Anatomy of an Attack

Government of BC – Security Day

Chris Parker-James – Consulting Systems Engineer

May 23rd 2018

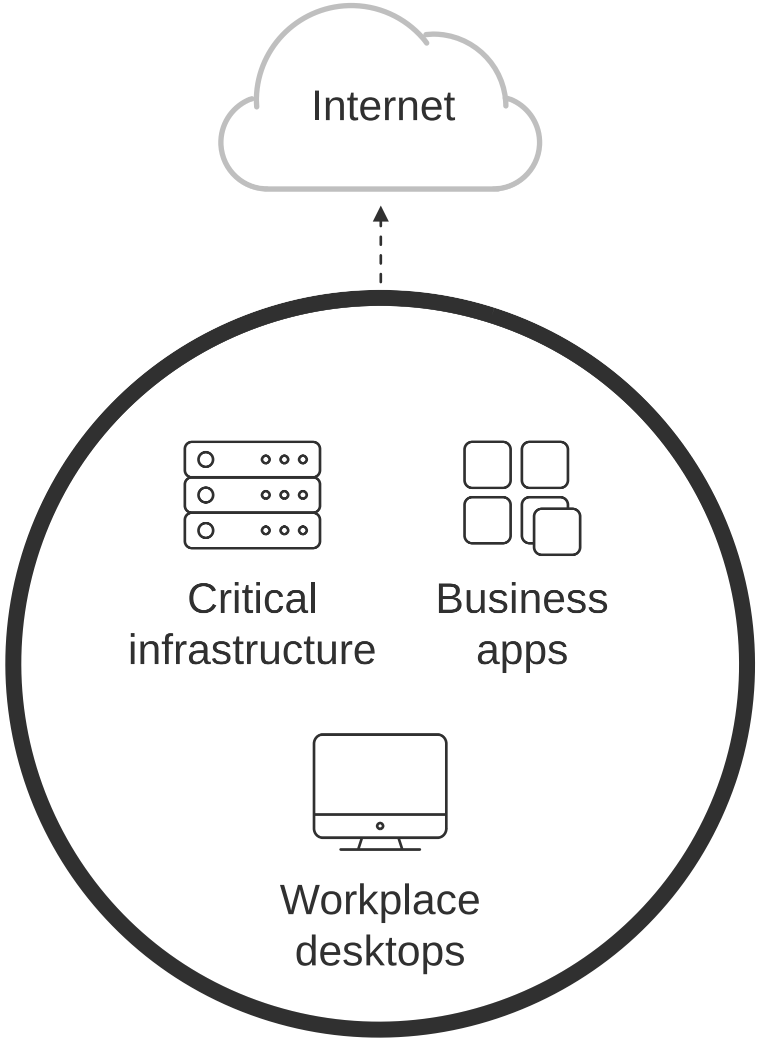
Agenda

- Cloud security challenges
- Attack: Ransomware
- Attack: OAuth
- Securing access to the cloud
- Securing cloud services
- Q & A

© 2018 Cisco and/or its affiliates. All rights reserved.

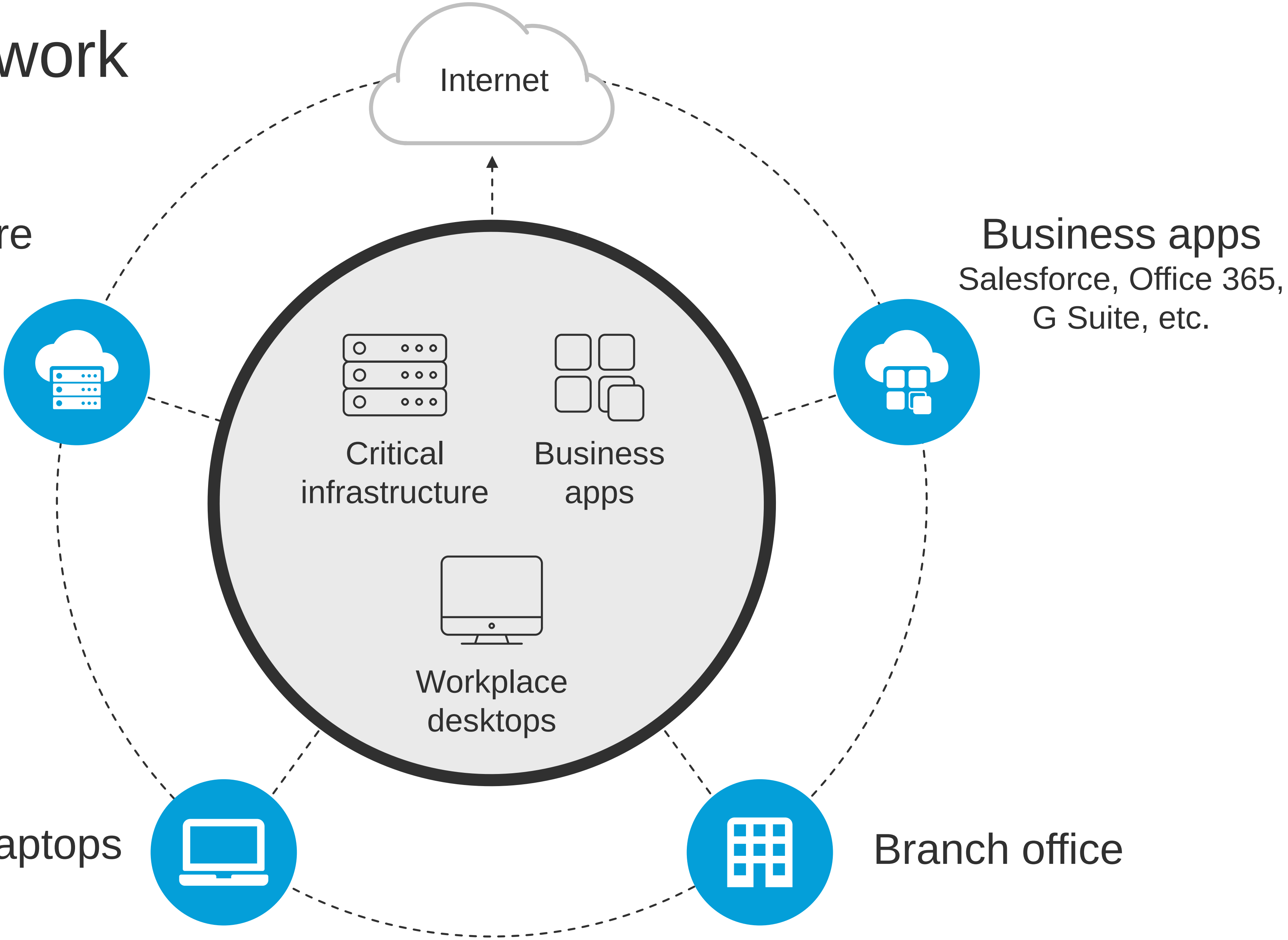
Cloud security challenges

How IT was built



© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The way we work has changed



© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Users and apps have adopted the cloud , security must too

49%
of the workforce is mobile

82%
admit to not using the VPN

70%
increase in SaaS usage

70%
of branch offices have DIA

Security controls must shift to the cloud

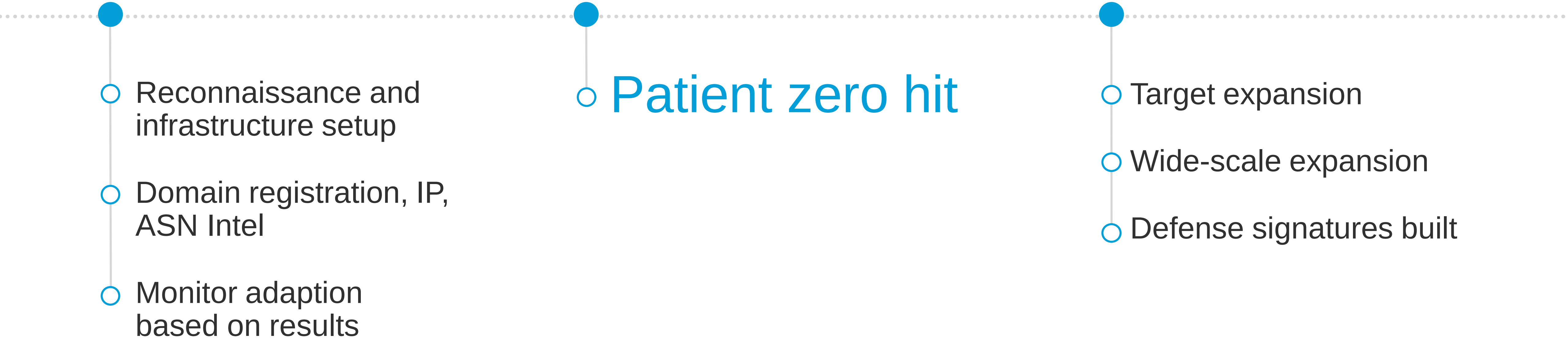
© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Today’s cloud security challenges

- Malware and ransomware
- Gaps in visibility and coverage
- Cloud apps and shadow IT
- Difficult to manage security

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Anatomy of a cyber attack



- Reconnaissance and infrastructure setup
- Domain registration, IP, ASN Intel
- Monitor adaption based on results

Patient zero hit

- Target expansion
- Wide-scale expansion
- Defense signatures built

© 2016 Cisco and/or its affiliates. All rights reserved.

