# The Tipping Point from the Network Perimeter to the Cloud

## Security in the New Era with Cisco

Eric Chaves

Consulting Solutions Engineering Manager

January 19, 2017

# Today,

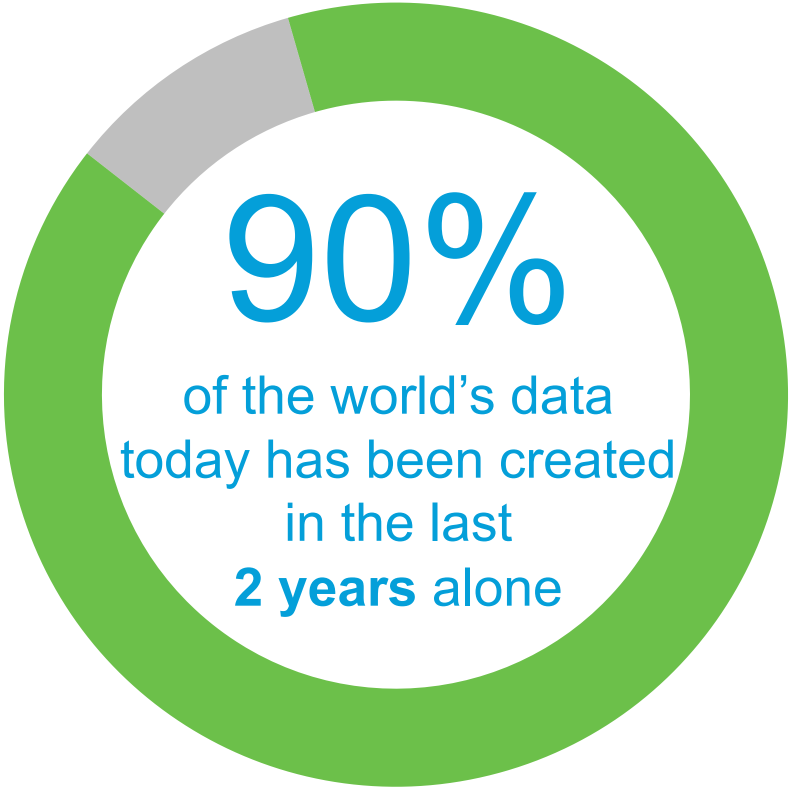
# DATA

# is where the money is

# Every day we create

2,500,000,
000,000,
000,000

(2.5 Quintillion) bytes of data



90%

of the world’s data today has been created in the last **2 years** alone

Source: Ben Walker, Marketing Executive at vouchercloud – April 5, 2015

By 2020, 92 percent of global data center traffic will come from the cloud.

Cisco® Global Cloud Index (GCI)

# Perimeter security used to be effective

Headquarters
Branch offices

By 2018, Gartner estimates:

# 25% of corporate data traffic will bypass perimeter security.

# Your challenges

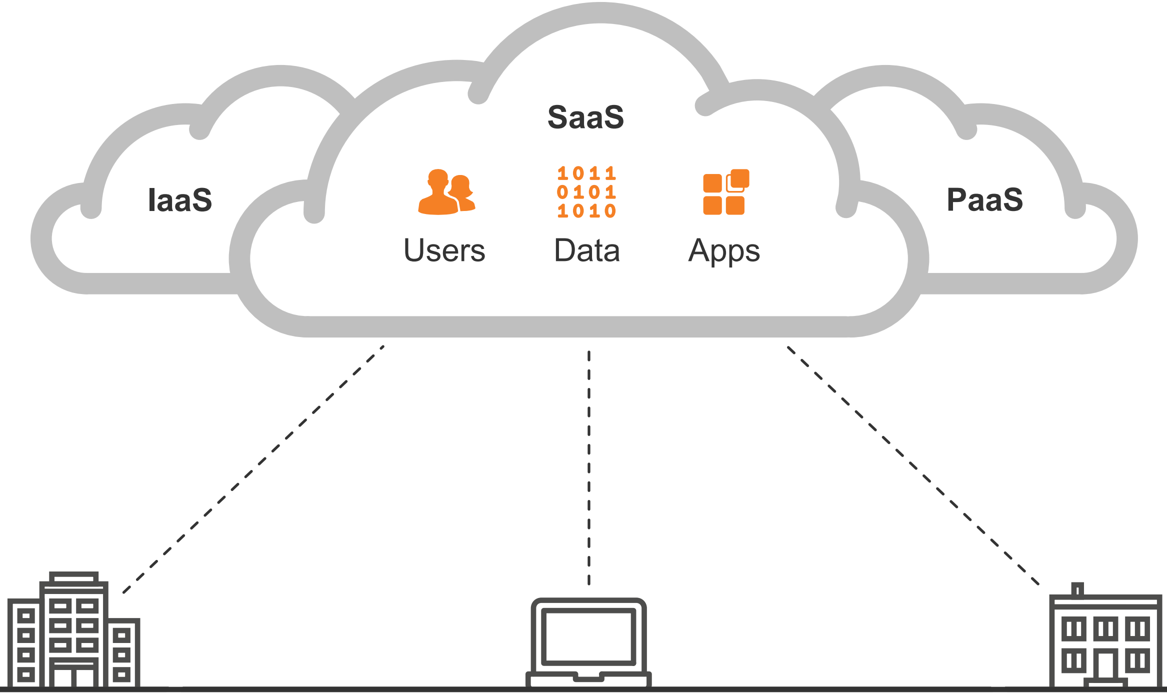
Malware and ransomware

Gaps in visibility and coverage

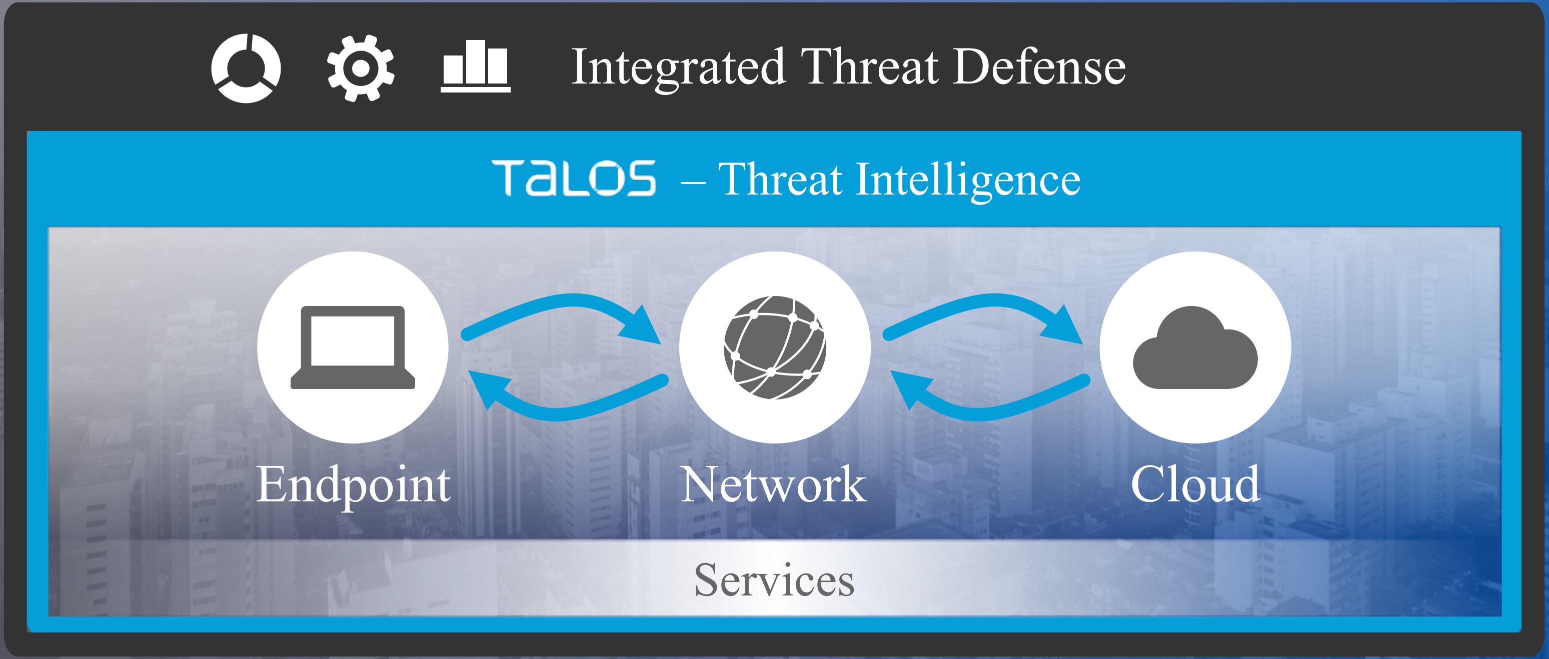
Compromised accounts and malicious insiders

Data breaches and compliance

# Security challenges have evolved



# Industry's Most Effective Security Portfolio



Integrated Threat Defense

TALOS – Threat Intelligence

Endpoint

Network

Cloud

Services

# How Customers can protect their business today

## with Cisco's Advanced Threat Focused Solutions

### Protect against Ransomware & other advanced threats

*'Ransomware Defense Solution'*

Cloud, or On-Prem

Stop ransomware from entering the network - detect & contain if it's already present

### Add a Layer of Security from the Cloud

*'Cisco Umbrella & Cloudlock'*

First line of defense via cloud DNS for on-prem and mobile users

Gain visibility & control of cloud apps, data and users

### Deploy an Advanced Malware Solution

*'AMP Everywhere'* across End Points, network & cloud

Detect advanced threats enterprise wide or single instance, automatic protection everywhere

### Protect the Interior of Your Network

*'Network as a Sensor'* w/Stealthwatch Analytics & TrustSec

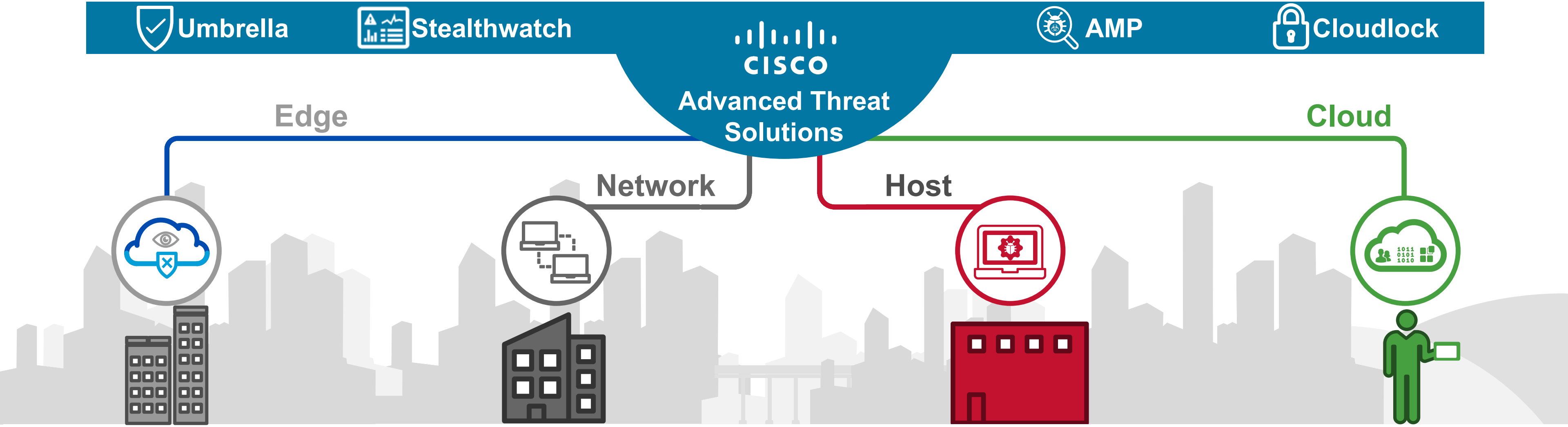
See what's happening on internal network to identify threats and anomalous behavior

