



451

Research®

The Road Ahead FOR SECURITY, IT AND DEVOPS

Scott Crawford
Research Vice President
 @s_crawford
 Qualys.
NOVEMBER 2019



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?





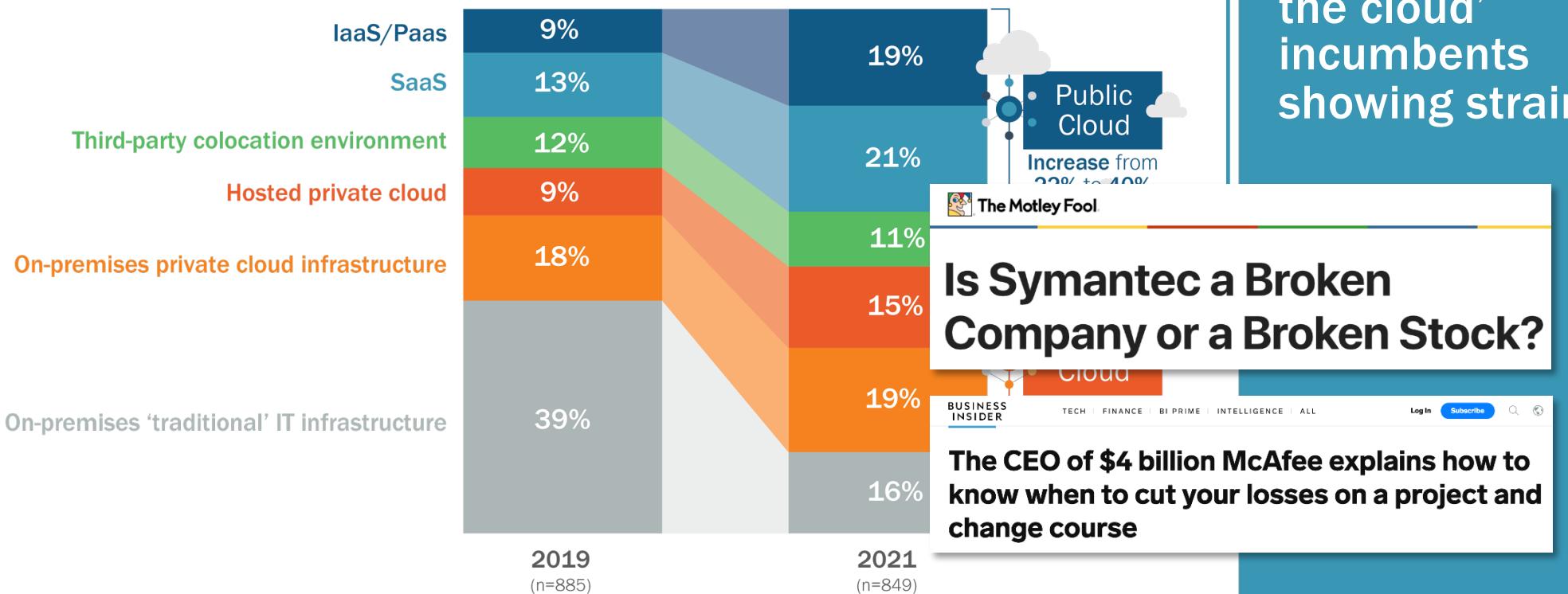
Here comes
the **BOOM!**

451

5

It's not just about adoption...

Primary workload deployment venue



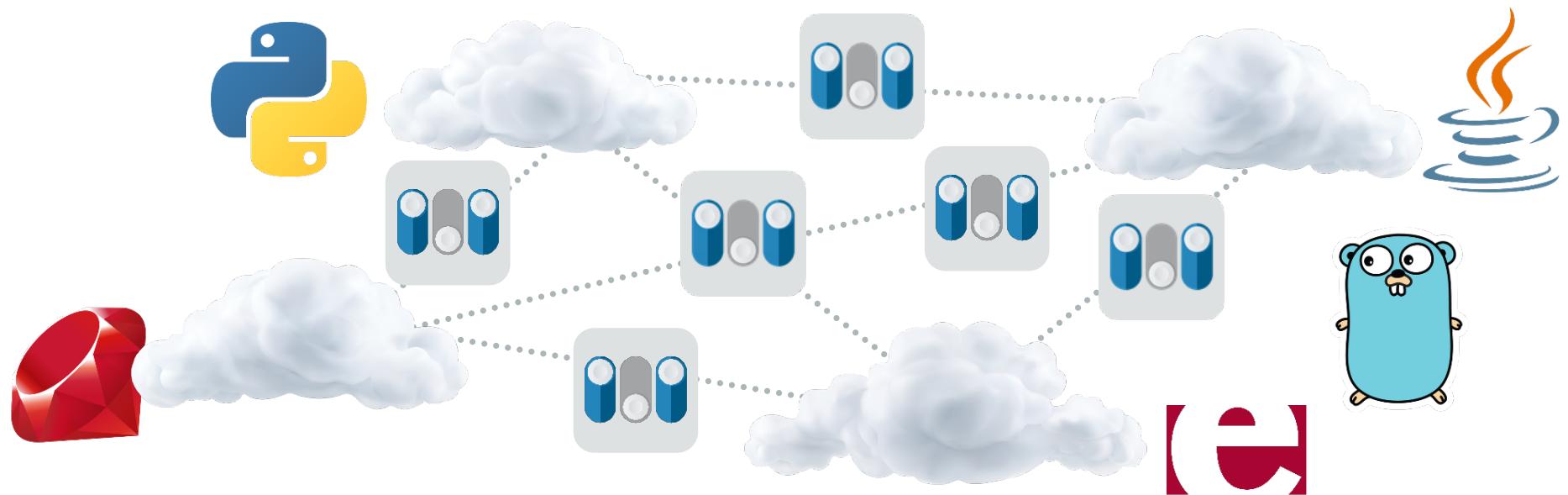
Pre-'born in the cloud' incumbents showing strain