Attack: Ransomware

Ransomware

Malicious Software

Encrypts Critical Data

Demands Payment

© 2018 Cisco and/or its affiliates. All rights reserved.

Business Impacts

- Permanent Data Loss
- Operational Downtime
- Reputation Damage

© 2018 Cisco and/or its affiliates. All rights reserved.

Did You Know?

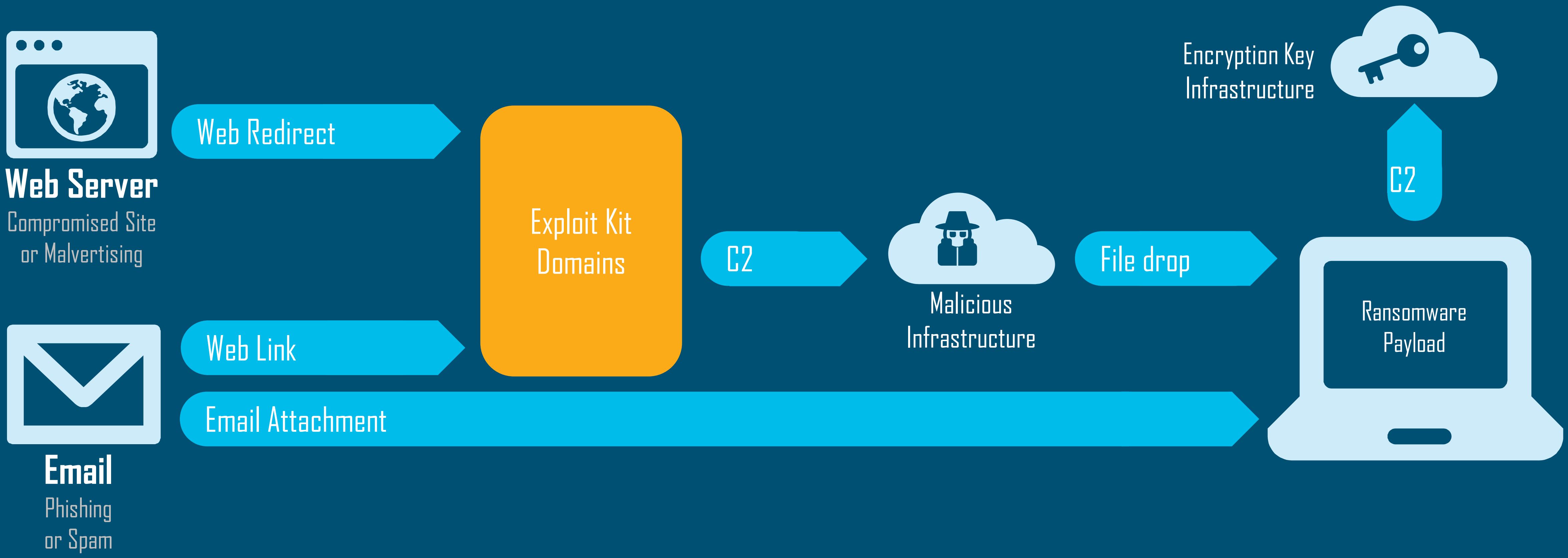
Over 99%

of malware is sent by either

web server or email

© 2018 Cisco and/or its affiliates. All rights reserved.

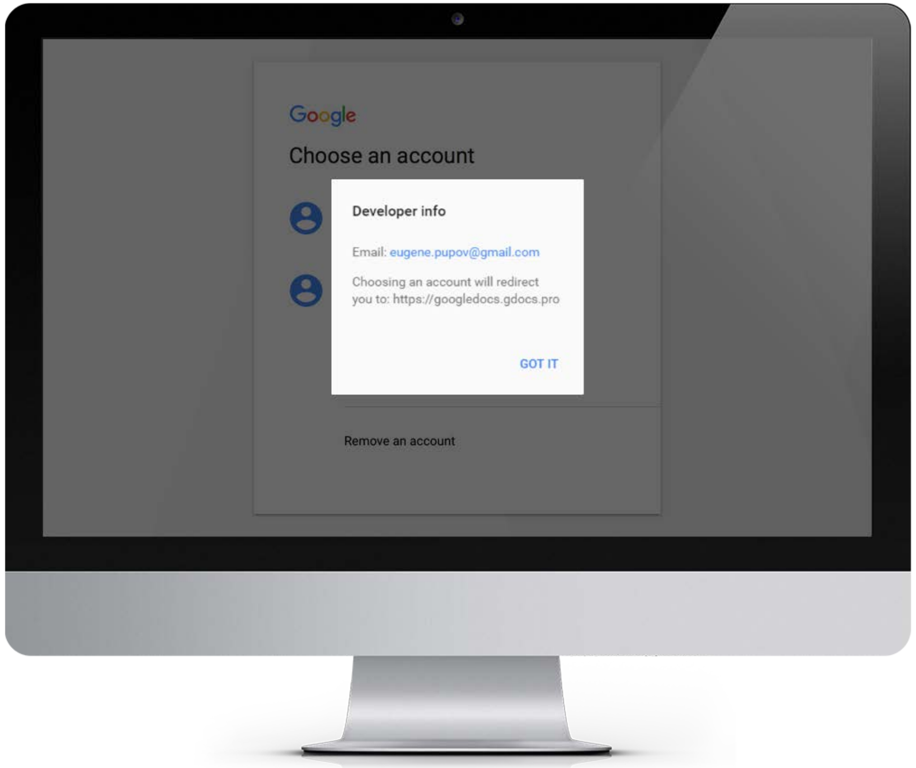
Ransomware Email and Web Delivery



© 2018 Cisco and/or its affiliates. All rights reserved.

Attack: OAuth

The attack itself is very simple



Google

Choose an account

Developer info

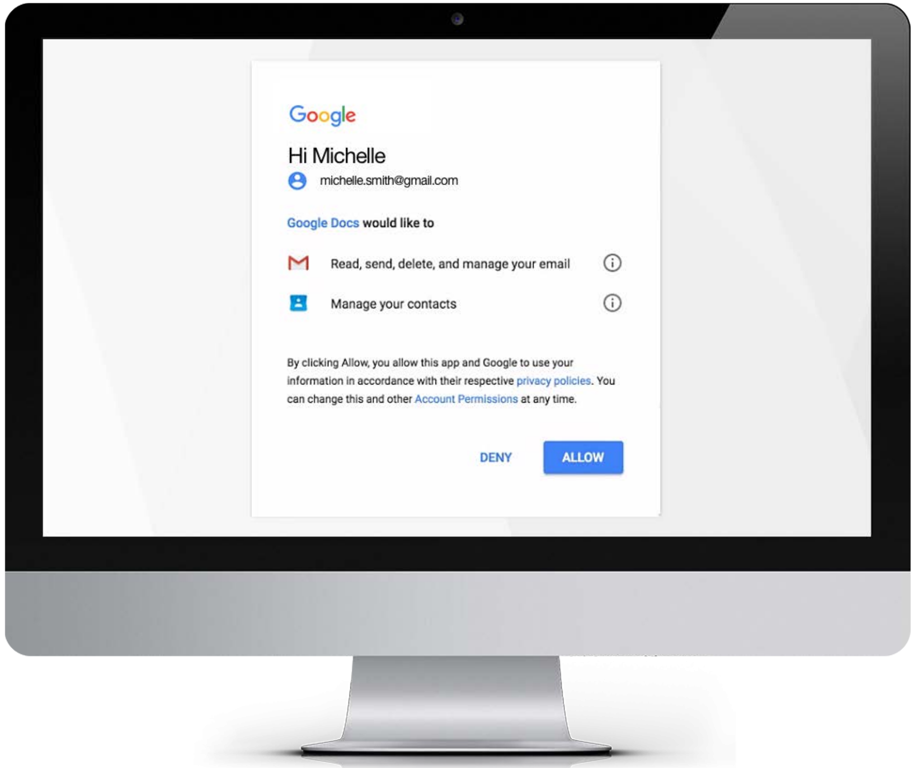
Email: eugene.pupov@gmail.com

Choosing an account will redirect you to: https://googledocs.gdocs.pro

GOT IT

Remove an account

Attacker created an app listing on Google



Google

Hi Michelle

michelle.smith@gmail.com

Google Docs would like to

- Read, send, delete, and manage your email
- Manage your contacts

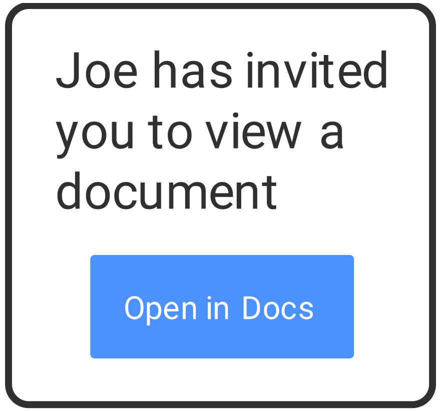
By clicking Allow, you allow this app and Google to use your information in accordance with their respective privacy policies. You can change this and other Account Permissions at any time.

DENY ALLOW

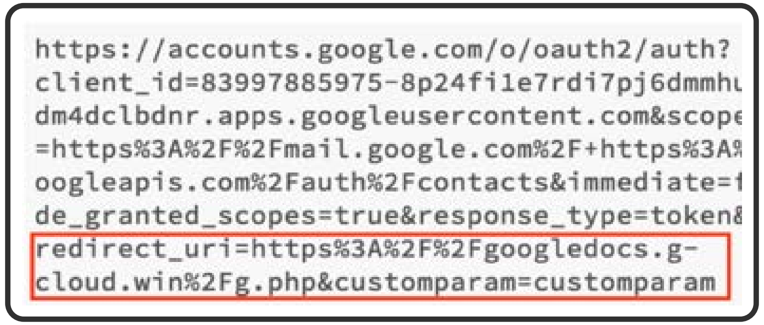
Recipient authorized the app

© 2016 Cisco and/or its affiliates. All rights reserved.

