Cloud Security

An Introduction

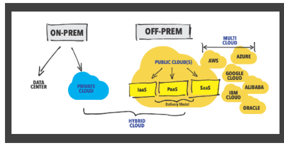
Christian Schwarzer, schwarzer@avantec.ch

AVANTEC

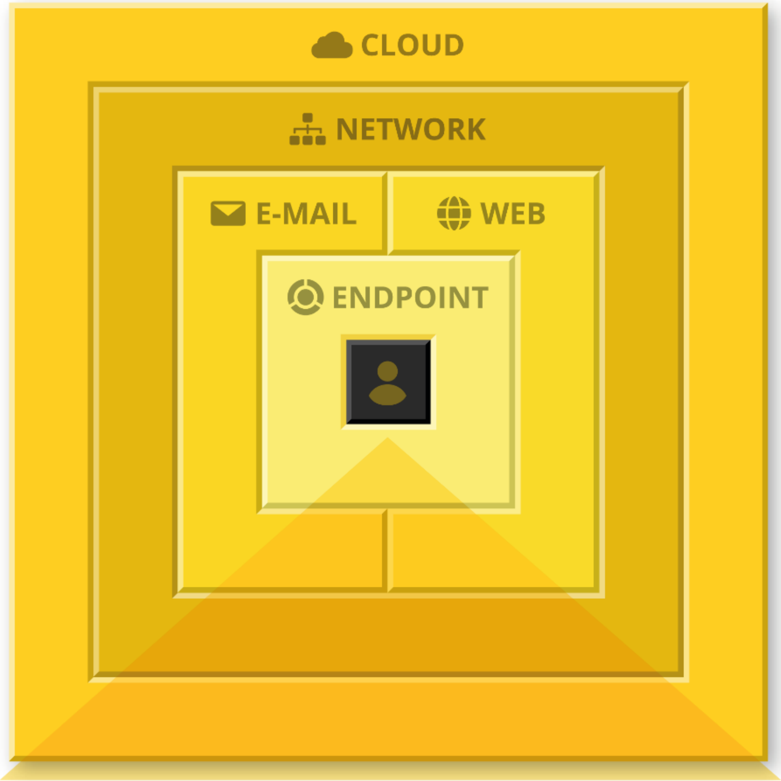
Competence. Security. Trust.

Security Engineering und Integration

Advertisement (0:00)



You can skip to cloud presentation in 20

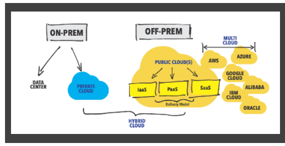


- CLOUD SECURITY
- NETWORK SECURITY
- E-MAIL SECURITY
- WEB SECURITY
- ENDPOINT SECURITY
- USER
- SANDBOXING

AVANTEC
Competence. Security. Trust.

Unsere Partner

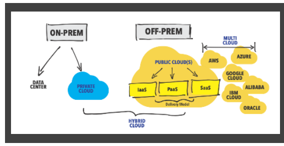
Advertisement (0:10)



You can skip to cloud presentation in 10

algosec	Avecto	BLUE COAT	Br Bromium®
Check Point® SOFTWARE TECHNOLOGIES LTD.	CISCO IRONPORT™	FireEye™	FORTINET®
gemalto	Pulse Secure®	QuoVadis	SEPPMAIL SWISS E-MAIL SECURITY
Symantec.cloud	TREND MICRO™	VECTRA®	zscaler

Über 200 Kunden können sich nicht irren

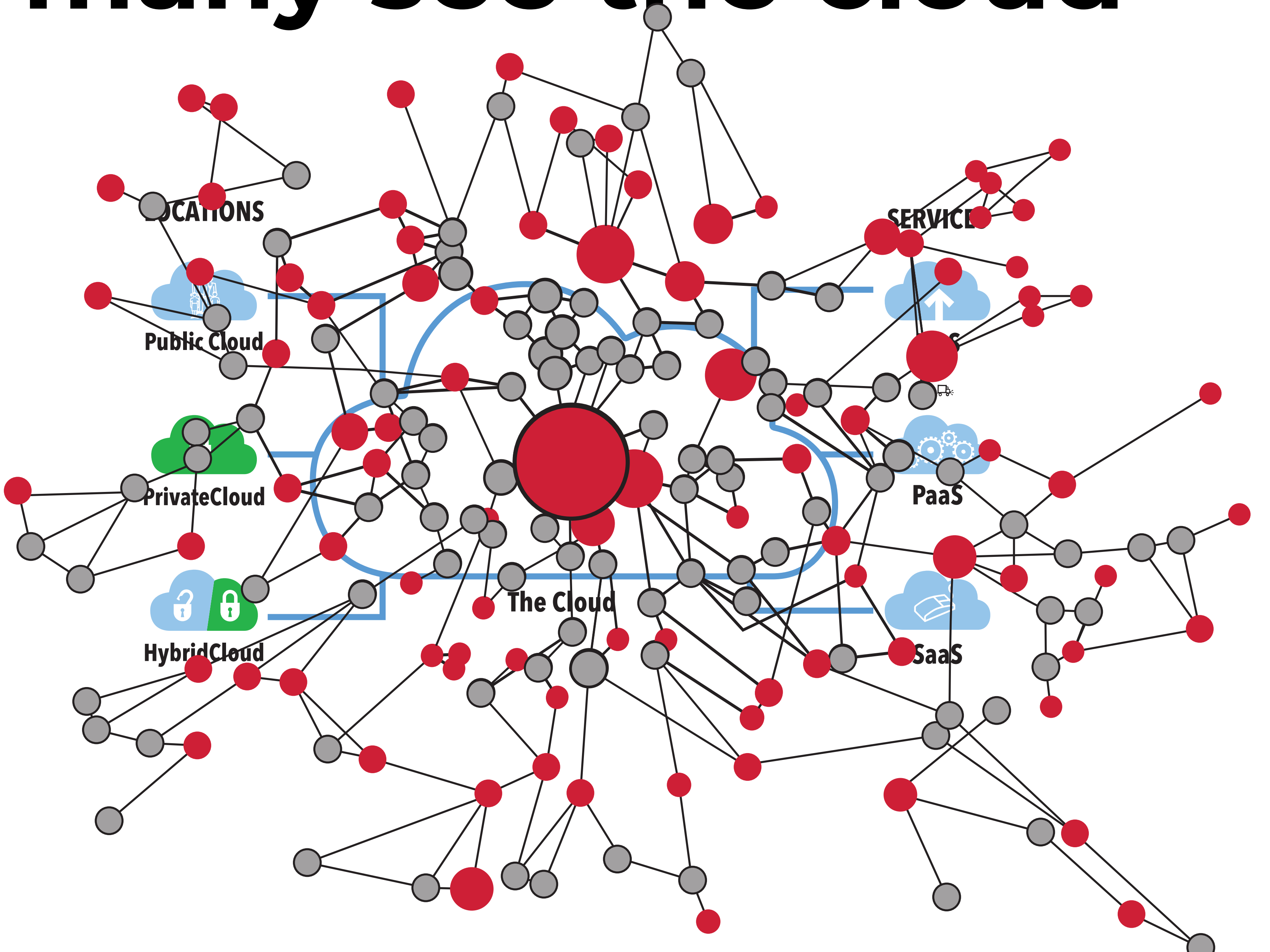


AARGAU	Julius Bär	DIE POST	MIGROS	HGC	Ricola	Schwyzer Kantonalbank	teka	Basler Versicherungen
selecta	UniversitätsSpital Zürich	coop	Zuger Kantonalbank	EFG Bank	MeteoSchweiz	Investec	glaströsch	CKW/// ENERGIE UND DIENSTLEISTUNGEN
AMMANN	Davidoff CIGARS	LGT	Charles Vögele Switzerland	straumann	BEDAG	Neue Zürcher Zeitung	finnova	Together ahead. RUAG
HIRSLANDEN	JOWA	Helsana	swissgrid	R&M	JUMBO DO IT · DECO · GARDEN	PANALPINA on 6 continents	zh aw	FREUDENBERG INNOVATING TOGETHER
maxon motor driven by precision	HUBER+SUHNER	MANOR	AC	AMSTEIN+WALTHERT	SIX GROUP	BINDELLA	Liechtensteinische Landesbank 1861	Kanton Zug
ETH	PRIVATBANKIERS REICHMUTH & CO INTEGRALE VERMÖGENSVERWALTUNG	KANTON LUZERN	Swiss Re	STADT THUN	mibelle	KSW KANTONSSPITAL WINTERTHUR	ANLIKER	Stadt Zürich
FALCON PRIVATE BANK SWISS PRIVATE BANKING	Schweizer Paraplegiker Zentrum	advaltech	Schweizerisches Rotes Kreuz	CONCORDIA	KPMG	QUILVEST	Universität Basel	Stadt Winterthur
Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra	ANDRITZ Hydro	SRG SSR	KISTLER measure. analyze. innovate.	Marionnaud	VIFOR PHARMA	KANTON URI	Hoval Verantwortung für Energie und Umwelt	Lonza

