
451 Research
The Road Ahead
FOR SECURITY, IT AND DEVOPS
Scott Crawford
Research Vice President
@s_crawford
Qualys.
NOVEMBER 2019


451

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

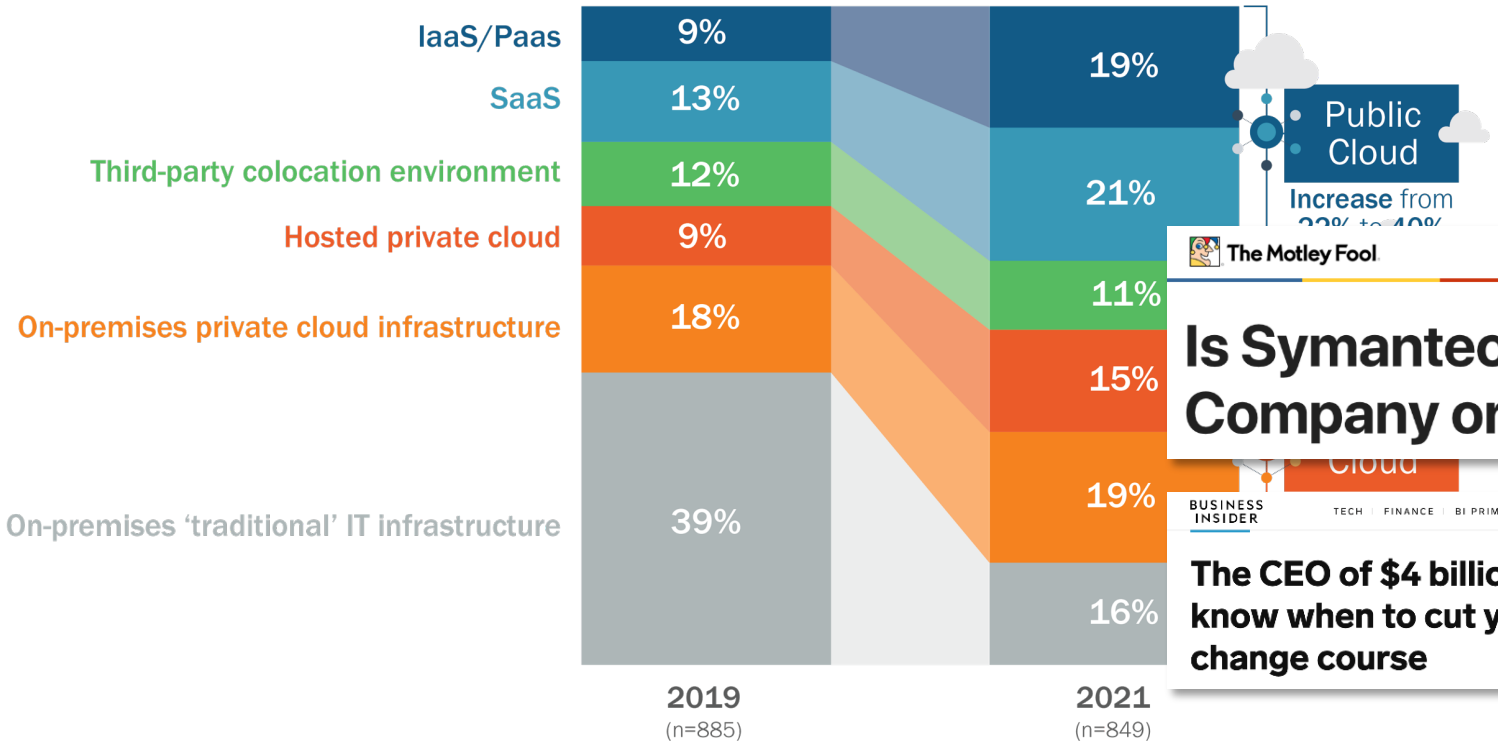
Security's incumbents and the 'Innovator's Dilemma'

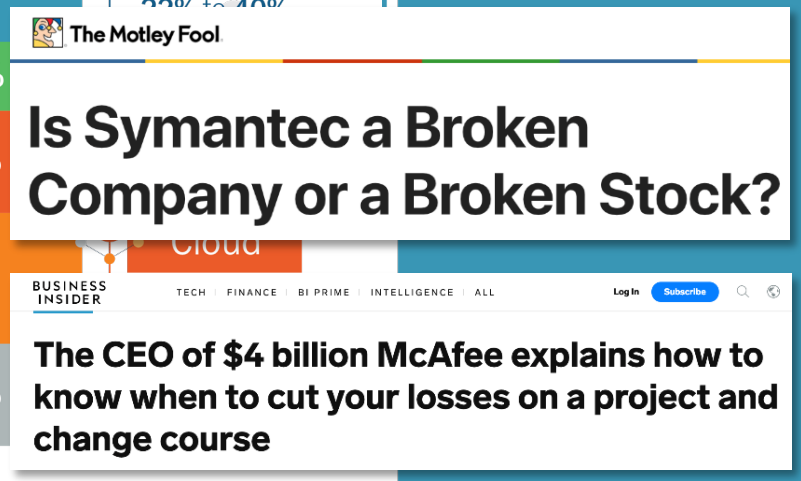
- Bet on the future, at the risk of under-investing in current traction?
- Or double down on current success – but risk missing out on tomorrow's opportunities?


Here comes
the BOOM!

It’s not just adoption…

Primary workload deployment venue





Pre-‘born in the cloud’ incumbents showing strain

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?

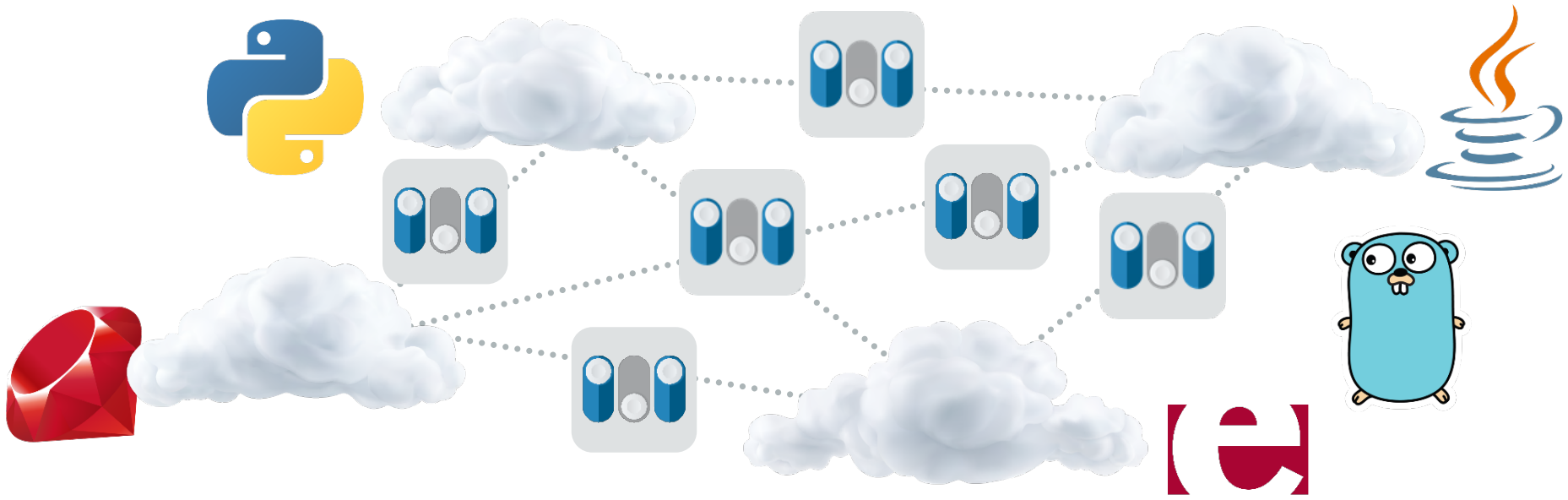
Source: 451 Research’s Voice of the Enterprise: Digital Pulse, Workloads & Key Projects 2019