### Use Your Network to Shrink Attack Surface

*'Network as Enforcer'* w/ Stealthwatch, ISE, software defined segmentation

Enforce policy to limit threats from expanding inside network once they are detected

# Advanced solutions to secure a modern digital network



- Detect and stop threats *before* they get to your edge
- Enterprise wide deployment in minutes
- Built into the foundation of the internet and delivered from the cloud

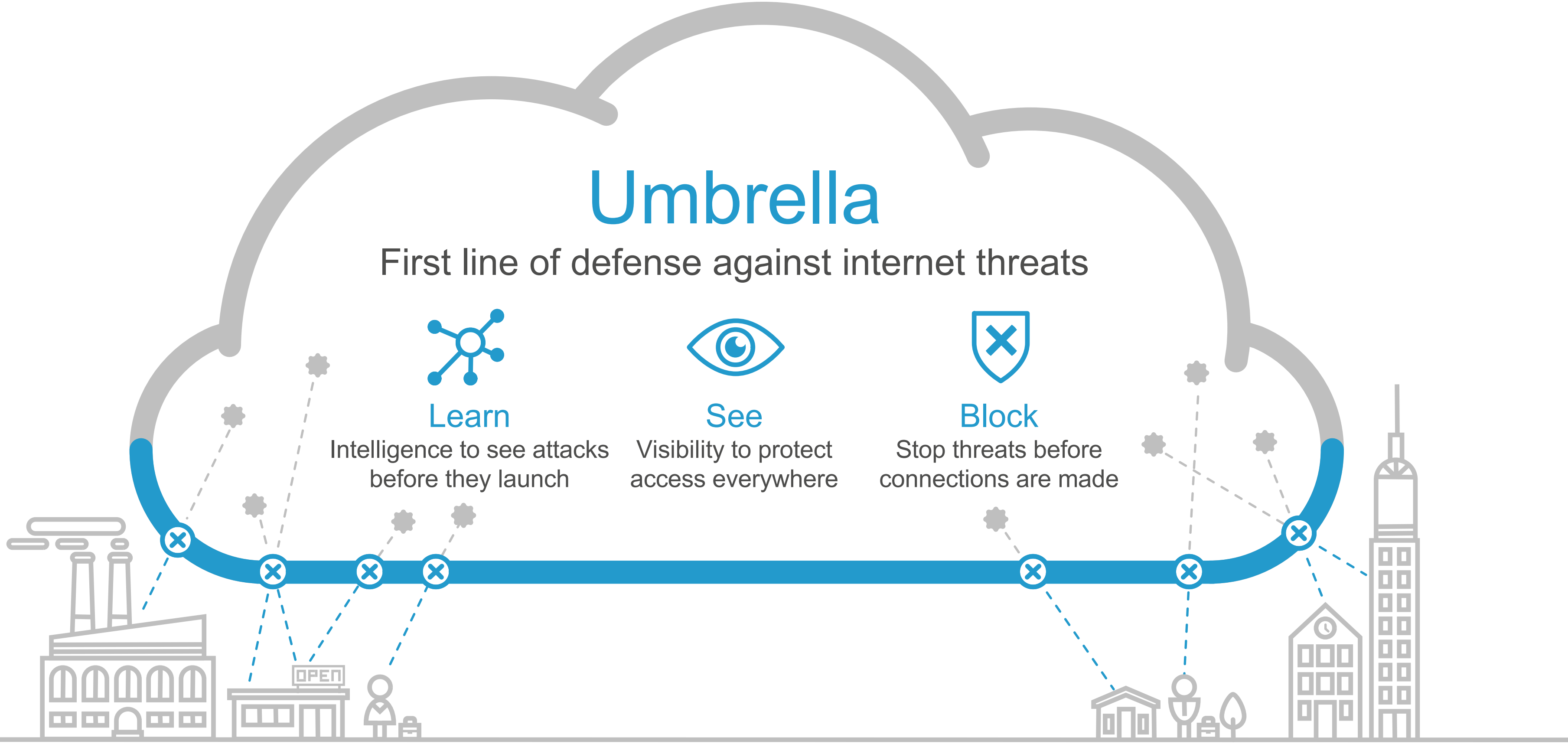
- Gain unique visibility across your business
- Simplify network segmentation; detect and prevent the lateral movement of threats
- Address threats faster and enable your network to take action

- Continuously detect and monitor malware, immediately and retrospectively
- Correlate discrete events into coordinated attacks
- Detect and block exploit attempts, malicious files, and policy-violating files

- Detect that anomalous behavior and compromised accounts in the cloud
- Protect organizations against data breaches in any cloud environment and app
- Discover and control malicious cloud apps connected to your corporate environment

Cisco Services and Customer Success

# Cloud services have security risks in three areas



## Umbrella

First line of defense against internet threats

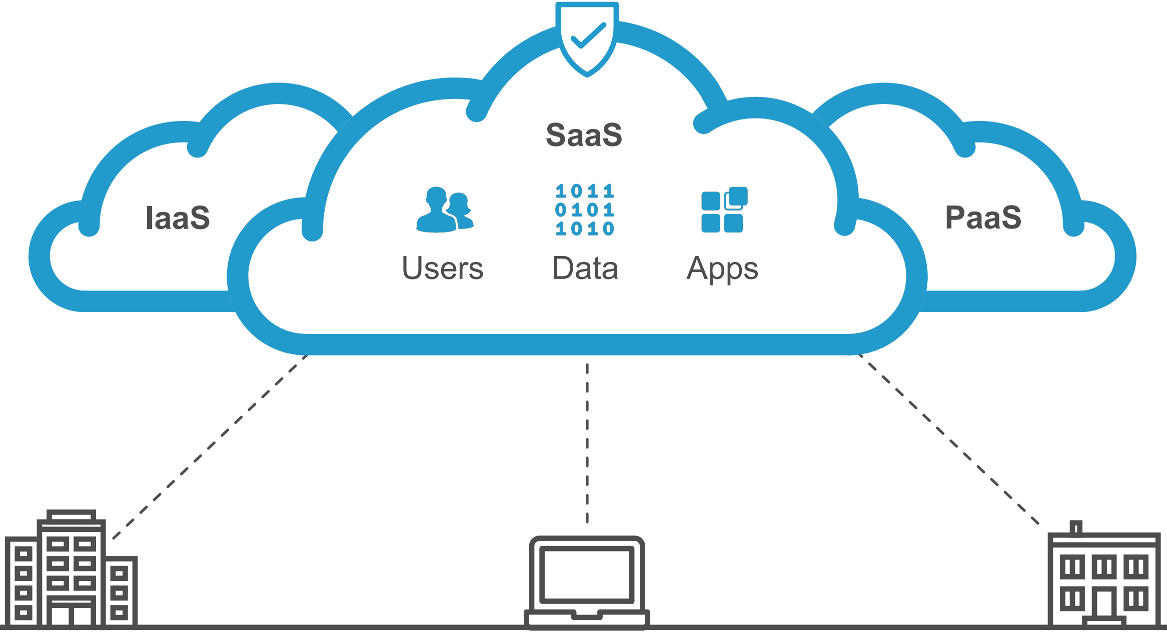
**Learn**
Intelligence to see attacks before they launch

**See**
Visibility to protect access everywhere

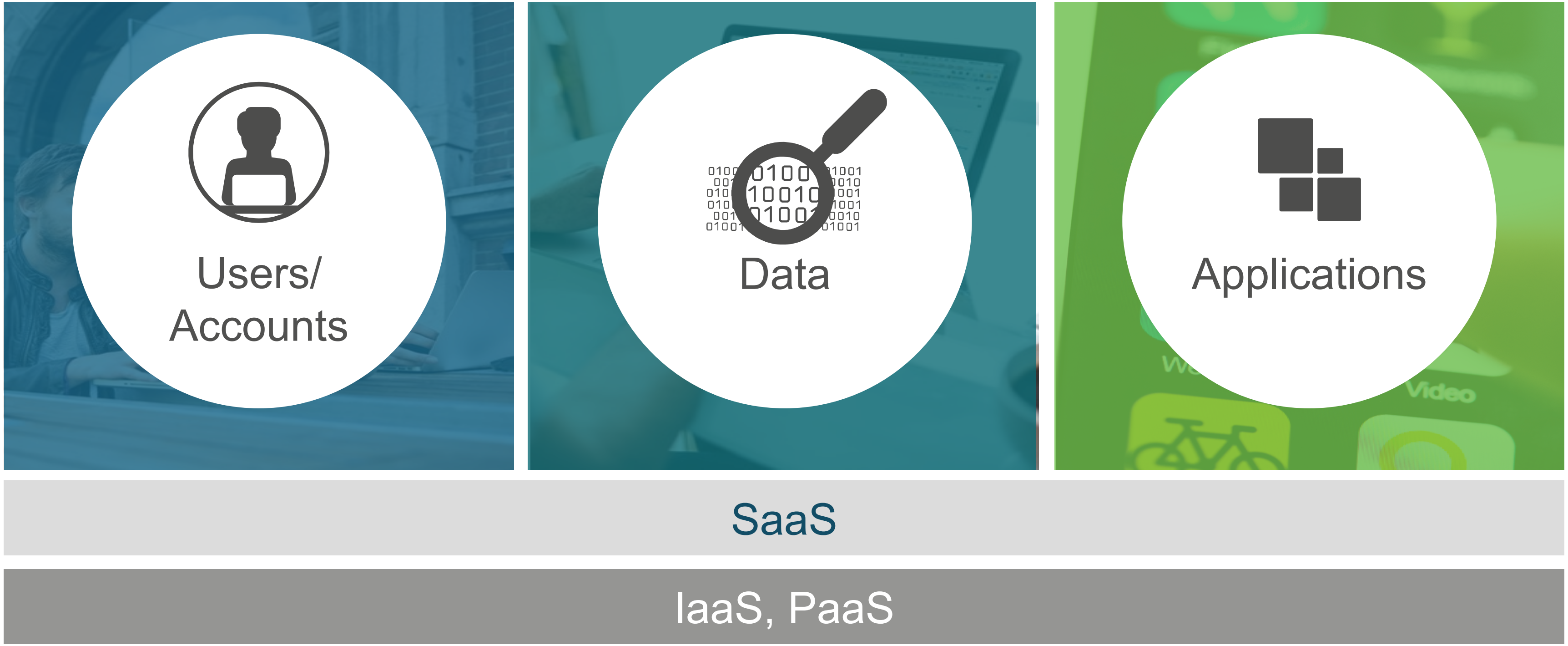
**Block**
Stop threats before connections are made

