



ACCENTURE SECURITY

FROM BEING HACKED ... TO BECOMING A SECURITY LEADER

SECURITY
CASE
STUDIES

Accenture Security Services

Around the world and around the clock

350+
pending
and issued
Patents related to security



5 billion+
raw security events
processed daily



330+
Clients
spanning
67 countries

People
5,000+



20+ years
of experience helping clients
secure their organizations



Washington, DC

Naples




Prague (~120 FTE)

Tel Aviv






Manila

Bangalore

Buenos Aires

-  Cyber Labs
-  Centers of Excellence
-  Cyber Fusion Centers

Covering the entire Security Lifecycle

 Strategy & Risk	 Cyber Defense	 Digital Identity	 Application Security	 Managed Security
Security advisory services for boards & executives	Breach readiness & response	Automated identity governance	Data security & privacy	Managed cyber defense
Cybersecurity strategy & operating model development	Attack surface reduction	Digital identity for consumers	API security	Managed digital identity
Security in M&A	Security transformation	Digital identity innovation	Enterprise application security	Managed compliance
Governance, risk & compliance	Advanced threat services		Secure application development	
Business continuity & cyber resilience				

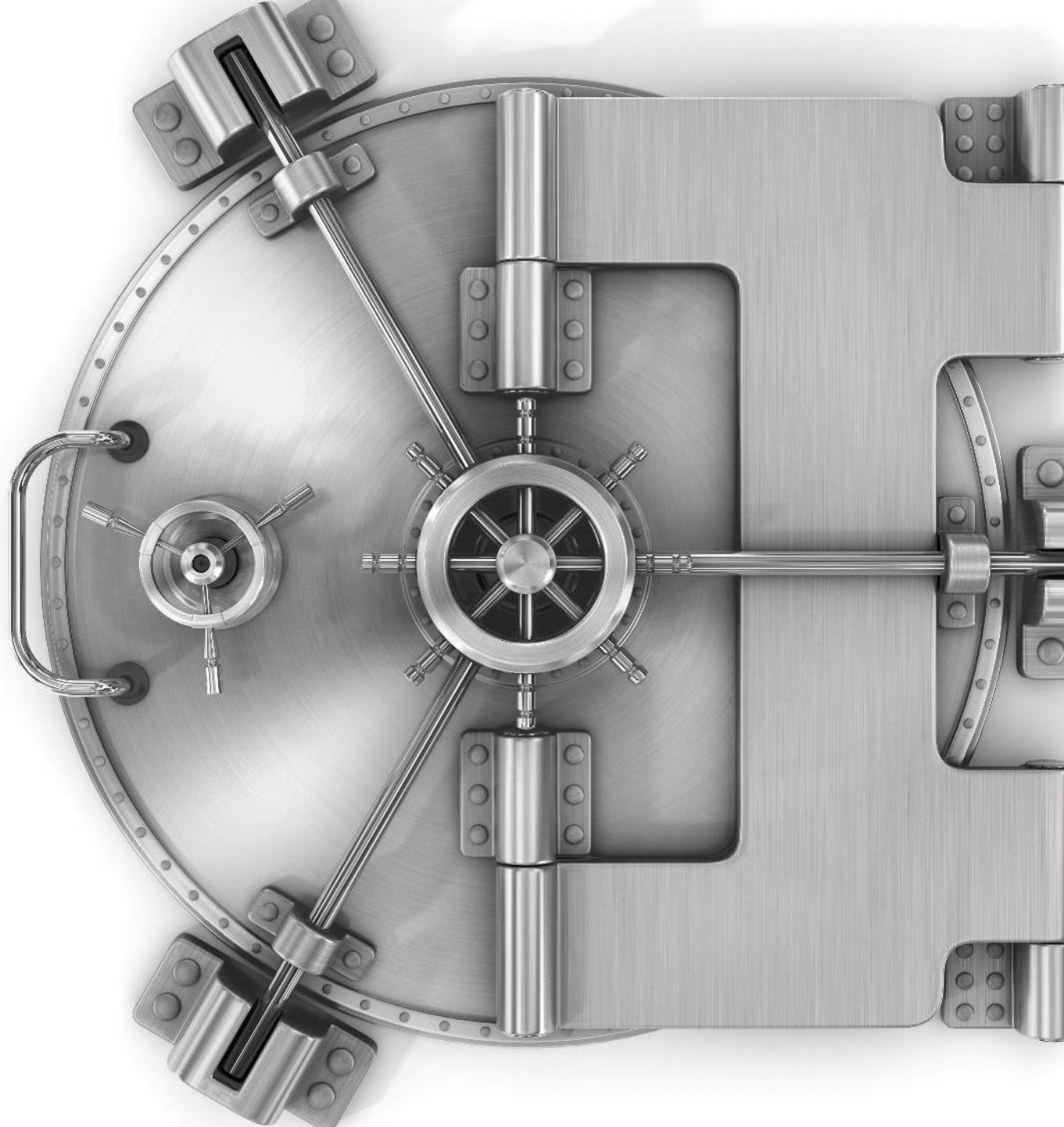
CASE #1

**OUR CLIENT
LOCAL BANK DECOUPLED FROM
A GLOBAL BANKING GROUP**

**IN 2017, ACCENTURE WAS
ASKED BY THE BANK TO
UNDERTAKE A SECURITY
ASSESSMENT**