Sequence of events (1 of 2)



Joe has invited you to view a document



```
https://accounts.google.com/o/oauth2/auth?
client_id=83997885975-8p24fi1e7rdi7pj6dmmhu
dm4dclbdnr.apps.googleusercontent.com&scope
=https%3A%2F%2Fmail.google.com%2F+https%3A%
oogleapis.com%2Fauth%2Fcontacts&immediate=f
de_granted_scopes=true&response_type=token&
redirect_uri=https%3A%2F%2Fgoogledocs.g-
cloud.win%2Fg.php&customparam=customparam
```

1

Attacker
sets up infrastructure and fake app; sends phishing email

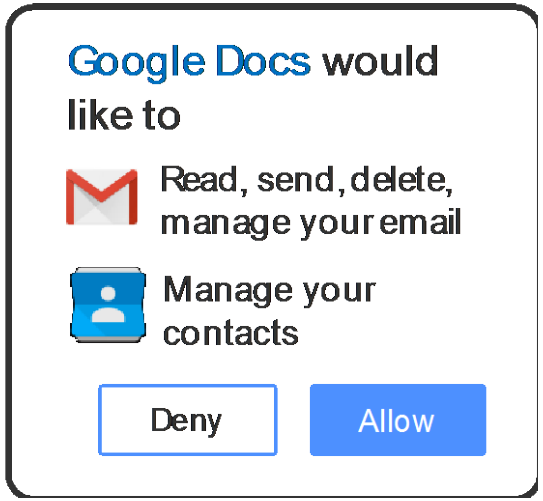
2

Victim
opens email and clicks link

Victim is sent to Google's OAuth page for authentication and to grant permissions. Then the user will be redirected to an attacker-controlled website

© 2016 Cisco and/or its affiliates. All rights reserved.

Sequence of events (2 of 2)



Google Docs would like to

Read, send, delete, manage your email

Manage your contacts

3

Victim
prompted to allow/deny access

4

On the backend…
If allowed, Google provisions an OAuth token, appends it to redirect_uri, and instructs victim's browser to redirect to attacker's domain

g-cloud[.]win

5

Attacker
gains access to OAuth token once the user is redirected to one of the attacker-controlled domains

Note: users were redirected to these domains whether they clicked Deny or Allow

6

Attacker
uses the **granted privileges** (email contacts, delete emails, etc.)

Uses access to send emails from victim's account and **propagate the worm**

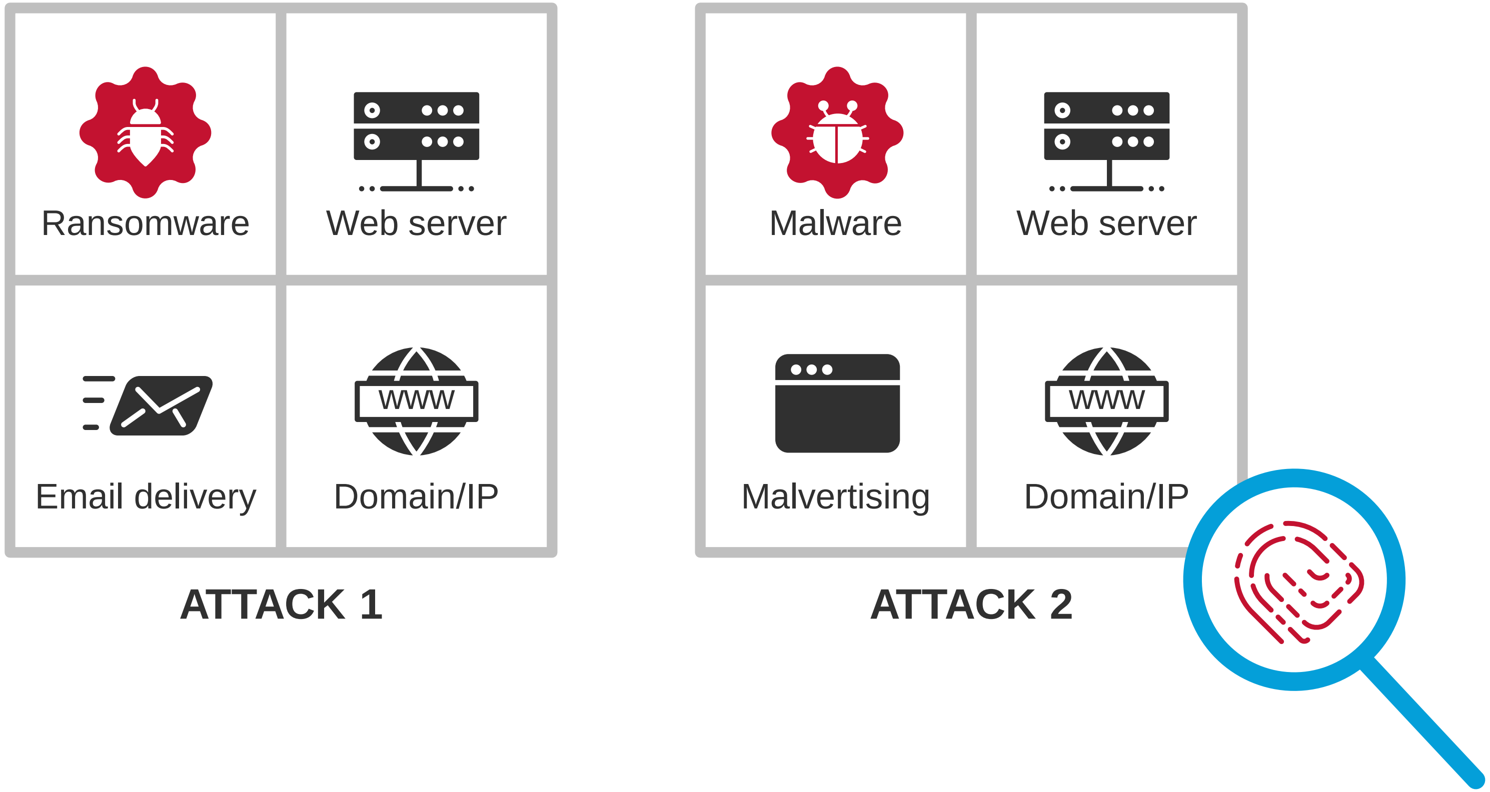
© 2016 Cisco and/or its affiliates. All rights reserved.

Securing access to the cloud

Malware doesn't just happen

Intelligence to see attacks before launched

Build. Test. Launch. Repeat.



© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Prevents connections before and during the attack

Web and email-based infection

Malvertising / exploit kit

Phishing / web link

Watering hole compromise

Command and control callback

Malicious payload drop

Encryption keys

Updated instructions

Stop data exfiltration and ransomware encryption

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Securing cloud services

Key questions organizations have

Users/Accounts

- Who is doing what in my cloud applications?
- How do I detect account compromises?
- Are malicious insiders extracting information?

1 0 1 1
0 1 0 1
1 0 1 0

Data

- Do I have toxic and regulated data in the cloud?
- Do I have data that is being shared inappropriately?
- How do I detect policy violations?

Applications

- How can I monitor app usage and risk?
- Do I have any 3rd party connected apps?
- How do I revoke risky apps?

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Areas of focus

Discover and Control

Compromised Accounts

Insider Threats

User and Entity Behavior Analytics

Data Exposures and Leakages

Privacy and Compliance Violations

1011
0101
1010 Cloud Data Loss Prevention (DLP)

