Don't Get Caught with an Unsecured Cloud

paloalto NETWORKS®

Simon Crocker
Director, Systems Engineering

Our Everyday World Has Changed

fitbit

YouTube

Google

UBER

WhatsApp

STRAVA

Google Play

amazon prime video

music

Linked in

iCloud

Spotify

The Positive Disruption of Cloud in Business

- Flexibility
- Business Agility - Time to Market
- Collaboration
- Mobility of Staff
- Disaster Recovery
- Reliability
- Scale
- *Security

Business Is Adopting Cloud
But you Need to Ask Who is Adopting What???

OFFICE 365

BOX.COM

GITHUB

GOOGLE DRIVE

SFDC

DROPBOX

YAMMER

SLACK

SECURE DATA SPACE

JIVE

SERVICE NOW

amazon web services

Microsoft Azure

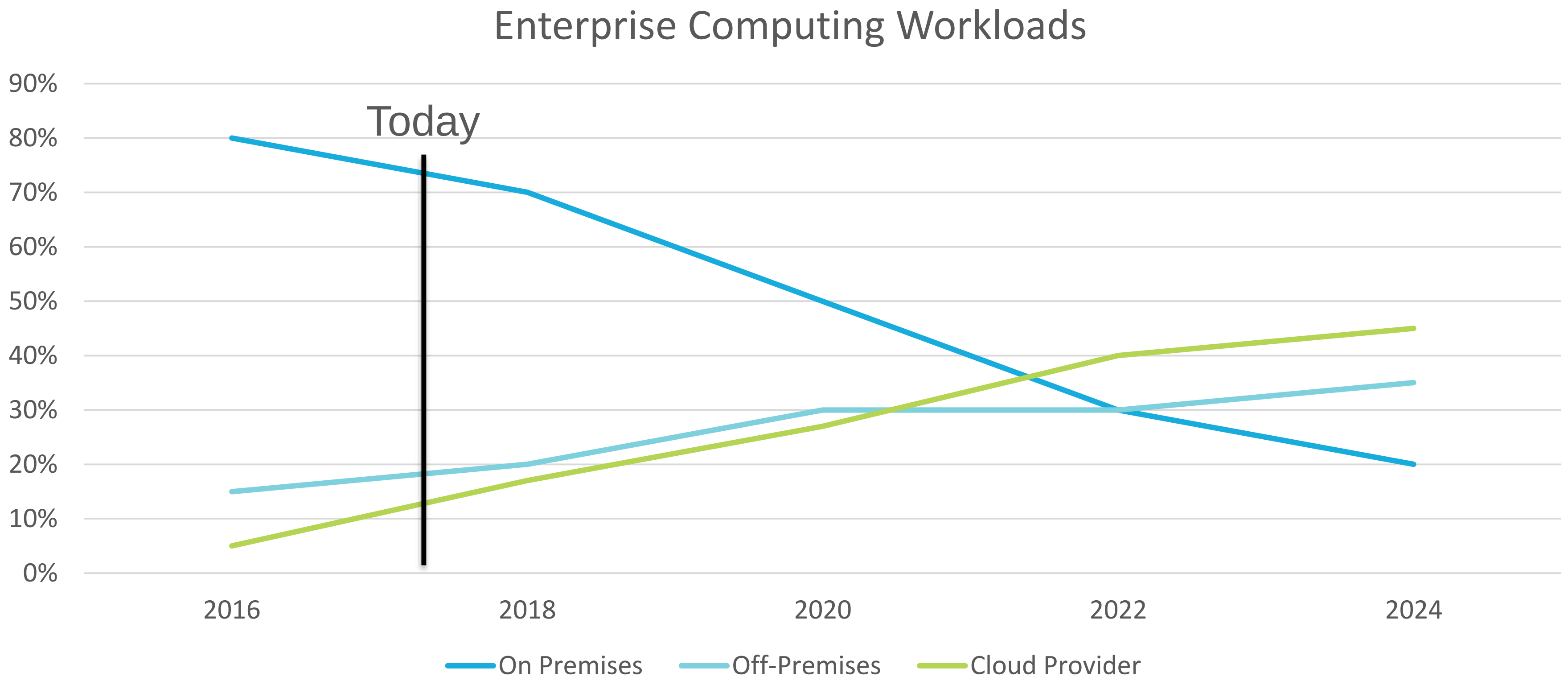
Google Cloud Platform

docker

By 2020, a Corporate "No-Cloud" Policy, Will Be as Rare as a "No-Internet" Policy Is Today.

— *Gartner*, 2016

Where's Your Data Going? Not Where It Is Today.