**TASK: FIND A WAY TO BREAK
INTO THE BANK AND STEAL THE
“KEYS TO THE SAFE”**

**PRAGUE SOC MOBILIZED FOR
THE TEST**



EMAIL PHISHING CAMPAIGN

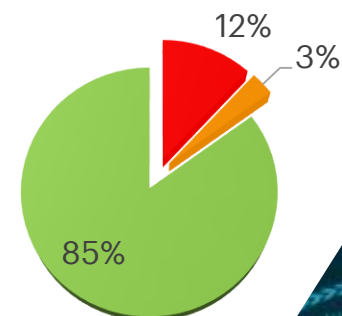
Phishing email advertising a brand new benefit for the employees sent to 1000 people

12% of people opened the email and inserted their credentials

3% of people clicked the URL without inserting their credentials

85% did not open the URL

E-mail campaign



PHONE PHISHING CAMPAIGN

Impersonating IT Help Desk calling from a mobile phone to open a URL

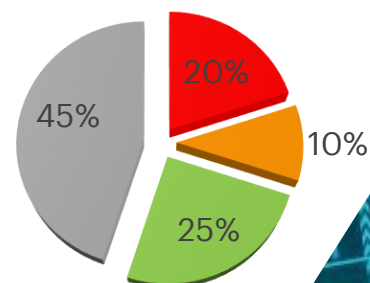
4 (30%) employees have visited the phishing portal and submitted their credentials

2 (10%) employees only visited the phishing portal

5 (25%) employees have uncovered phishing attempt

9 (45%) employees have not picked the phone

Phone campaign



VULNERABILITY TESTING

Identified vulnerabilities of network infrastructure and/or existing applications running in the environment of the Bank and acquired access to various applications

TREATMENT OF IDENTIFIED VULNERABILITIES AND GAPS

- ✓ BLOCK OF EXTERNAL EMAILS THAT MIMIC CLIENT'S DOMAIN
- ✓ MULTIFACTOR AUTHENTICATION FOR DOMAIN ACCOUNTS
- ✓ MANAGEMENT OF ADMINISTRATIVE ACCOUNT BY PRIVILEGED IDENTITY MANAGEMENT SOLUTION

INTRODUCTION OF SECURITY AND INNOVATIVE PROJECTS

- ✓ SECURITY AWARENESS PROGRAM FOR ALL EMPLOYEES
- ✓ EXECUTIVE & PRIVILEGED USERS INTRODUCTION TO INFORMATION AND CYBER SECURITY