Implications

No single point of control

Polyglot applications

A lot of interconnections




DevOps
PLAN
CODE
BUILD
TEST
RELEASE
DEPLOY
OPERATE & MONITOR
33
RedBull

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

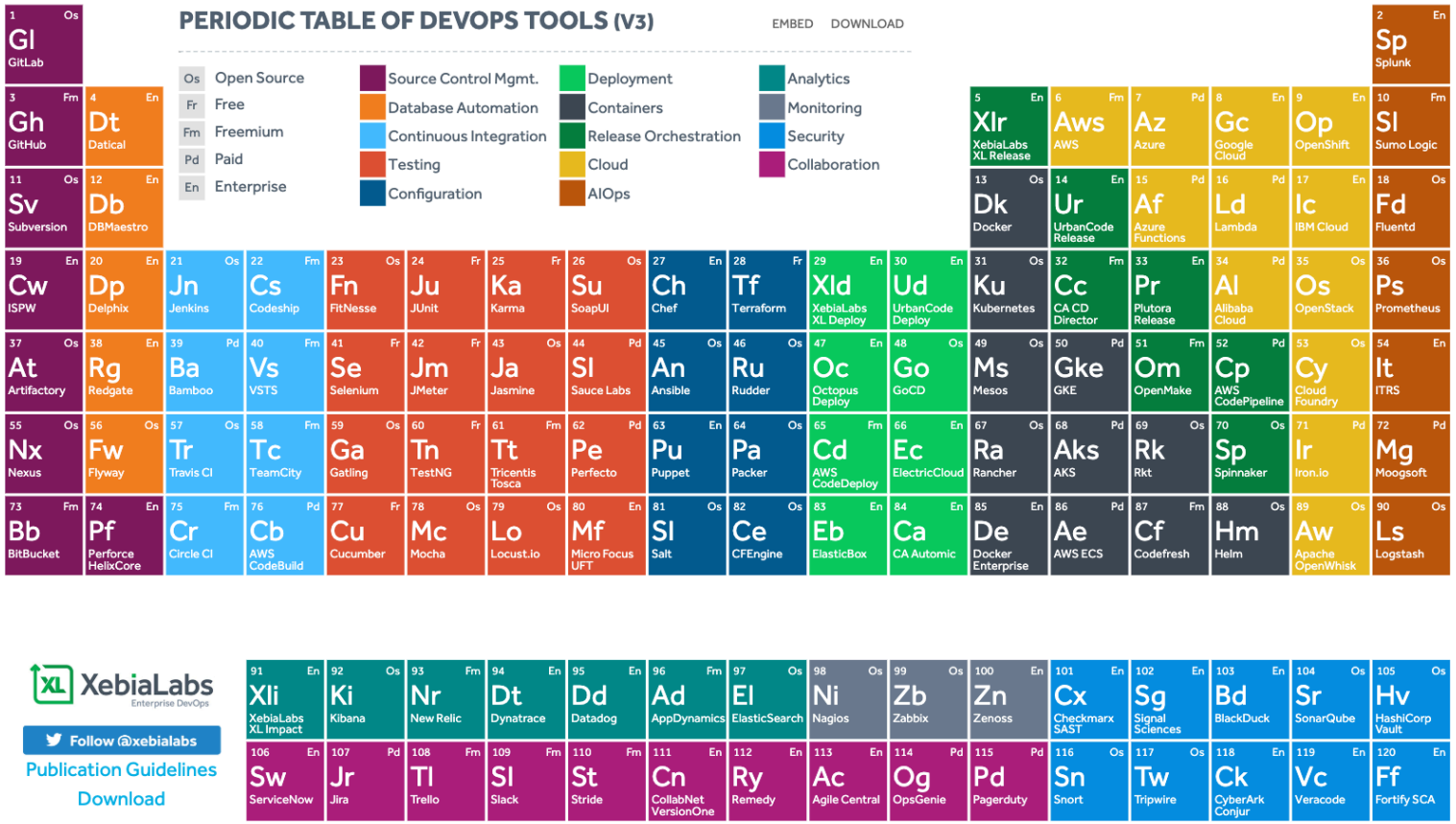
- Gating for security policy, compliance
- Vulnerability checks

- Vulnerability assessment
- Threat activity monitoring

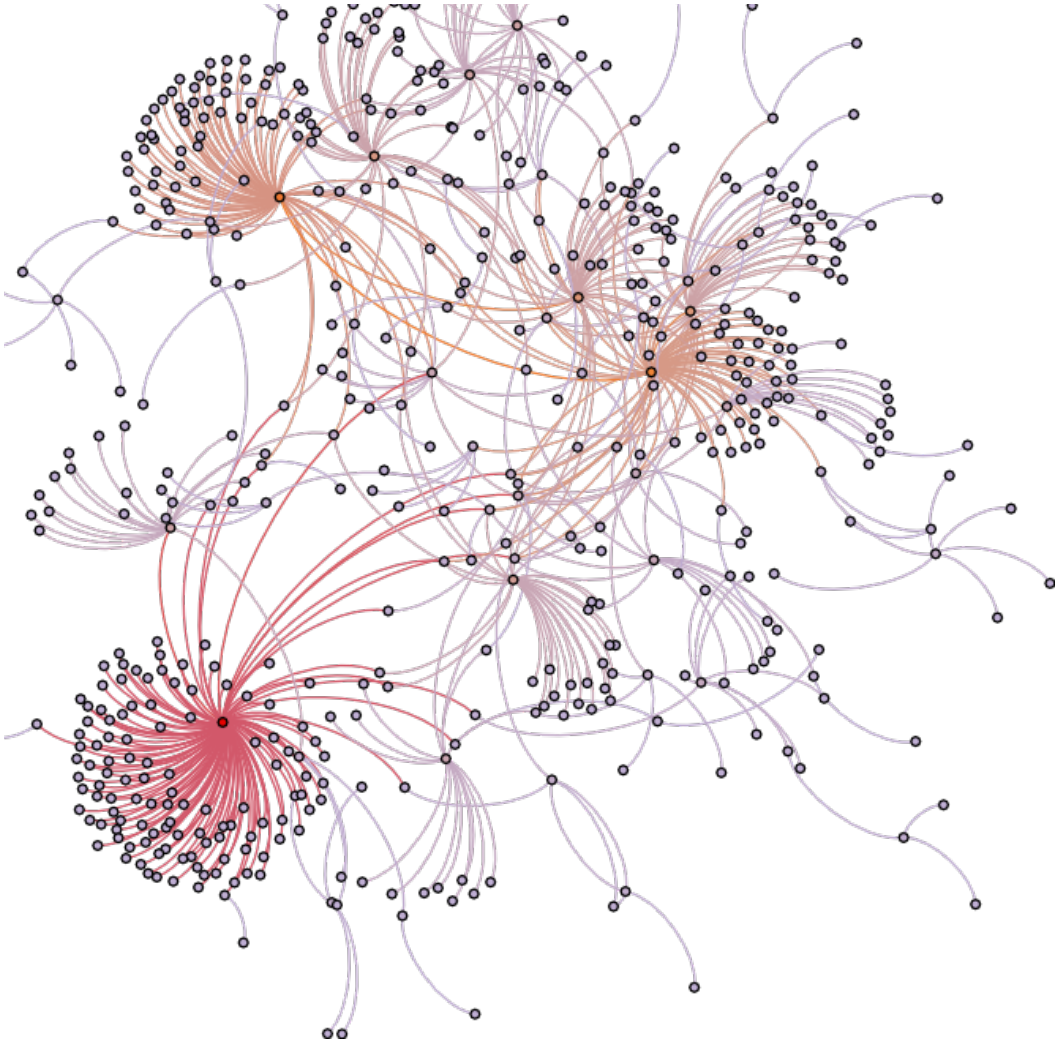
But they don't exactly love us…

- Pace
- Functional and business requirements *first*
- What's the incentive for developers?
- Toolchain integration