The Cloud

means different things to different people

How many see the cloud

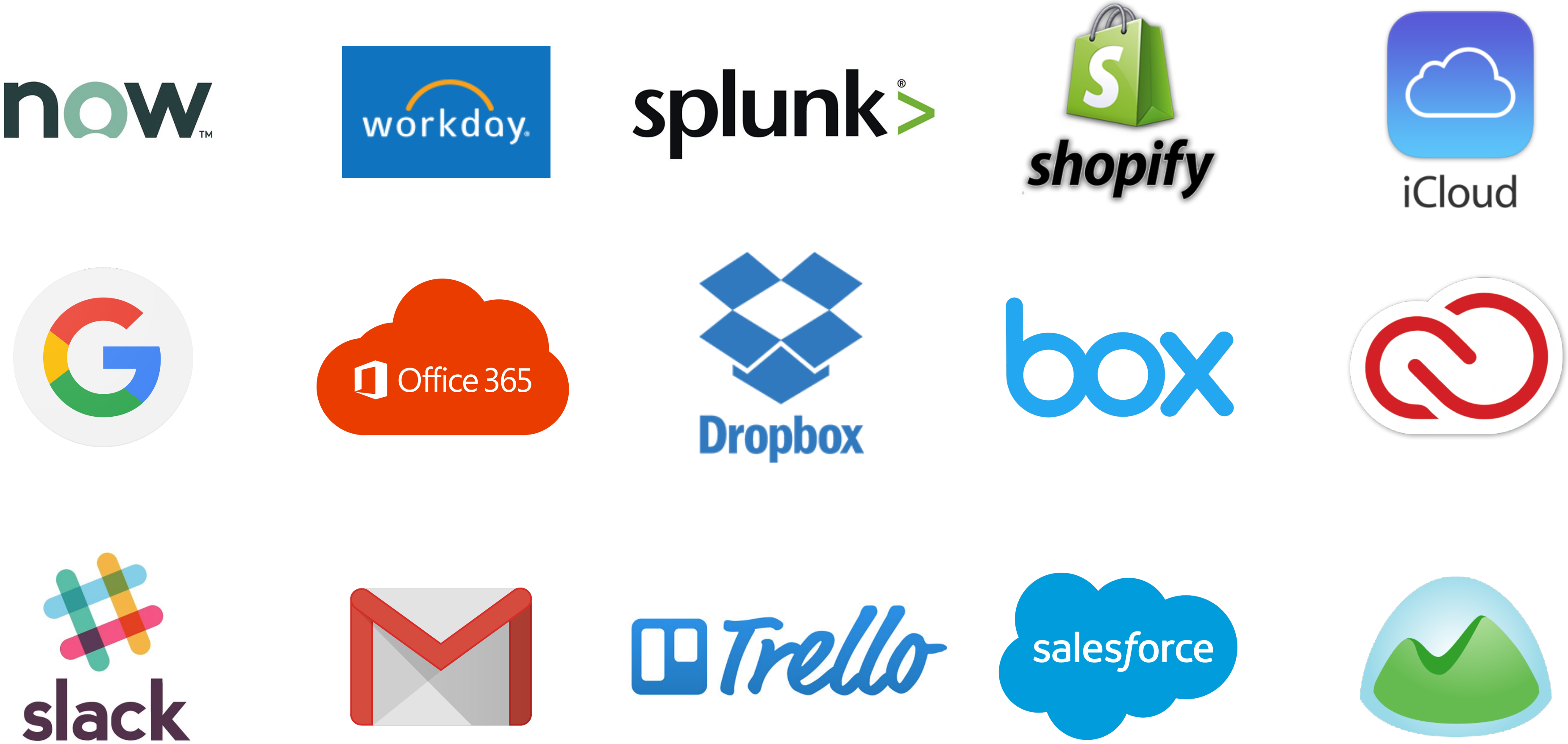


AVANTEC
Competence. Security. Trust.

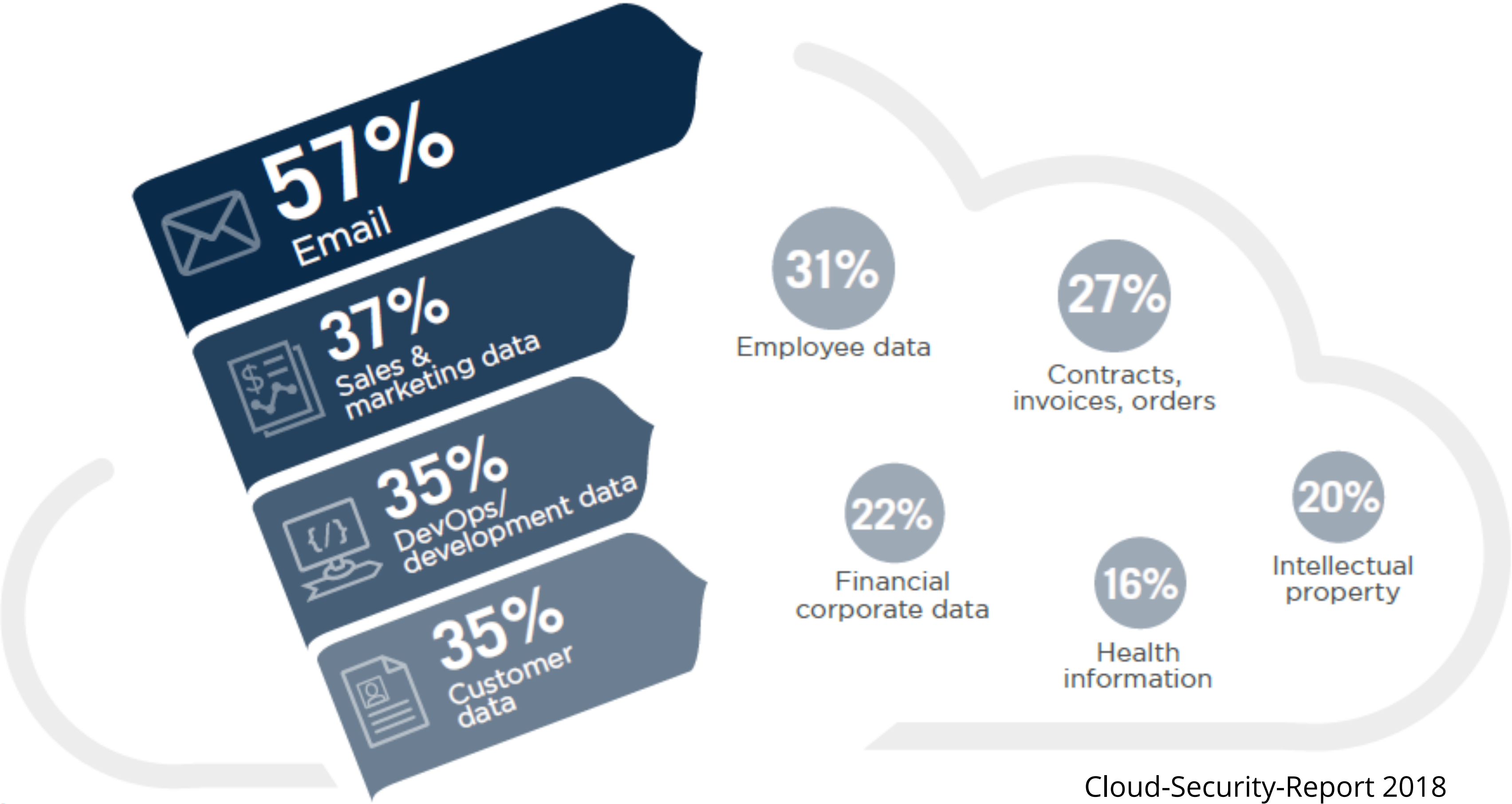
MY REPORT COMES TO THE CONCLUSION THAT CLOUD TECHNOLOGY IS OF NO USE TO THIS COMPANY. I'LL UPLOAD IT TO DROP BOX SO YOU CAN TAKE A LOOK AT IT.

© D.Fletcher for CloudTweaks.com

But we’re all using it already



What types of corporate information do you store in the cloud?