# CloudLock

## Cloud Access Security Broker (CASB)



# Cloud services have security risks in three areas



Users/ Accounts

Data

Applications

SaaS

IaaS, PaaS

# Cloud Shared Responsibility  - SaaS/PaaS/IaaS

| Infrastructure as a Service (IaaS) | Platform as a Service (PaaS) | SaaS |
|---|---|---|
| ⬜ People | ⬜ People | ⬜ People |
| ⬜ Data | ⬜ Data | ⬜ Data |
| ⬜ Applications | ⬜ Applications | 🟩 Applications |
| ⬜ Runtime | 🟩 Runtime | 🟩 Runtime |
| ⬜ Middleware | 🟩 Middleware | 🟩 Middleware |
| ⬜ Operating System | 🟩 Operating System | 🟩 Operating System |
| ⬜ Virtual Network | 🟩 Virtual Network | 🟩 Virtual Network |
| 🟩 Hypervisor | 🟩 Hypervisor | 🟩 Hypervisor |
| 🟩 Servers | 🟩 Servers | 🟩 Servers |
| 🟩 Storage | 🟩 Storage | 🟩 Storage |
| 🟩 Physical Network | 🟩 Physical Network | 🟩 Physical Network |

🟩 CSR Responsibility

⬜ Customer Responsibility

*Gartner Research Paper: Mind the SaaS Security Gaps Published: 19 May 2016

# Security Weaknesses of Native Cloud Service Providers

Single Platform Only

Solves Fewer Problems

Lack of Security Expertise & Focus

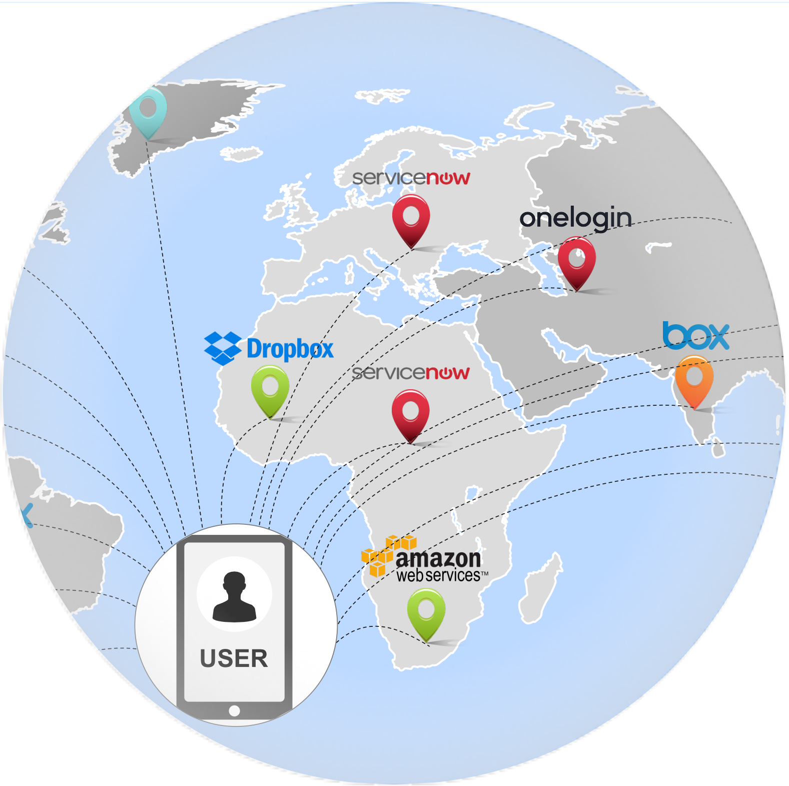
Upcharge

No Incident Management

Weak Remediation Capabilities

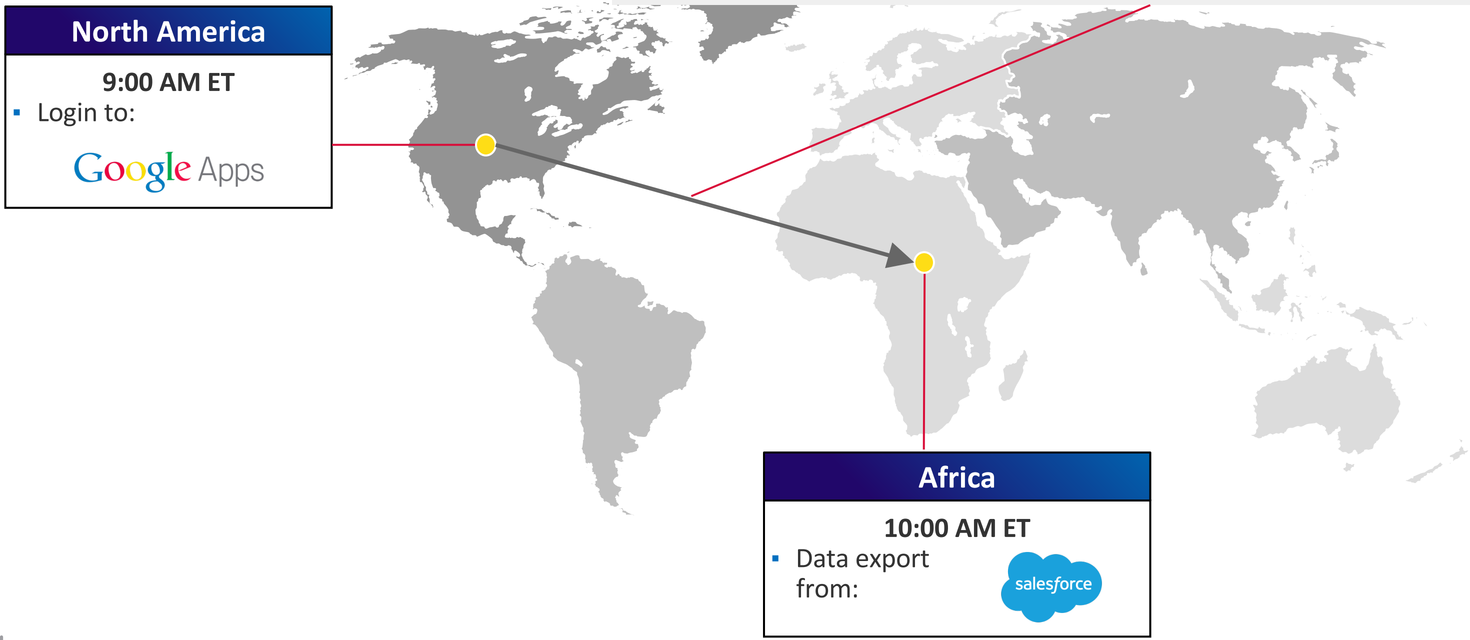
# Cloud Users

# Without CASB, companies are blind to the most obvious malicious traffic



# Here’s an example of why you need cloud user security

- Distance from the US to the Central African Republic: 7,362 miles
- At a speed of 800 mph, it would take 9.2 hours to travel between them



**North America**

**9:00 AM ET**

- Login to:

Google Apps

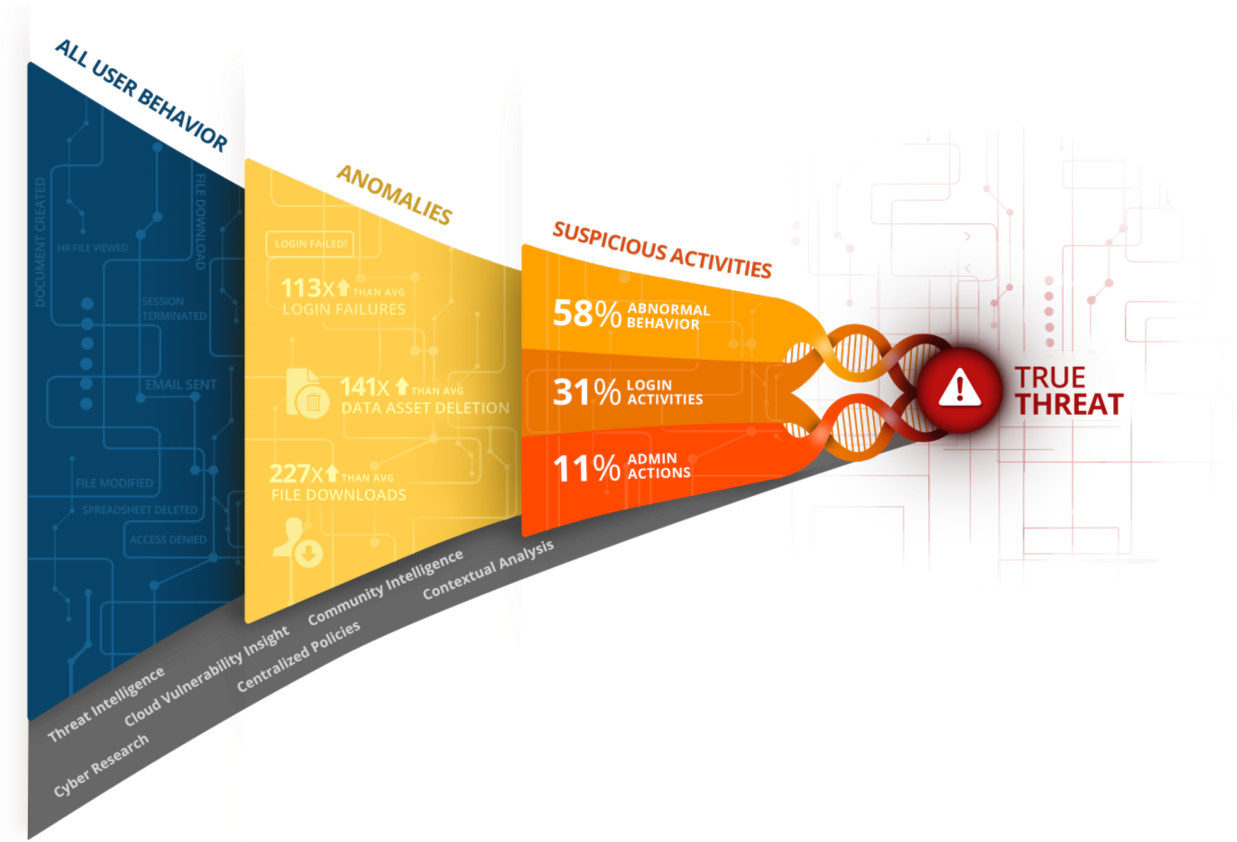
**Africa**

**10:00 AM ET**

- Data export from:

