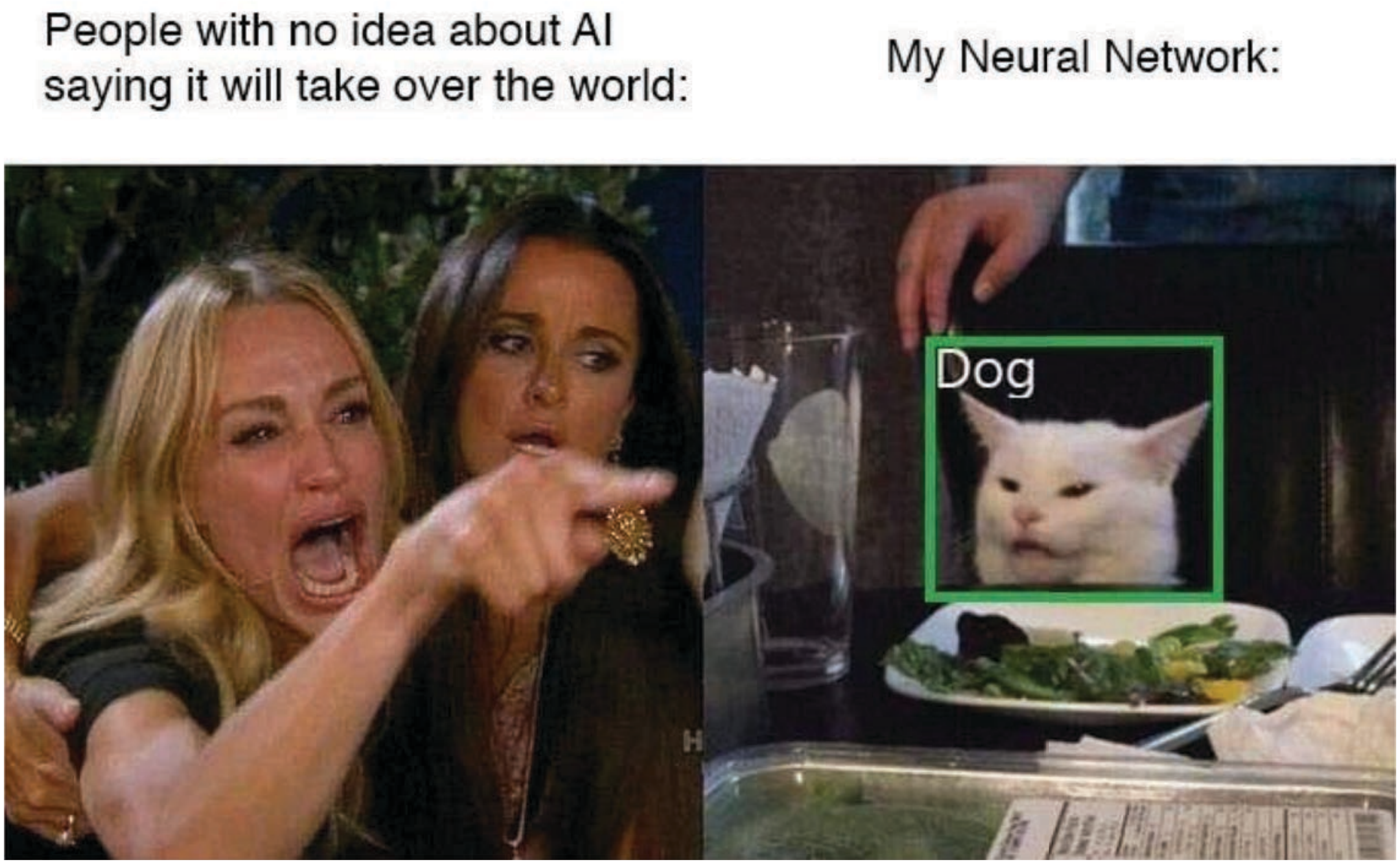
Expand your thinking about…

Security analytics

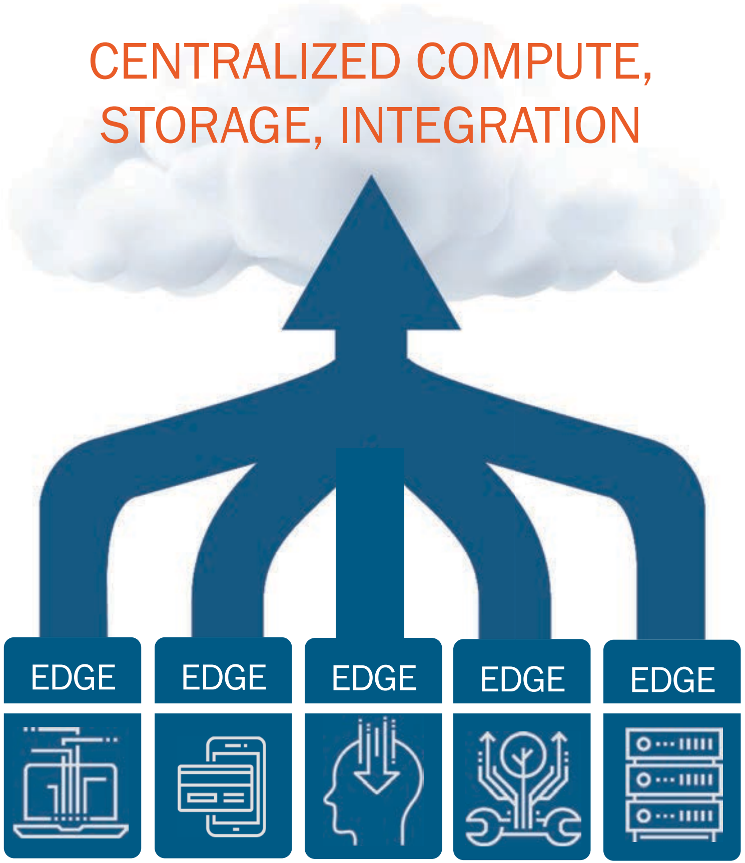
It can’t all be done in one place

Distributed compute now
may be nothing compared
to what’s coming