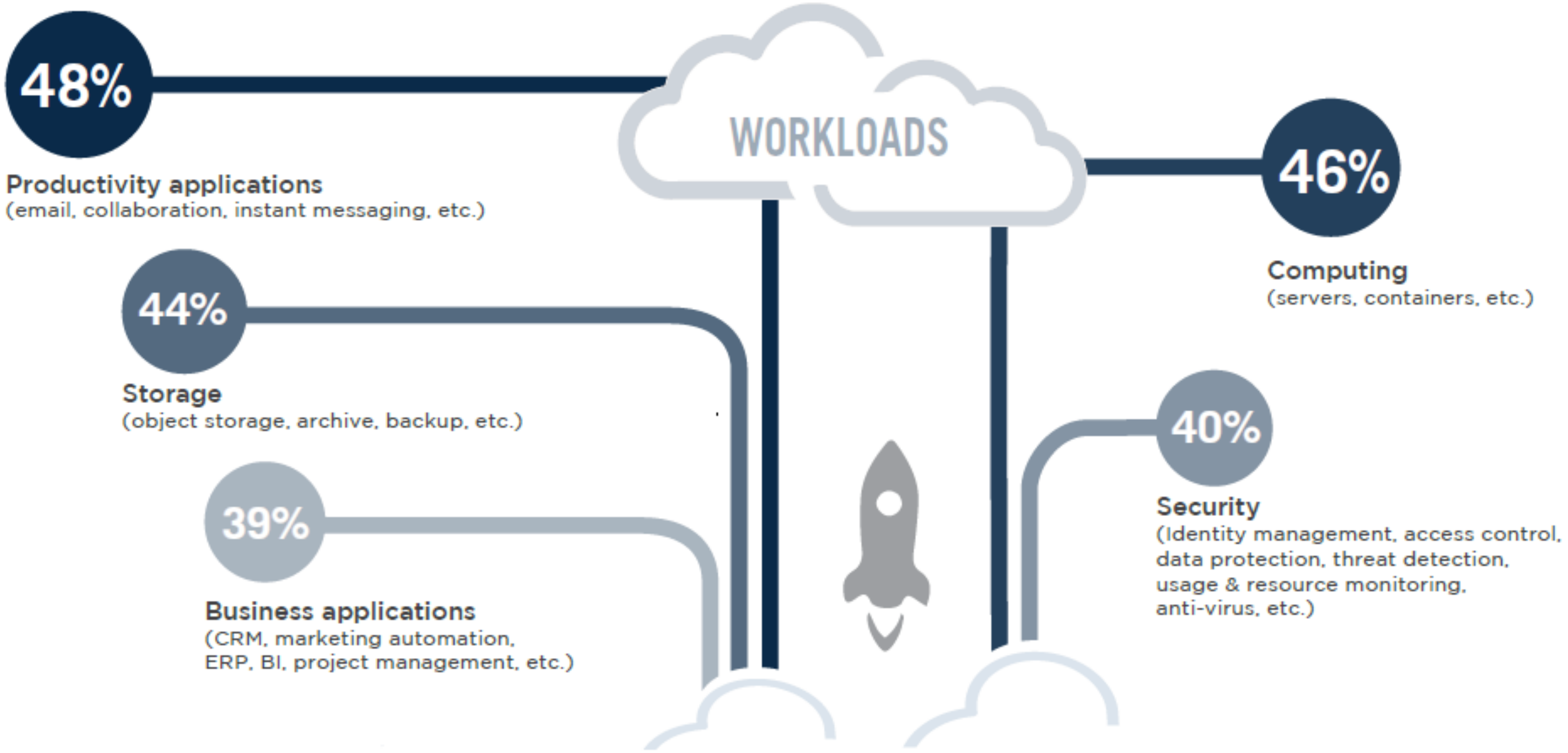


Not sure/other 24%

Cloud-Security-Report 2018
Worldwide

AVANTEC
Competence. Security. Trust.

What services & workloads is your organization deploying in the cloud?



WORKLOADS

48% **Productivity applications**
(email, collaboration, instant messaging, etc.)

44% **Storage**
(object storage, archive, backup, etc.)

39% **Business applications**
(CRM, marketing automation, ERP, BI, project management, etc.)

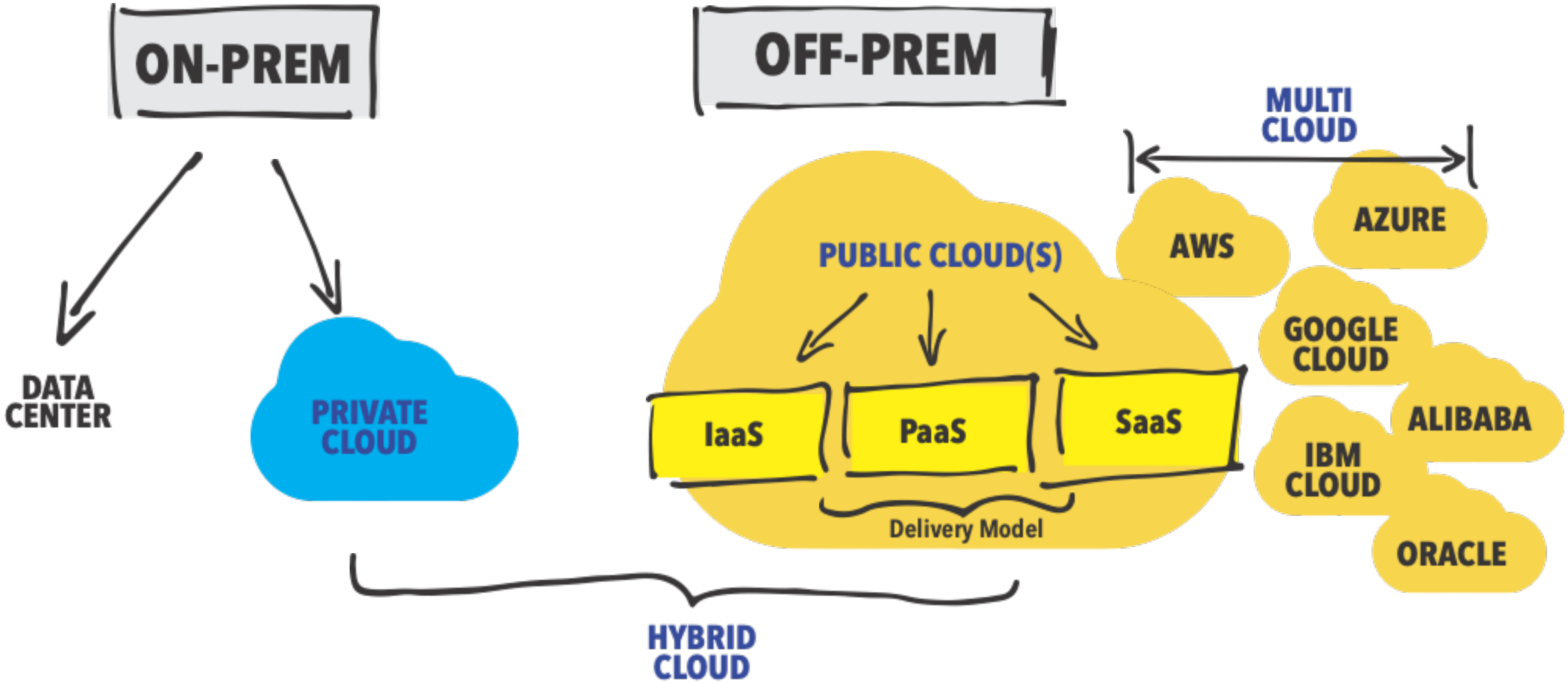
46% **Computing**
(servers, containers, etc.)

40% **Security**
(Identity management, access control, data protection, threat detection, usage & resource monitoring, anti-virus, etc.)

Database (relational, NoSQL, caching, etc.) 37% | Virtualization 37% | Developer/Testing Applications 37% | Networking (virtual private cloud, DNS, etc.) 34% | IT Operations Applications (administration, backup, provisioning monitoring, etc.) 31% | Operating System 29% | Middleware 17% | Runtime 10% | Not sure/other 22%

Cloud-Security-Report 2018 Worldwide

What we mean by cloud



AVANTEC
Competence. Security. Trust.