Implications

No single point
of control

Polyglot
applications

A lot of
interconnections

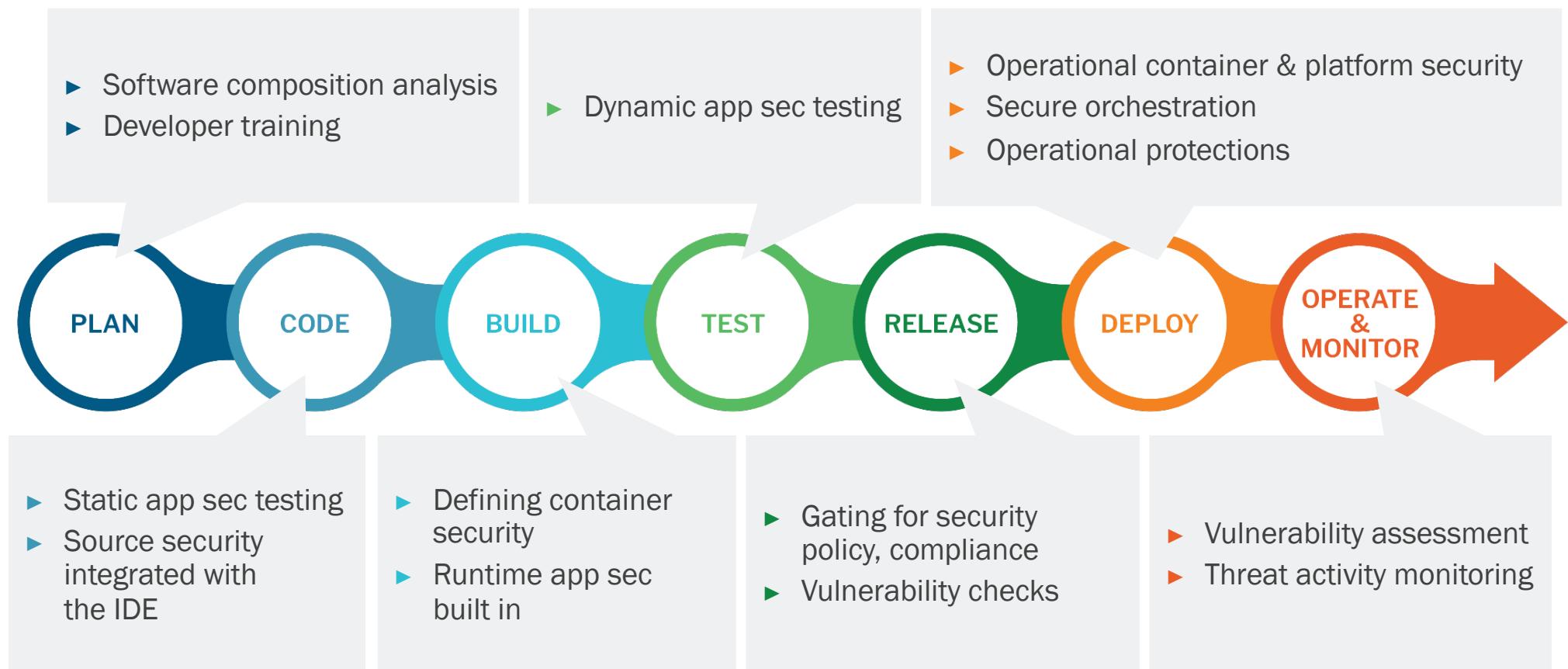


The background of the slide features a large, scenic waterfall cascading down a rocky cliff into a pool of water, surrounded by dense green foliage and trees.

DevOps



Security has lots of opportunities...



But they don't exactly love us...

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

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

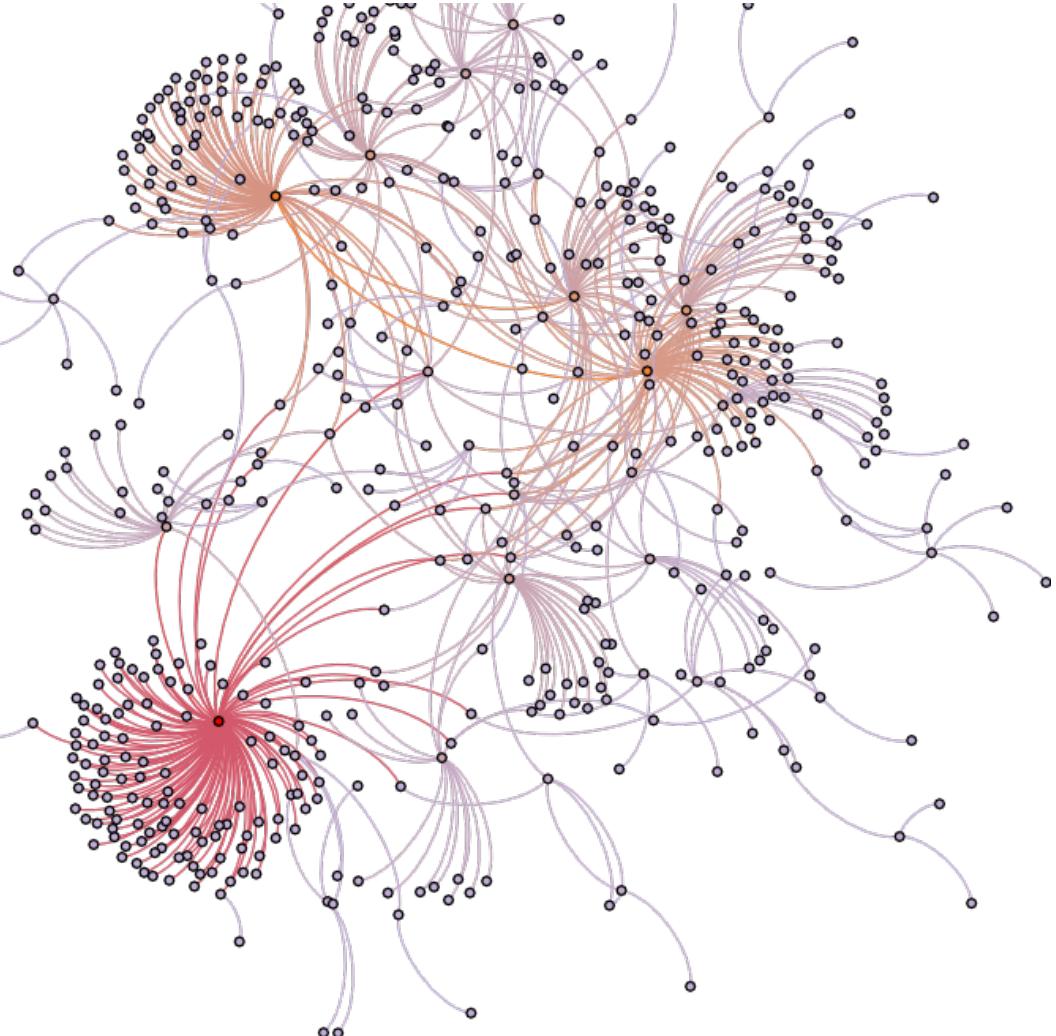


And each shop has its own toolset preferences

PERIODIC TABLE OF DEVOPS TOOLS (V3)																		EMBED		DOWNLOAD	
1	Os																	2	En		
Gl	GitLab																	Sp	Splunk		
3	Fm	4	En															10	Fm		
Gh	GitHub		Dt	Datalic														SI	Sumo Logic		
11	Os	12	En															18	Os		
Sv	Subversion		Db	DBMaestro														Fd	Fluentd		
Cw	ISPW		Dp	Delphix														Ps	Prometheus		
19	En	20	En															36	Os		
Jn	Jenkins		Cs	Codeship														It	ITRS		
Fn	FitNesse		Ju	JUnit														Mg	Moogsoft		
21	Os	22	Fm															72	Pd		
Ka	Karma		Su	SoapUI														Ir	Iron.io		
23	Os	24	Fr															73	Os		
Ch	Chef		Tf	Terraform														Bb	BitBucket		
25	Fr	26	Os															Pf	Perforce		
Xld	XebiaLabs XL Deploy		Ud	UrbanCode Deploy														74	En		
27	En	28	Fr															Cr	Circle CI		
Ku	Kubernetes		Oc	Octopus Deploy														75	Fm		
31	Os	32	Fm															Cb	AWS CodeBuild		
Cc	CA CD Director		Pr	Plutora Release														76	Pd		
33	En	34	Pd															77	Fr		
Al	Alibaba Cloud		Os	OpenMake														78	Os		
35	Os	36	Os															79	Os		
Os	OpenStack		Cp	AWS CodePipeline														80	En		
37	Os	38	En															81	Os		
Rg	Redgate		Go	GoCD														82	Os		
At	Artifactory		Ms	Mesos														83	En		
Ba	Bamboo		Gke	GKE														84	En		
Vs	VSTS		Om	OpenMake														85	En		
39	Pd	40	Fm	Pe	Perfecto													86	Pd		
Se	Selenium		Pu	Puppet														87	Fm		
41	Fr	42	Fr	Tn	TestNG													88	Os		
Jm	JMeter		Pa	Packer														89	Os		
43	Os	44	Pd	Cd	AWS CodeDeploy													90	Os		
Ja	Jasmine		Ec	ElectricCloud																	
45	Os	46	Os	Ra	Rancher																
An	Ansible		Aks	AKS																	
46	Os	47	En	Rkt	Rkt																
Ru	Rudder		Sp	Spinnaker																	
47	En	48	Os	Ra	Rancher																
Oc	Octopus Deploy		Aks	AKS																	
48	Os	49	Os	Rkt	Rkt																
Go	GoCD		Sp	Spinnaker																	
50	Pd	51	Fm	Rkt	Rkt																
Gke	GKE		Ir	Iron.io																	
51	Fm	52	Pd	Sp	Spinnaker																
Om	OpenMake		Itr	ITRS																	
Cp	AWS CodePipeline		Mg	Moogsoft																	
52	Pd	53	Os																		
Cy	Cloud Foundry																				
53	Os	54	En																		
It	ITRS																				
Nx	Nexus																				
Fw	Flyway																				
Tr	Travis CI																				
Tc	TeamCity																				
Ga	Gatling																				
Tn	TestNG																				
Tt	Tricentis Tosca																				
Pe	Perfecto																				
Mf	Micro Focus UFT																				
Si	Salt																				
80	En	81	Os	Ce	CFEngine													101	En		
81	Os	82	Os	Eb	ElasticBox													102	En		
82	Os	83	En	Ca	CA Automic													103	En		
83	En	84	En	De	Docker Enterprise													104	Os		
84	En	85	En	Ae	AWS ECS													105	Os		
85	En	86	Pd	Cf	Codefresh																
86	Pd	87	Fm	Hm	Helmi																
87	Fm	88	Os	Aw	Apache OpenWhisk																
88	Os	89	Os	Ls	Logstash																
89	Os	90	Os																		
90	Os																				