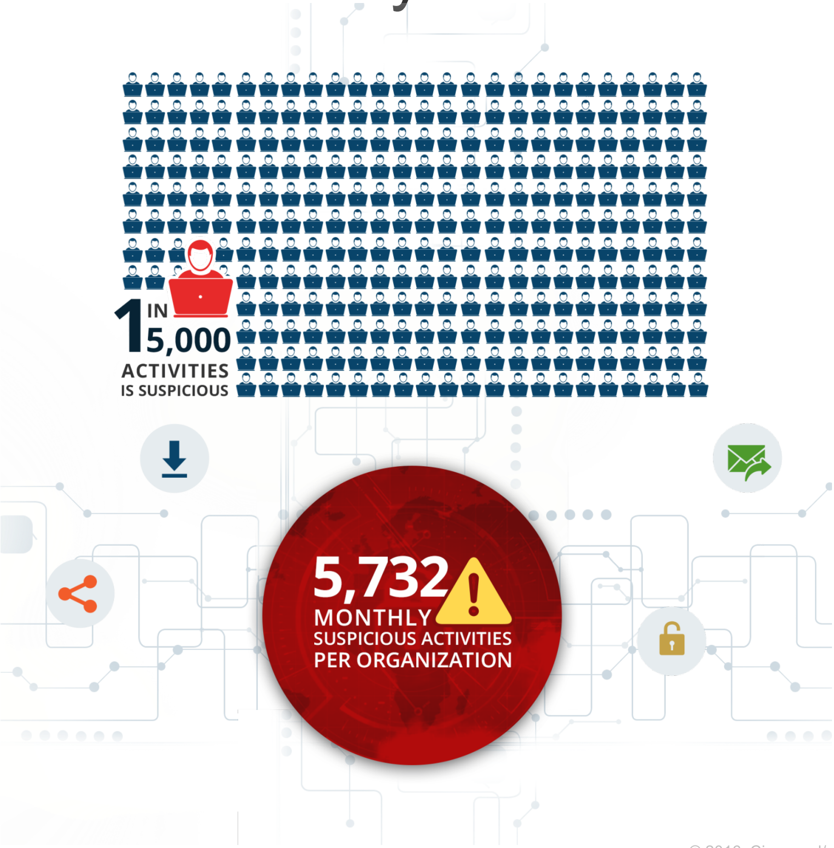
salesforce

# The Cloud Threat Funnel



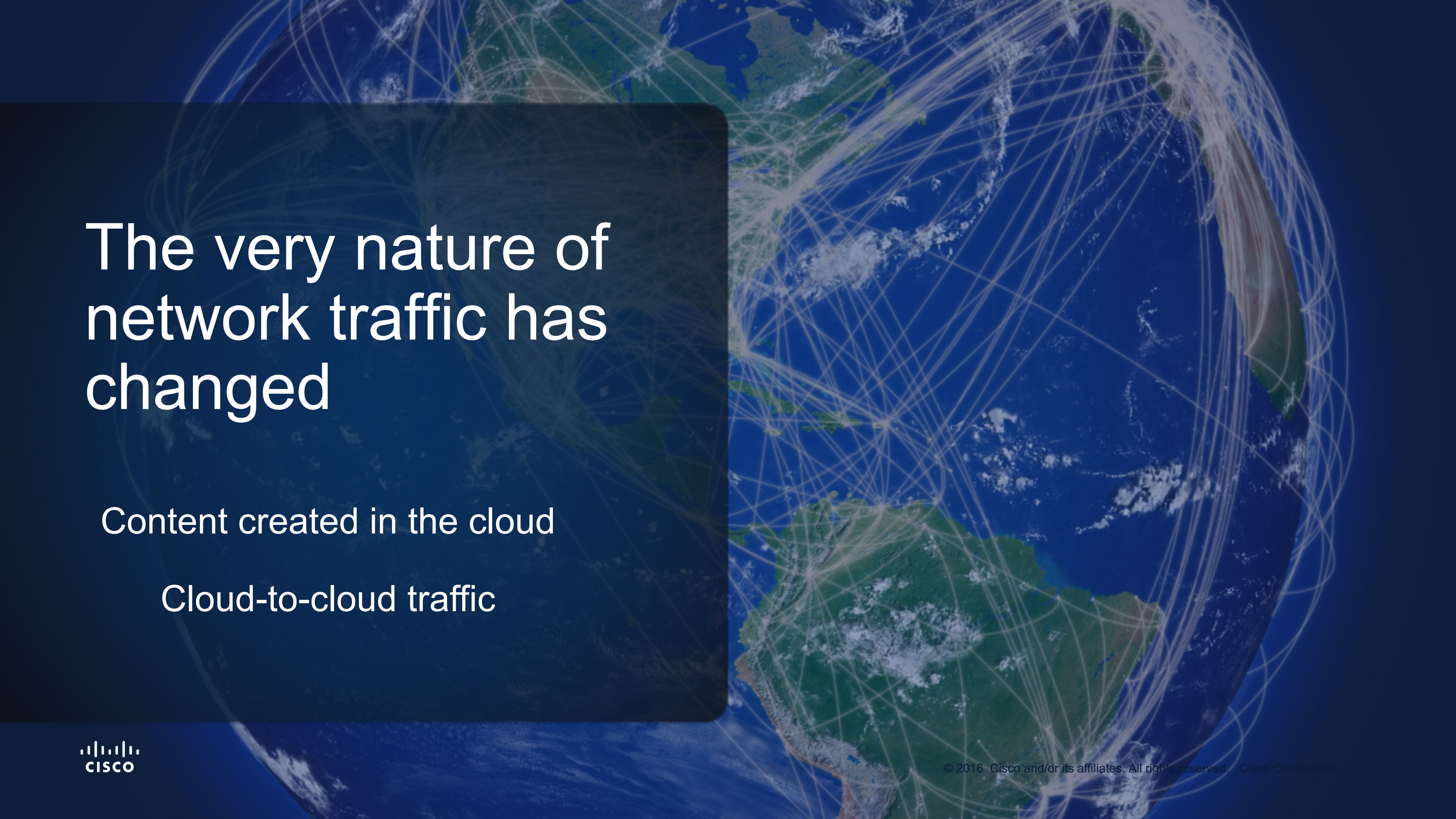
Source: CloudLock CyberLab

# Finding the needle in the haystack



Source: CloudLock CyberLab

# Cloud Data

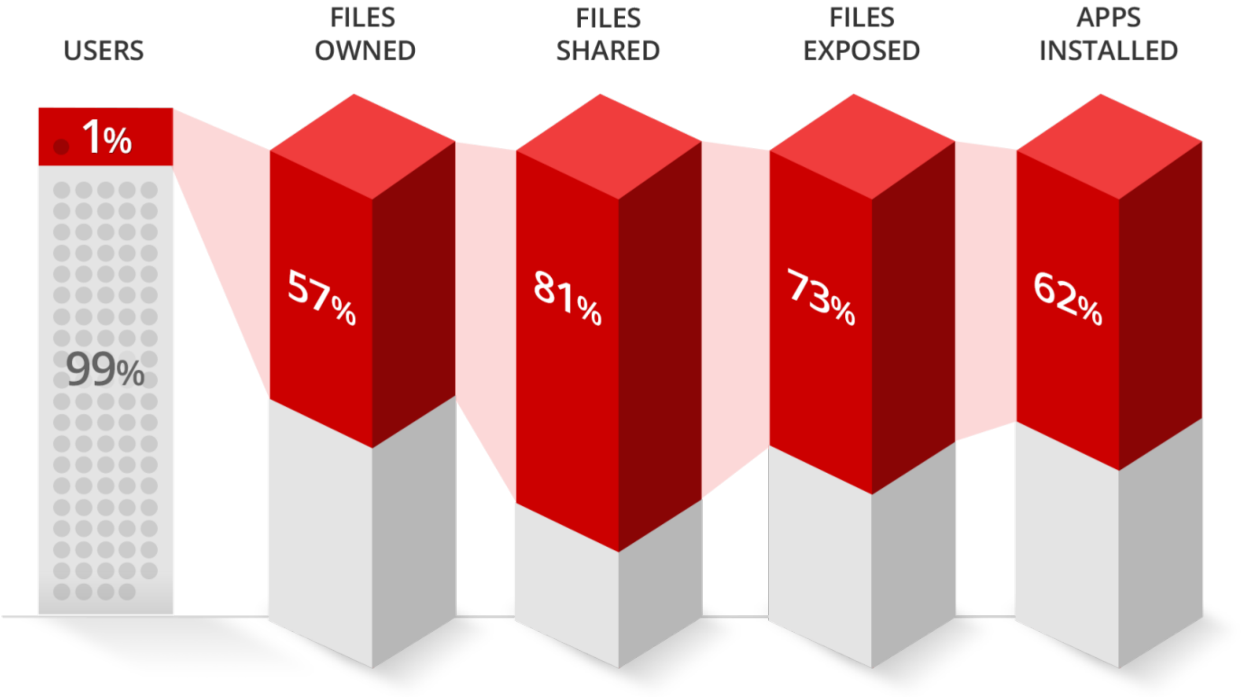


# The very nature of network traffic has changed

Content created in the cloud

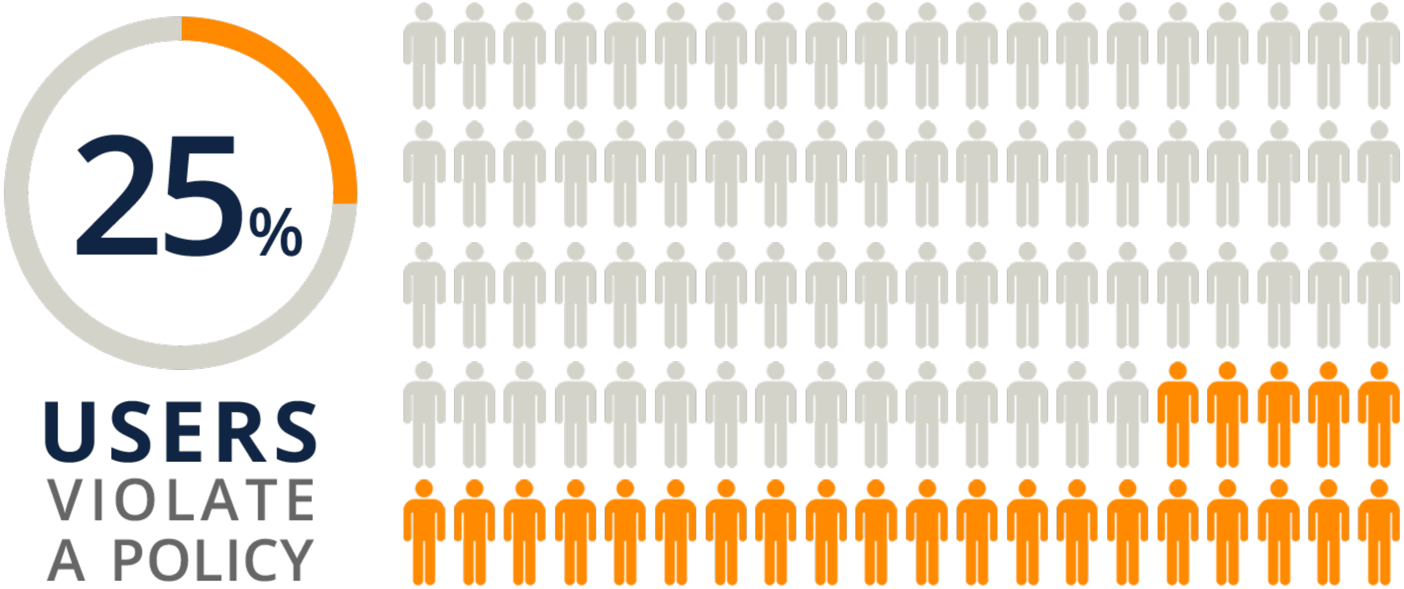
Cloud-to-cloud traffic

# Disproportionate Cloud Risk in Cloud Data



Source: CloudLock CyberLab

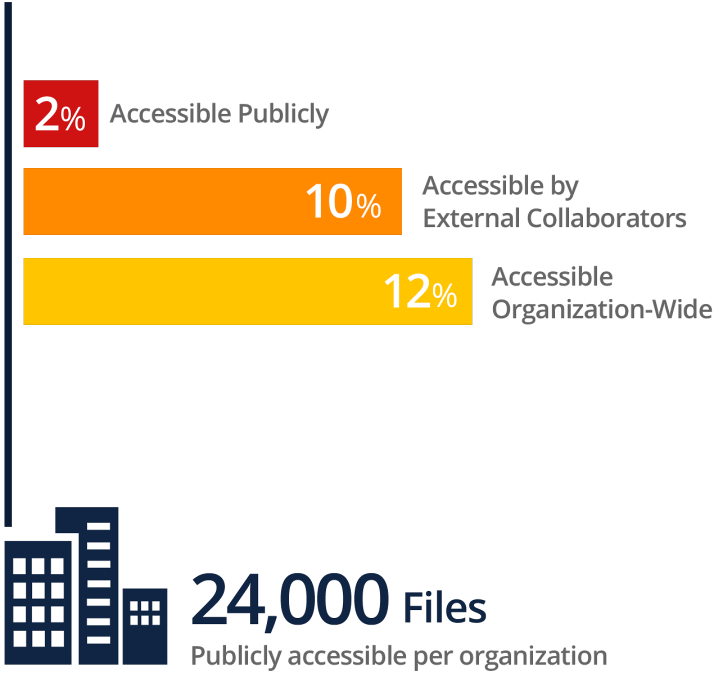
# Disproportionate Cloud Risk in Cloud Data