And each shop has its own toolset preferences

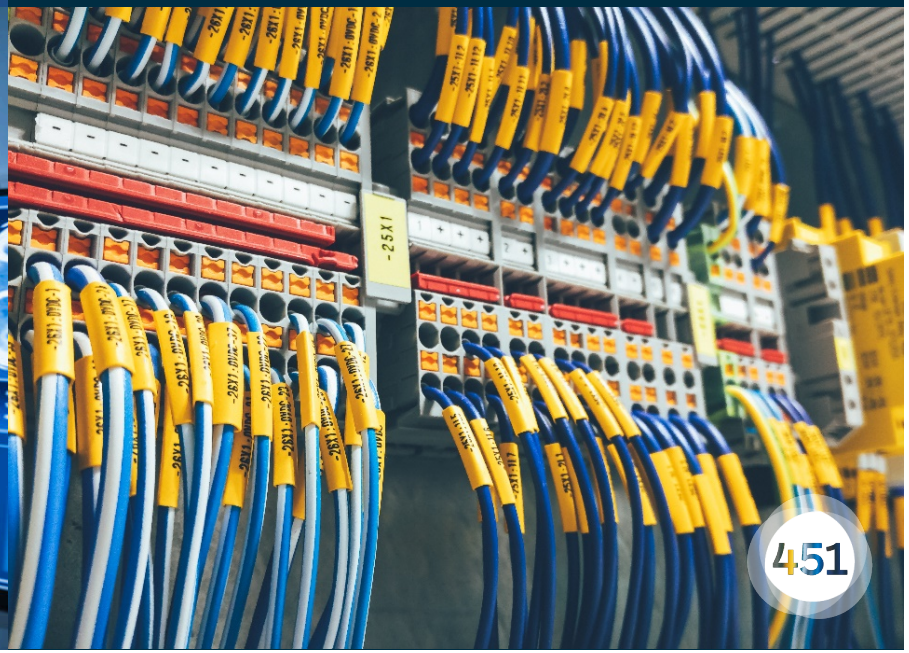


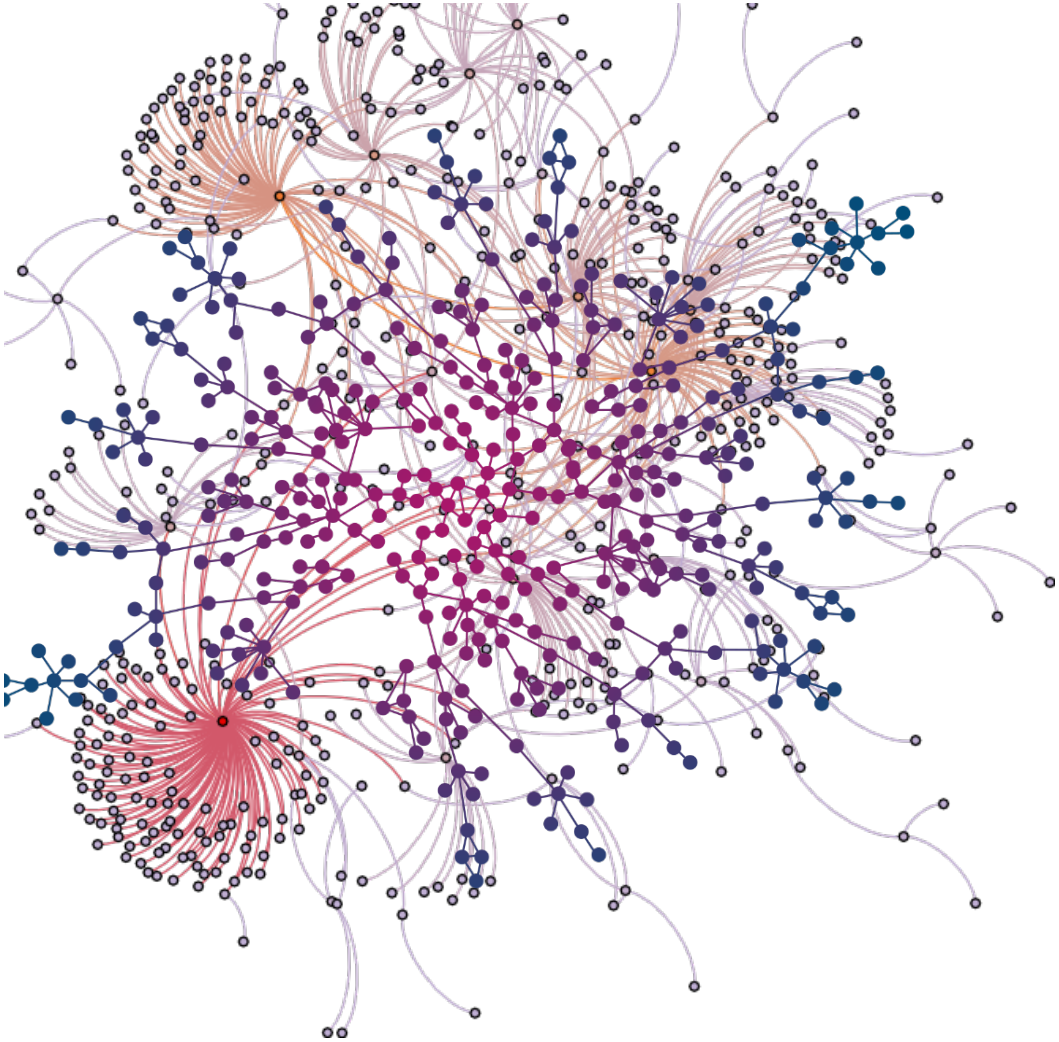
Source: https://xebialabs.com/periodic-table-of-devops-tools



Maybe a little complexity

What about all the ‘things’?