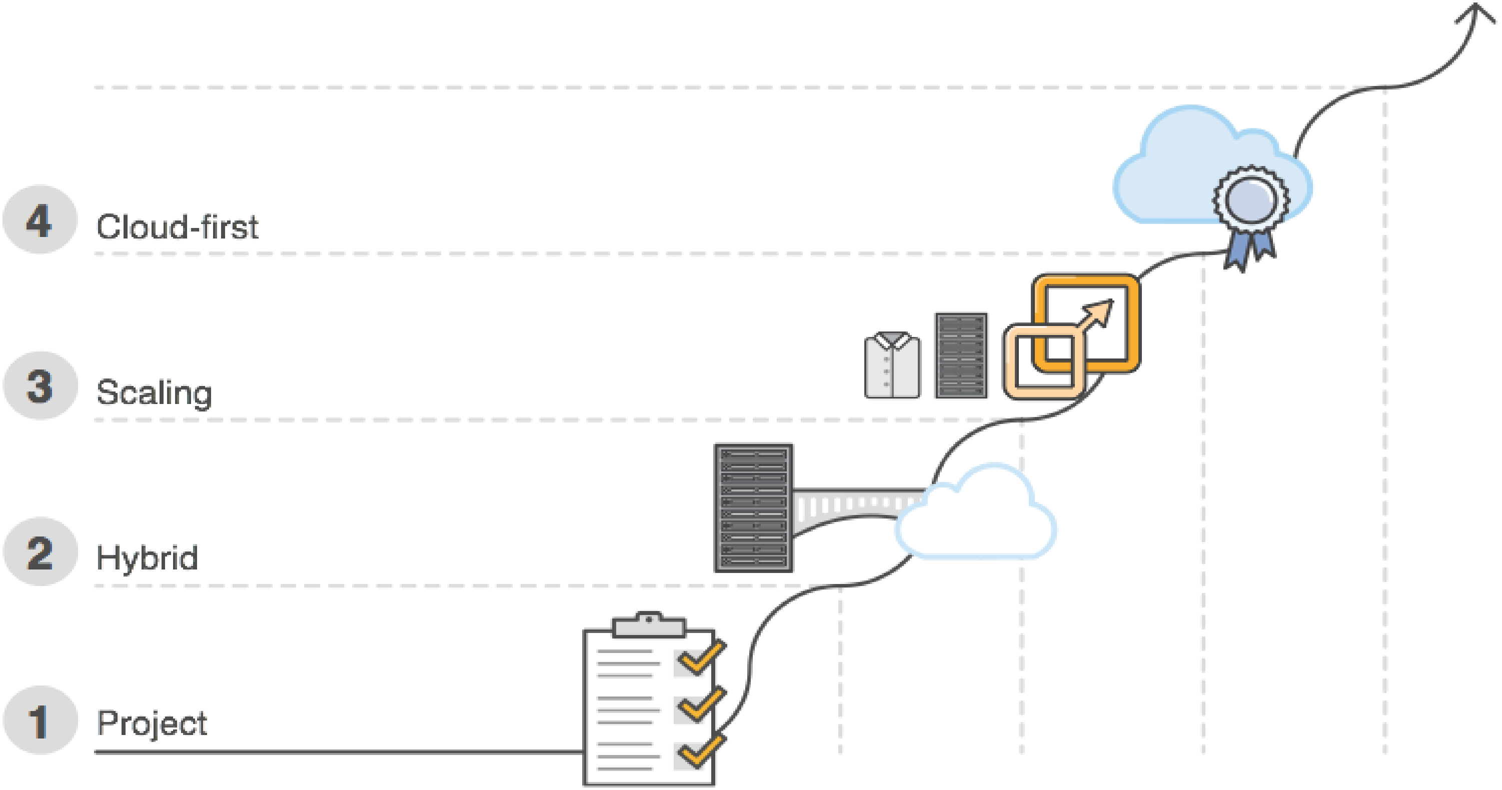
59% UK Businesses Use Cloud Services

67% store personal data relating to customers in the cloud

— Source: Cyber Security Breach Survey 2017

— HMG Department of Culture, Media and Sport. Sample 1,523 businesses

Journey to the Cloud



GDPR

May 2018

199 Days Away

We’re Safe
Right?

The Cloud is Secure, Right?

Yes, But – Reality Check!