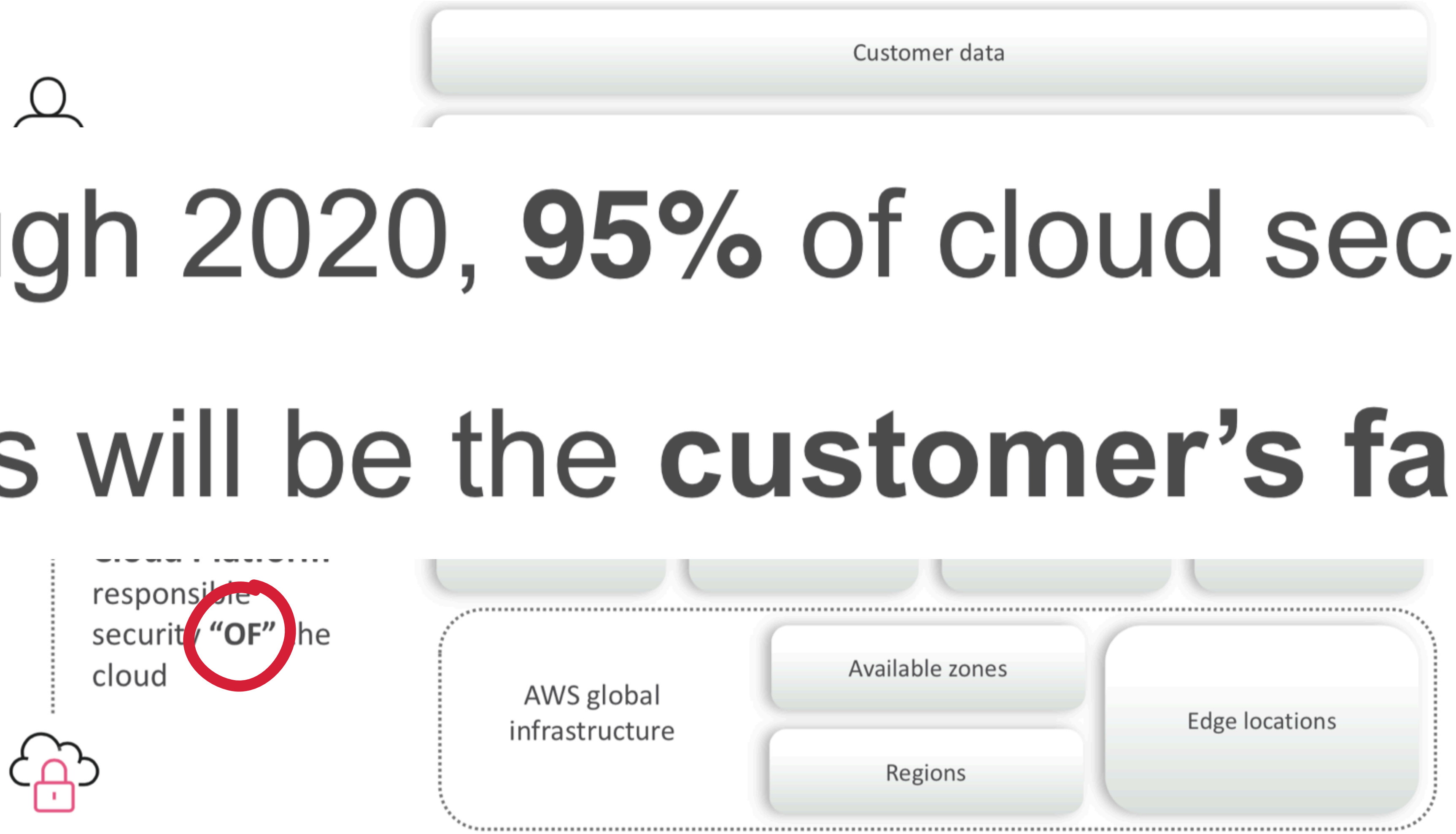
What defines the Cloud?

- **Elastic**
  Scale up and down quickly and easily to meet demand.
- **Metered**
  So you only pay for what you use (pay-as-you-go).
- **Self service**
  All the resources you need with self-service access.
- **Automatic**
  Everything can be accessed through API’s and Scripts.
- **Global**
  High availability and low-latency.

Shared responsibility

“Through 2020, **95%** of cloud security failures will be the **customer’s fault.**”

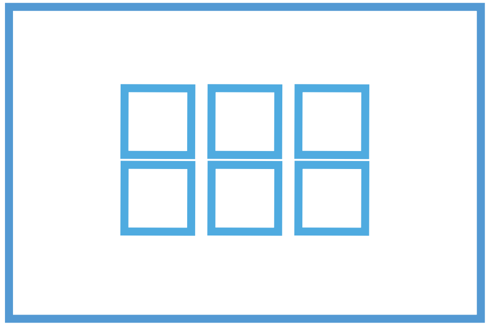
Gartner


Customer data
responsible security “OF” the cloud
AWS global infrastructure
Available zones
Regions
Edge locations

AVANTEC
Competence. Security. Trust.

Your responsibility (and know-how) is shared internally

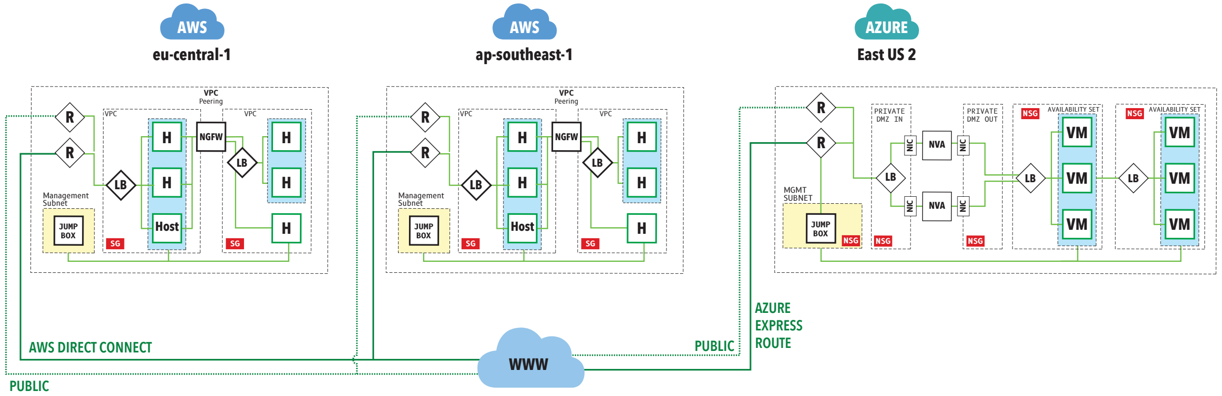
- **Many different teams will drive cloud deployments**
  Often business-driven
- **IT will not be in control of all cloud deployments**
  Can security deliver at the right speed?
- **Big difference between security in DC’s and in the Cloud**
  But cloud native is not a panacea
- **There is a big knowledge gap**
  Can you close it?



Simple

Traditional Data Center

On-Premises infra and applications deployed by highly trained teams. Tight control over security and standards.



Complex

Cloud Data Centers

Cloud applications and infra deployed by multiple teams, not under IT control. High likelihood of inconsistency and misconfiguration.

AVANTEC
Competence. Security. Trust.

Security Challenges in the Cloud

General issues

Shared responsibility

Minimal native visibility

Ever-changing workloads

Multi & Hybrid Cloud Architecture

Real time prevention

Inside threats

Misconfiguration

Credentials exploit

Insider threat

Compliance and regulations

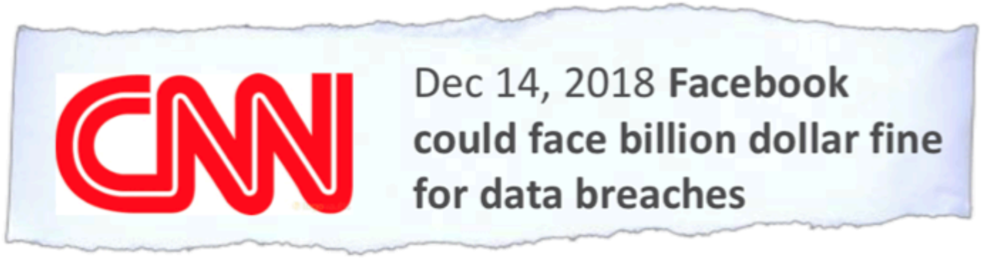
Outside threats

Malware

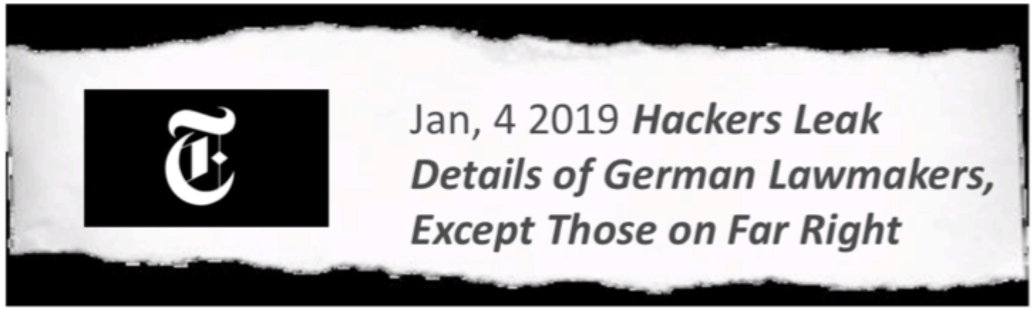
Zero-day threats

Account takeover

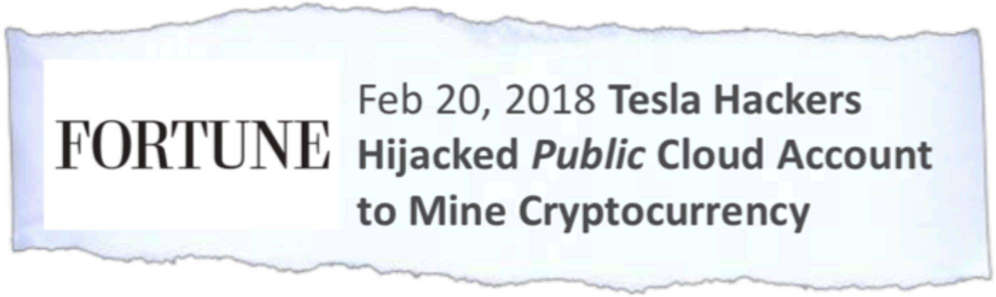
Next-gen attacks


CNN

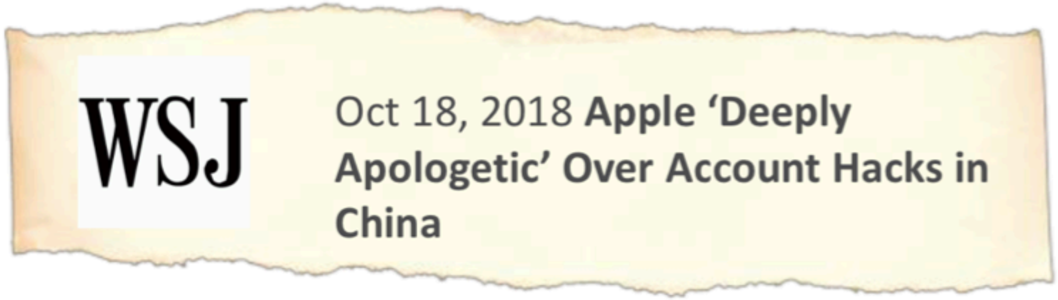
Dec 14, 2018 **Facebook could face billion dollar fine for data breaches**