People with no idea about AI saying it will take over the world:
My Neural Network:
Dog

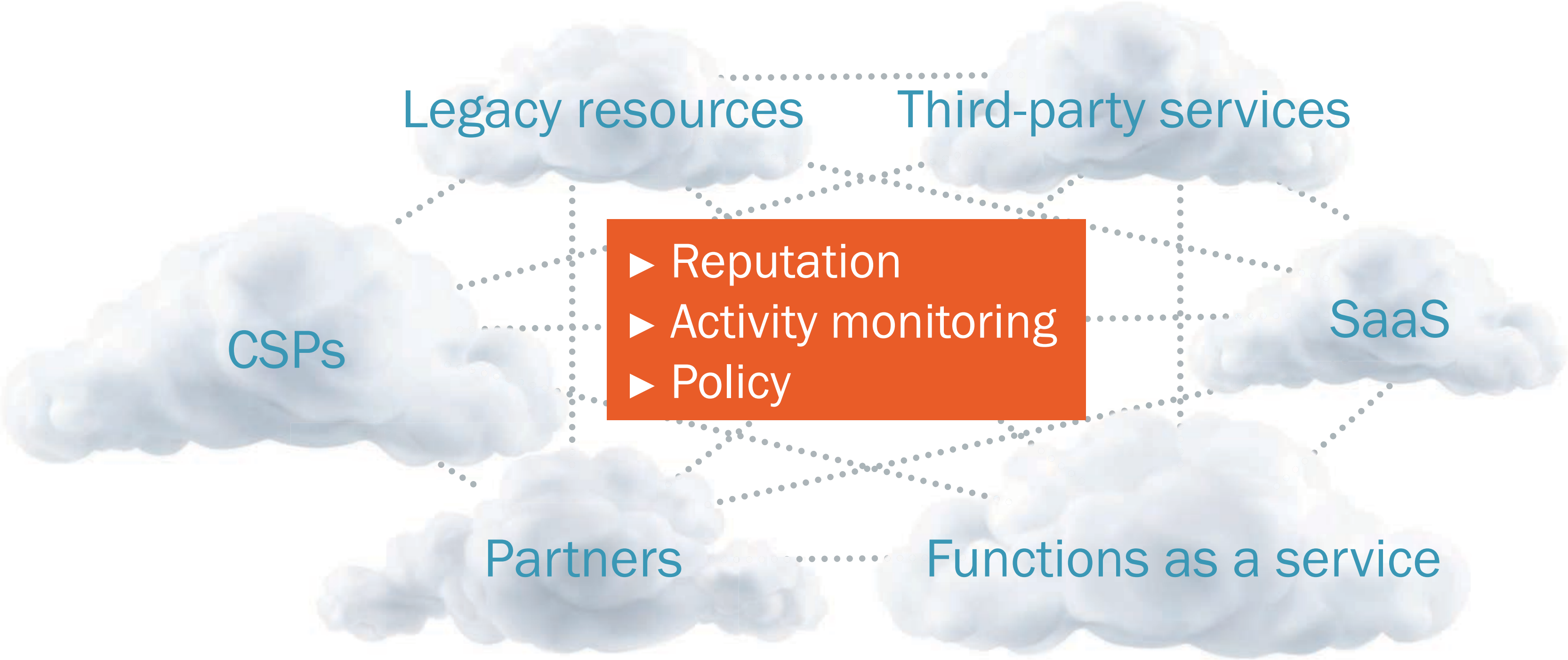
Twitter: @MVLibertas (Mat Vaillancourt)
https://twitter.com/mvlibertas/status/1195353071322304512