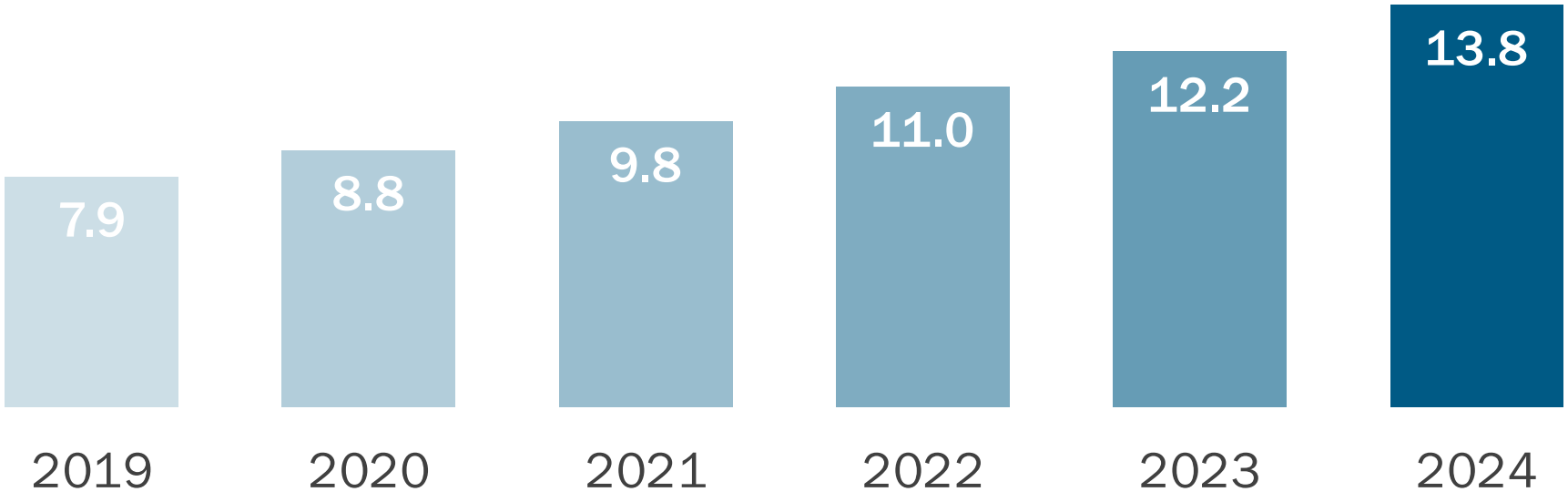




A bit more complexity

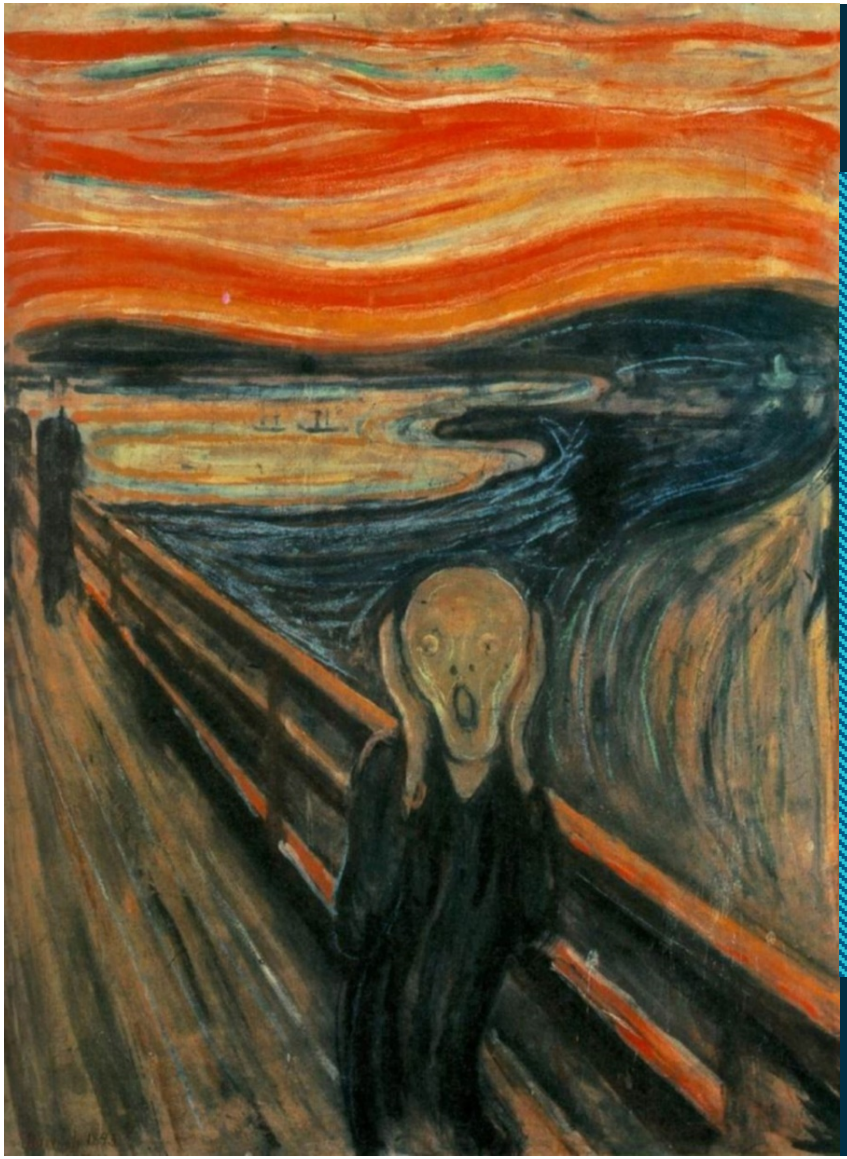
Okay, a **LOT** more complexity

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 IoT Market Monitor, June 2019