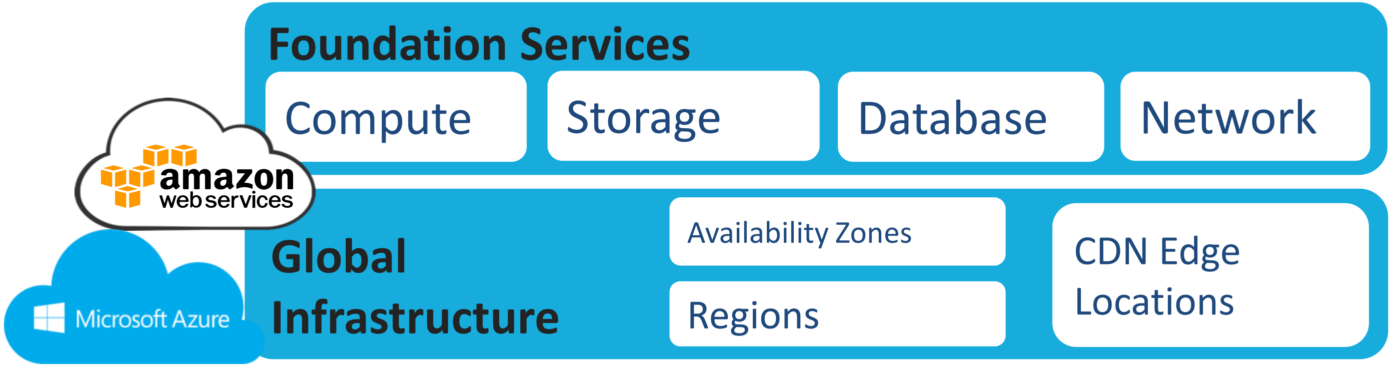
Cloud Security

#1 Priority

Source: AWS Cloud Security public slide deck

Cloud Security

- **SOC 1** (SSAE 16 & ISAE 3402) Type II
- **SOC 2 Type II** and public **SOC 3** report
- **ISO 27001**
- **ISO 9001**
- **PCI DSS Level 1** - Service Provider
- **ISO 27017** (security of the cloud)
- **ISO 27018** (personal data)



The Shared Responsibility Model

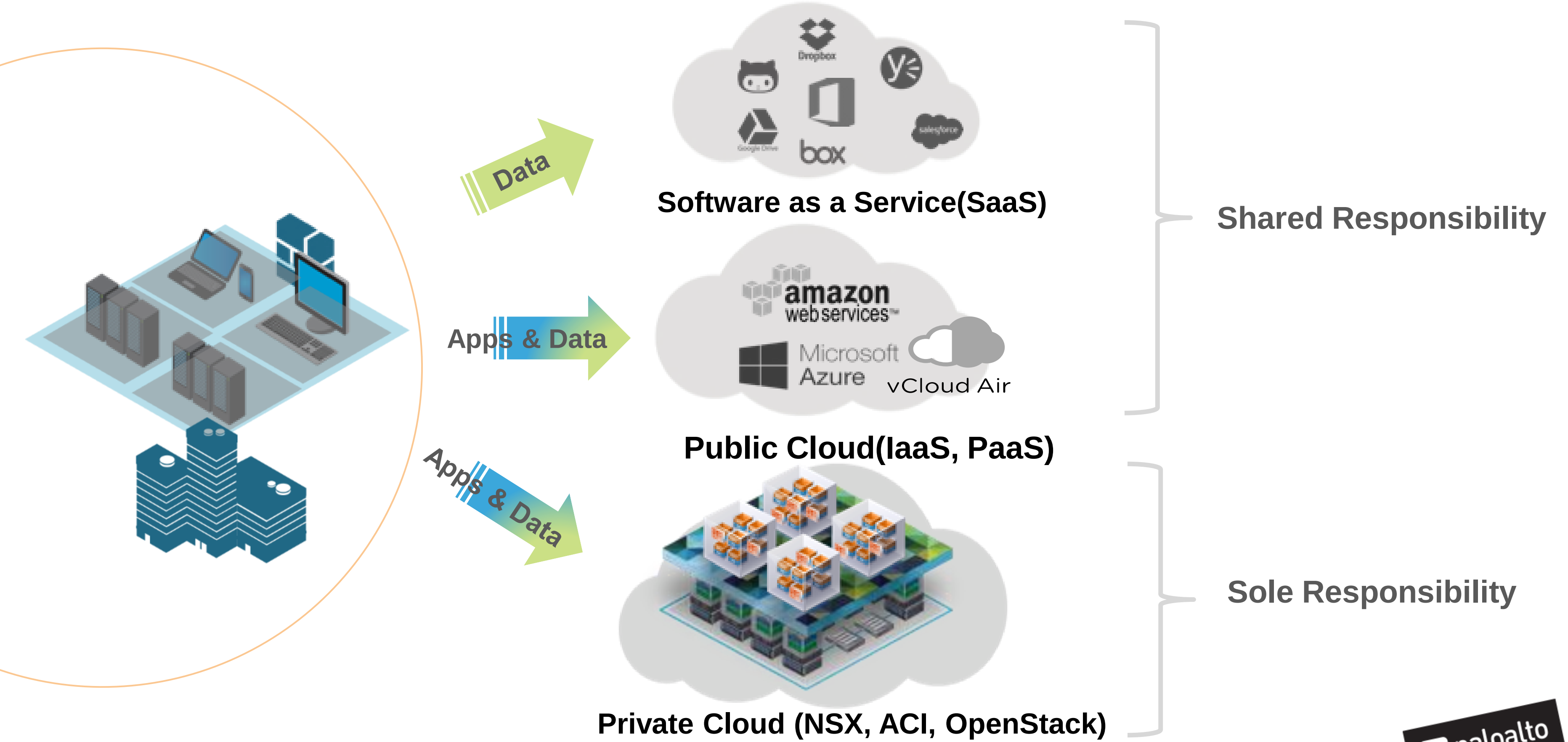
Security **(IN)** the Cloud

Managed by Customers, MSSP, or Partner

Security **(OF)** the Cloud

Managed by the Cloud Provider

Managing Risk Has Become More Complex



Data

Apps & Data

Apps & Data

Software as a Service(SaaS)