 Xebialabs
Enterprise DevOps
[Follow @xebialabs](#)
[Publication Guidelines](#)
[Download](#)

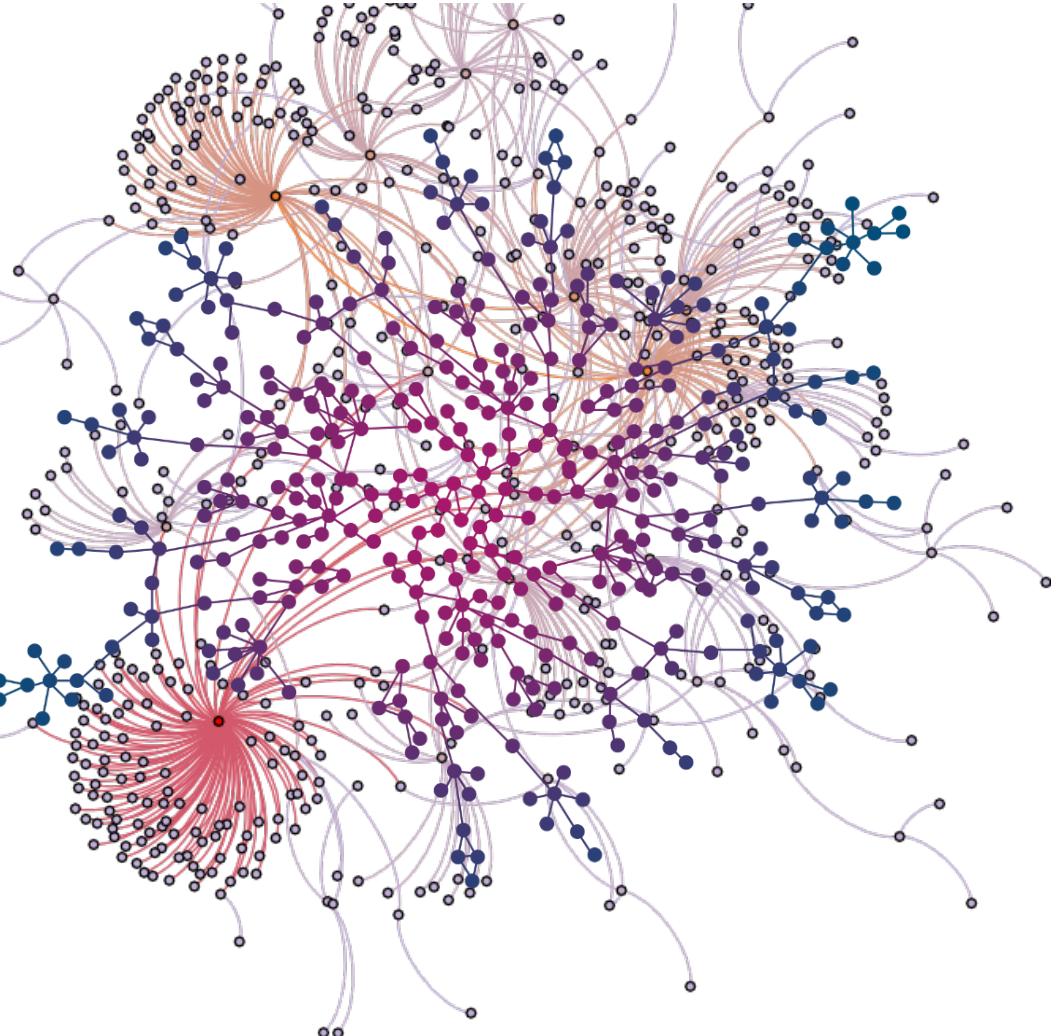
91	En	92	Os	93	Fm	94	En	95	En	96	Fm	97	Os	98	Os	99	Os	100	En	101	En	102	En	103	En	104	Os	105	Os
Xli	XebiaLabs XL Impact	Ki	Kibana	Nr	New Relic	Dt	Dynatrace	Dd	Datadog	Ad	AppDynamics	EI	ElasticSearch	Ni	Nagios	Zb	Zabbix	Zn	Zenoss	Cx	Checkmark SAST	Sg	Signal Sciences	Bd	BlackDuck	Sr	SonarQube	Hv	HashiCorp Vault
106	En	107	Pd	108	Fm	109	Fm	110	Fm	111	En	112	En	113	En	114	Pd	115	Pd	116	Os	117	Os	118	En	119	En	120	En
Sw	ServiceNow	Jr	Jira	Tl	Trello	Sl	Slack	St	Stride	Cn	CollabNet VersionOne	Ry	Remedy	Ac	Agile Central	Og	OpsGenie	Pd	Pagerduty	Sn	Snort	Tw	Tripwire	Ck	CyberArk Conjur	Vc	Veracode	Ff	Fortify SCA



Maybe
a little
complexity



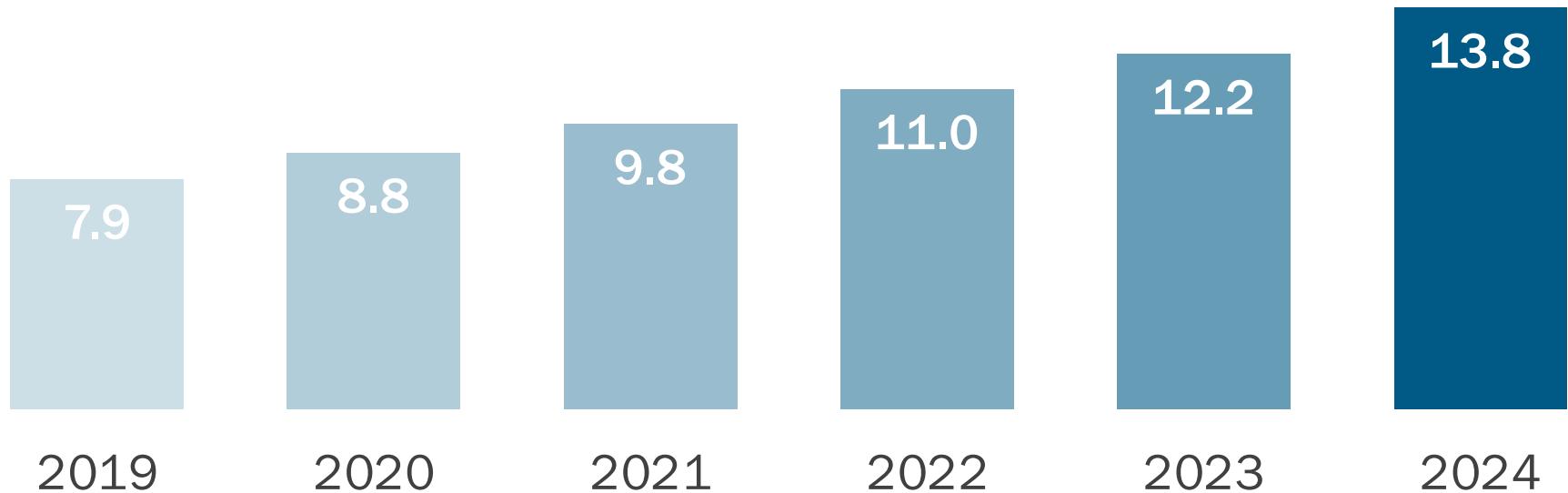
What about all
the ‘things’?