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

451

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

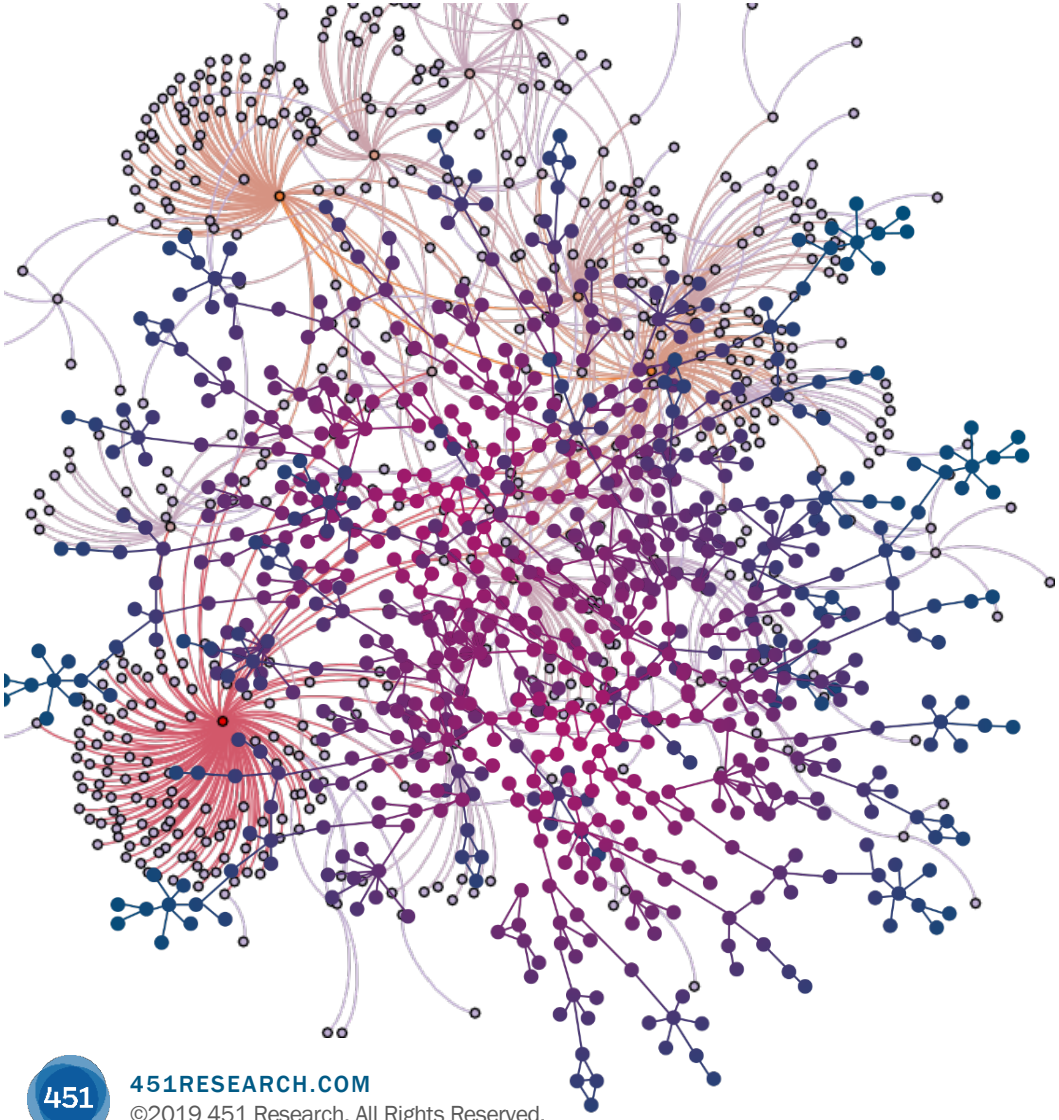
June 4, 2018 | Microsoft News Center

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

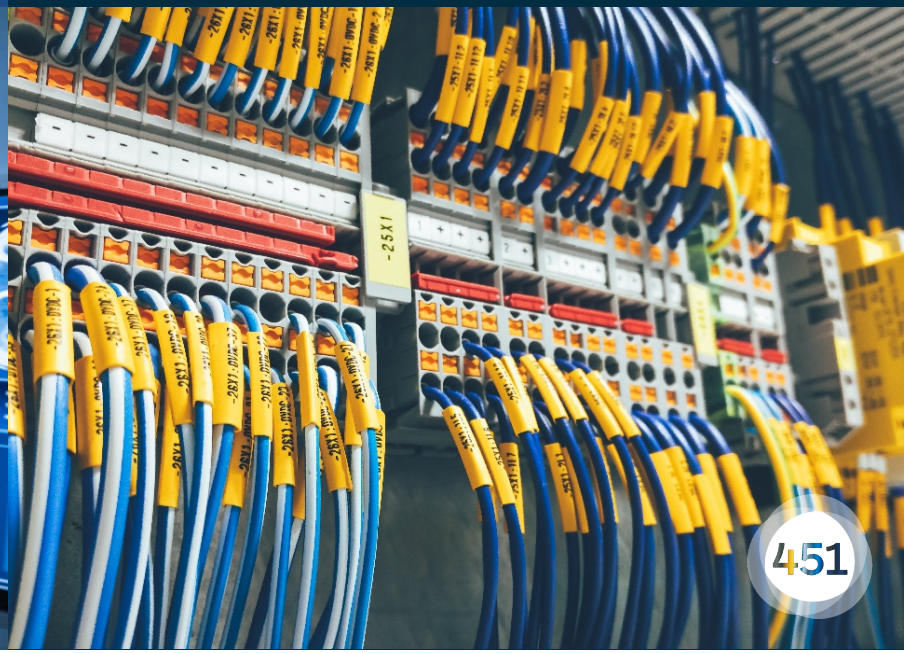
Example: Struts 2 vulnerability

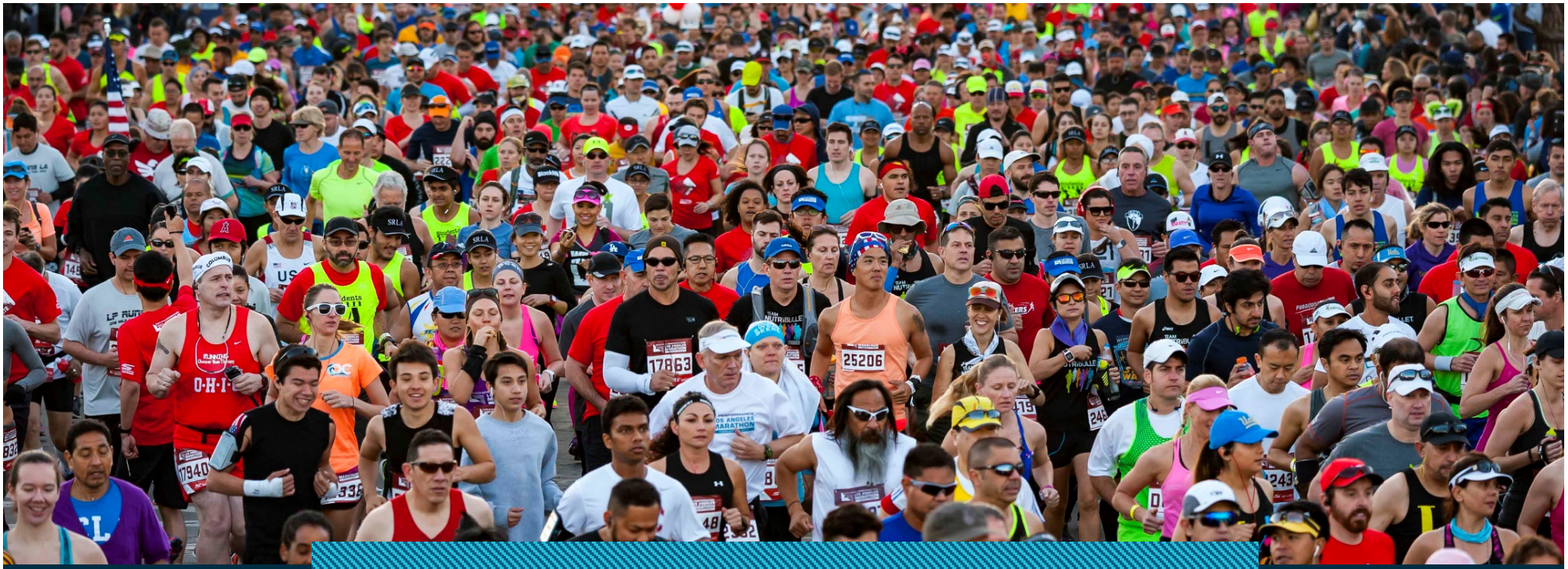
- …which extends the Java Servlet API
- …had a vulnerability in OGNL (remote code execution exposure)
- …which is incorporated in Jakarta
- …which was part of Apache



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

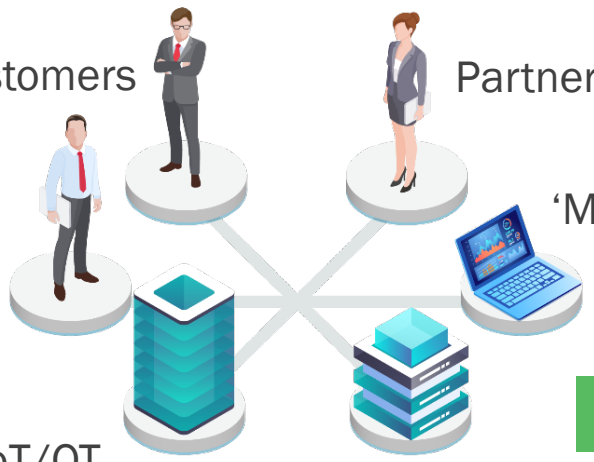
Customers

Partners

'M2M'

IoT/OT

Traditional IT endpoints



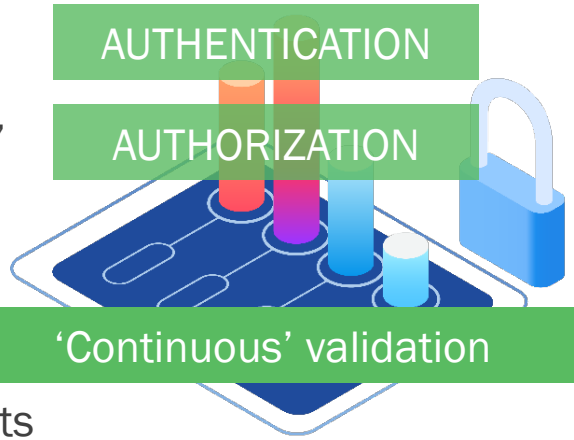
Under ***what*** conditions?