𝕿

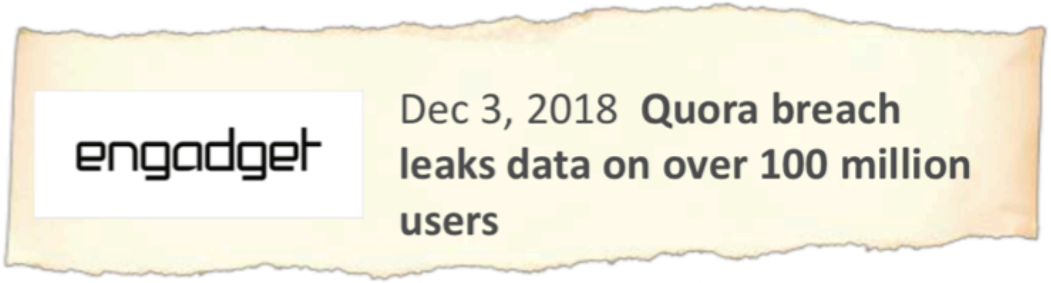
Jan, 4 2019 ***Hackers Leak Details of German Lawmakers, Except Those on Far Right***


FORTUNE

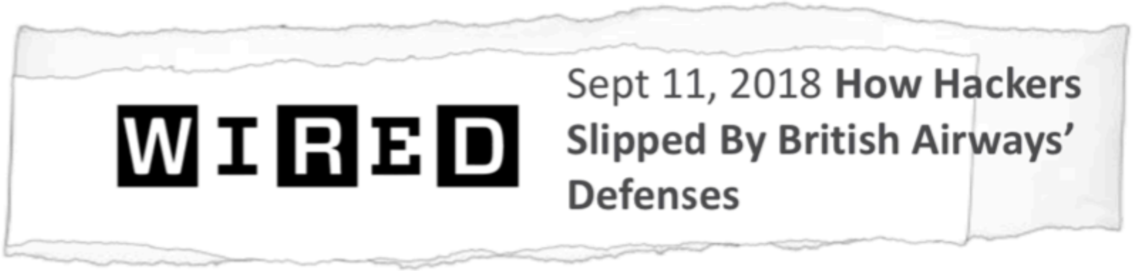
Feb 20, 2018 **Tesla Hackers Hijacked *Public* Cloud Account to Mine Cryptocurrency**


WSJ

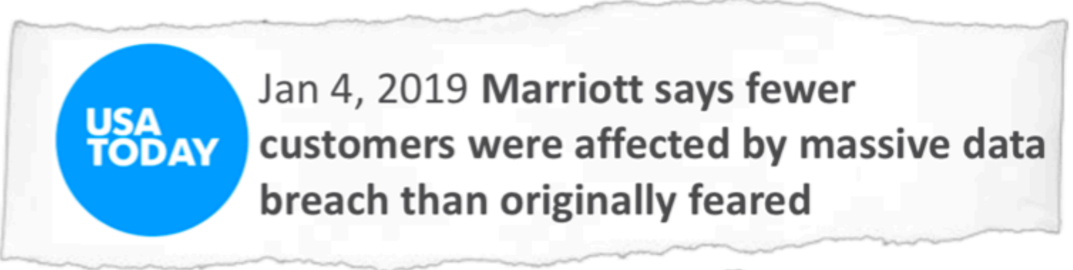
Oct 18, 2018 **Apple 'Deeply Apologetic' Over Account Hacks in China**


engadget

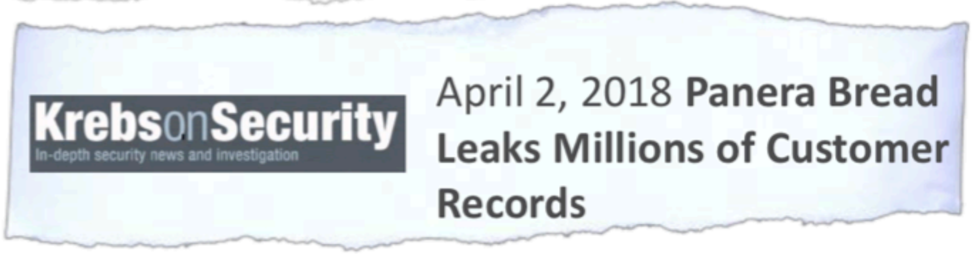
Dec 3, 2018 **Quora breach leaks data on over 100 million users**


WIRED

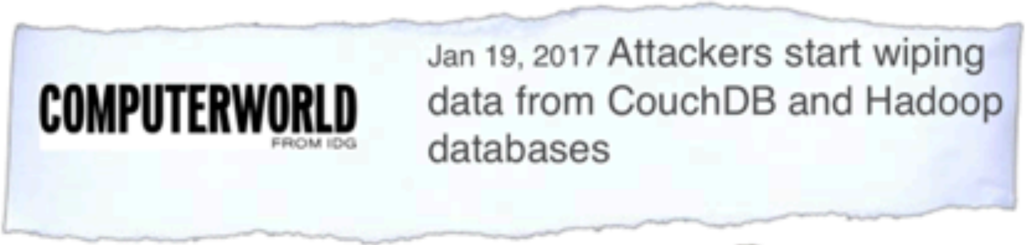
Sept 11, 2018 **How Hackers Slipped By British Airways' Defenses**


USA TODAY

Jan 4, 2019 **Marriott says fewer customers were affected by massive data breach than originally feared**

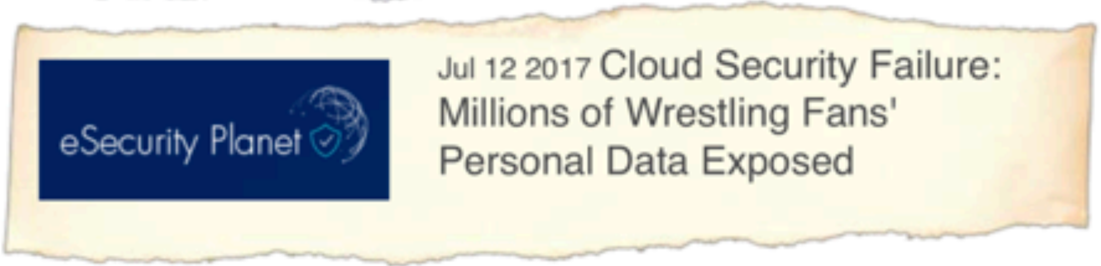

KrebsonSecurity
In-depth security news and investigation

April 2, 2018 **Panera Bread Leaks Millions of Customer Records**



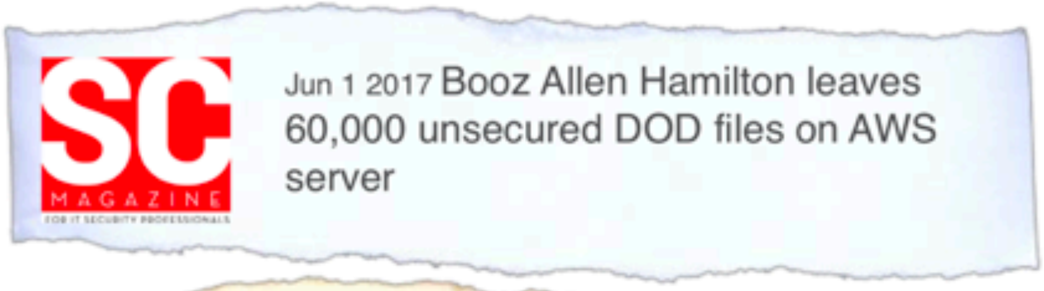
COMPUTERWORLD FROM IDG

Jan 19, 2017 Attackers start wiping data from CouchDB and Hadoop databases



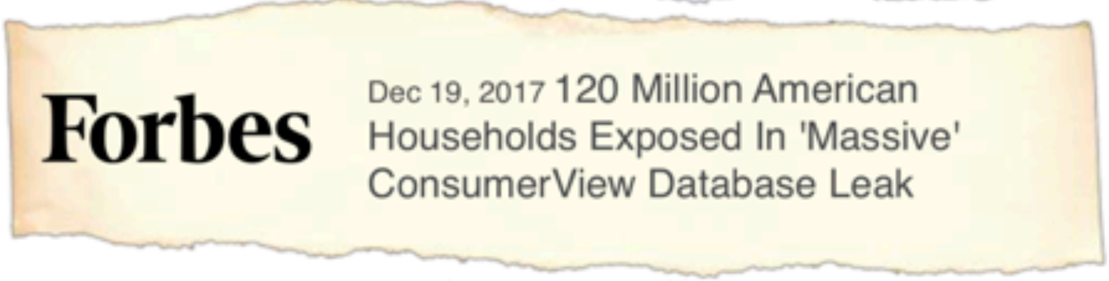
eSecurity Planet

Jul 12 2017 Cloud Security Failure: Millions of Wrestling Fans' Personal Data Exposed