A bit more complexity

Okay, a LOT more complexity

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



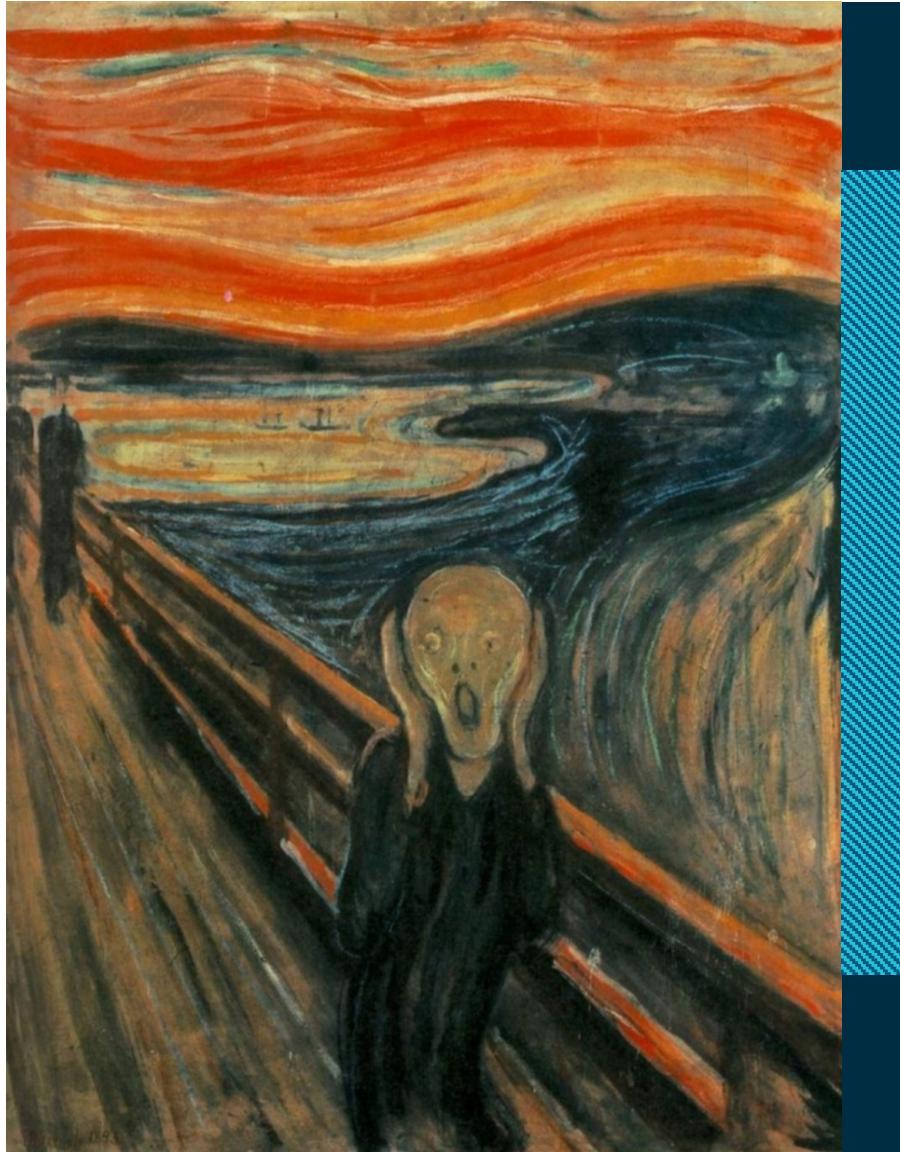
*Not including consumer devices (e.g. PCs, smart TVs, game consoles)



451RESEARCH.COM

©2019 451 Research. All Rights Reserved.

Source: 451 Research IoT Market Monitor, June 2019



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

Oh.



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

Thank you for 100 million repositories



Jason Warner

451

451RESEARCH.COM

©2019 451 Research. All Rights Reserved.