Decision-making:
AI/ML-enabled

AUTHENTICATION

AUTHORIZATION

'Continuous' validation



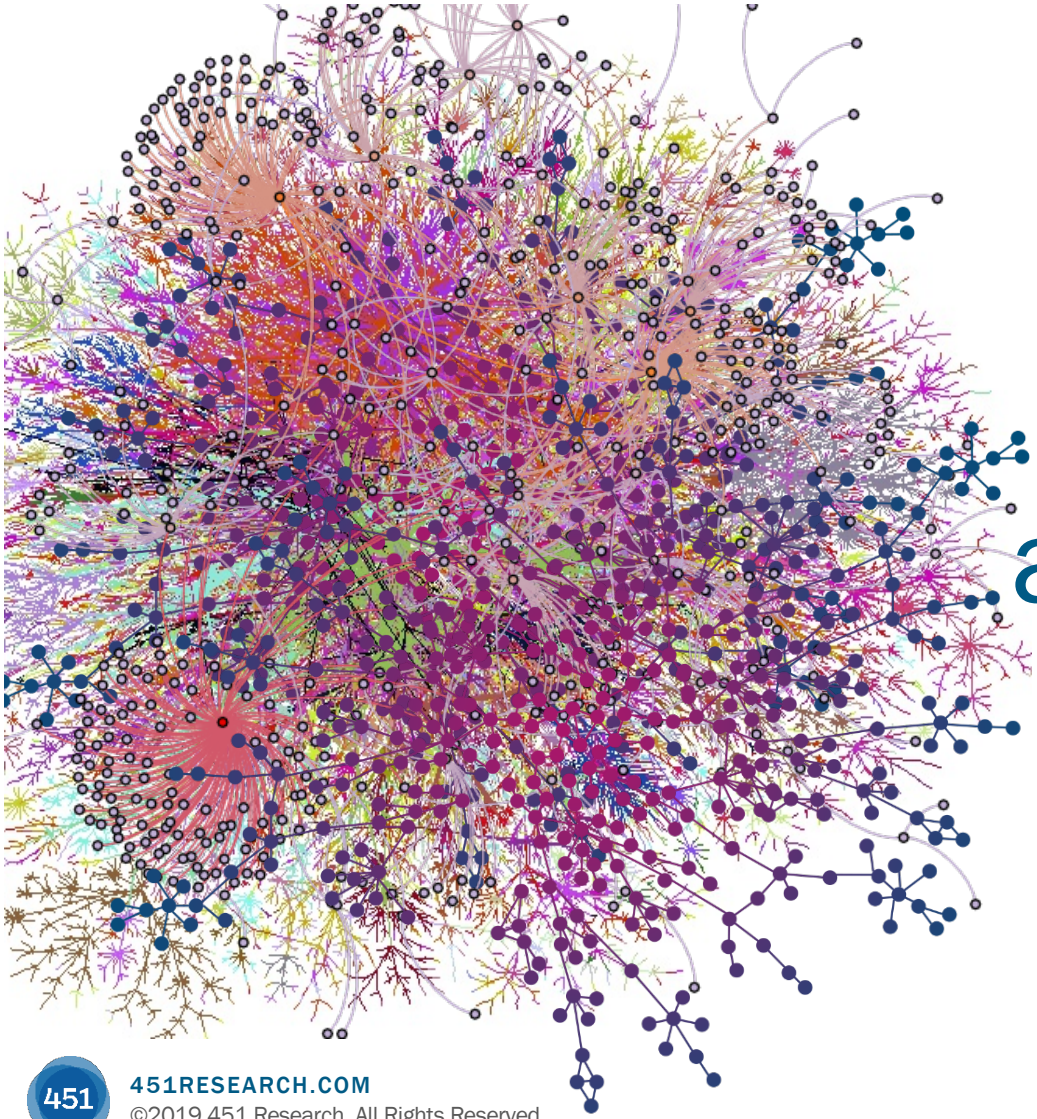
To ***which*** targets?

Fine-grained
access control

Applications, cloud resources, APIs, SaaS, etc.

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

WITH SECURITY FOR DATA THROUGHOUT



Now, multiply each decision on a scale of billions.

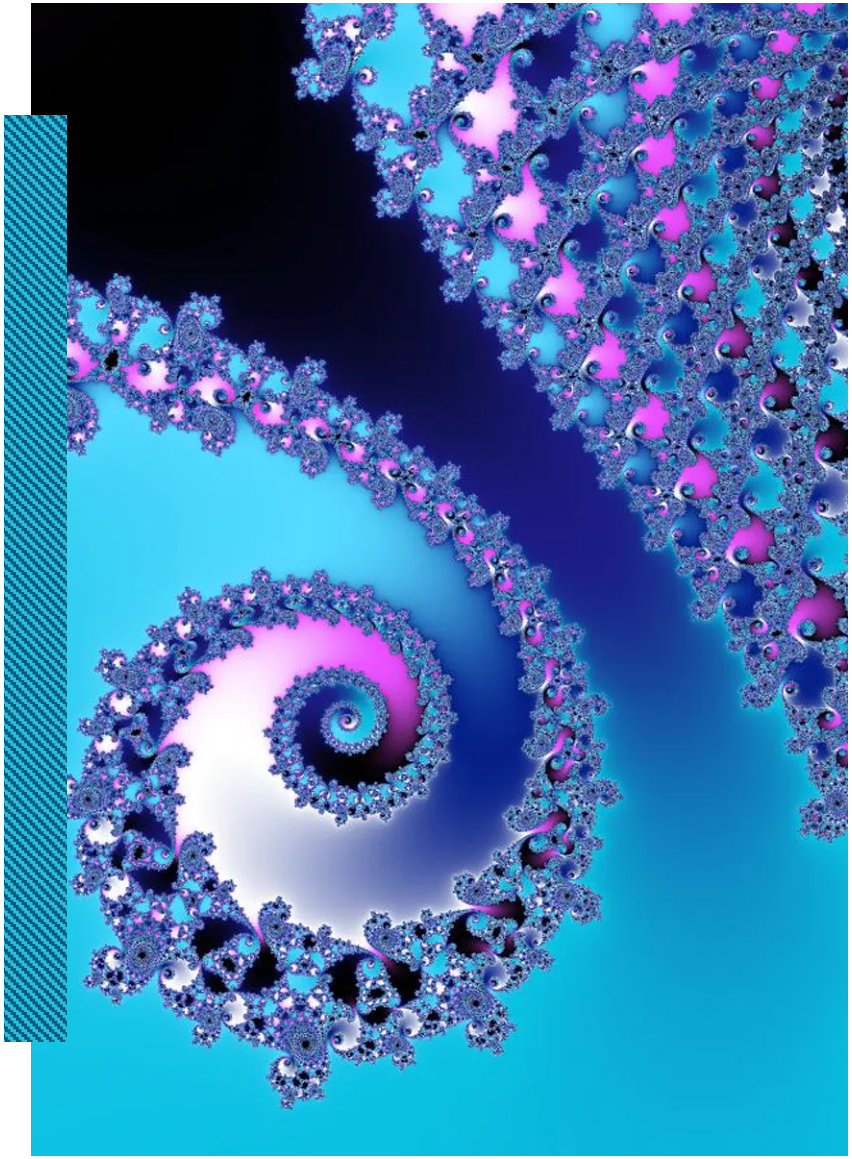
Continuously.


Expand
your
thinking
about...

Security analytics

It can’t all be done in one place

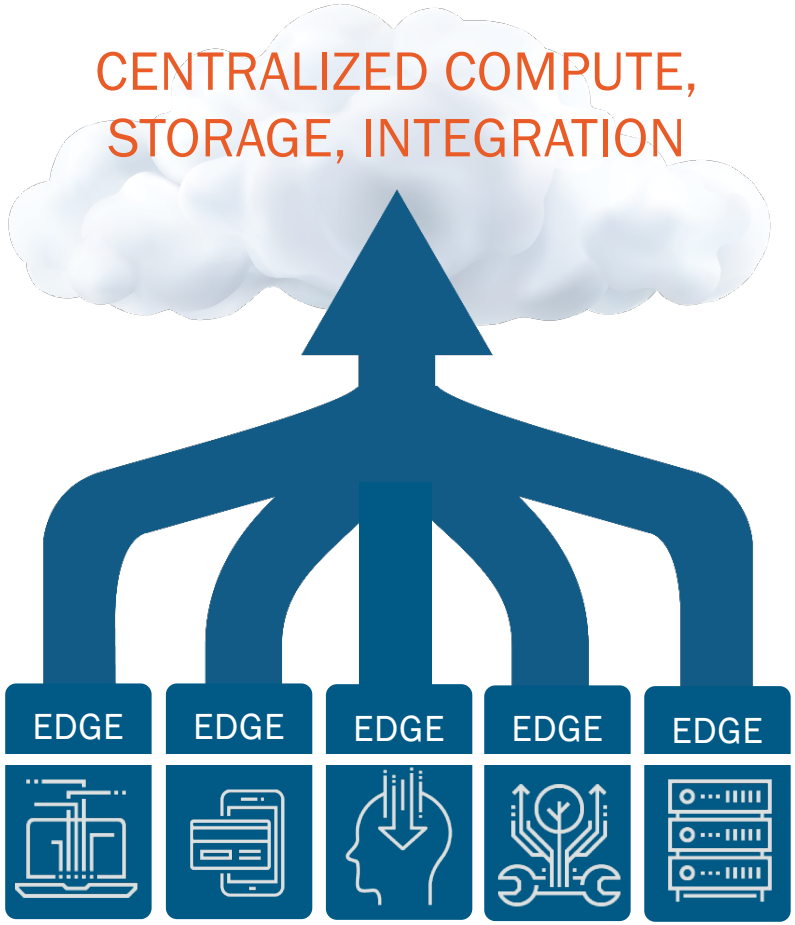
Distributed compute now may be nothing compared to what’s coming