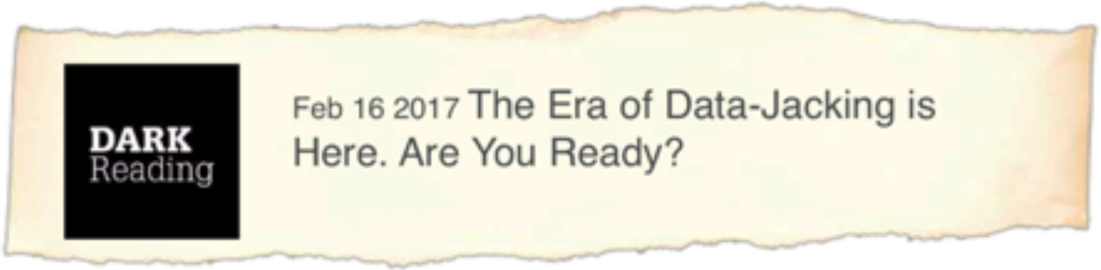
SC MAGAZINE FOR IT SECURITY PROFESSIONALS

Jun 1 2017 Booz Allen Hamilton leaves 60,000 unsecured DOD files on AWS server



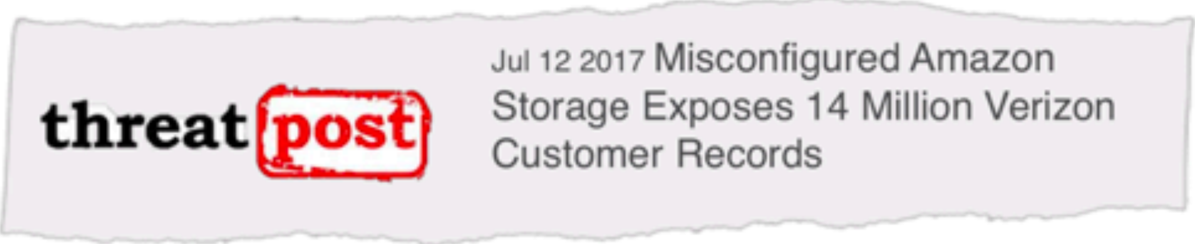
Forbes

Dec 19, 2017 120 Million American Households Exposed In 'Massive' ConsumerView Database Leak



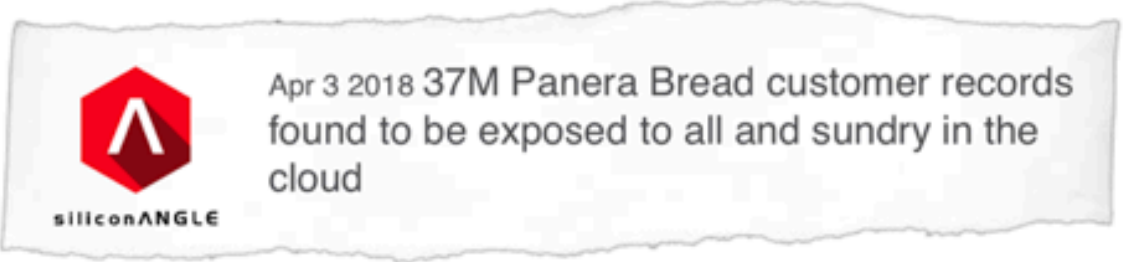
DARK Reading

Feb 16 2017 The Era of Data-Jacking is Here. Are You Ready?



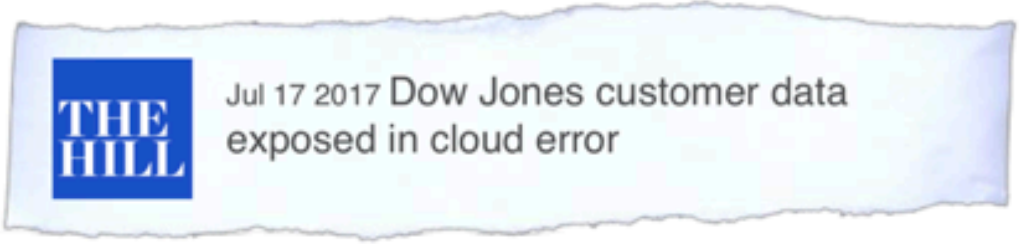
threatpost

Jul 12 2017 Misconfigured Amazon Storage Exposes 14 Million Verizon Customer Records



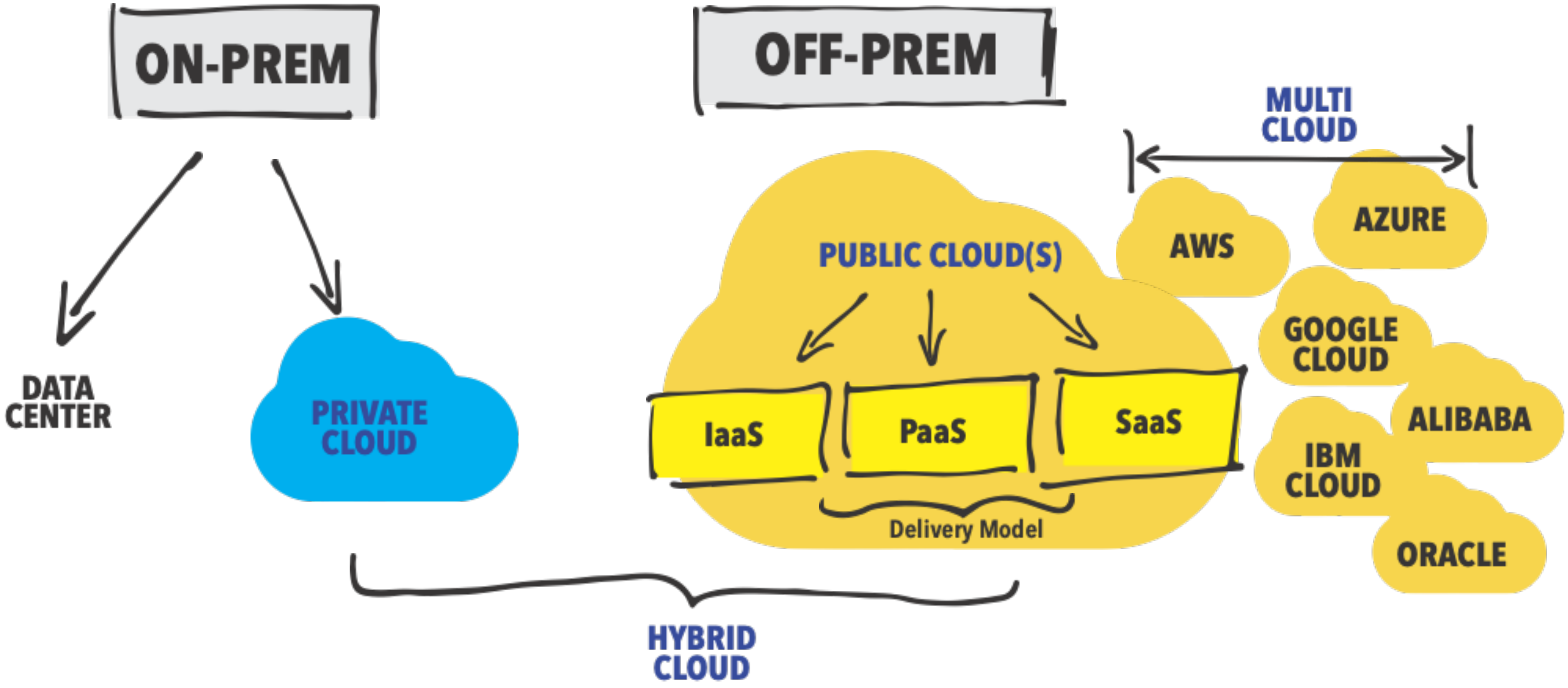
siliconANGLE

Apr 3 2018 37M Panera Bread customer records found to be exposed to all and sundry in the cloud