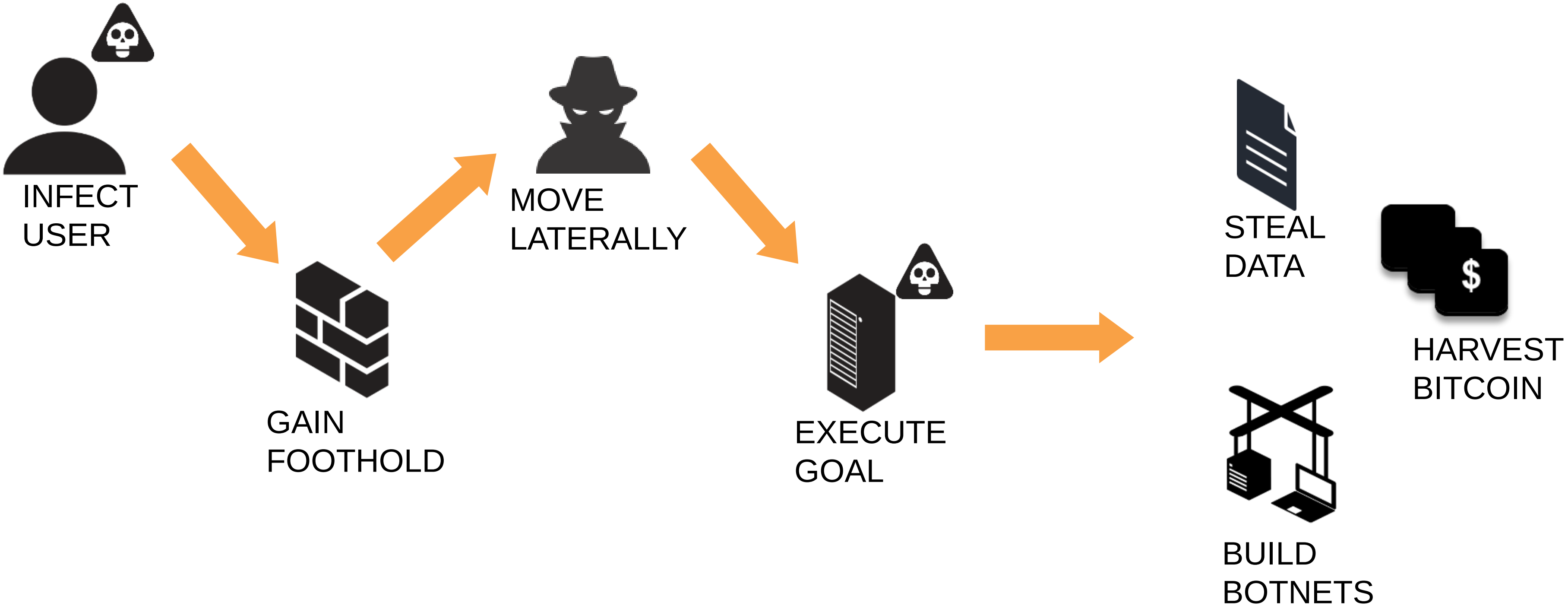
Public Cloud(IaaS, PaaS)

Private Cloud (NSX, ACI, OpenStack)

Shared Responsibility

Sole Responsibility

Are The Cloud Security Risks Different?



INFECT USER

GAIN FOOTHOLD

MOVE LATERALLY

EXECUTE GOAL

STEAL DATA

HARVEST BITCOIN

BUILD BOTNETS

Cloud Has Some Greater Areas of Risk!

MALWARE PROPAGATION

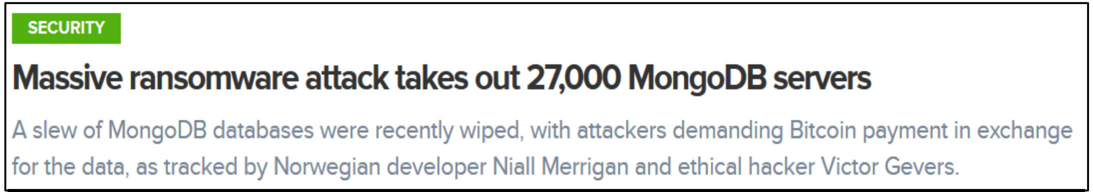
COLLABORATION
IT UPDATES etc.