People with no idea about AI saying it will take over the world:

My Neural Network:

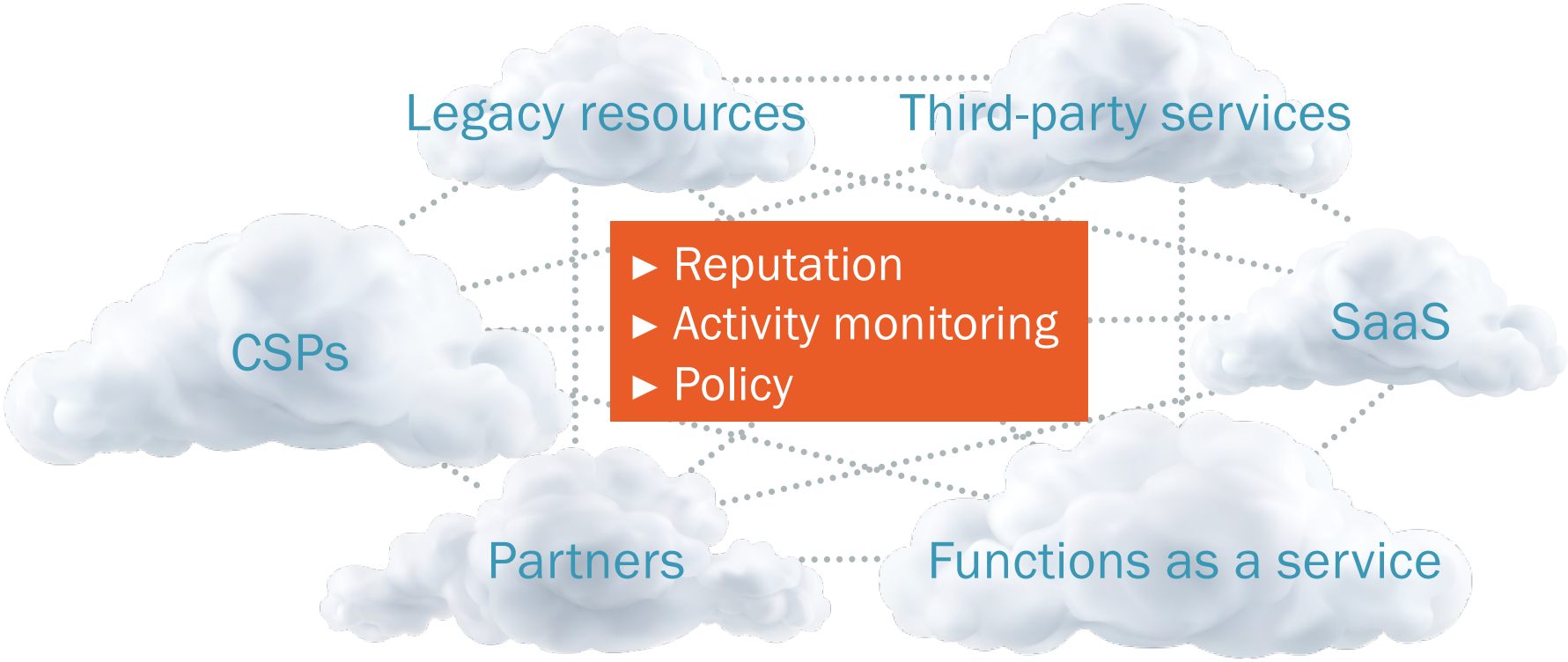
Twitter: @MVLibertas (Mat Vaillancourt)
https://twitter.com/mvlibertas/status/1195353071322304512



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



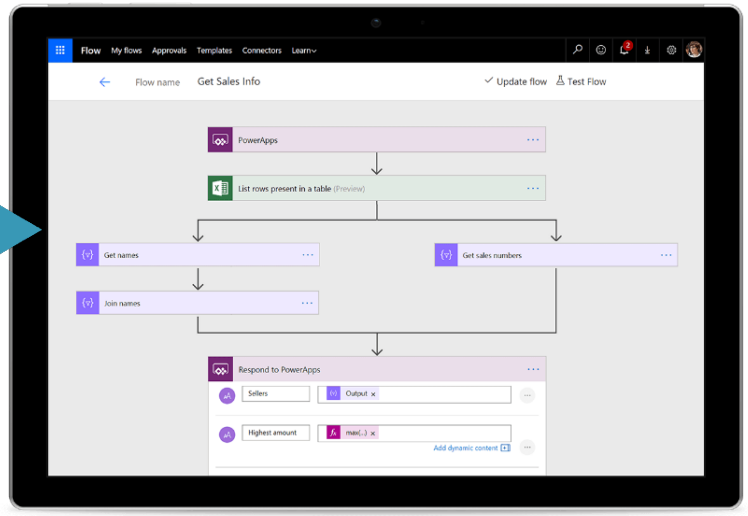
Automation: Similar patterns here, too

IT AUTOMATION

Security Automation & Orchestration ('SOAR')

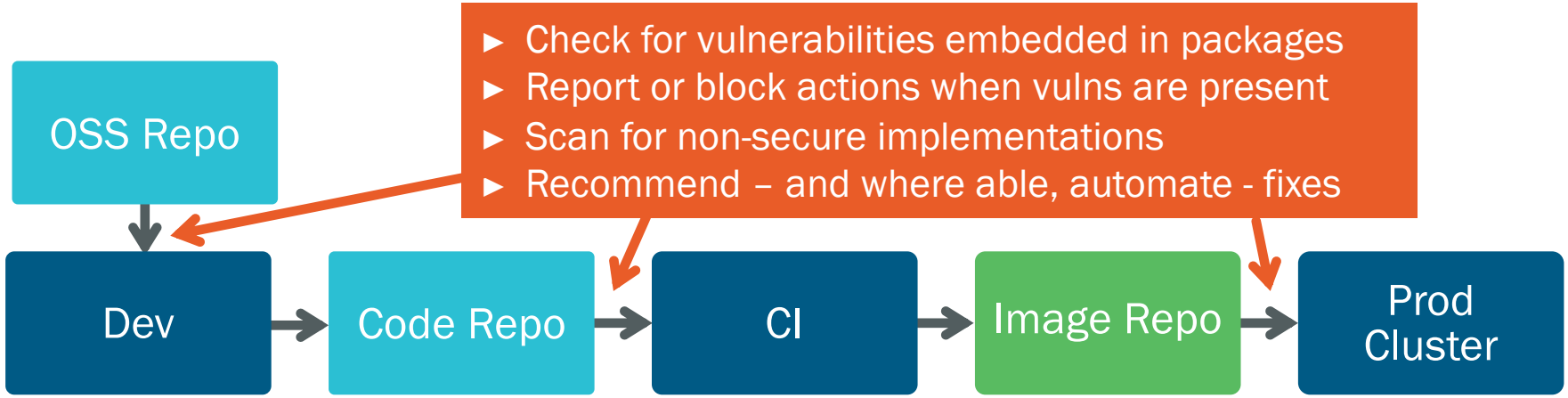
CI/CD

Robotic Process Automation (RPA)