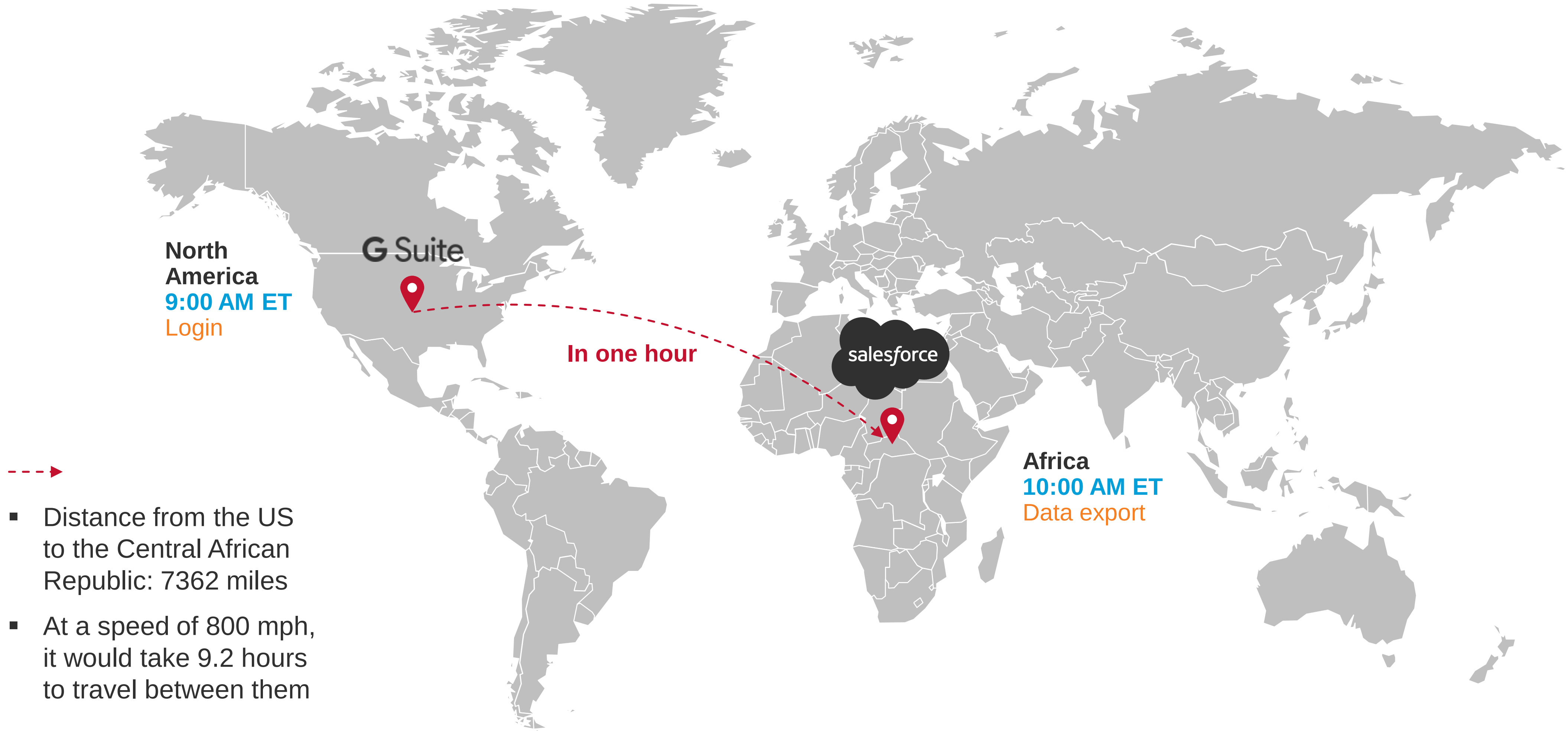
Cloud Malware

Shadow IT/OAuth Discovery and Control

3rd Party Cloud Apps

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cloud security awareness



- Distance from the US to the Central African Republic: 7362 miles
- At a speed of 800 mph, it would take 9.2 hours to travel between them

Cisco Umbrella

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Have you ever been to 68 countries in one week?

Cisco Umbrella

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Cloudlock addresses customers' most critical cloud security use cases

Discover and Control

Compromised Accounts

Insider Threats

User and Entity Behavior Analytics

Data Exposures and Leakages

Privacy and Compliance Violations

1011
0101
1010 Cloud Data Loss Prevention (DLP)

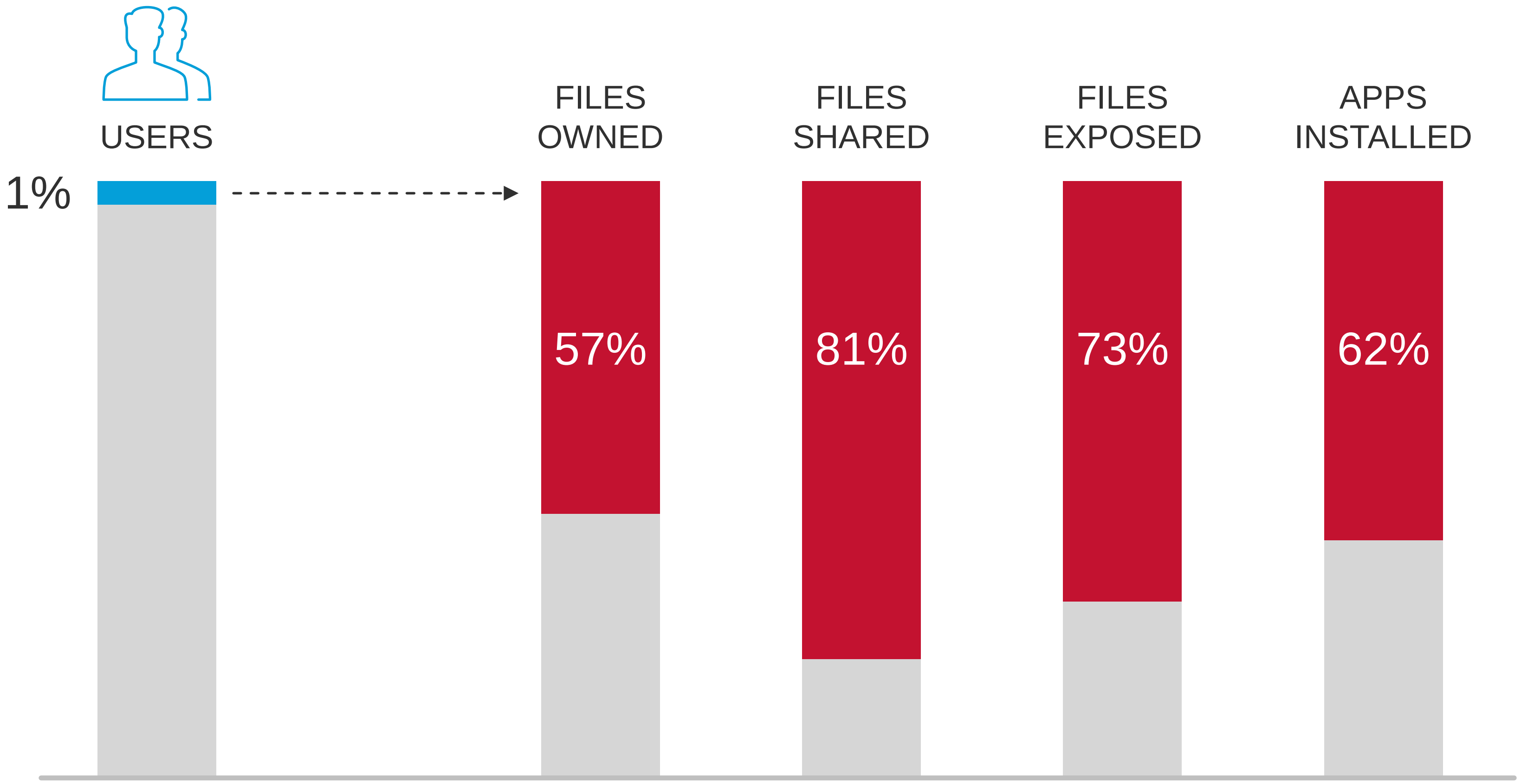
Cloud Malware

Shadow IT/OAuth Discovery and Control

3rd Party Cloud Apps

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Disproportionate cloud risk in cloud data