Distributed analytics and control fits other emerging patterns

- Ways to distribute high-volume analysis
- (And offload compute for less capable endpoints)
- Edge – or ‘fog’ – computing
- Stream analytics
- ‘Zero trust’ access enforcement

Sources of security insight – talking to each other, too



Legacy resources

Third-party services

CSPs

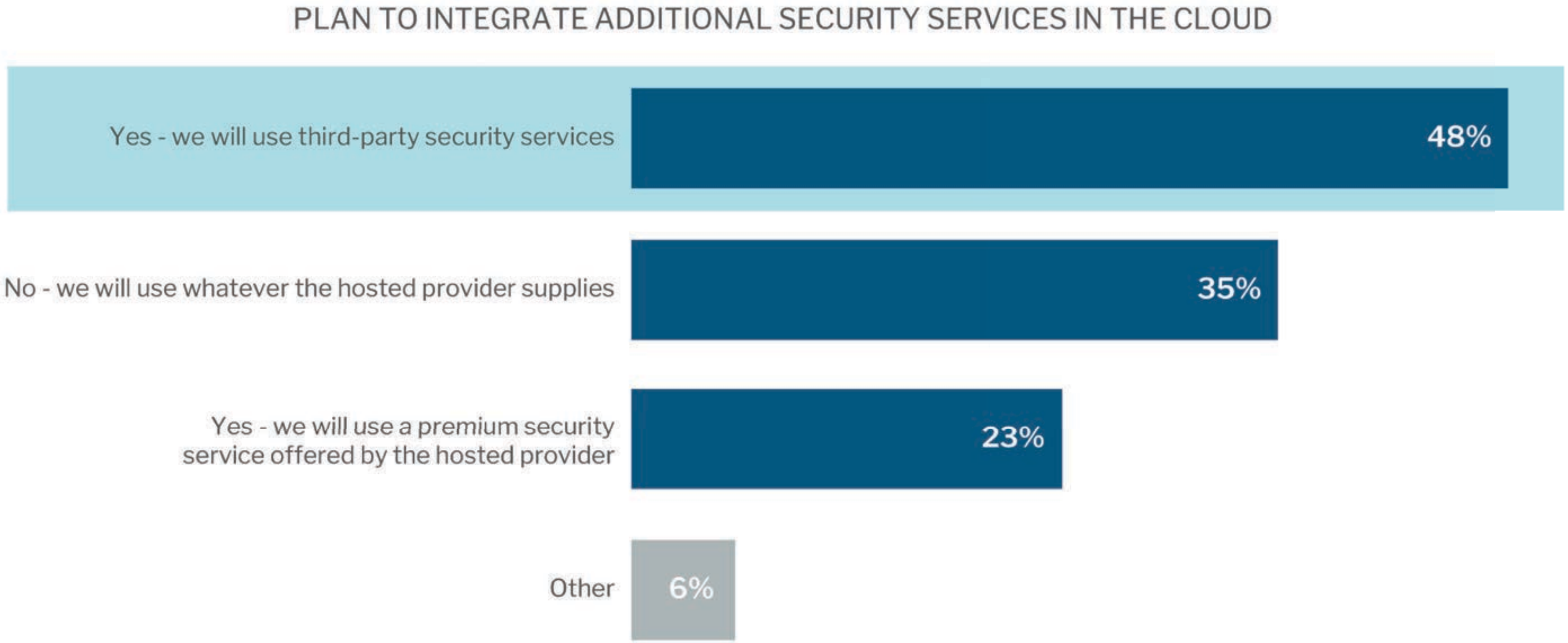
SaaS

- ▶ Reputation
- ▶ Activity monitoring
- ▶ Policy

Partners

Functions as a service

Those integrating third-party security solutions outnumber those that will rely exclusively on a cloud provider's services