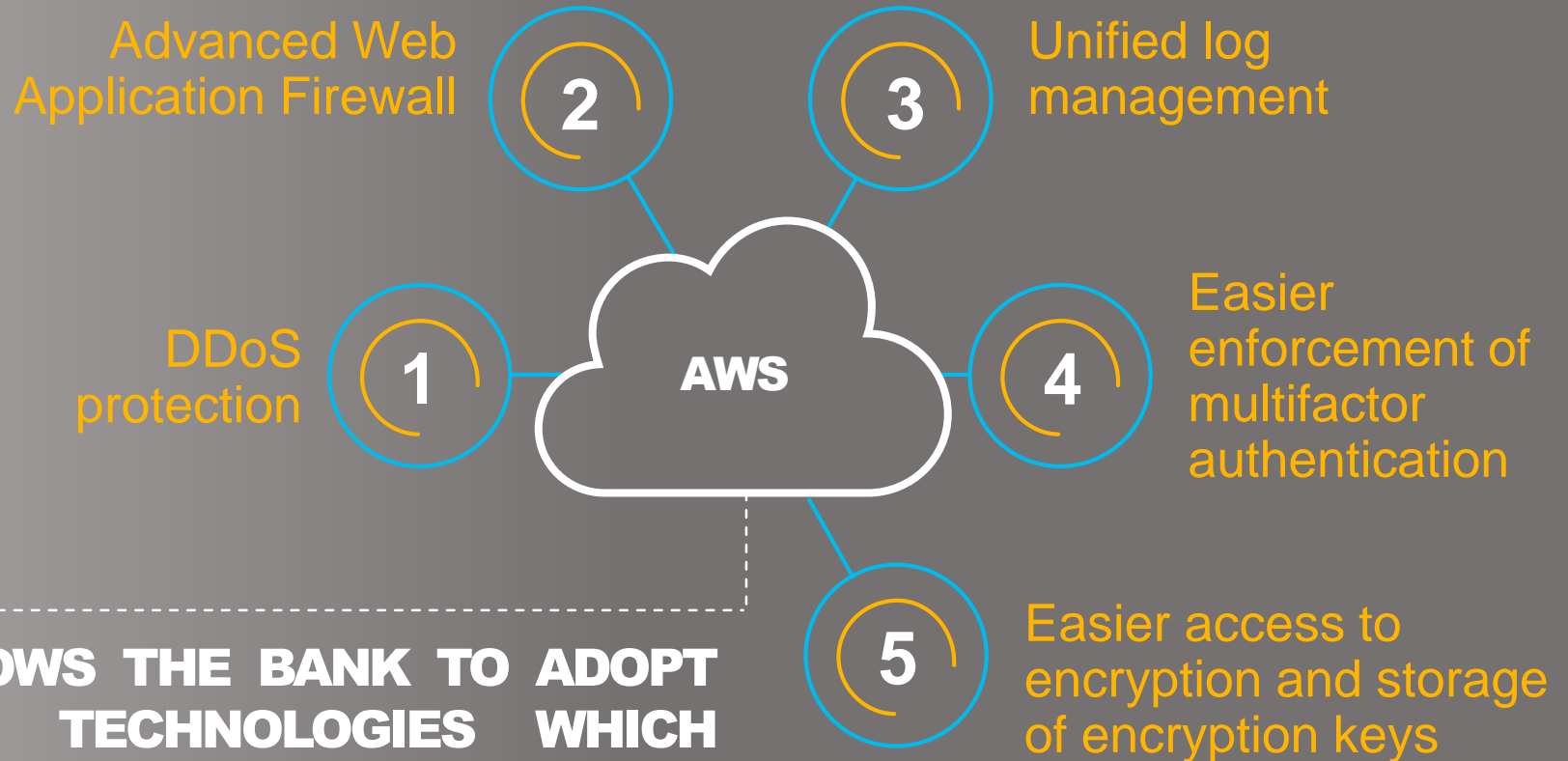
IMPROVE SECURITY POSTER BY MIGRATING TO THE CLOUD



BANK DECIDED TO GO TO THE CLOUD ENVIRONMENT TO IMPROVE ITS SECURITY POSTURE

**RISK ASSESSMENT UNCOVERED
THERE ARE MANY RISKS FOR THE
BANK BUT MANY CAN BE EASILY
TREATED WITH THE:**

- **COMPREHENSIVE SET OF TOOLS**
- **EASY MONITORING OF ANY ACTIVITY**
- **COMPLIANCE OF INDIVIDUAL RESOURCES WITH SECURITY REQUIREMENTS**