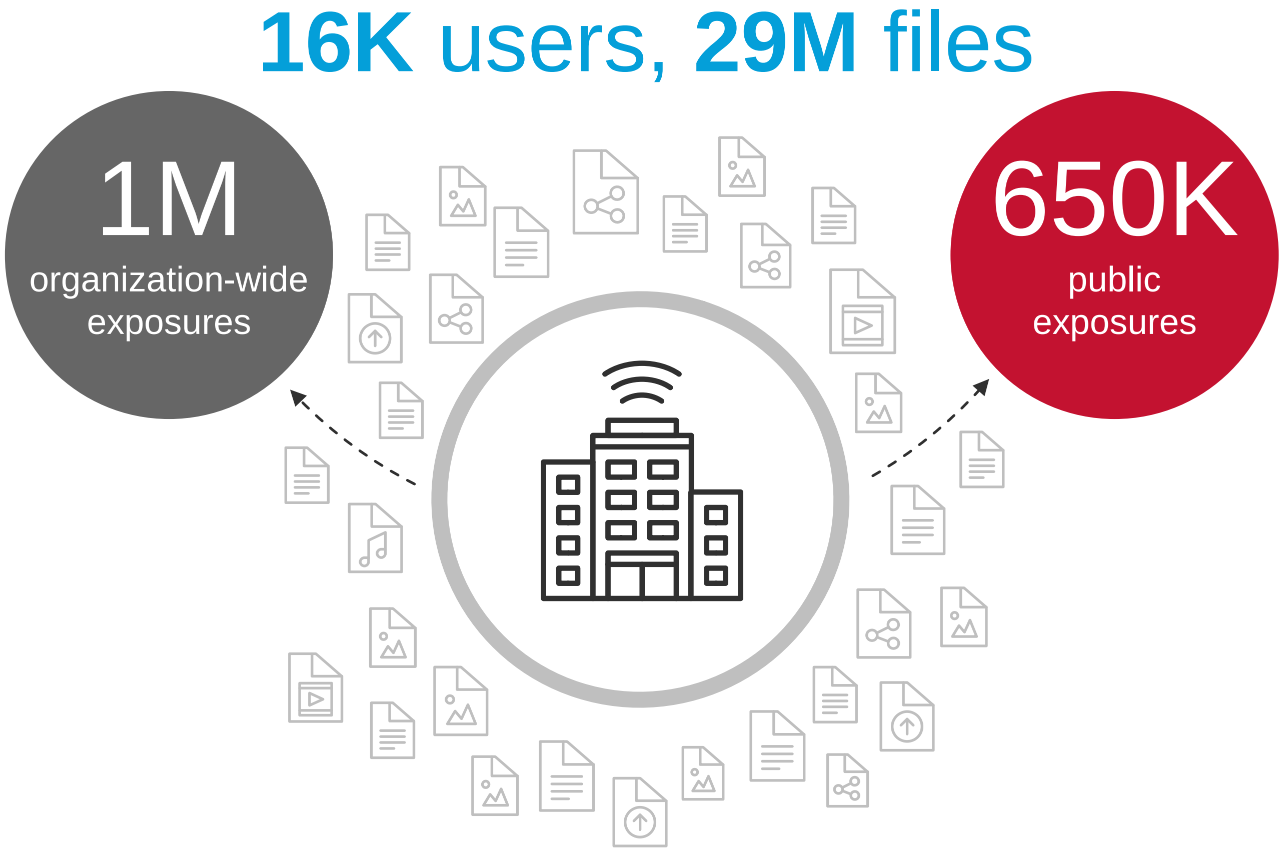


Source: Cloudlock CyberLab

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

CASE STUDY

The true risk of dense data users



Hi-Tech customer based in the Silicon Valley

Highly confidential IP

Design docs

Patents

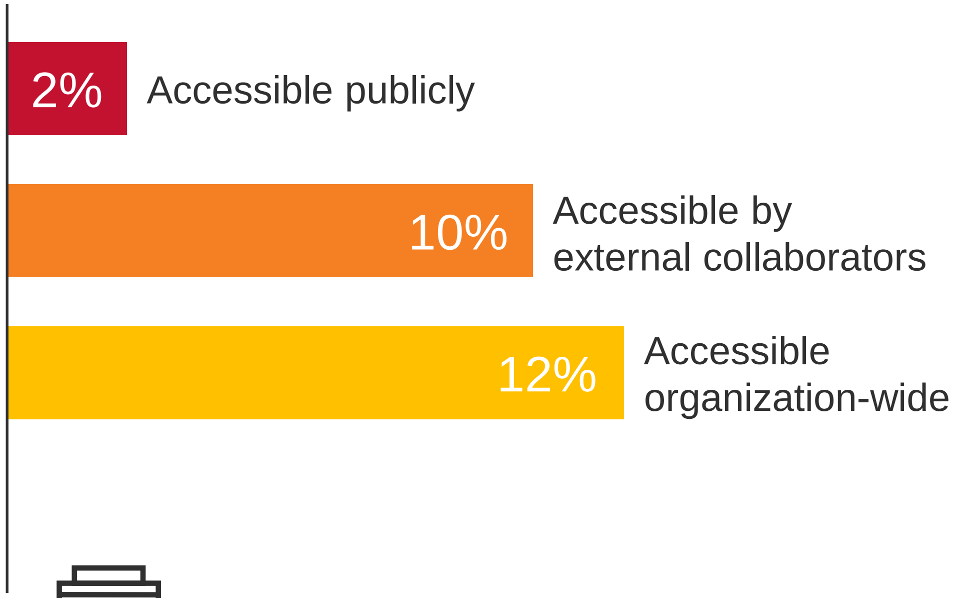
Engineering code

Cisco Umbrella

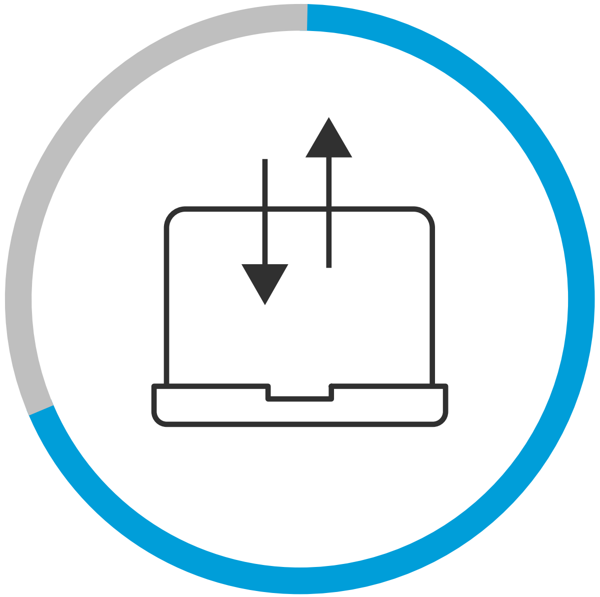
© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

More than 24,000 files per organization publicly accessible

Data exposure per organization



24,000 files
publicly accessible per organization



70% of external sharing done with non-corporate email addresses

Source: Cloudlock CyberLab

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Cloudlock addresses customers’ most critical cloud security use cases

Discover and Control

Compromised Accounts

Insider Threats

User and Entity Behavior Analytics

Data Exposures and Leakages

Privacy and Compliance Violations

1011 0101 1010 Cloud Data Loss Prevention (DLP)

Cloud Malware

Shadow IT/OAuth Discovery and Control

3rd Party Cloud Apps

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Hackers are exploiting a cloud protocol called OAuth

GOOGLE PHISHING ATTACK

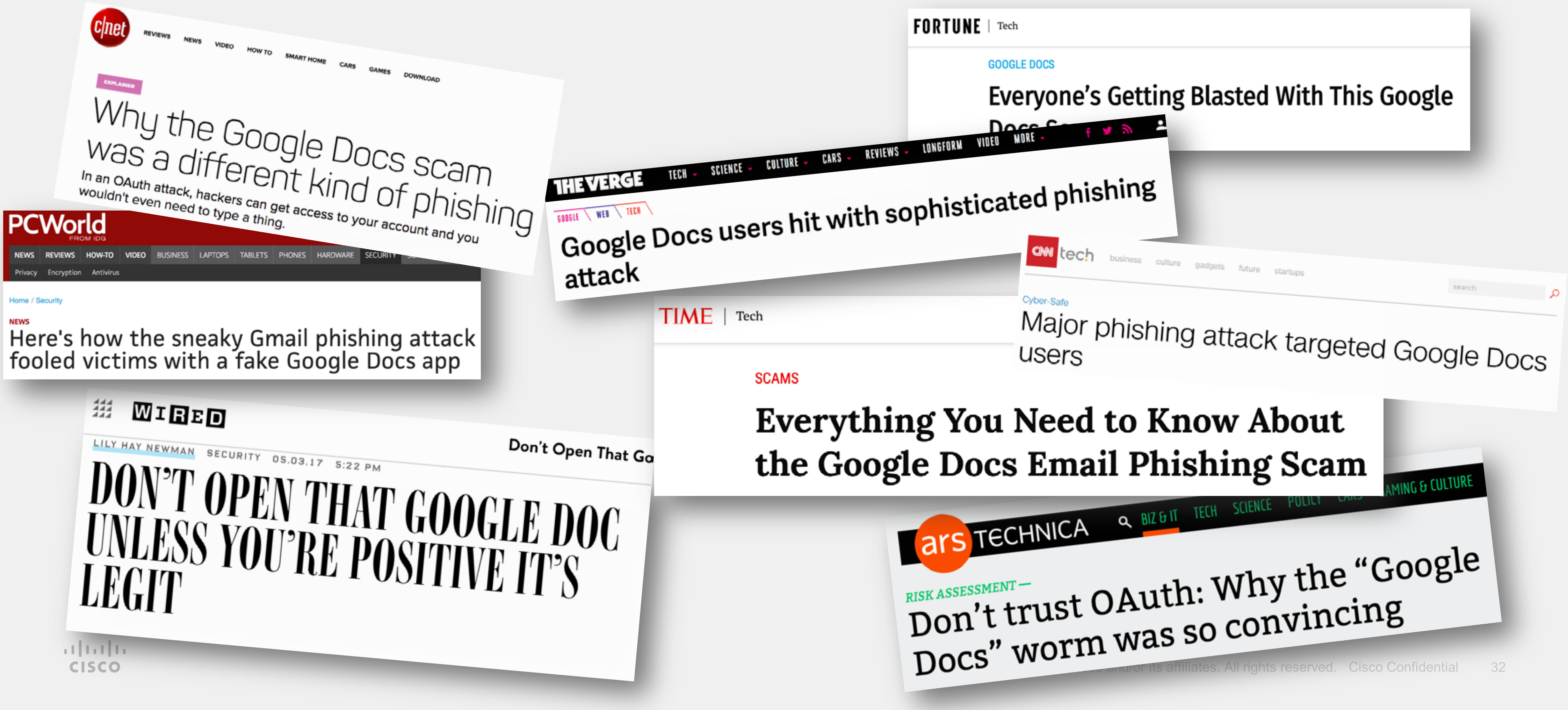
FANCY BEAR/PAWN STORM

1 MILLION+ ACCOUNTS COMPROMISED

WITHIN **2 HOURS**

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

These recent attacks were headline news globally



Why the Google Docs scam was a different kind of phishing

In an OAuth attack, hackers can get access to your account and you wouldn't even need to type a thing.