Source: CloudLock CyberLab

# More than 24,000 Files per Organization Publicly Accessible

Data Exposure per Organization



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

Source: CloudLock CyberLab

# CloudLock has over 70 pre-defined policies

## PII

- SSN / ID numbers
- Driver license numbers
- Passport numbers

## Education

- Inappropriate content
- Student Loan application information
- FERPA compliance

## General

- Email address
- IP address
- Passwords/Login information

## PHI

- HIPAA
- Health Identification numbers (global)
- Medical prescriptions

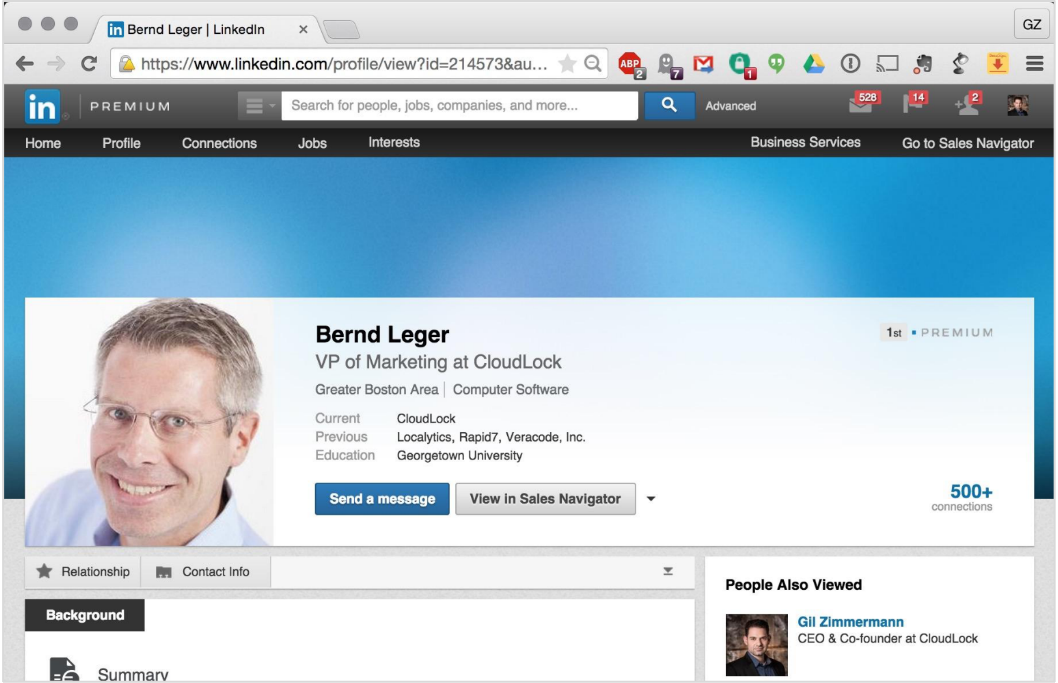
## PCI

- Credit card numbers
- Bank account numbers
- SWIFT codes

# Cloud Apps

# Keys to the Kingdom: Third-Party Apps

Let’s start with an example

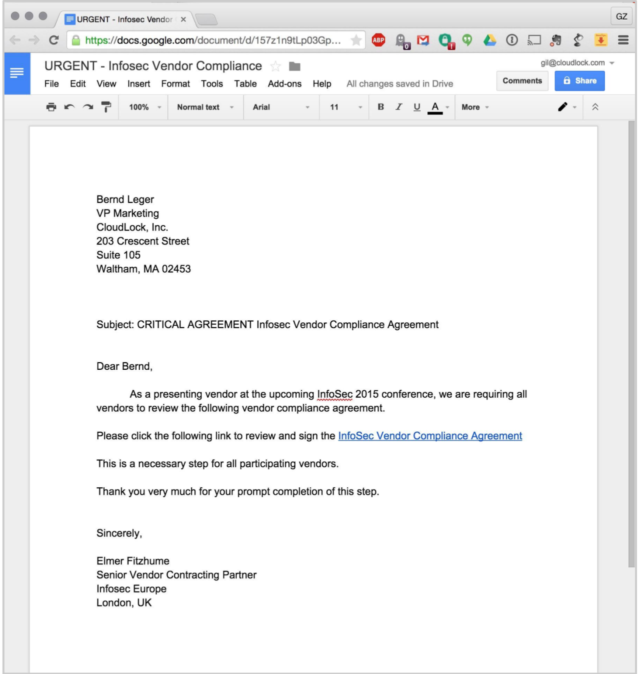


Bernd Leger
VP of Marketing at CloudLock
Greater Boston Area | Computer Software

Current CloudLock
Previous Localytics, Rapid7, Veracode, Inc.
Education Georgetown University

Gil Zimmermann
CEO & Co-founder at CloudLock

# Personalizing the attack


URGENT - Infosec Vendor
https://docs.google.com/document/d/157z1n9tLp03Gp...
GZ
URGENT - Infosec Vendor Compliance
gil@cloudlock.com
File Edit View Insert Format Tools Table Add-ons Help All changes saved in Drive
Comments
Share
100% Normal text Arial 11 B I U A More

Bernd Leger
VP Marketing
CloudLock, Inc.
203 Crescent Street
Suite 105
Waltham, MA 02453

Subject: CRITICAL AGREEMENT Infosec Vendor Compliance Agreement

Dear Bernd,

As a presenting vendor at the upcoming InfoSec 2015 conference, we are requiring all vendors to review the following vendor compliance agreement.

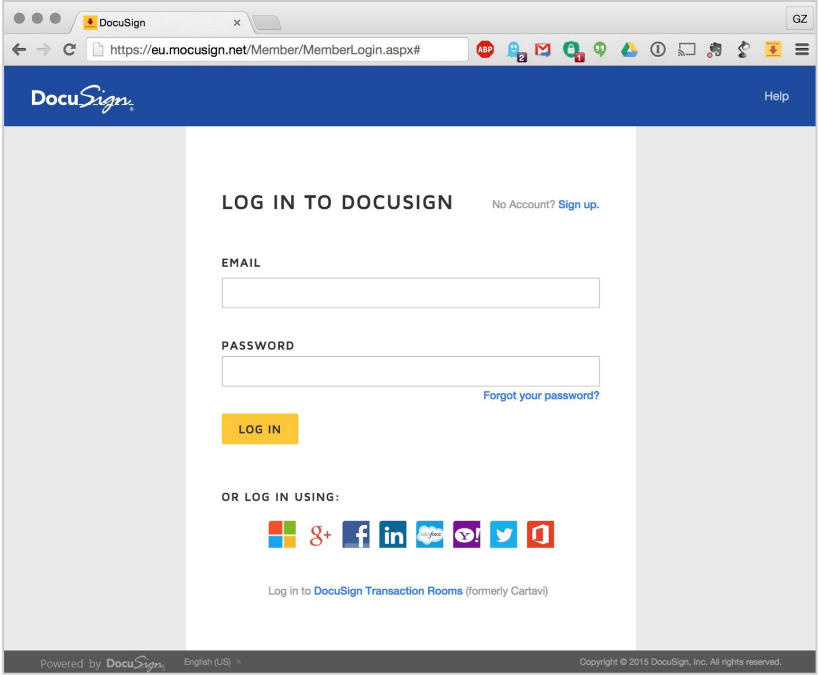
Please click the following link to review and sign the InfoSec Vendor Compliance Agreement

This is a necessary step for all participating vendors.

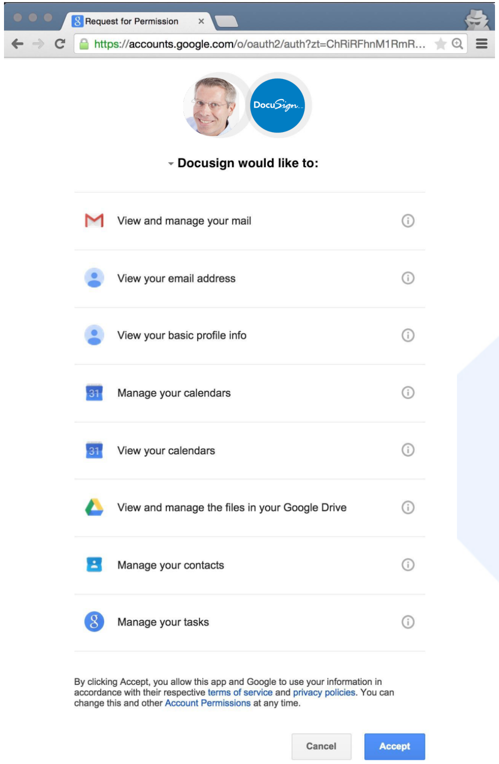
Thank you very much for your prompt completion of this step.

Sincerely,

Elmer Fitzhume
Senior Vendor Contracting Partner
Infosec Europe
London, UK


DocuSign
https://eu.mocusign.net/Member/MemberLogin.aspx#
GZ
DocuSign
Help
LOG IN TO DOCUSIGN
No Account? Sign up.
EMAIL
PASSWORD
Forgot your password?
LOG IN
OR LOG IN USING:
Log in to DocuSign Transaction Rooms (formerly Cartavi)
Powered by DocuSign
English (US)
Copyright © 2015 DocuSign, Inc. All rights reserved.

# OAuth-Connected Apps Have Extensive Access to Corporate Environments



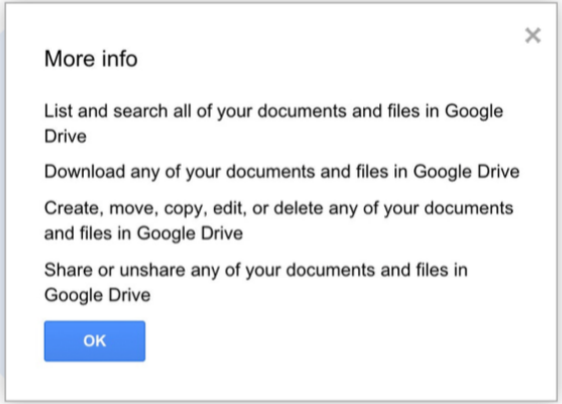
Request for Permission

https://accounts.google.com/o/oauth2/auth?zt=ChRiRFhnM1RmR...