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



Microsoft to acquire GitHub for \$7.5 billion

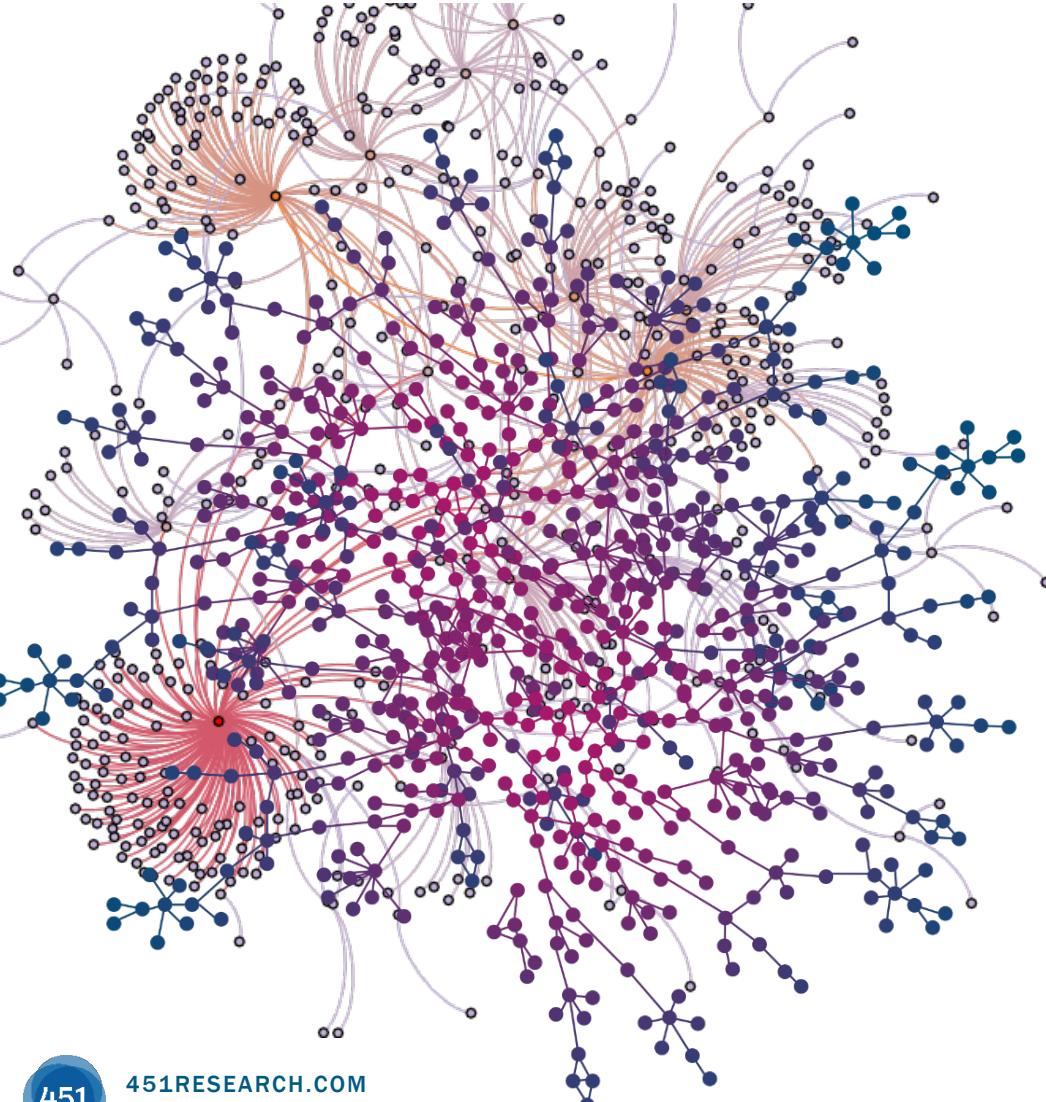
June 4, 2018 | Microsoft News Center



Vulnerability remediation and the ‘Russian doll’ of open source

Example: Struts 2 vulnerability

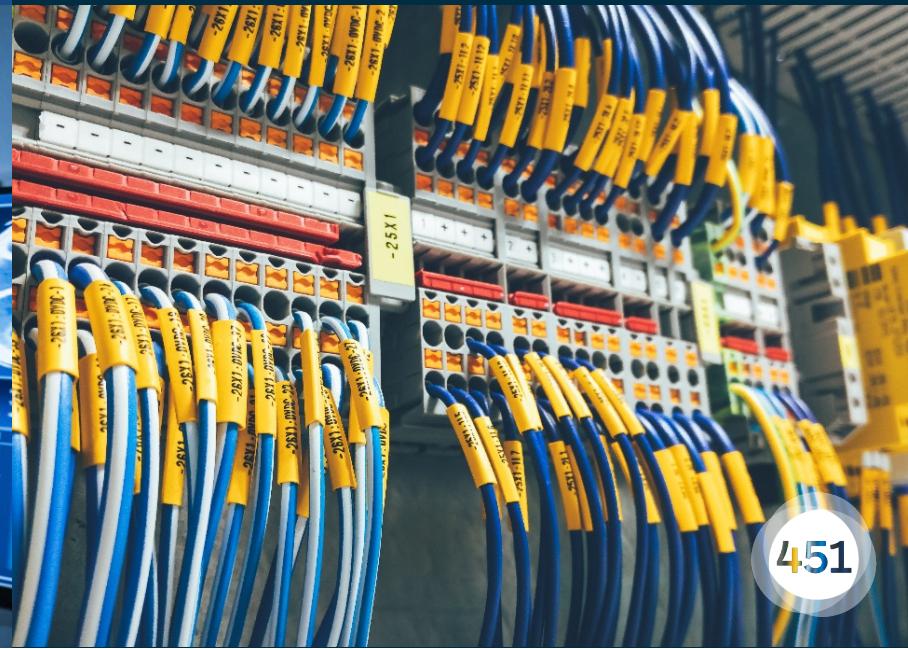
- ▶ ...which extends the Java Servlet API
- ▶ ...had a vulnerability in OGNL (remote code execution exposure)
- ▶ ...which is incorporated in Jakarta
- ▶ ...which was part of Apache



Still more complexity



Let's get
'em **all** on
the network!

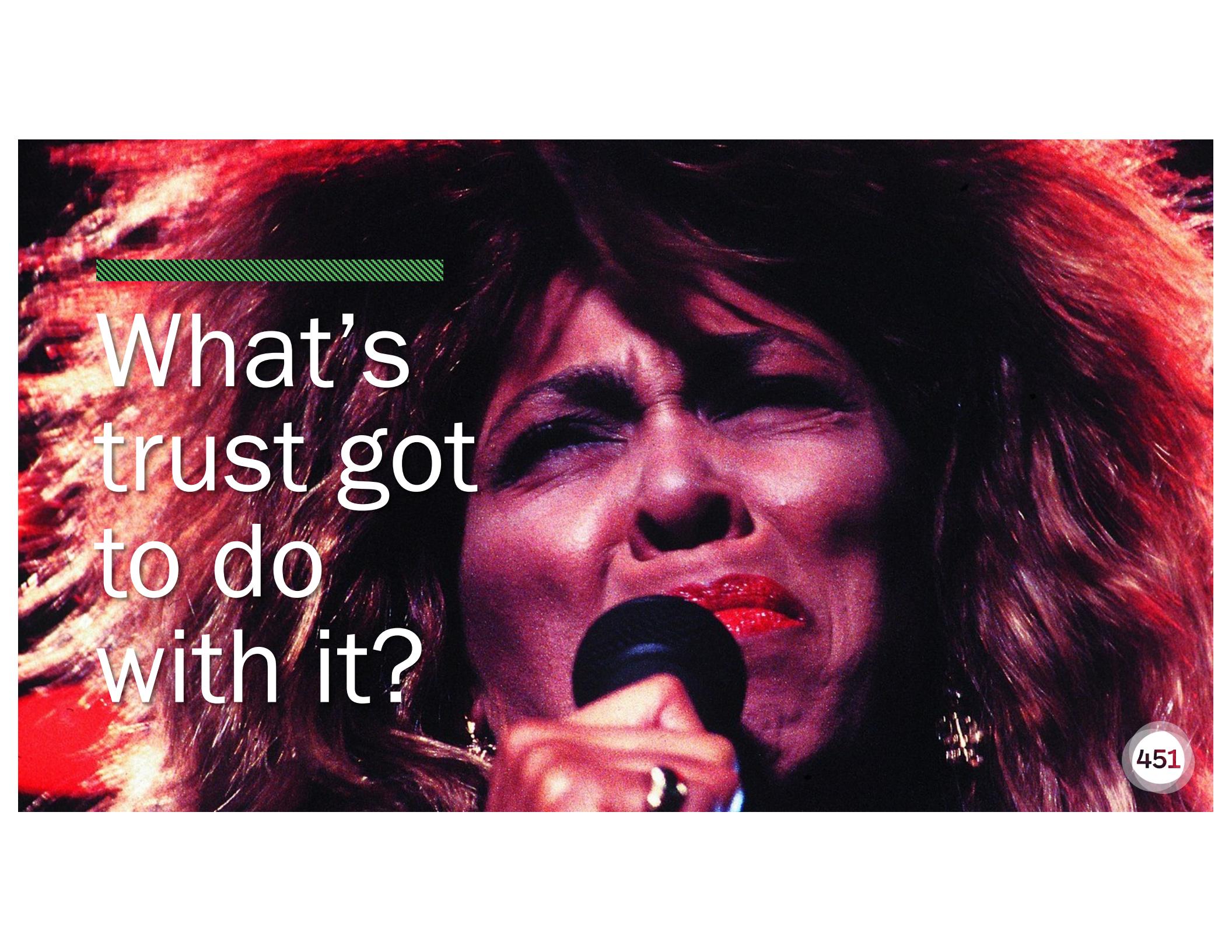




How many people?