Here's how the sneaky Gmail phishing attack fooled victims with a fake Google Docs app

LILY HAY NEWMAN SECURITY 05.03.17 5:22 PM

DON'T OPEN THAT GOOGLE DOC UNLESS YOU'RE POSITIVE IT'S LEGIT

Everyone's Getting Blasted With This Google Docs S

Google Docs users hit with sophisticated phishing attack

Major phishing attack targeted Google Docs users

Everything You Need to Know About the Google Docs Email Phishing Scam

Don't trust OAuth: Why the "Google Docs" worm was so convincing

The potential for damages is staggering given the number of people and organizations that are using cloud services

SAAS DEPLOYMENTS

account for 50% new software implementations, according to Gartner

G Suite

Used by more than 3 million paying businesses,

Office 365

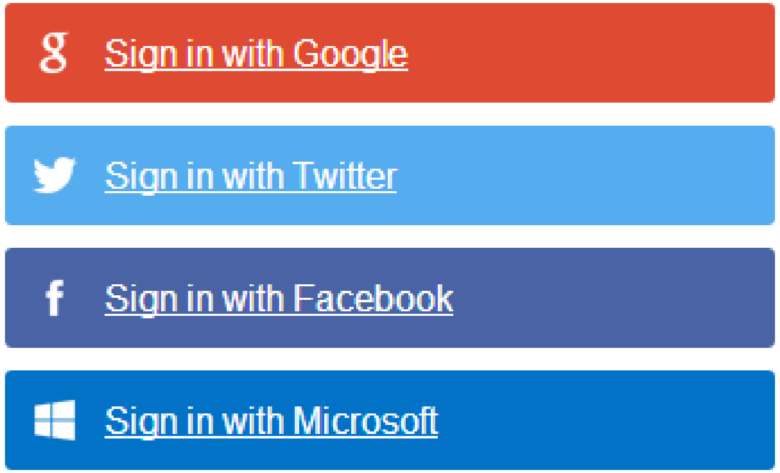
100 million users, adding 2.5 million new users per month

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

What is OAuth (Open Authorization)?

OAuth, or open standard for authorization, is a standardized way for internet accounts to link with third-party applications. It is universally adopted by almost all web-based applications and platforms – including consumer as well as enterprise applications such as Google Apps, Microsoft Office 365, Salesforce, and many others.

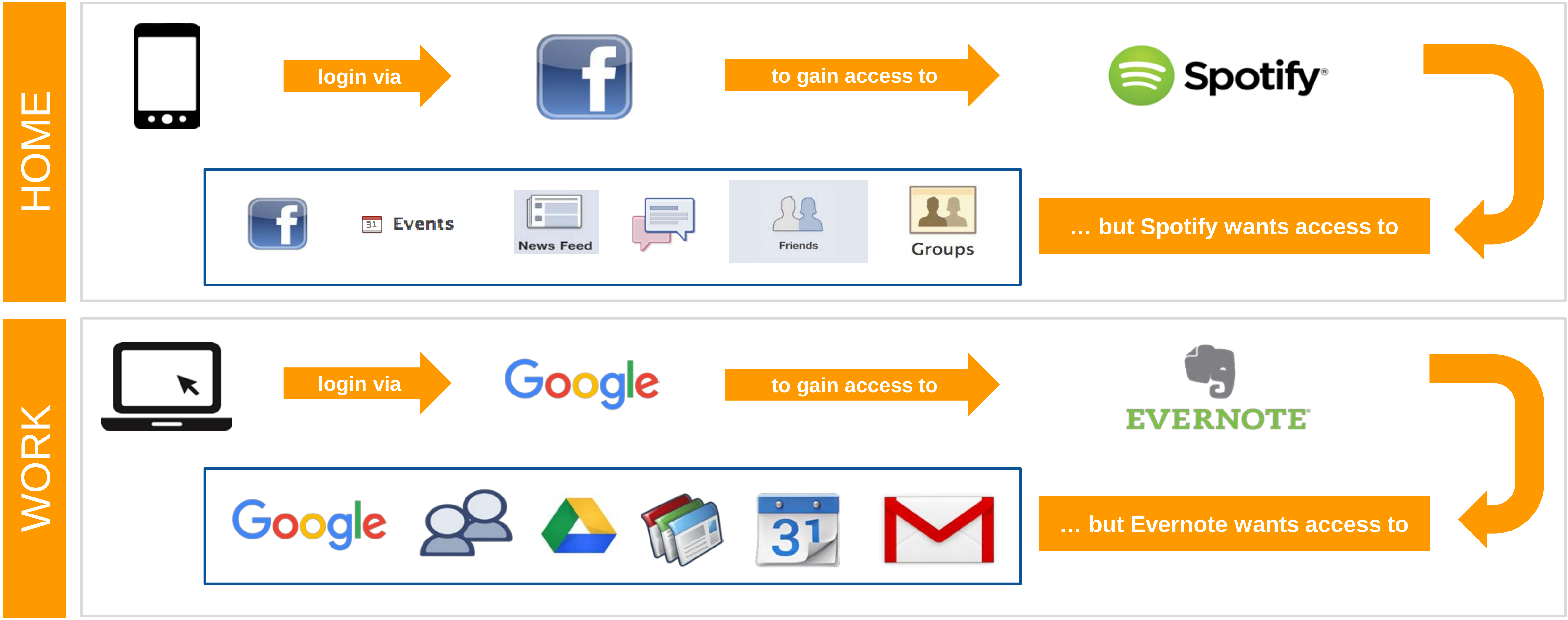
Nearly everyone uses OAuth, knowingly or not



Have you ever used buttons like these?

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

OAuth enables the cloud both at home and at work



HOME

login via

to gain access to

… but Spotify wants access to

WORK

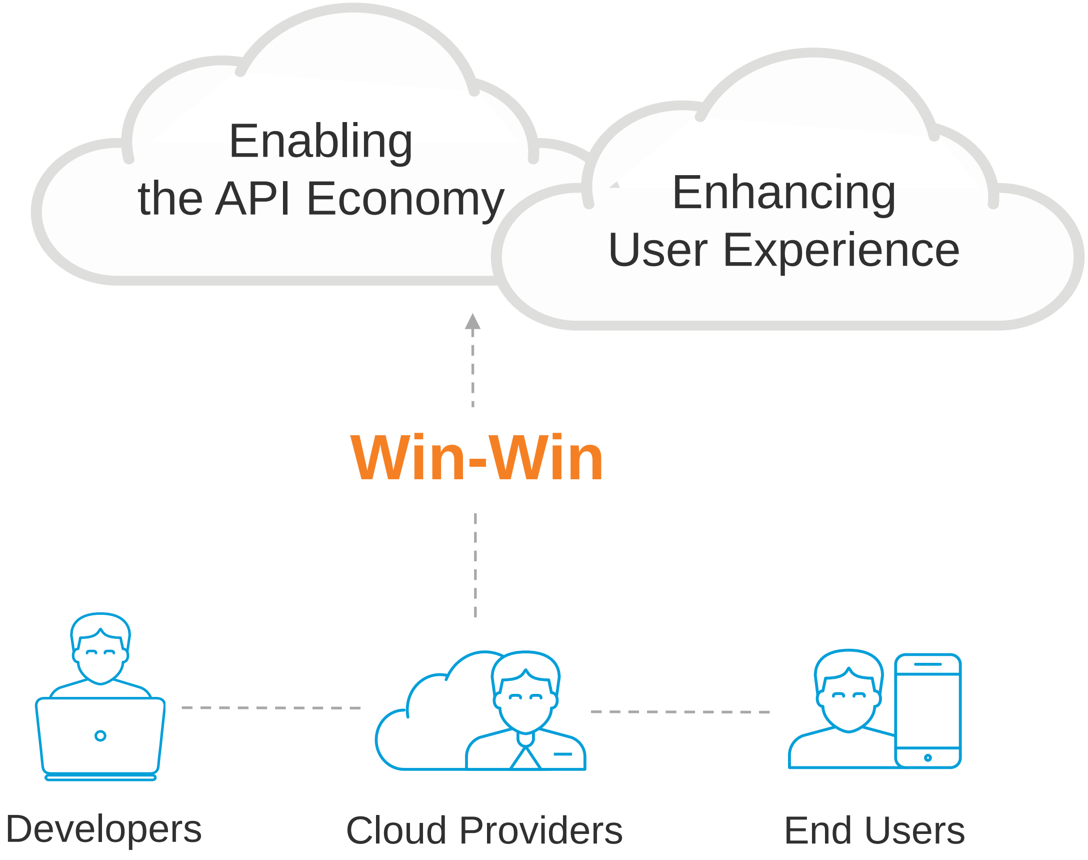
login via

to gain access to

… but Evernote wants access to

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

OAuth Powers the Cloud



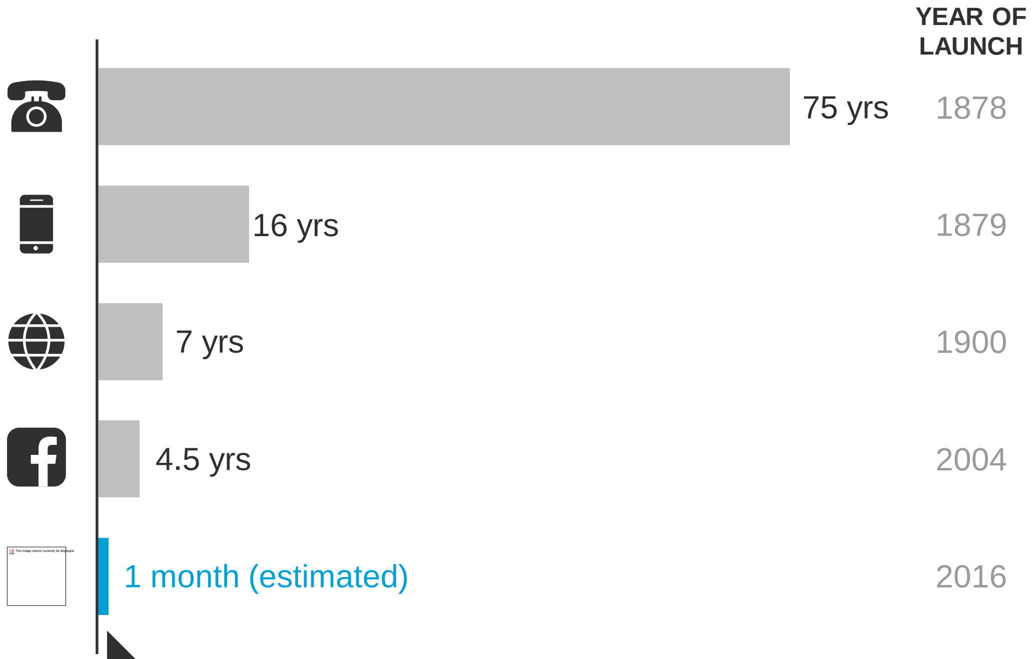
In the wrongs hands,
OAuth can be a weapon