ACCIDENTAL DATA EXPOSURE

USER ERROR
MISCONFIGURATION

MALICIOUS DATA EXFILTRATION

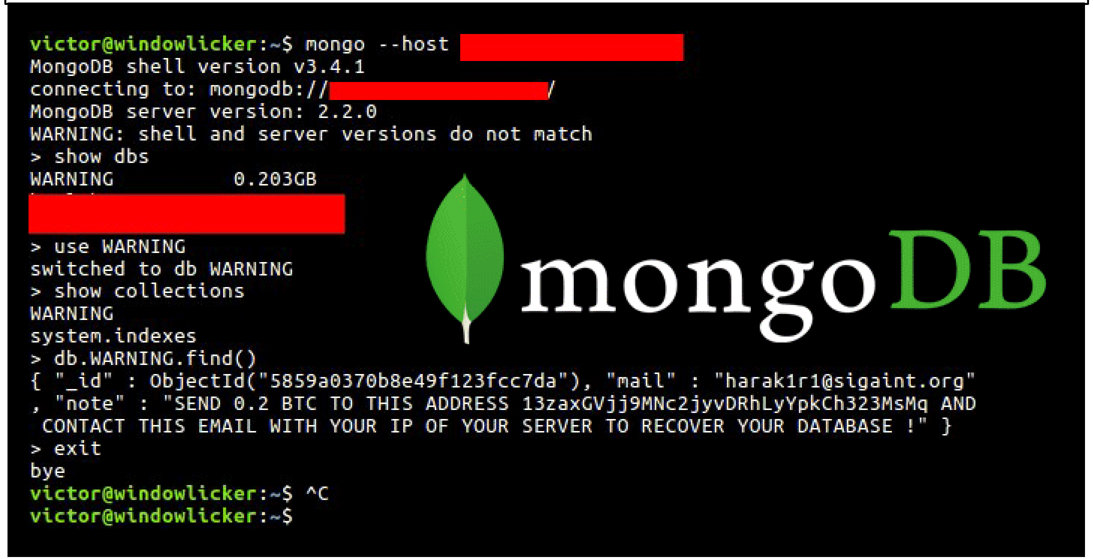
General
Data
Protection
Regulation



SECURITY

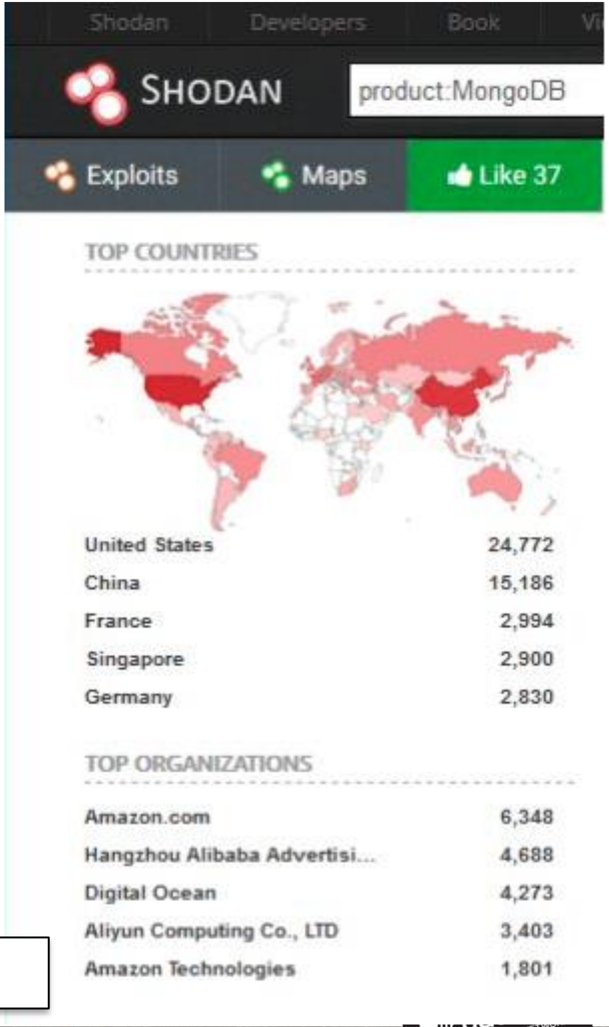
Massive ransomware attack takes out 27,000 MongoDB servers