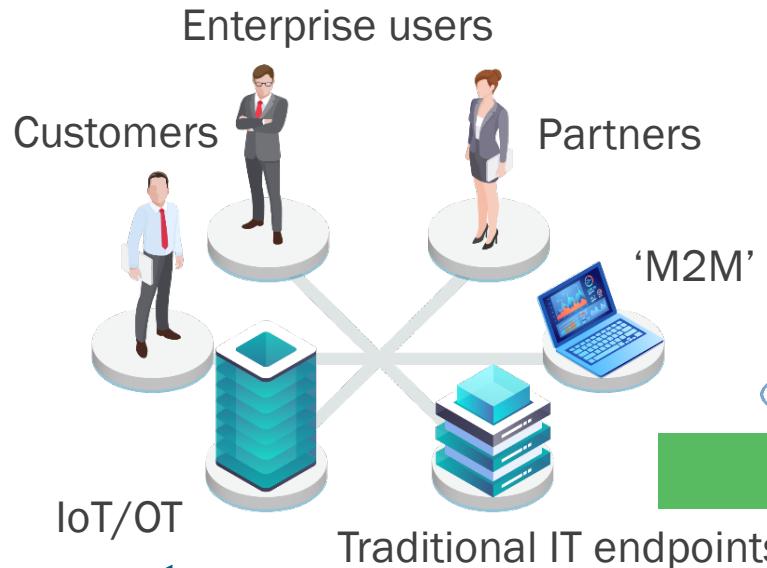
451RESEARCH.COM
©2019 451 Research. All Rights Reserved.



What's
trust got
to do
with it?

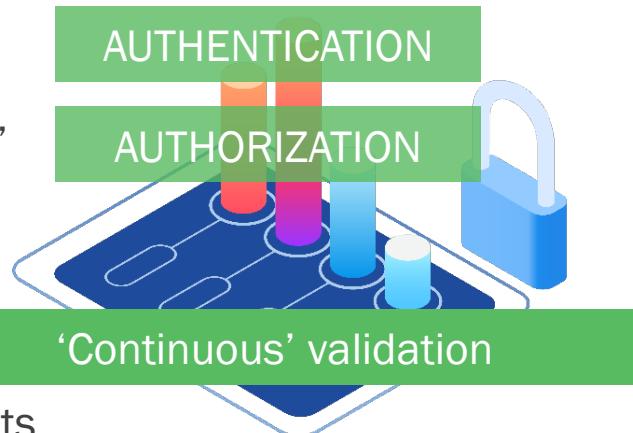
It's all about *proof*

Who seeks access?



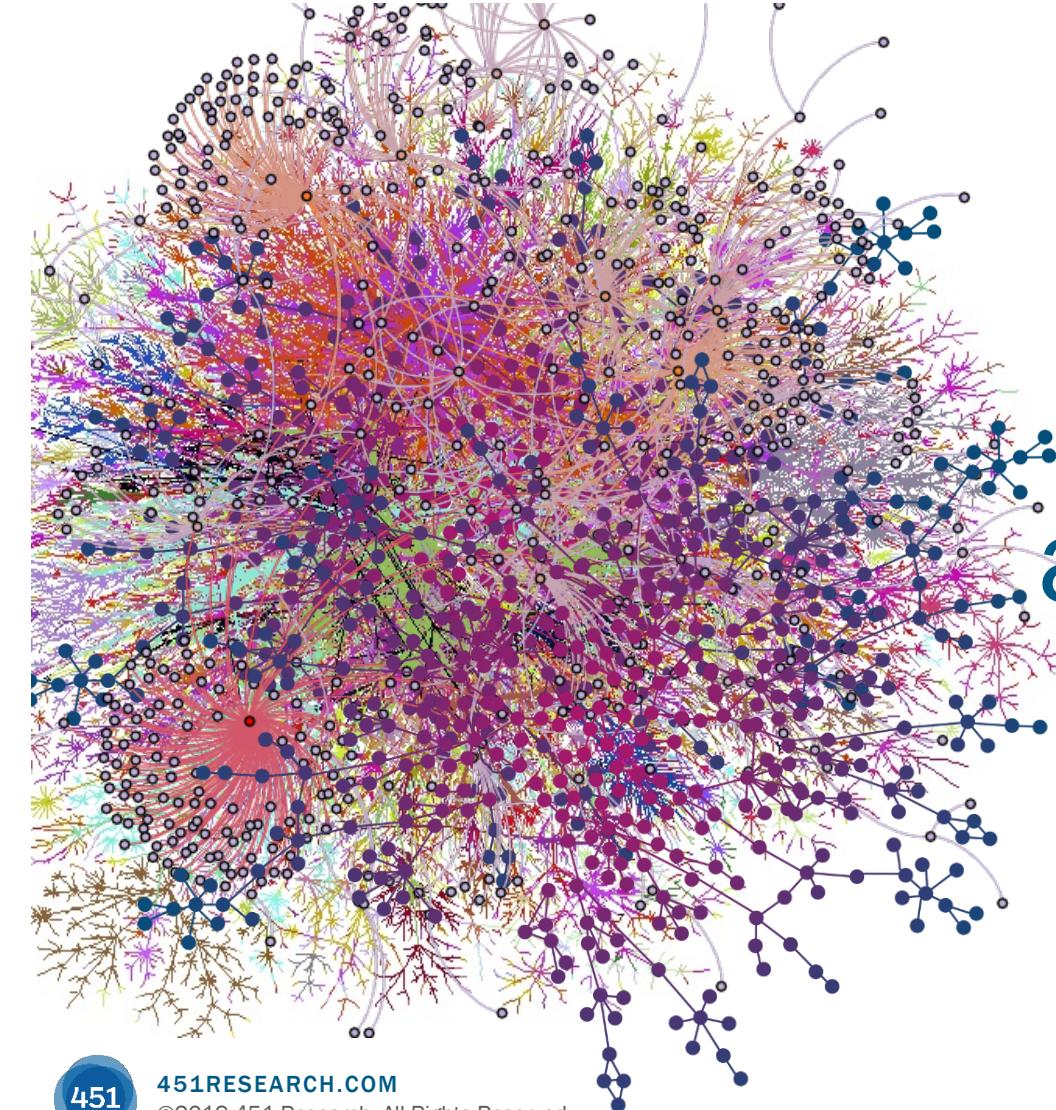
Under *what* conditions?

Decision-making:
AI/ML-enabled



To *which* targets?





Now, multiply
each decision on
a scale of billions.
Continuously.



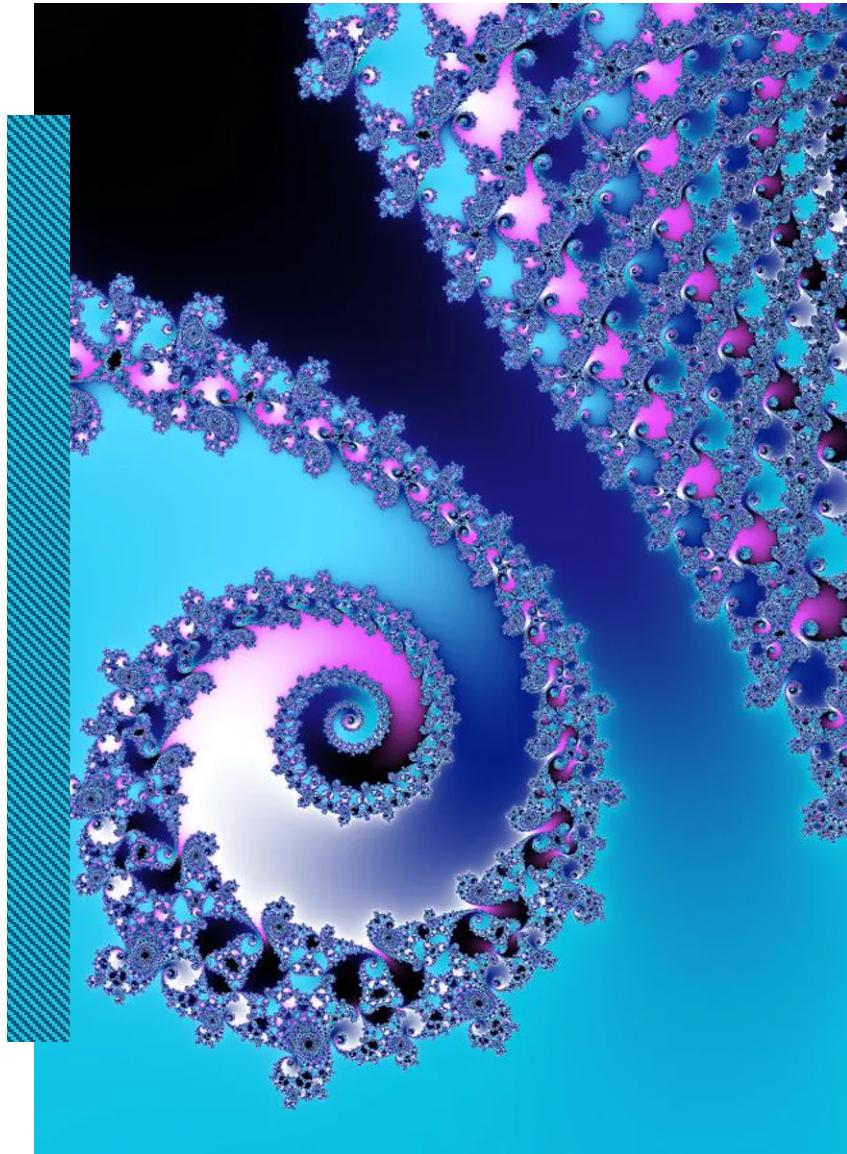
Expand
your
thinking
about...