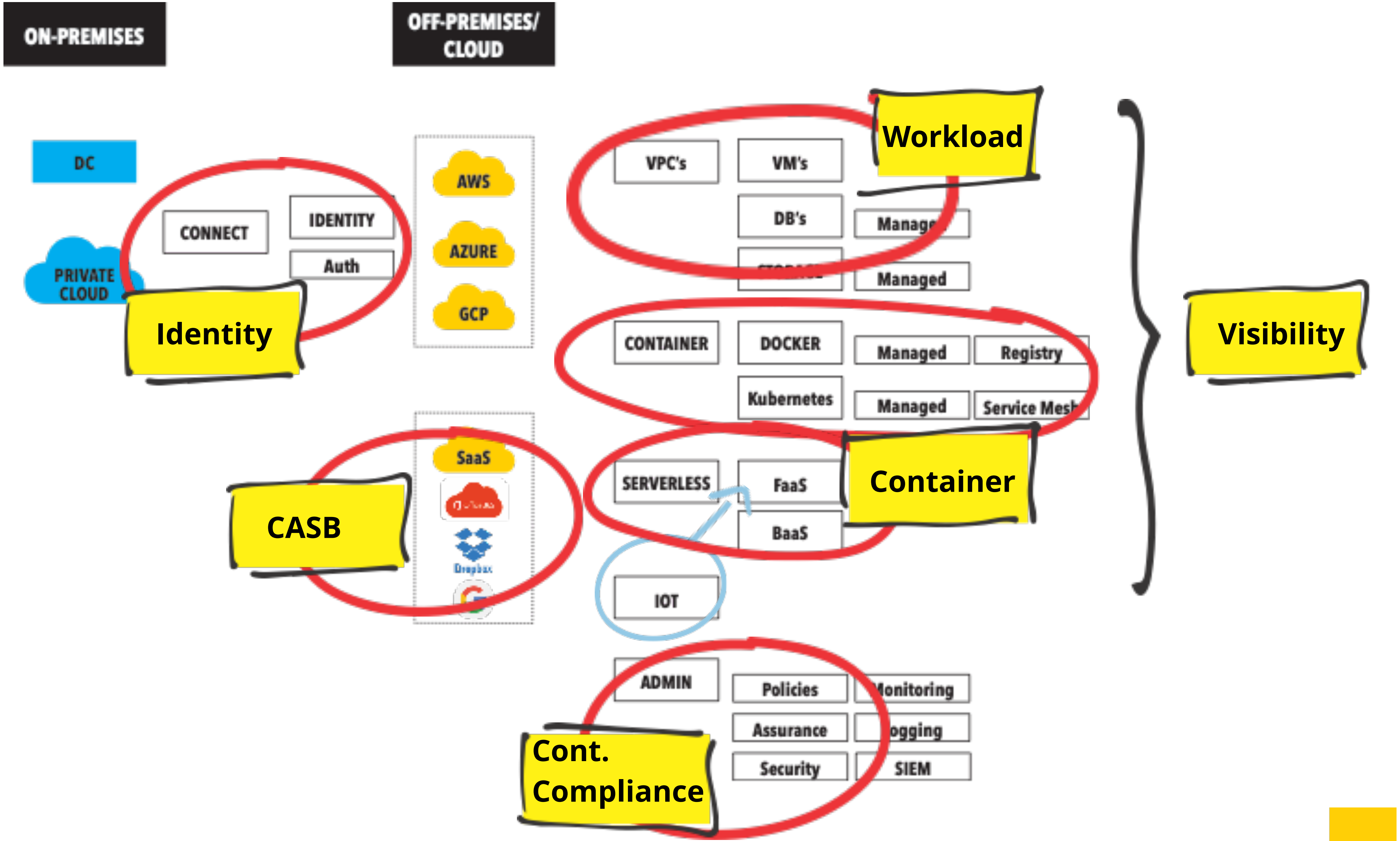


THE HILL

Jul 17 2017 Dow Jones customer data exposed in cloud error



AVANTEC
Competence. Security. Trust.



ON-PREMISES

OFF-PREMISES/ CLOUD

DC

PRIVATE CLOUD

CONNECT

IDENTITY

Auth

Identity

AWS

AZURE

GCP

SaaS

Dropbox

CASB

VPC's

VM's

DB's

Manag

Managed

Workload

CONTAINER

DOCKER

Managed

Registry

Kubernetes

Managed

Service Mes

SERVERLESS

FaaS

BaaS

Container

IOT

ADMIN

Policies

onitoring

Assurance

ogging

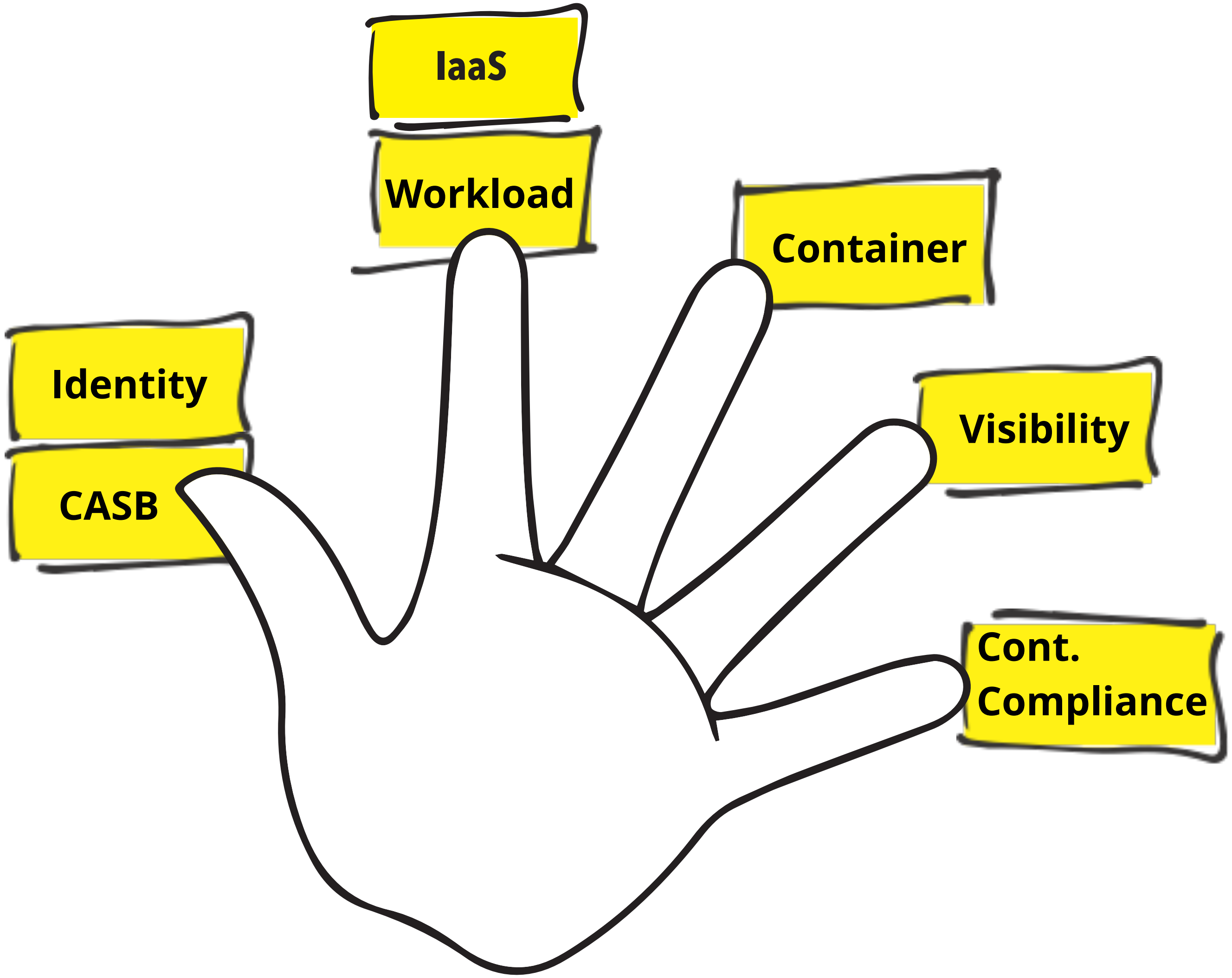
Security

SIEM

Cont. Compliance

Visibility

AVANTEC
Competence. Security. Trust.



IaaS

Workload

Identity

CASB

Container

Visibility

Cont. Compliance

Handout

CLOUD SECURITY EVENT
28. März 2019

AVANTEC

Competence. Security. Trust.

…TY, SAAS UND CASB

…nd
…s
…Sie im
…n
…en?