A slew of MongoDB databases were recently wiped, with attackers demanding Bitcoin payment in exchange for the data, as tracked by Norwegian developer Niall Merrigan and ethical hacker Victor Gevers.



```
victor@windowlicker:~$ mongo --host [redacted]
MongoDB shell version v3.4.1
connecting to: mongodb://[redacted]/
MongoDB server version: 2.2.0
WARNING: shell and server versions do not match
> show dbs
WARNING           0.203GB
[redacted]
> use WARNING
switched to db WARNING
> show collections
WARNING
system.indexes
> db.WARNING.find()
{ "_id" : ObjectId("5859a0370b8e49f123fcc7da"), "mail" : "harak1r1@sigaint.org"
, "note" : "SEND 0.2 BTC TO THIS ADDRESS 13zaxGVjj9MNc2jyvDRhLyYpkCh323MsMq AND
 CONTACT THIS EMAIL WITH YOUR IP OF YOUR SERVER TO RECOVER YOUR DATABASE !" }
> exit
bye
victor@windowlicker:~$ ^C
victor@windowlicker:~$
```

Issue: Running on default ports (27017, ..) and by default authentication is not required



TOP COUNTRIES

United States	24,772
China	15,186
France	2,994
Singapore	2,900
Germany	2,830

TOP ORGANIZATIONS

Amazon.com	6,348
Hangzhou Alibaba Advertisi...	4,688
Digital Ocean	4,273
Aliyun Computing Co., LTD	3,403
Amazon Technologies	1,801

Estimated 26,000 new victims in September 2017

What Happens When Cloud Storage is Not Secured?

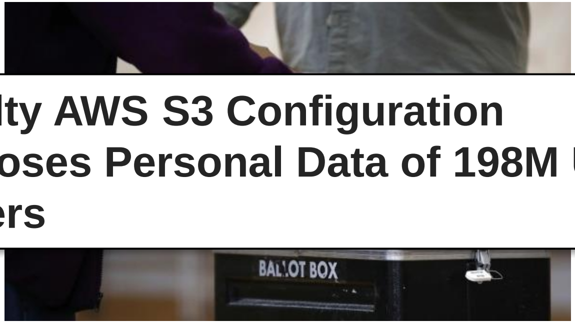
May 2017

Top Defense Contractor Left Sensitive Pentagon Files on Amazon Server With No Password

What happened?

- **Publically Accessible** Amazon S3 bucket
- Leaked by Defense Contractor
- 60K files, 28GB of data, unencrypted passwords

June 2017

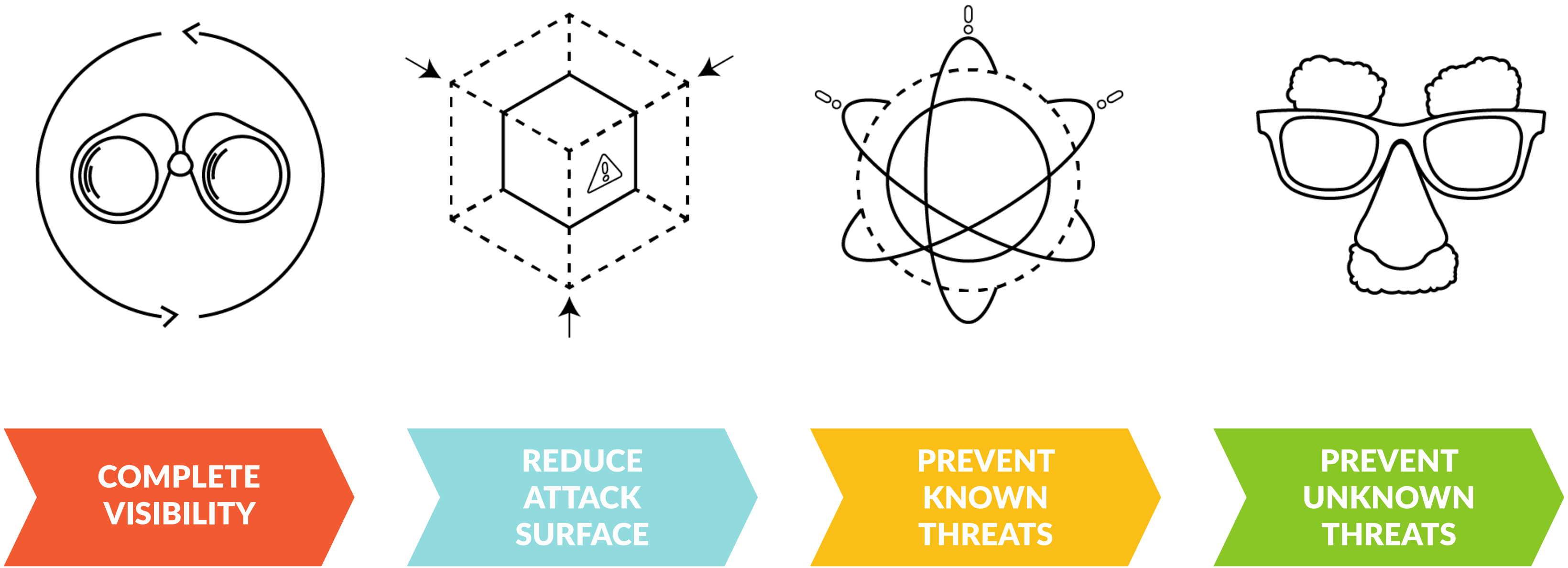


Faulty AWS S3 Configuration Exposes Personal Data of 198M U.S. Voters

What happened?