**AWS ALLOWS THE BANK TO ADOPT
SECURITY TECHNOLOGIES WHICH
ARE CURRENTLY NOT USED IN ITS
ENVIRONMENT DUE TO INITIAL
COSTS FOR IMPLEMENTATION**

CASE #2

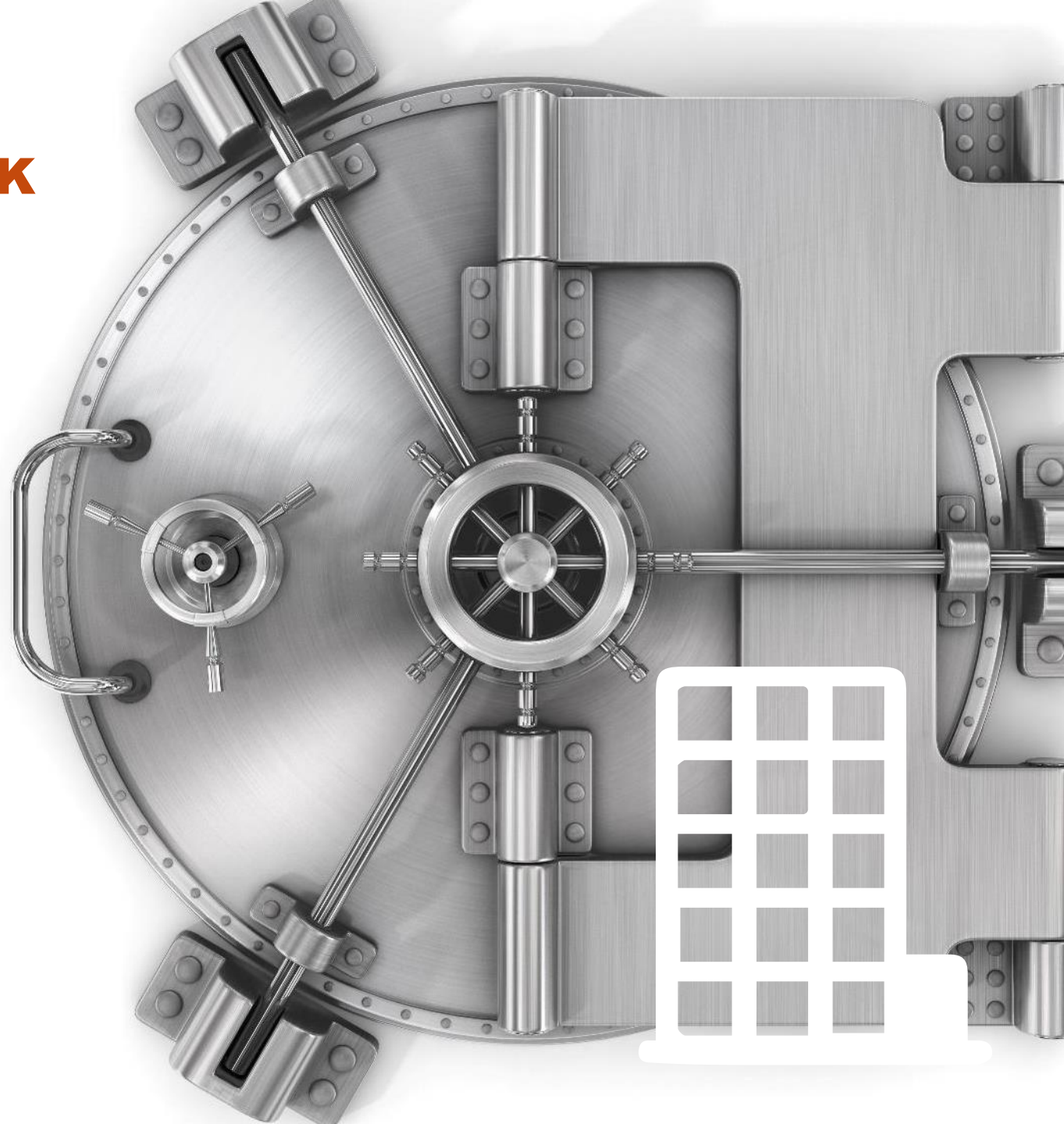
**OUR CLIENT
IS A VERY LARGE AMERICAN BANK**