Q. Do you plan to acquire additional security services for your hosted architecture in 2019?
Base: All respondents (n=231)
Source: 451 Research's Voice of the Enterprise: Information Security, Budgets and Outlook 2019

Cyber risk scoring: The ‘new black’

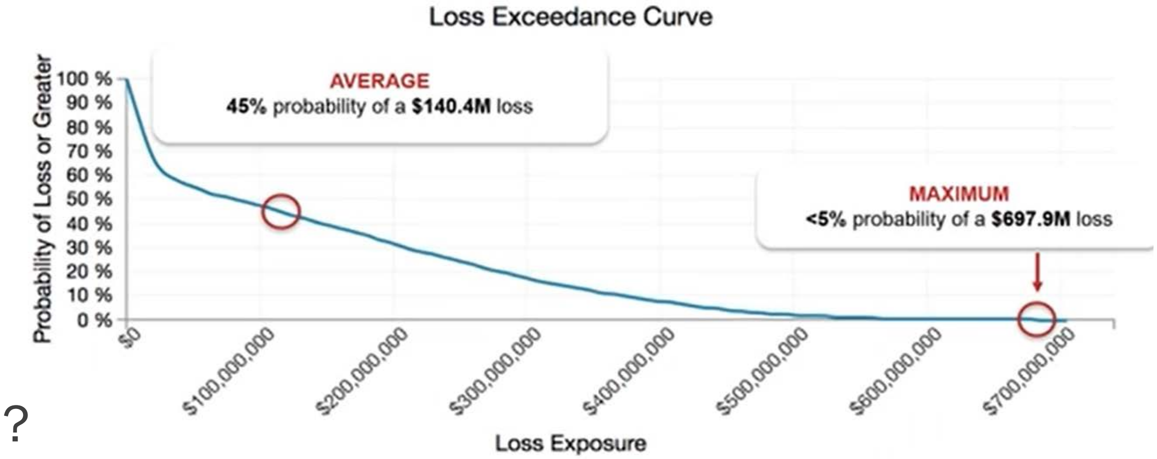
Or rather, a color palette

- Too much high – low

Third party and supplier risk ratings are ‘in’

Challenges

- Visible attack surface?
- *Business impact?*



451RESEARCH.COM

Image: https://www.fairinstitute.org/blog/webinar-operationalizing-fair-in-your-organization-with-risklens

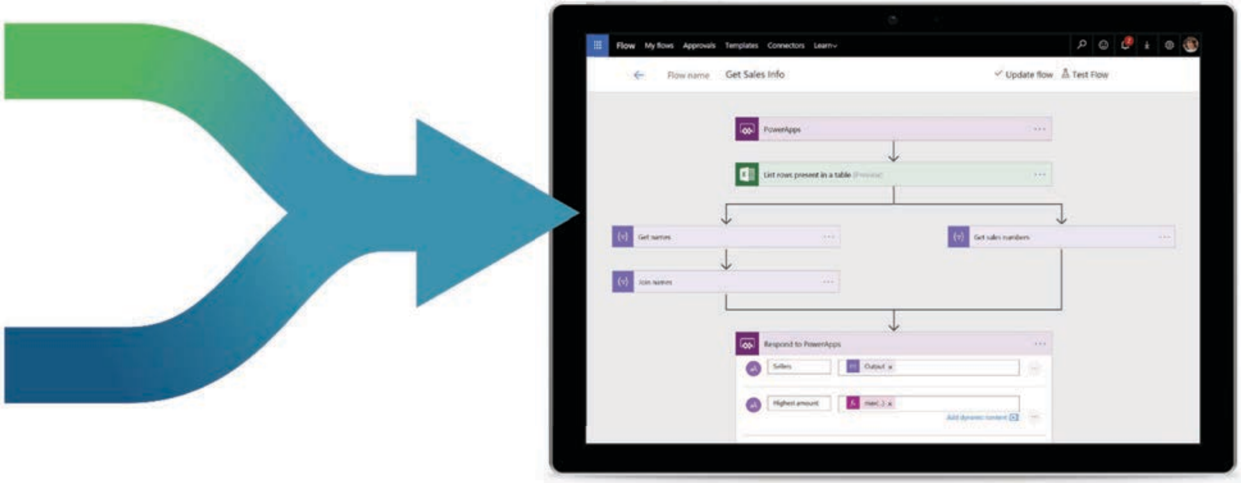
Automation: Similar patterns here, too

IT AUTOMATION

Security Automation & Orchestration (‘SOAR’)