A nightmare for IT Security teams

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

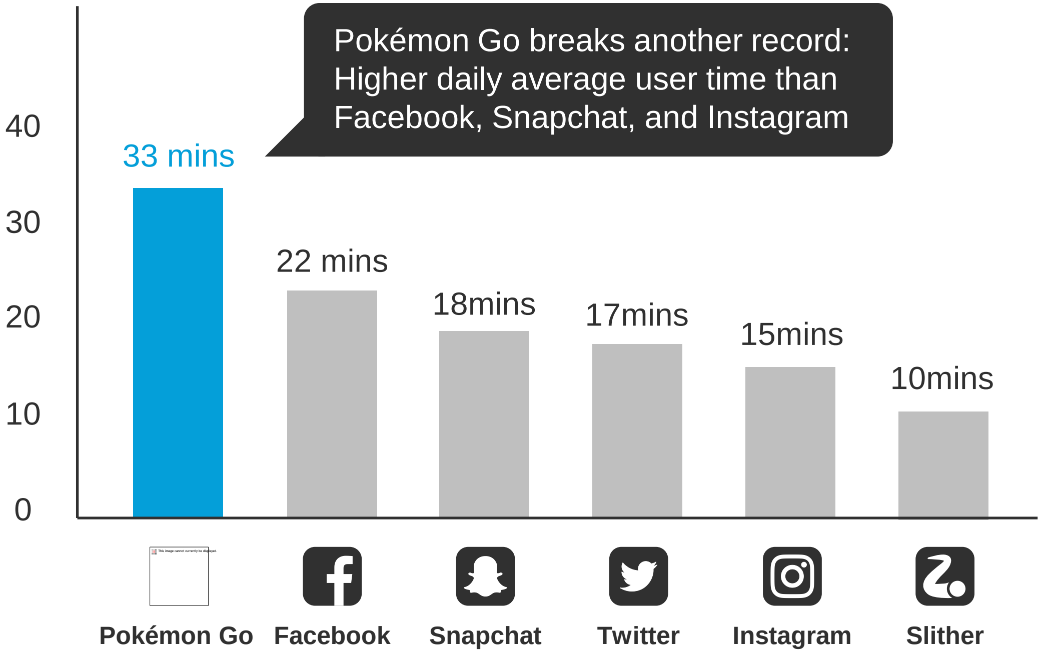
Consider “connected” cloud apps: Pokémon Go

Time to reach 100 million users worldwide



An Unusual Start: Pokémon Go breaking all mobile gaming records globally.

Daily time spent in Pokémon Go by average iOS user

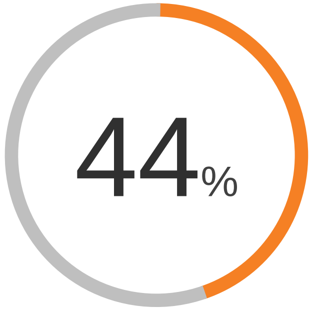


Pokémon Go breaks another record: Higher daily average user time than Facebook, Snapchat, and Instagram

Source: SensorTower

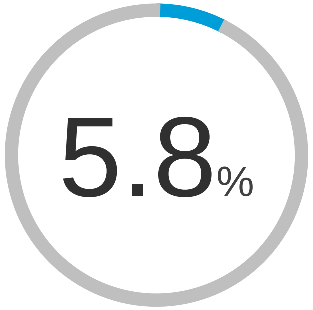
© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Consider Pokémon Go



44%

of all organizations have employees who granted access to Pokémon Go using their corporate credentials



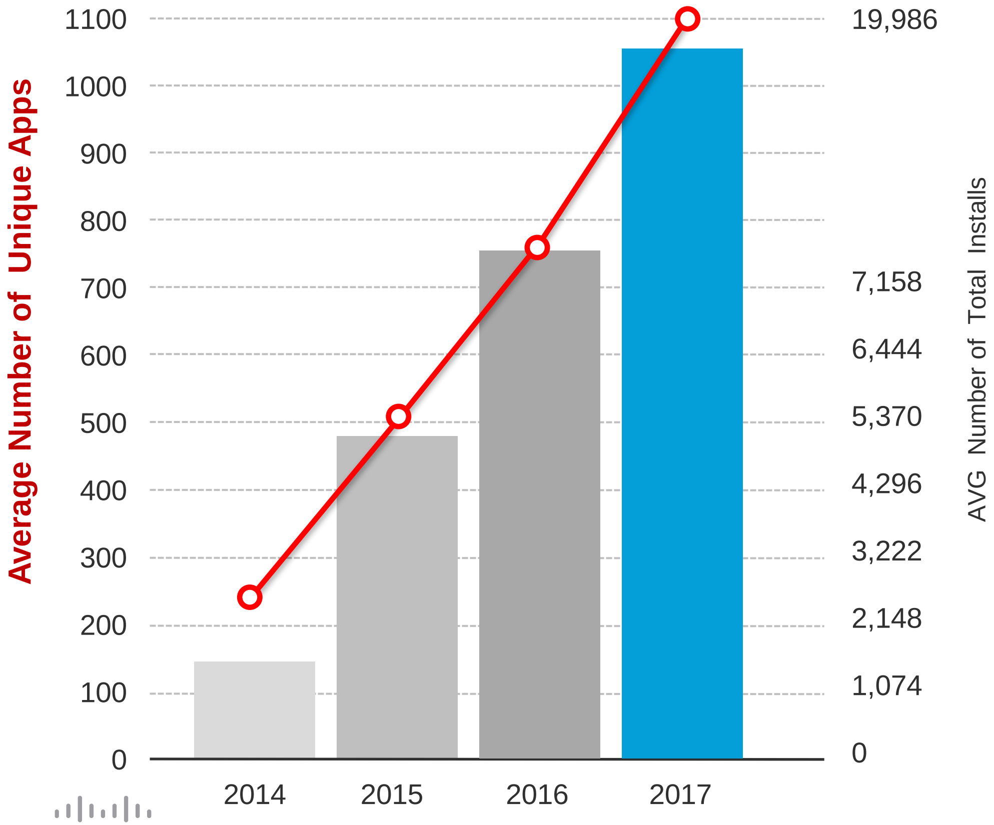
5.8%

of an organization’s employees have installed Pokémon Go on average

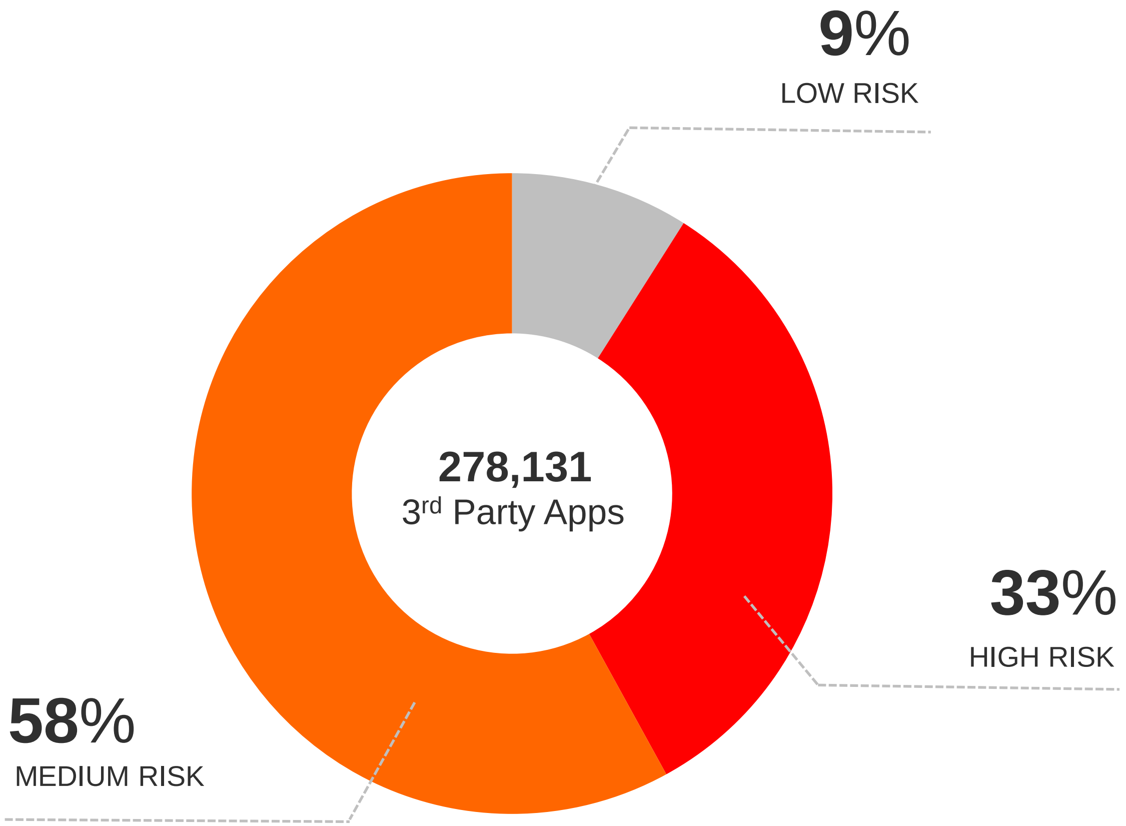
© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

It's more than just Pokémon

1,050 unique connected cloud apps per organization



The App Risk Levels are Rising



© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Addressing Common Misconceptions

OAuth-based attacks bypass all standard security layers including NGFWs, SWGs, SSOs, and more.