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`



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

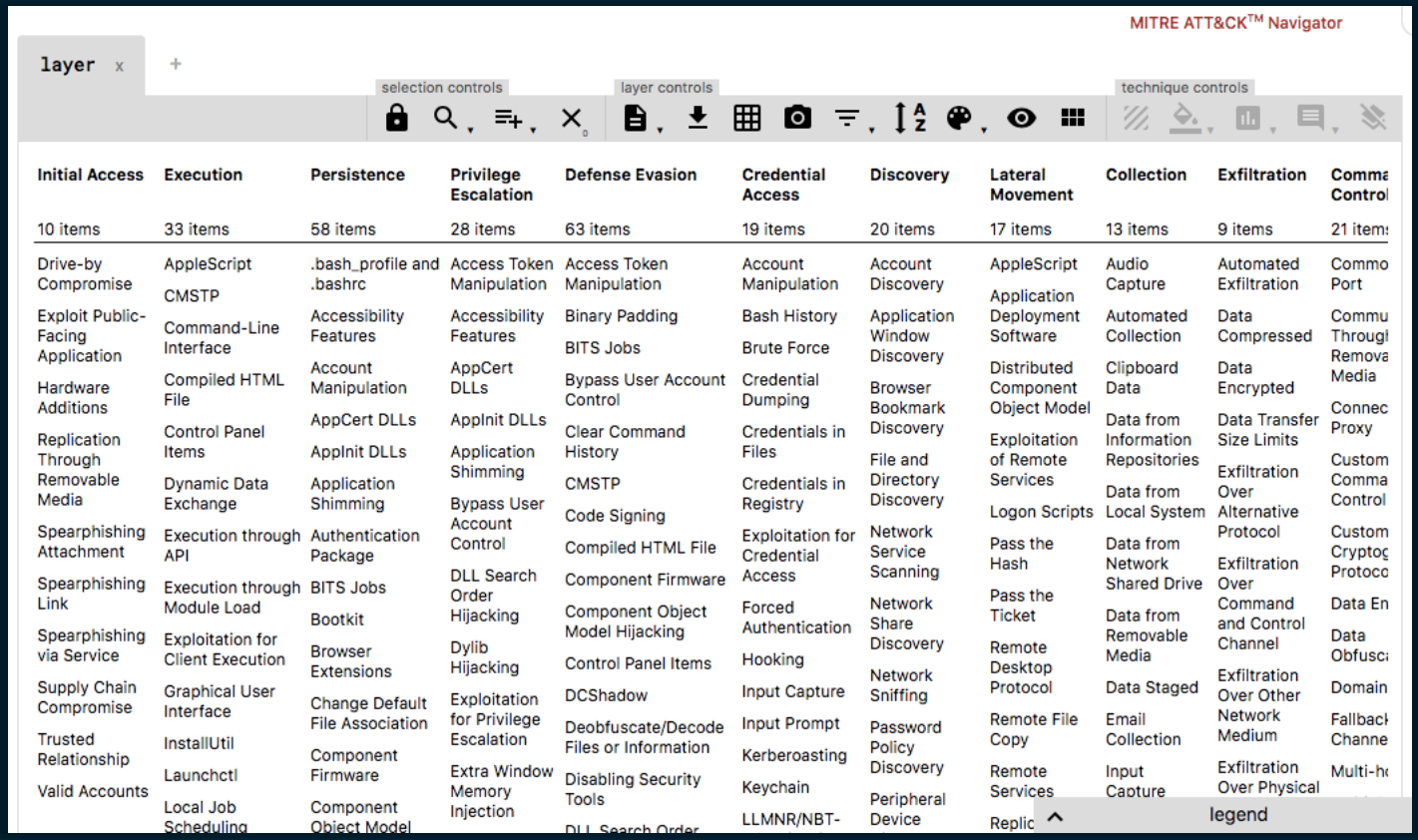
Forbes

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

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

The ‘GitHub-ification’ of security

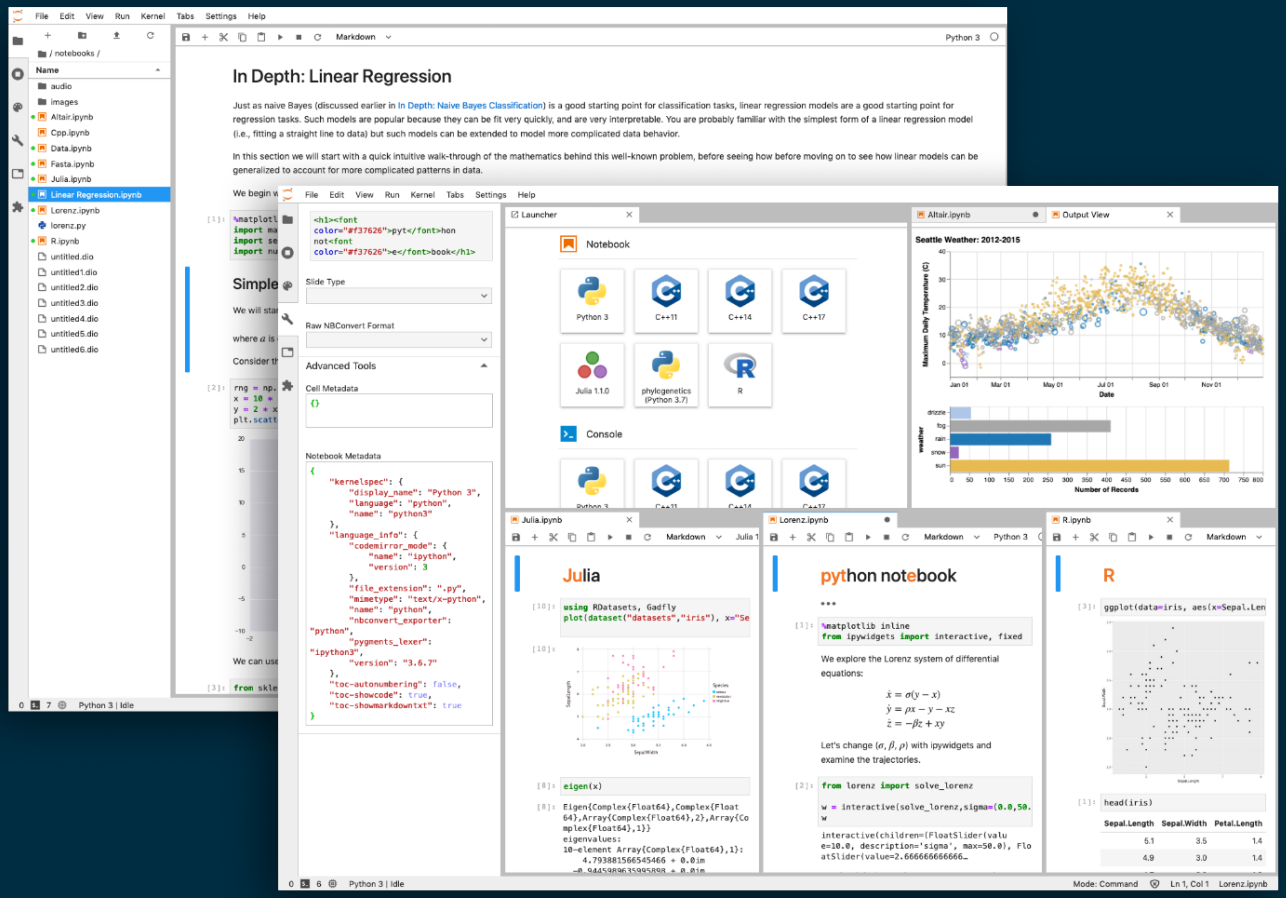
MITRE ATT&CK



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

The ‘GitHub-ification’ of analytics

Jupyter Notebooks



https://jupyter.org


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