CI/CD

Robotic Process Automation (RPA)



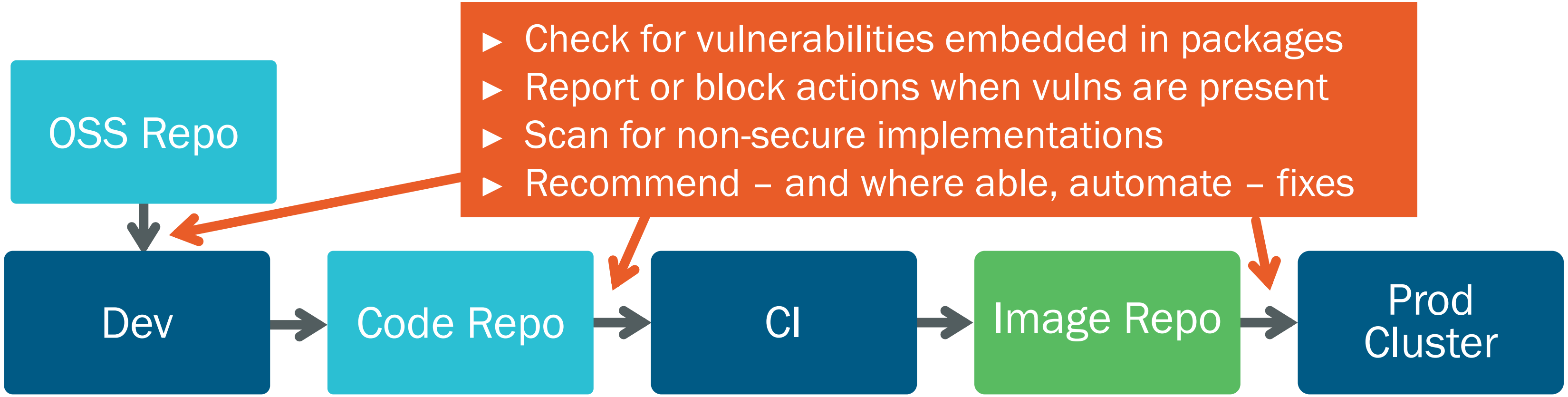
Sellers: Output

Highest amount: max(...)

GitOps: Putting security inline with CI/CD

- Automated pipelines deploy changes to infrastructure when changes are made to Git (using ‘diff,’ ‘sync’ tools)
- Helps isolate credential leakage across boundaries
- Performs actions on pull request

```
> git pull
```



- Check for vulnerabilities embedded in packages
- Report or block actions when vulns are present
- Scan for non-secure implementations
- Recommend – and where able, automate – fixes

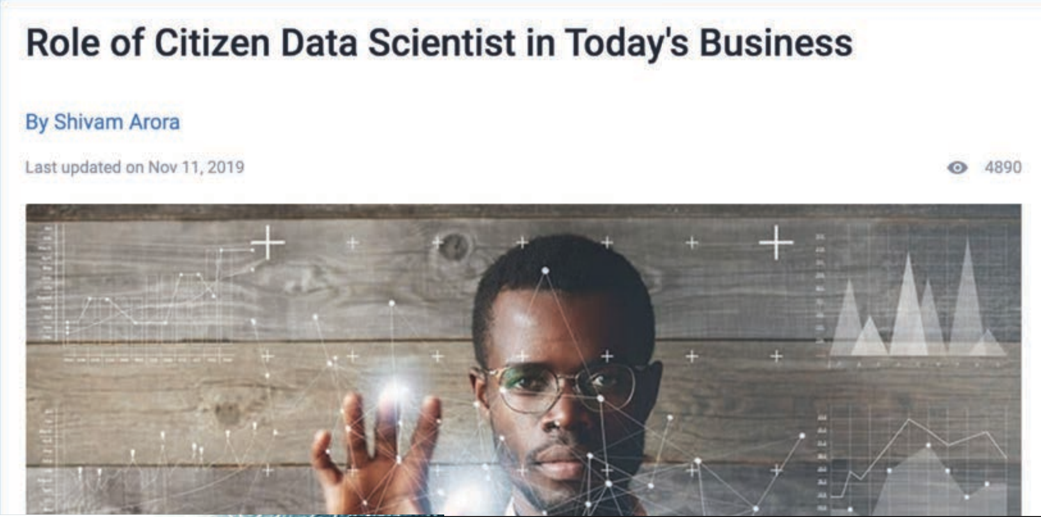
GitOps, or Why the Future Has No Dashboards