**Docusign would like to:**

- View and manage your mail
- View your email address
- View your basic profile info
- Manage your calendars
- View your calendars
- View and manage the files in your Google Drive
- Manage your contacts
- Manage your tasks

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



More info

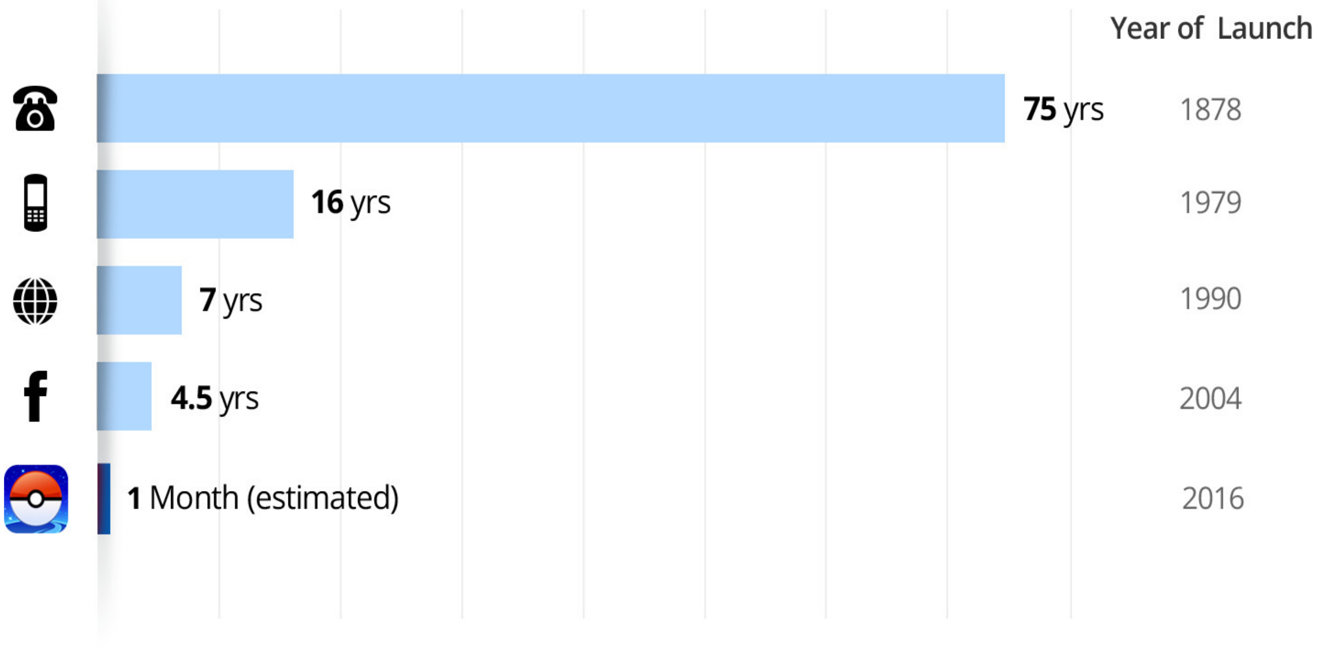
List and search all of your documents and files in Google Drive

Download any of your documents and files in Google Drive

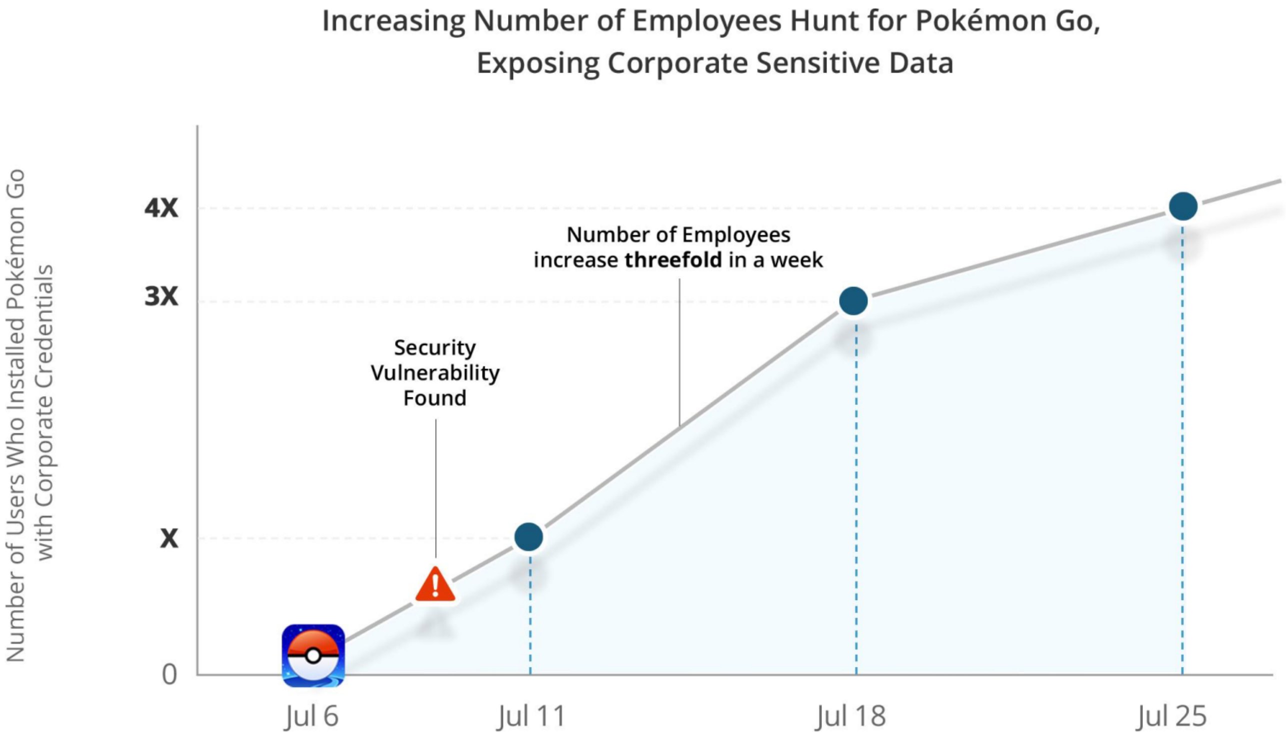
Create, move, copy, edit, or delete any of your documents and files in Google Drive

Share or unshare any of your documents and files in Google Drive

# Consider Pokémon Go


Time to Reach 100 Million Users Worldwide

# Consider Pokémon Go



Increasing Number of Employees Hunt for Pokémon Go, Exposing Corporate Sensitive Data

Number of Employees increase **threefold** in a week

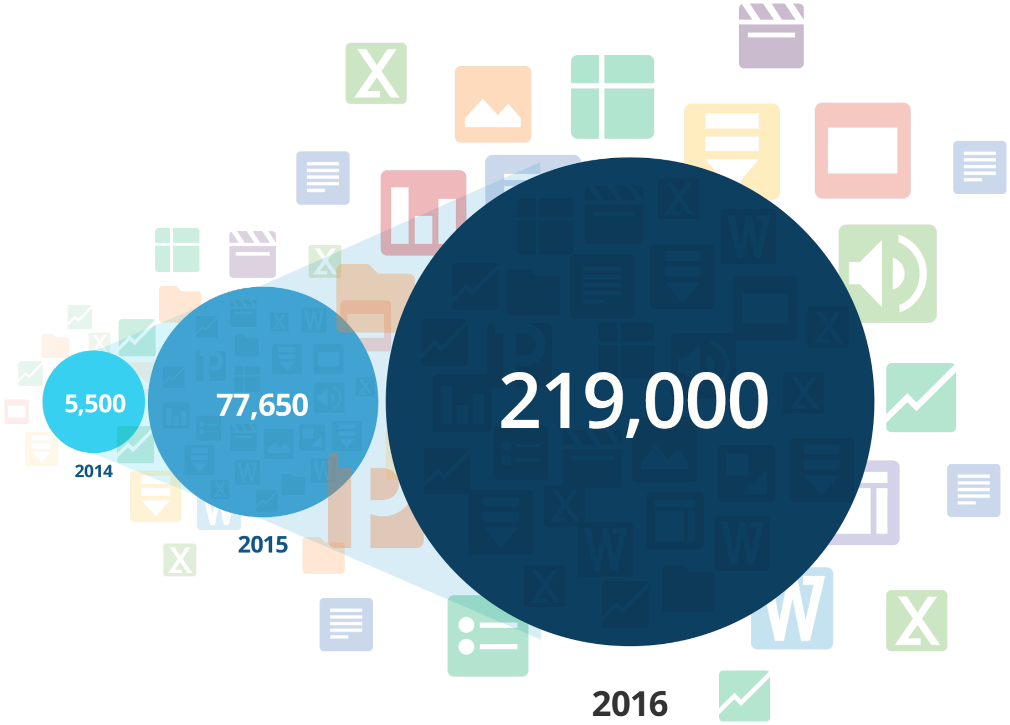
Security Vulnerability Found

# Consider Pokémon Go

**44%** of all organizations have employees who granted access to Pokémon Go using their corporate credentials

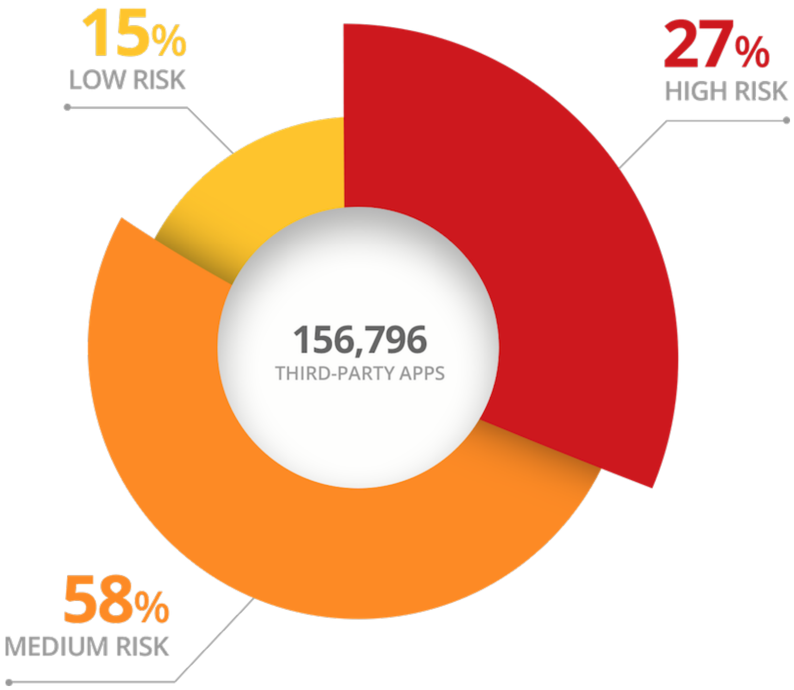
On average, **5.8%** of an organization's employees have installed Pokémon Go