- **Unsecured** Amazon S3 bucket
- 1.1 TB of personal voter data including names, addresses etc.

Prevention Security framework



COMPLETE VISIBILITY

REDUCE ATTACK SURFACE

PREVENT KNOWN THREATS

PREVENT UNKNOWN THREATS

Consistent Security Across ALL Locations

COMPLETE VISIBILITY

REDUCE ATTACK SURFACE

PREVENT KNOWN THREATS

PREVENT UNKNOWN THREATS

Internet Gateway

Datacenter/ Private Cloud

Public Cloud

SaaS

Mobile Users

Endpoint

IoT

At What Stage is Your Organisation?

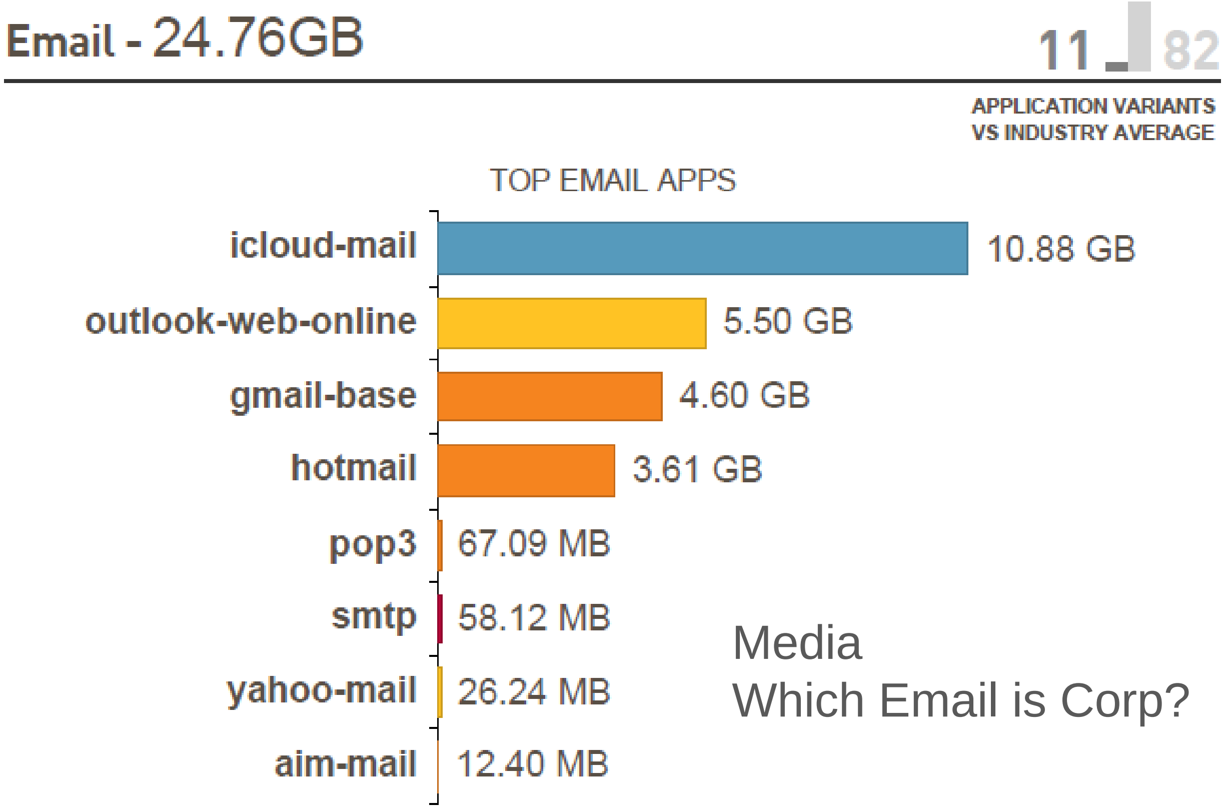
INVESTIGATING
PUBLIC CLOUD

MOVING ENTERPRISE
APPLICATIONS TO
PUBLIC CLOUD

DATACENTER
RETIREMENT

MS &
AWS
Focus

Do You Have Visibility of Cloud?