February 13th 2019

TWEET THIS

By Arthur Schmunk (@schmunk)
https://hackernoon.com/gitops-or-why-the-future-has-no-dashboards-38ce026a3c56

How are we going to source all this?



Role of Citizen Data Scientist in Today's Business

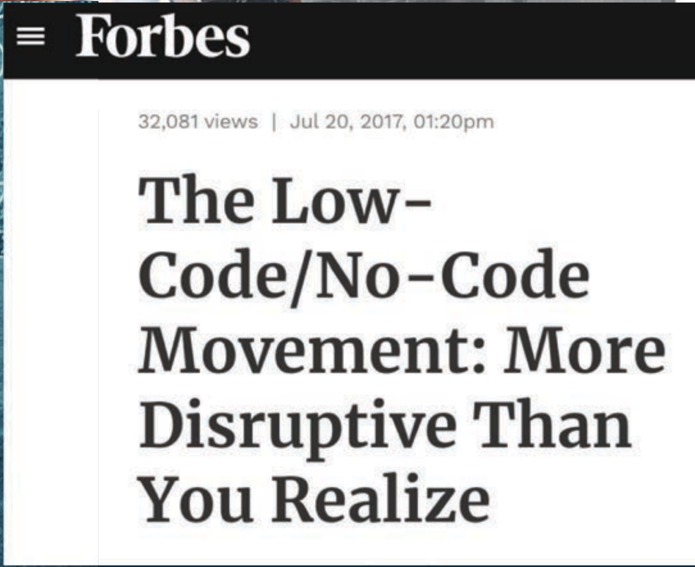
By Shivam Arora

Last updated on Nov 11, 2019

4890

MEET THE

Citizen Developer



≡ Forbes

32,081 views | Jul 20, 2017, 01:20pm

The Low-Code/No-Code Movement: More Disruptive Than You Realize

Coming soon, to a major industry con near you

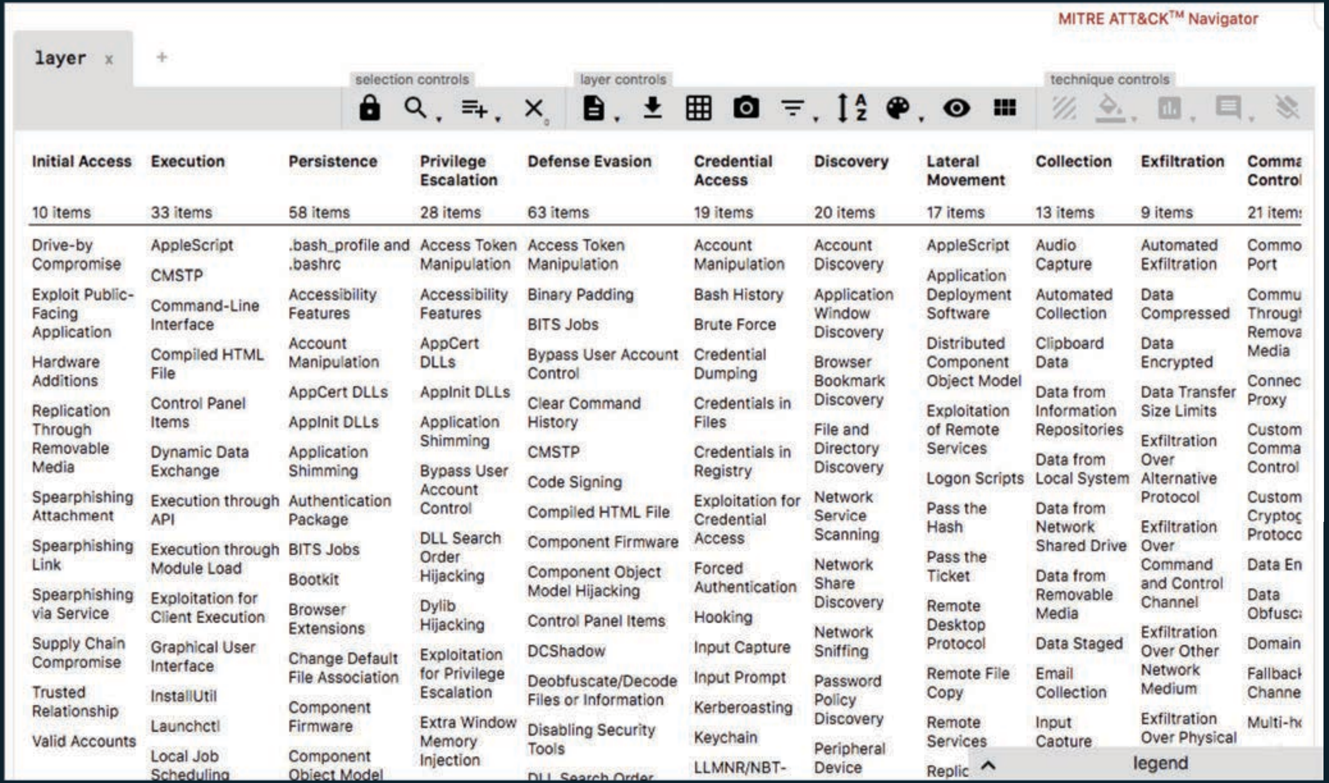
You inspired this year's theme. The Human Element at RSAC 2020.