# Explosion of Connected Third-Party Apps



Source: CloudLock CyberLab

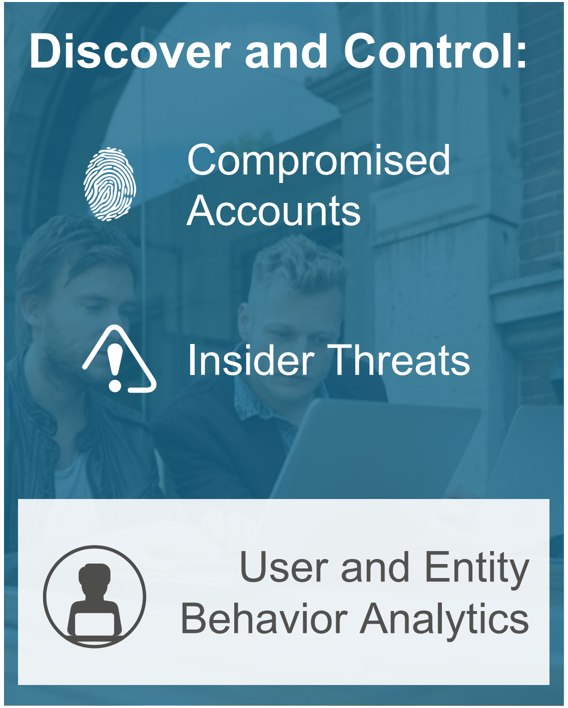
# More than 25% of those Apps are of High Risk



Source: CloudLock CyberLab

# There’s a better way

# Cisco CloudLock addresses customers’ most critical cloud security use cases



## Discover and Control:

- Compromised Accounts
- Insider Threats

User and Entity Behavior Analytics

## Discover and Control:

- Data Exposures & Leakages
- Privacy & Compliance Violations

Cloud Data Loss Prevention (DLP)

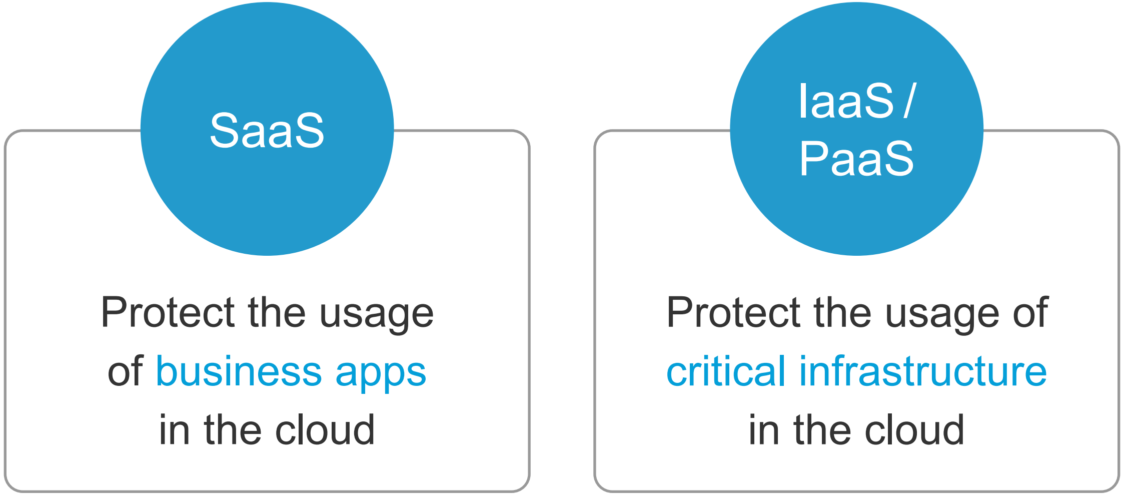
## Discover and Control:

- Cloud Malware
- Shadow IT/OAuth Discovery & Control

Apps Firewall

# The Cloud Security Fabric™

Office 365
salesforce
box
G Suite
Dropbox
slack
servicenow



SaaS

Protect the usage of business apps in the cloud

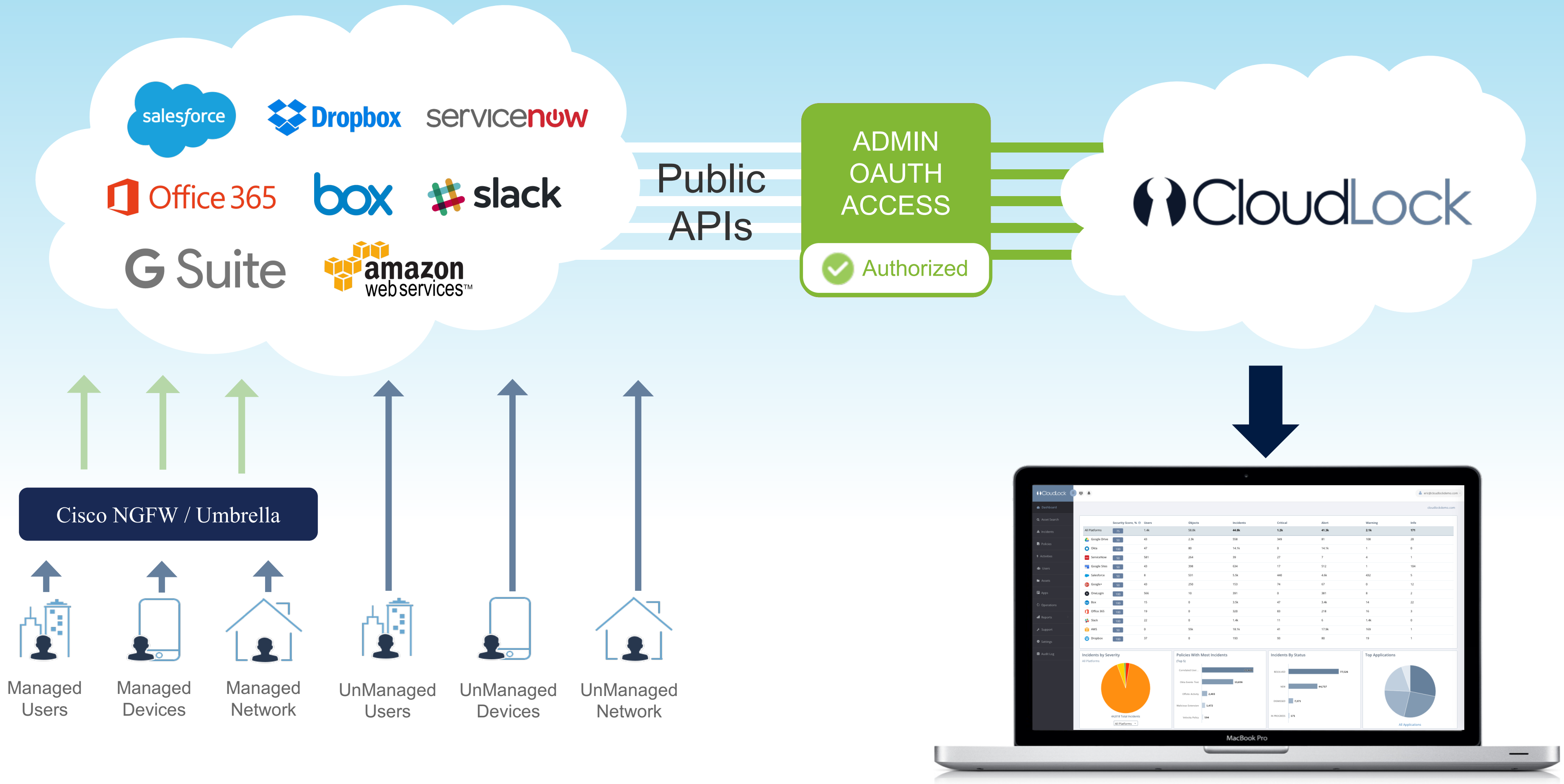
IaaS / PaaS

Protect the usage of critical infrastructure in the cloud

amazon web services
force.com

CloudLock

# CASB - API Access (Cloud to Cloud)



| | Security Score, % | Users | Objects | Incidents | Critical | Alert | Warning | Info |
|---|---|---|---|---|---|---|---|---|
| All Platforms | 75 | 1.4k | 58.8k | 44.8k | 1.2k | 41.3k | 2.1k | 171 |
| Google Drive | 50 | 43 | 2.3k | 558 | 349 | 81 | 108 | 20 |
| Okta | 100 | 47 | 80 | 14.1k | 0 | 14.1k | 1 | 0 |
| ServiceNow | 50 | 581 | 264 | 39 | 27 | 7 | 4 | 1 |
| Google Sites | 50 | 43 | 398 | 634 | 17 | 512 | 1 | 104 |
| Salesforce | 50 | 8 | 531 | 5.5k | 440 | 4.6k | 432 | 5 |
| Google+ | 50 | 43 | 250 | 153 | 74 | 67 | 0 | 12 |
| OneLogin | 100 | 566 | 10 | 391 | 0 | 381 | 8 | 2 |
| Box | 100 | 15 | 0 | 3.5k | 47 | 3.4k | 14 | 22 |
| Office 365 | 100 | 19 | 0 | 320 | 83 | 218 | 16 | 3 |
| Slack | 100 | 22 | 0 | 1.4k | 11 | 6 | 1.4k | 0 |
| AWS | 50 | 0 | 55k | 18.1k | 41 | 17.9k | 169 | 1 |
| Dropbox | 100 | 37 | 0 | 193 | 93 | 80 | 19 | 1 |