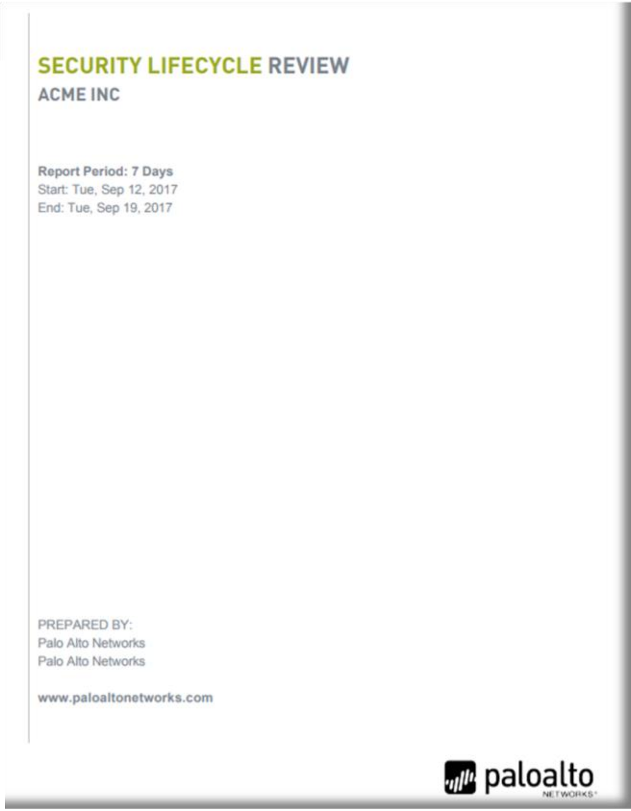
Email - 24.76GB

11 82

APPLICATION VARIANTS
VS INDUSTRY AVERAGE

TOP EMAIL APPS

Media
Which Email is Corp?



SECURITY LIFECYCLE REVIEW
ACME INC

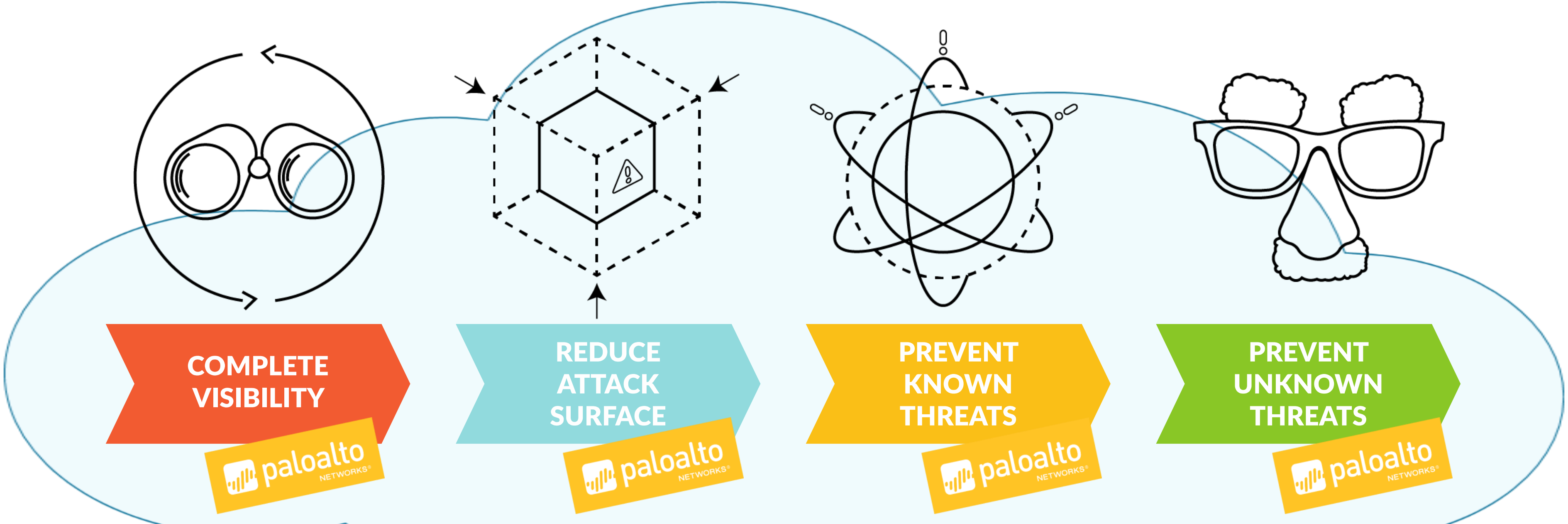
Report Period: 7 Days
Start: Tue, Sep 12, 2017
End: Tue, Sep 19, 2017

PREPARED BY:
Palo Alto Networks
Palo Alto Networks

www.paloaltonetworks.com

paloalto NETWORKS

GDPR Also Applies To Your Data In The Cloud



COMPLETE VISIBILITY

REDUCE ATTACK SURFACE

PREVENT KNOWN THREATS

PREVENT UNKNOWN THREATS

General
Data
Protection
Regulation

It’s YOUR Responsibility!

Don’t Get Caught Out.

paloalto
NETWORKS®