Join cybersecurity leaders and peers as we explore our critical role in ensuring a safer, more secure future. Access expert-led sessions and keynotes, exciting innovation programs, in-depth tutorials and trainings, expanded networking opportunities, product demos and more.

...But not exactly our first rodeo.

The ‘GitHub-ification’ of security

MITRE ATT&CK

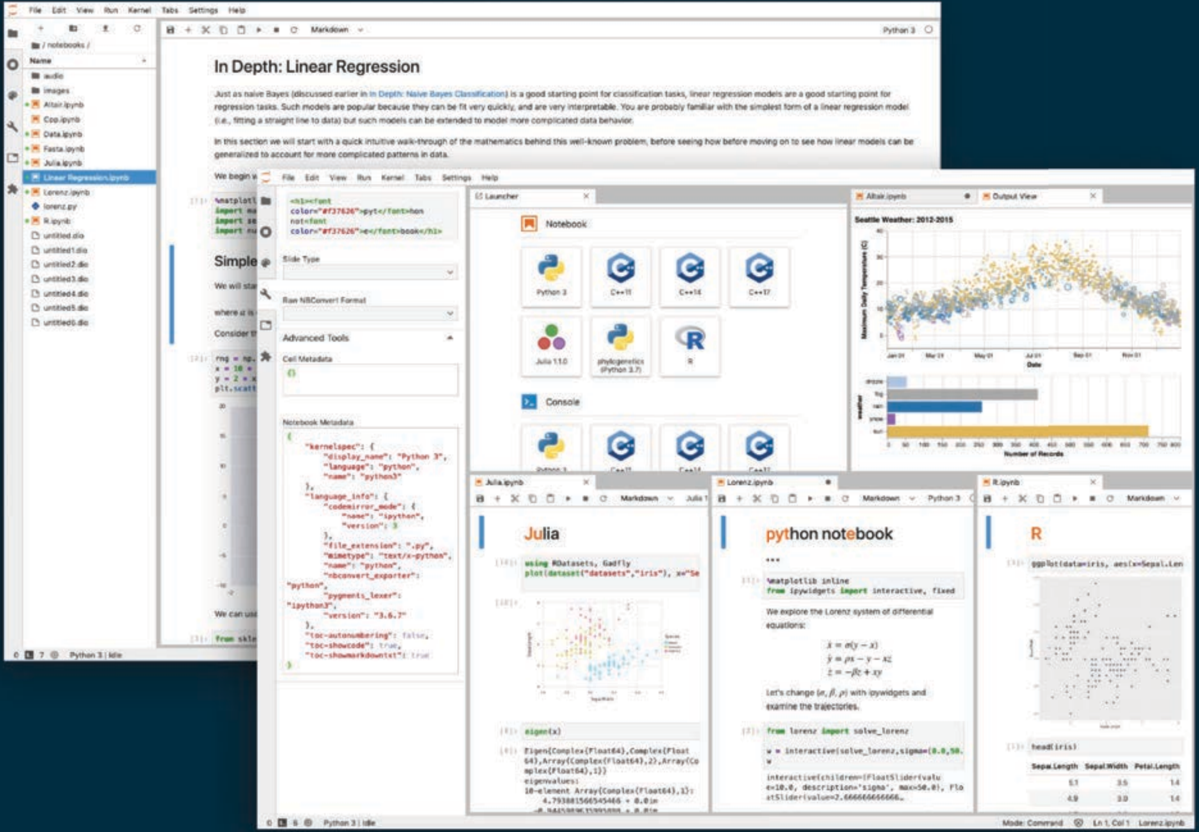


Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma Control
10 items	33 items	58 items	28 items	63 items	19 items	20 items	17 items	13 items	9 items	21 item:
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commo Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Commu Throug Remova Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connec Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Comma Control
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptoc Protoco
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data En
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfusc:
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical	Domain
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device	Remote File Copy	Email Collection		Fallbacl Channe
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture		Remote Services	Input Capture		Multi-hc
	InstallUtil	Change Default File Association		Control Panel Items	Input Prompt		Replic			
	Launchctl	Component Firmware		DCShadow	Kerberoasting					
	Local Job Scheduling	Component Object Model		Deobfuscate/Decode Files or Information	Keychain					
				Disabling Security Tools	LLMNR/NBT-					
				DLL Search Order						

https://mitre.github.io/attack-navigator/enterprise/

The 'GitHub-ification' of analytics

Jupyter Notebooks



In Depth: Linear Regression

Just as naive Bayes (discussed earlier in In Depth: Naive Bayes Classification) is a good starting point for classification tasks, linear regression models are a good starting point for regression tasks. Such models are popular because they can be fit very quickly, and are very interpretable. You are probably familiar with the simplest form of a linear regression model (i.e., fitting a straight line to data) but such models can be extended to model more complicated data behavior.