Security analytics

It can't all be done in one place

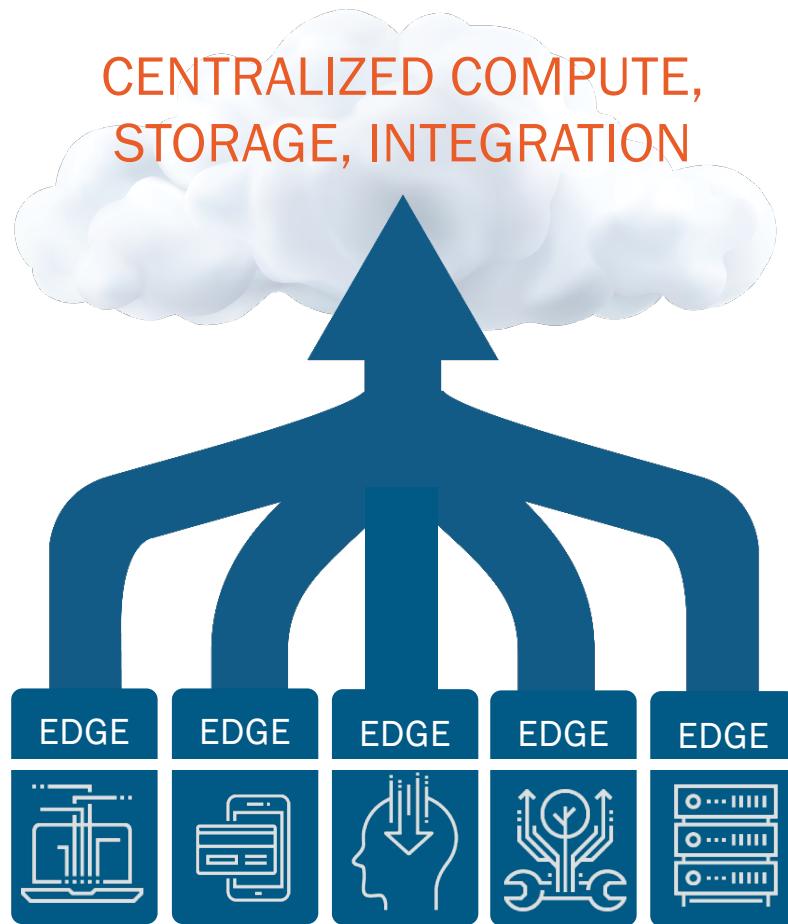
Distributed compute now
may be nothing compared
to what's coming



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

My Neural Network:

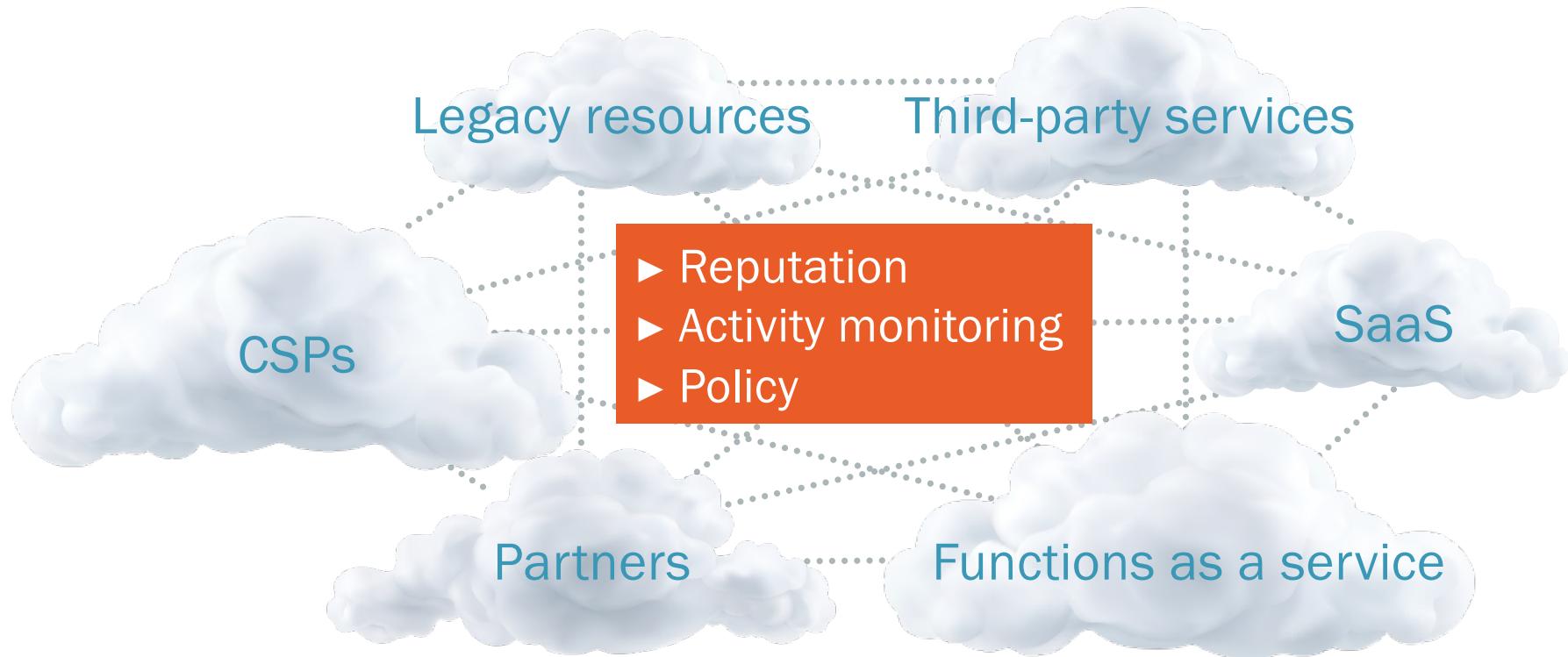




Distributed analytics and control fits other emerging patterns

- ▶ 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

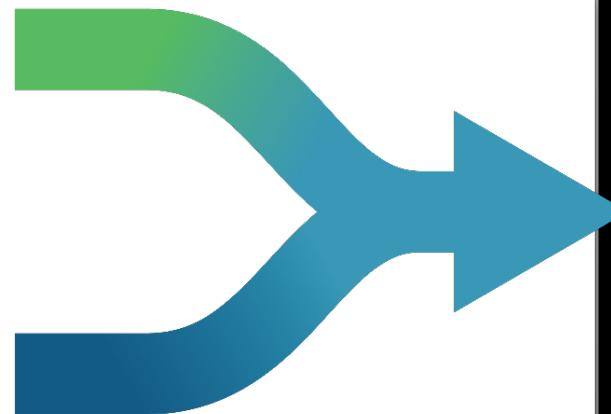


Automation: Similar patterns here, too

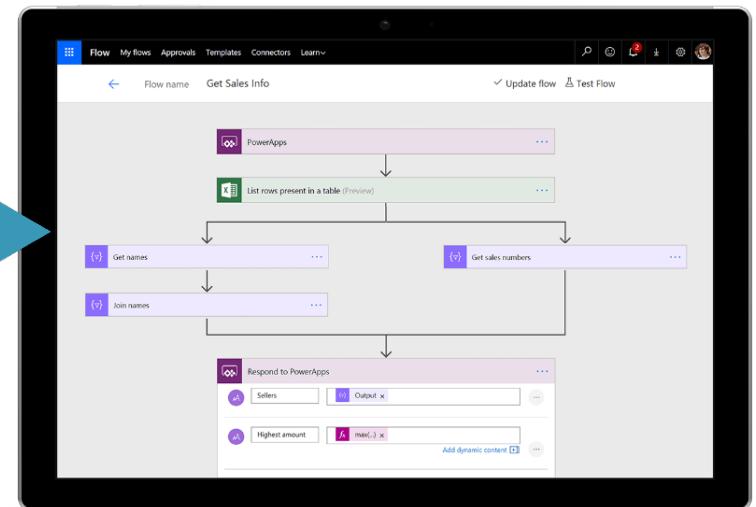
Security Automation & Orchestration ('SOAR')

CI/CD

Robotic Process Automation (RPA)

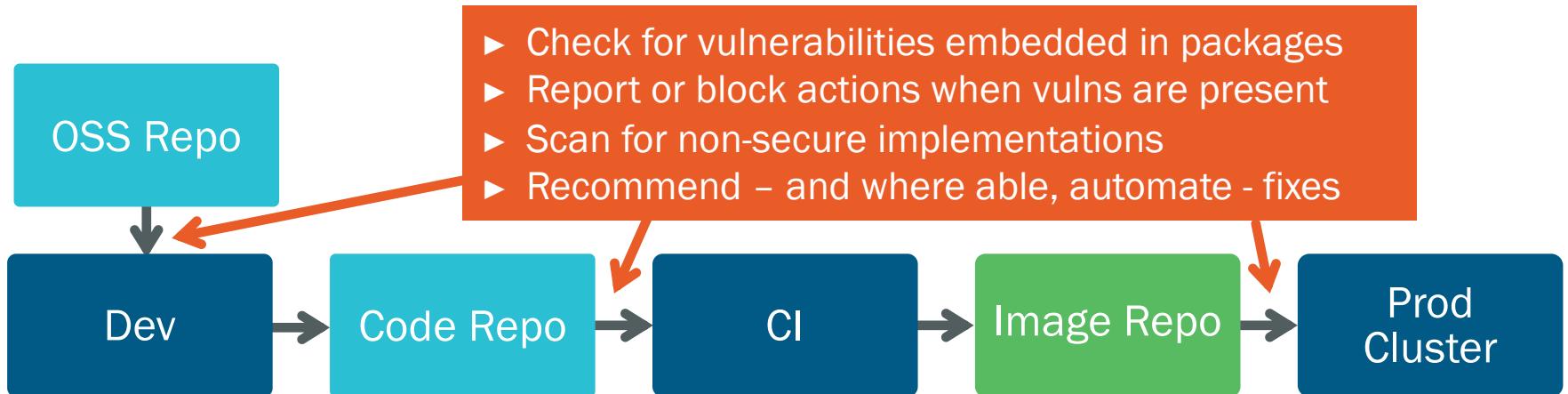


IT AUTOMATION



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



How are we going to source all this?



MEET THE
Citizen Developer

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

MITRE ATT&CK

The ‘GitHub-ification’ of security

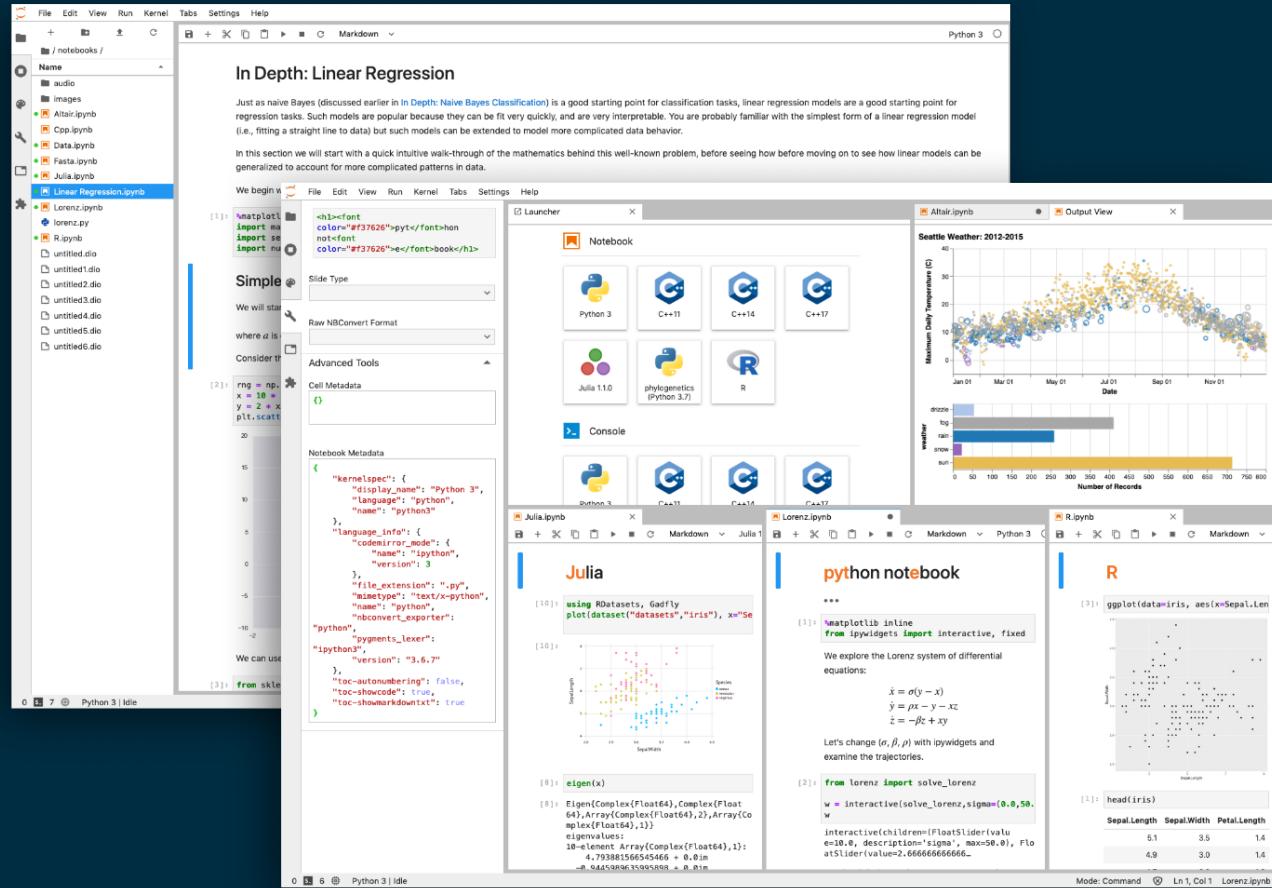
MITRE ATT&CK™ Navigator

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

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

The ‘GitHub-ification’ of analytics

Jupyter Notebooks



<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



451RESEARCH.COM
©2019 451 Research. All Rights Reserved.