Changing Passwords

will **not** address the issue

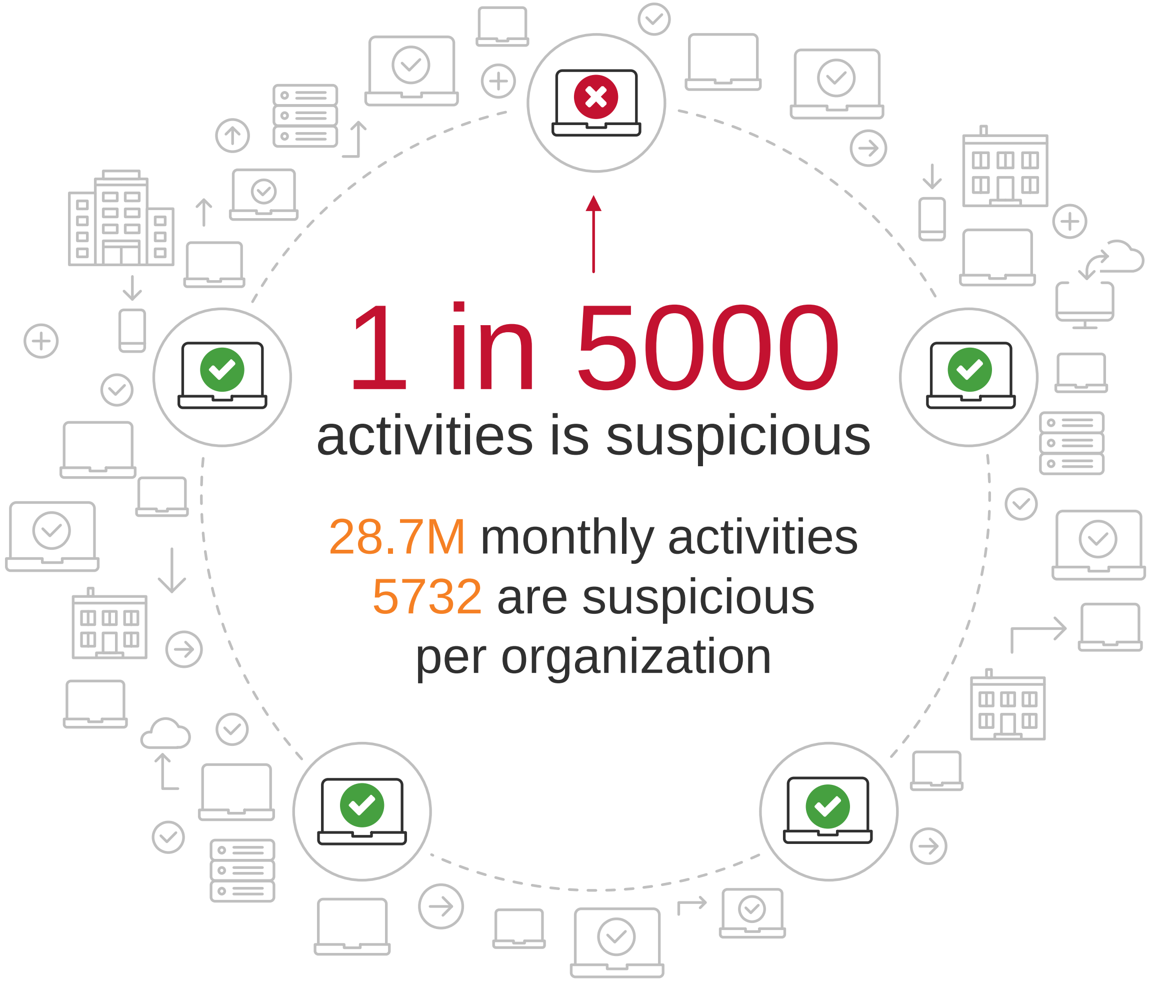
Enabling Multi-factor Authentication

will **not** mitigate the risk

OAuth-Based Attacks

are **not** Google only

Finding the needle in the haystack



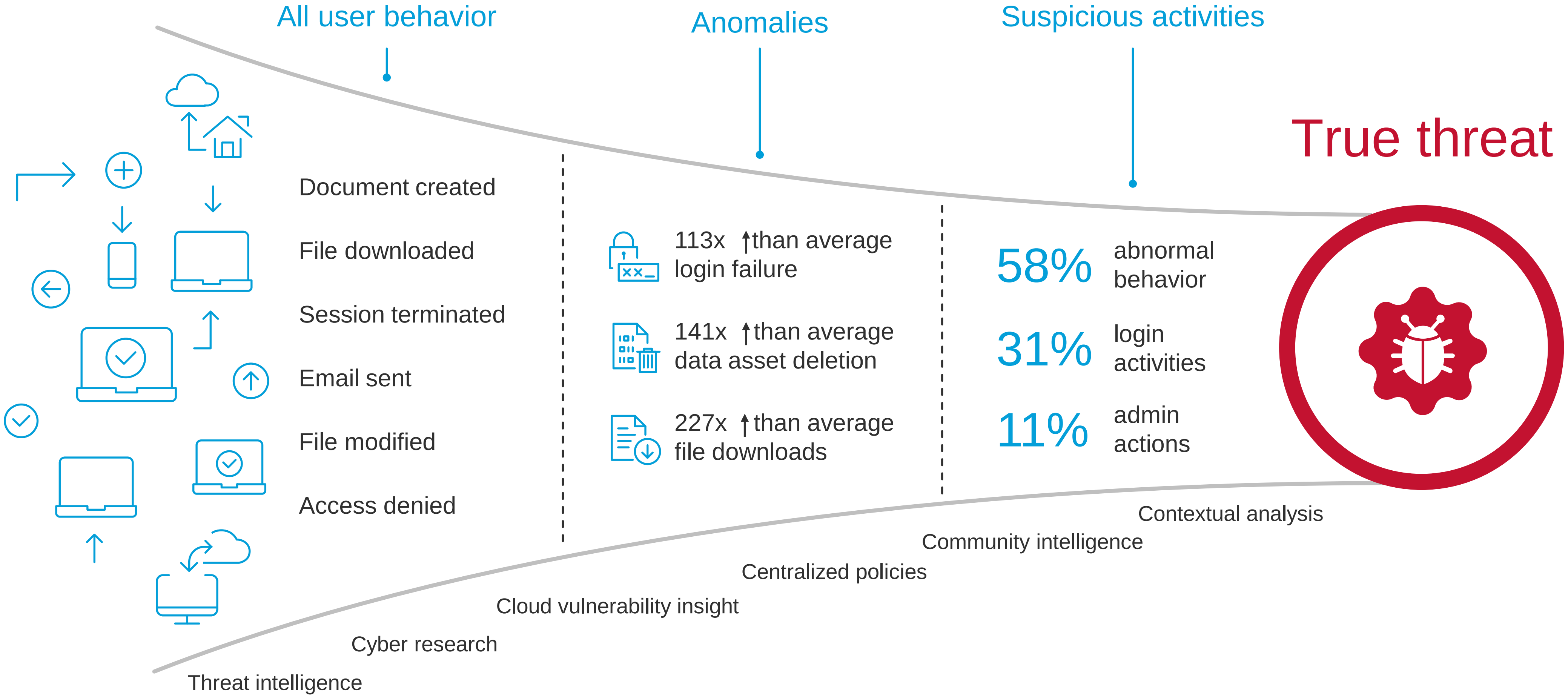
1 in 5000

activities is suspicious

28.7M monthly activities
5732 are suspicious
per organization

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The cloud threat funnel



All user behavior

Document created

File downloaded

Session terminated

Email sent

File modified

Access denied

Anomalies

113x ↑than average login failure

141x ↑than average data asset deletion

227x ↑than average file downloads

Suspicious activities

58% abnormal behavior

31% login activities

11% admin actions

True threat

Contextual analysis

Community intelligence

Centralized policies

Cloud vulnerability insight

Cyber research

Threat intelligence

Cisco Cloudlock

Source: Cloudlock CyberLab

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cloud Security Fundamentals

	Access	Applications
Visibility and control	For all internet activity	For Shadow IT and connected cloud apps (OAuth)
Threat protection	Stop connections to malicious internet destinations	Protect cloud accounts from compromise and malicious insiders
Forensics	Investigate attacks with internet-wide visibility	Analyze audit cloud logs
Data protection	Block C2 callbacks and prevent data exfiltration	Assess cloud data risk and ensure compliance
Malware / ransomware	Prevent initial infection and C2 callbacks	Prevent cloud-native (OAuth) attacks

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Q & A

cisco