In this section we will start with a quick intuitive walk-through of the mathematics behind this well-known problem, before seeing how before moving on to see how linear models can be generalized to account for more complicated patterns in data.

```
<h1><font color="#f37626">pyt</font>hon
not<font color="#f37626">e</font>book</h1>
```

```
{
    "kernelspec": {
        "display_name": "Python 3",
        "language": "python",
        "name": "python3"
    },
    "language_info": {
        "codemirror_mode": {
            "name": "ipython",
            "version": 3
        },
        "file_extension": ".py",
        "mimetype": "text/x-python",
        "name": "python",
        "nbconvert_exporter":
"python",
        "pygments_lexer":
"ipython3",
        "version": "3.6.7"
    },
    "toc-autonumbering": false,
    "toc-showcode": true,
    "toc-showmarkdowntxt": true
}
```

Julia

```
using RDatasets, Gadfly
plot(dataset("datasets","iris"), x="Se
```

```
eigen(x)
```

```
Eigen{Complex{Float64},Complex{Float
64},Array{Complex{Float64},2},Array{Co
mplex{Float64},1}}
eigenvalues:
10-element Array{Complex{Float64},1}:
    4.793881566545466 + 0.0im
```

python notebook

```
%matplotlib inline
from ipywidgets import interactive, fixed
```

We explore the Lorenz system of differential equations:

$$\dot{x} = \sigma(y - x)$$
$$\dot{y} = \rho x - y - xz$$
$$\dot{z} = -\beta z + xy$$

Let's change (σ, β, ρ) with ipywidgets and examine the trajectories.

```
from lorenz import solve_lorenz

w = interactive(solve_lorenz,sigma=(0.0,50.
w
```

```
interactive(children=(FloatSlider(valu
e=10.0, description='sigma', max=50.0), Flo
atSlider(value=2.6666666666666...
```

R

```
ggplot(data=iris, aes(x=Sepal.Len
```

```
head(iris)
```

Sepal.Length	Sepal.Width	Petal.Length
5.1	3.5	1.4
4.9	3.0	1.4

https://jupyter.org

451

What’s YOUR role going to be?

Thank you

☎ US +1 212.505.3030 EUROPE +44 (0) 203.929.5700

451research.com

@451Research @s_crawford

New York
London
Boston
San Francisco