SOME CLOUD

(1) Haben Sie bereits ein Single Sign-on (SSO) für die SaaS-Applikationen erstellt?

(2) Haben Sie eine Identity-Lösung mit Conditional Access im Einsatz?

(3) Benutzen Sie ein Cloud SIEM oder haben Sie Ihre Identity-Lösung in Ihr on-premises SIEM eingebunden?

(4) Hat Ihr CASB eine integrierte Phishing Protection?

CLOUD FIRST

(1) Ist bei Ihnen Passwordless bereits ein Thema?

(2) Haben Sie bereits eine Privileged Identity Protection für Cloud Accounts im Einsatz?

(3) Sind Ihnen just-in-time (JIT) Privilege Elevations ein Begriff?

APPLICATION VISIBILITY

NO CLOUD

…der
…rem
…ren,
…ne

SOME CLOUD

(1) Haben Sie bereits Applikationen in der Cloud (private oder public), die mit Mikrosegmentierung geschützt werden und haben Sie die Mikrosegmentierung manuell erstellt?

(2) Können Sie verfolgen, welche Applikationen miteinander kommunizieren, auch über verschiedene Clouds hinweg (Multicloud)?

CLOUD FIRST

(1) Wenn Sie bereits eine Mikrosegmentierung in der Cloud einsetzen, wie stellen Sie sicher, dass neue Applikationen oder Server auch korrekt eingebunden sind?

(2) Wie setzen Sie das Baselining in Ihrer Visibility-Lösung ein?

(3) Haben Sie schon ein automatisches Policy-Enforcement im Einsatz?

IAAS / WORKLOADS SECURITY

NO CLOUD

…OME CLOUD

… Haben Sie VPCs / VNets …r VMs im Einsatz?

…ind Ihre internen Teams …as Bereitstellen der …truktur zuständig oder …en Sie einen Cloud …ed Service?

…viel automatisieren …ts und haben Sie …os Team, das …ei hilft?

CLOUD FIRST

(1) Haben Sie neben dem DevOps Team bereits ein SecDevOps Team im Einsatz oder geplant?

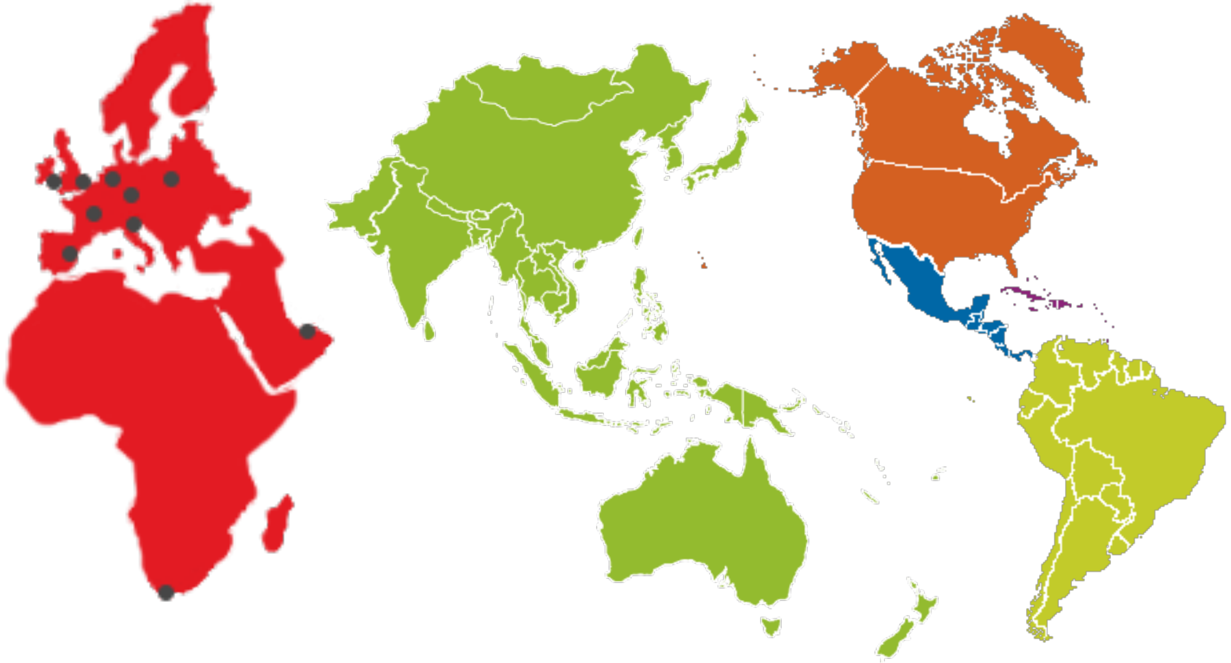
(2) Benutzen Sie Transit-VPCs und setzen Sie dafür NextGen FWs ein?

(3) Haben Sie Multicloud im Einsatz? Wenn ja, haben Sie ein Single Pane of Glass und vereinheitlichte Policies über alle Clouds hinweg?

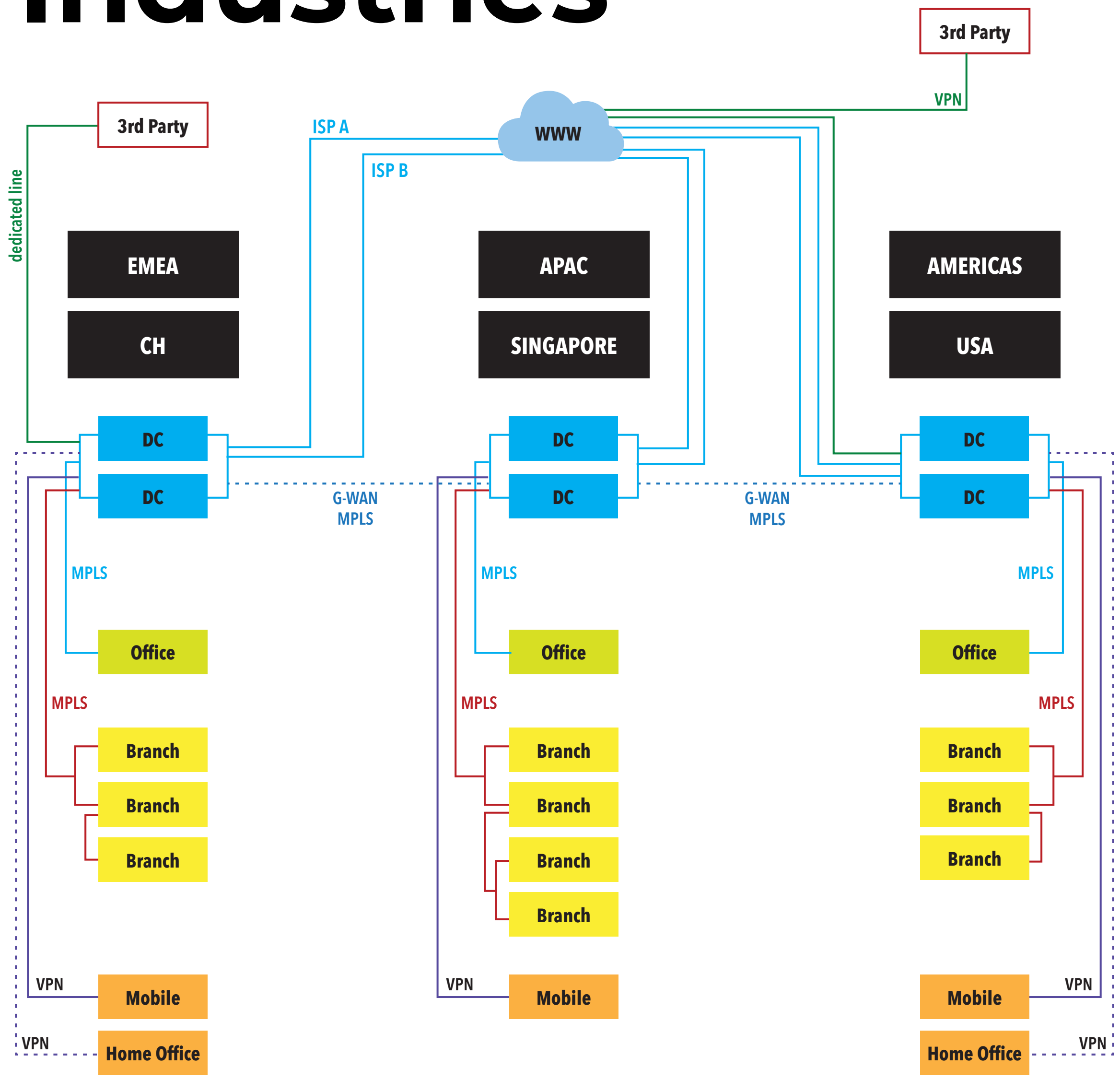
AVANTEC
Competence. Security. Trust.

TecByte Industries

TecByte Industries



TecByte Industries



Competence. Security. Trust.

Thank you

AVANTEC
Competence. Security. Trust.