# CloudLock provides automated response actions

**Notify User**

**Alert Admin**

**Revoke Sharing**

**Quarantine File**

**Encrypt**

# To be effective, cloud security must be

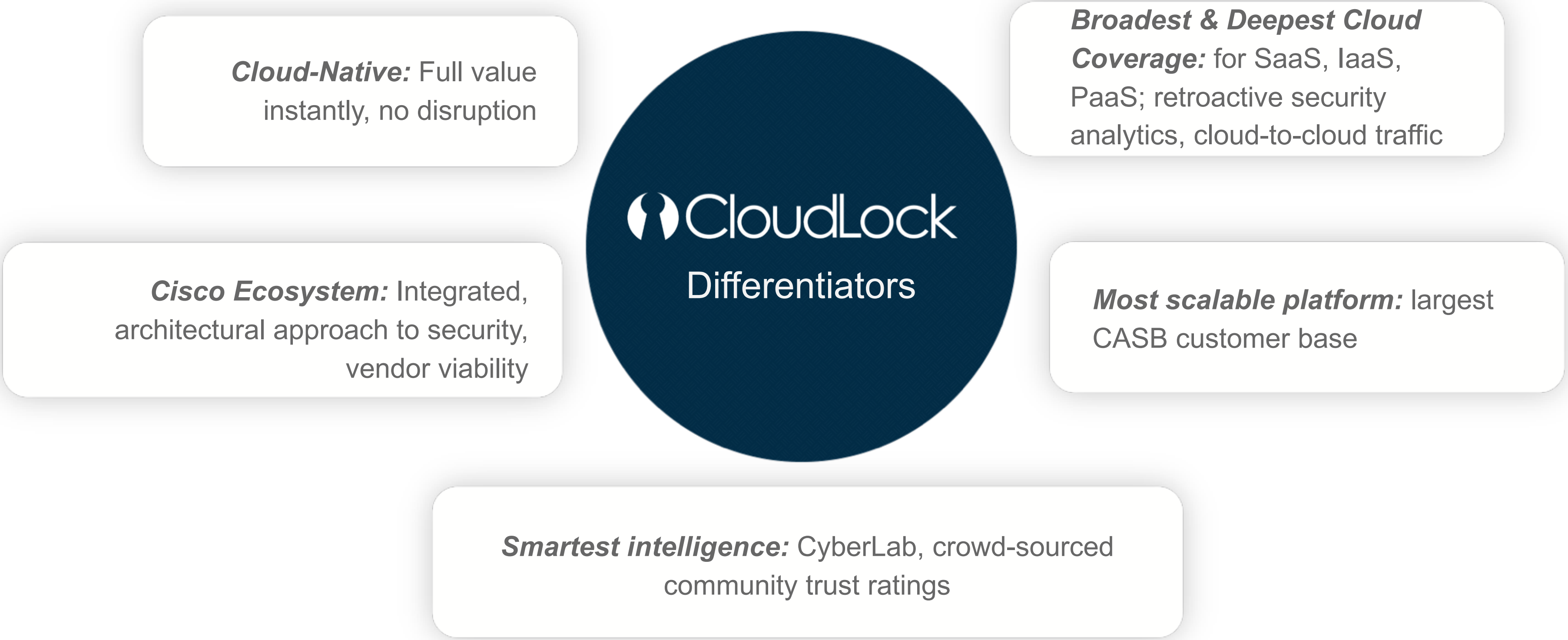
1 2 3

Simple

Open

Automated

# CloudLock Differentiators



CloudLock Differentiators

***Cloud-Native:*** Full value instantly, no disruption

***Broadest & Deepest Cloud Coverage:*** for SaaS, IaaS, PaaS; retroactive security analytics, cloud-to-cloud traffic

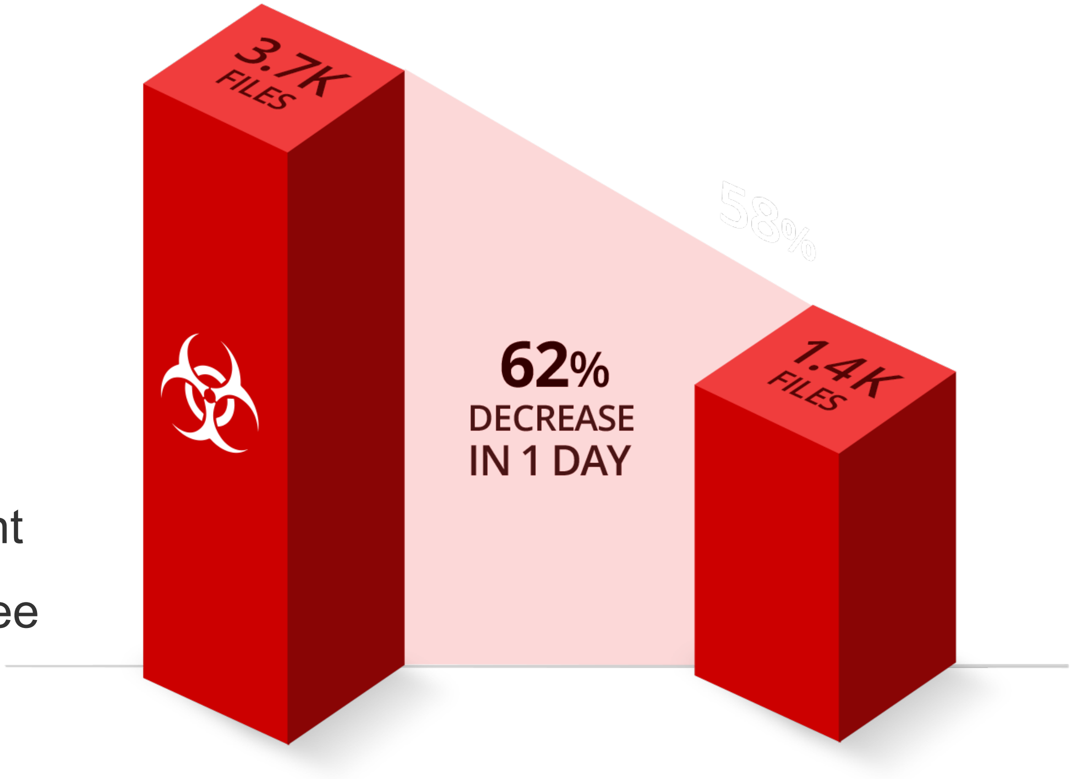
***Cisco Ecosystem:*** Integrated, architectural approach to security, vendor viability

***Most scalable platform:*** largest CASB customer base

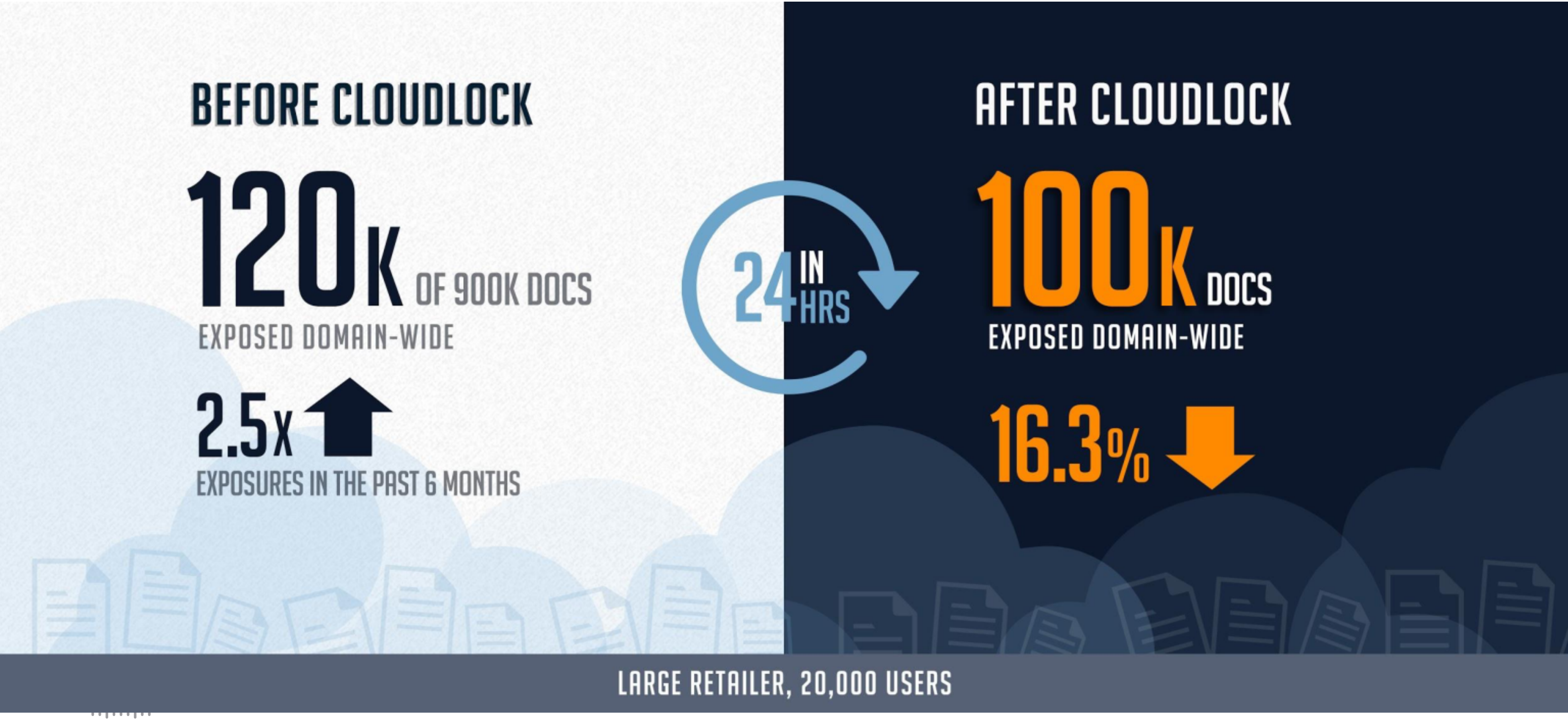
***Smartest intelligence:*** CyberLab, crowd-sourced community trust ratings

# Customer Success Story: Rapid ROI

- US based company in the travel industry.
- 62% of decrease in public exposures in one day by leveraging CloudLock
- Reached out to top users with public exposures
- Rapid return on investment
- Revealed gaps in employee security training



# 16.3% Decrease in Domain-Wide Exposures in 1 Day



BEFORE CLOUDLOCK

120K OF 900K DOCS

EXPOSED DOMAIN-WIDE

2.5X ⬆

EXPOSURES IN THE PAST 6 MONTHS

24 IN HRS

AFTER CLOUDLOCK

100K DOCS

EXPOSED DOMAIN-WIDE

16.3% ⬇

LARGE RETAILER, 20,000 USERS

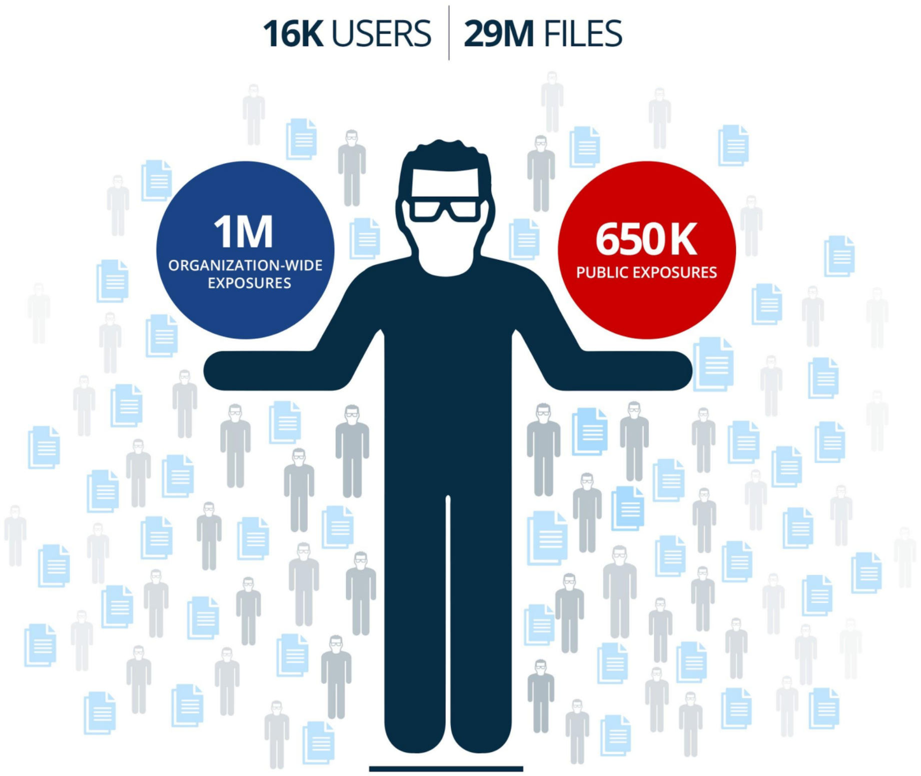
CISCO

# 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



# CloudLock CyberLab & Largest Cloud Usage Dataset

## CloudLock CyberLab

Combining Israeli military threat intelligence and the world's
Largest CASB and cloud security platform

| Cloud Cybersecurity Research | Breach Investigations | Cybersecurity Assessments |
|---|---|---|
| **1B+**<br>Daily Objects | **10M+**<br>Daily Users | **>200K**<br>Applications |

cisco

# The CloudLock Customer Advantage

Installation in less than 10 minutes

World-class customer success team with access to CloudLock CyberLab

CloudLock Connect Community with Peer Insights

Backed by World-Class Security Certifications