**THE CLIENT OPERATES
1,000+ BRANCHES AND
3,000+ ATMS**

MANY 1000 USERS

**LOTS OF SAAS APPLICATIONS
RUNNING**

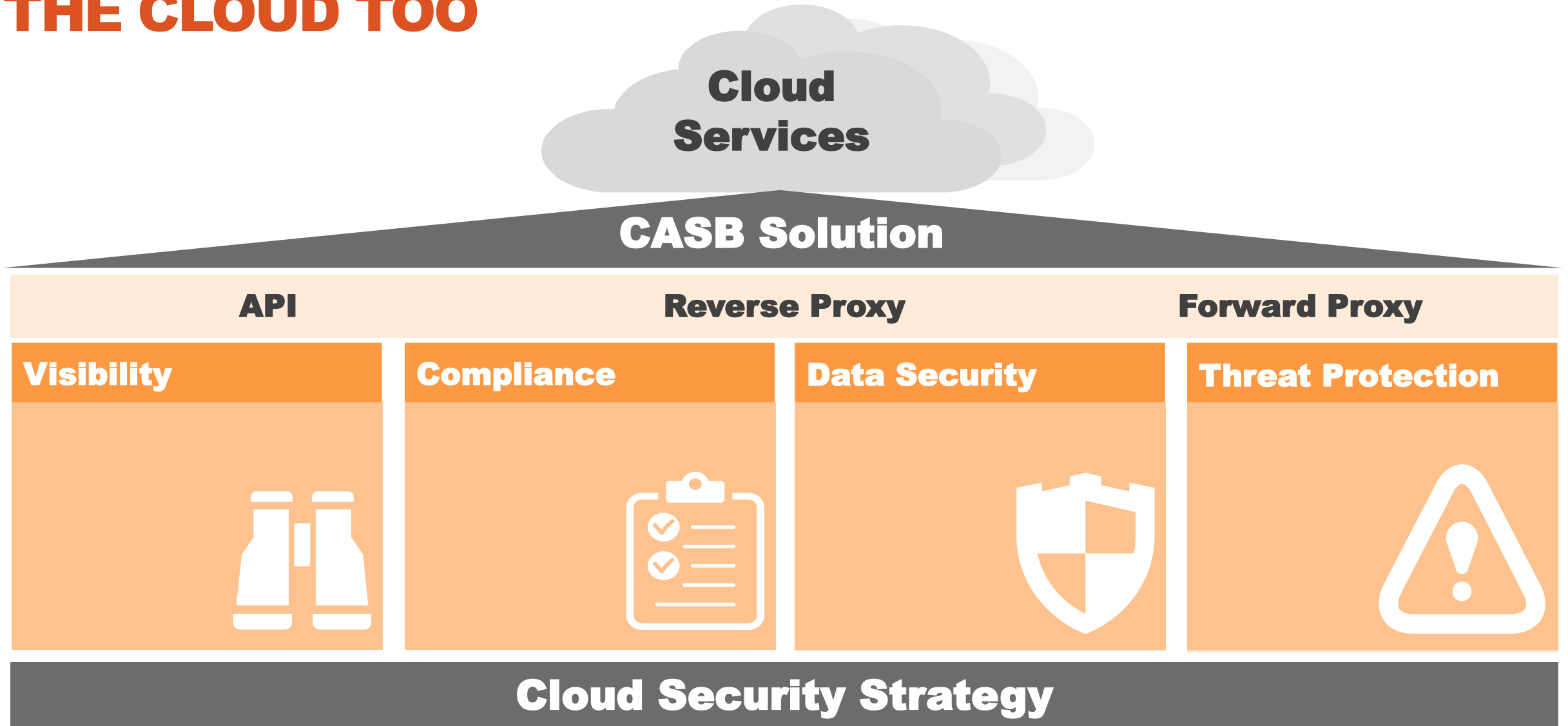
HOW MANY?



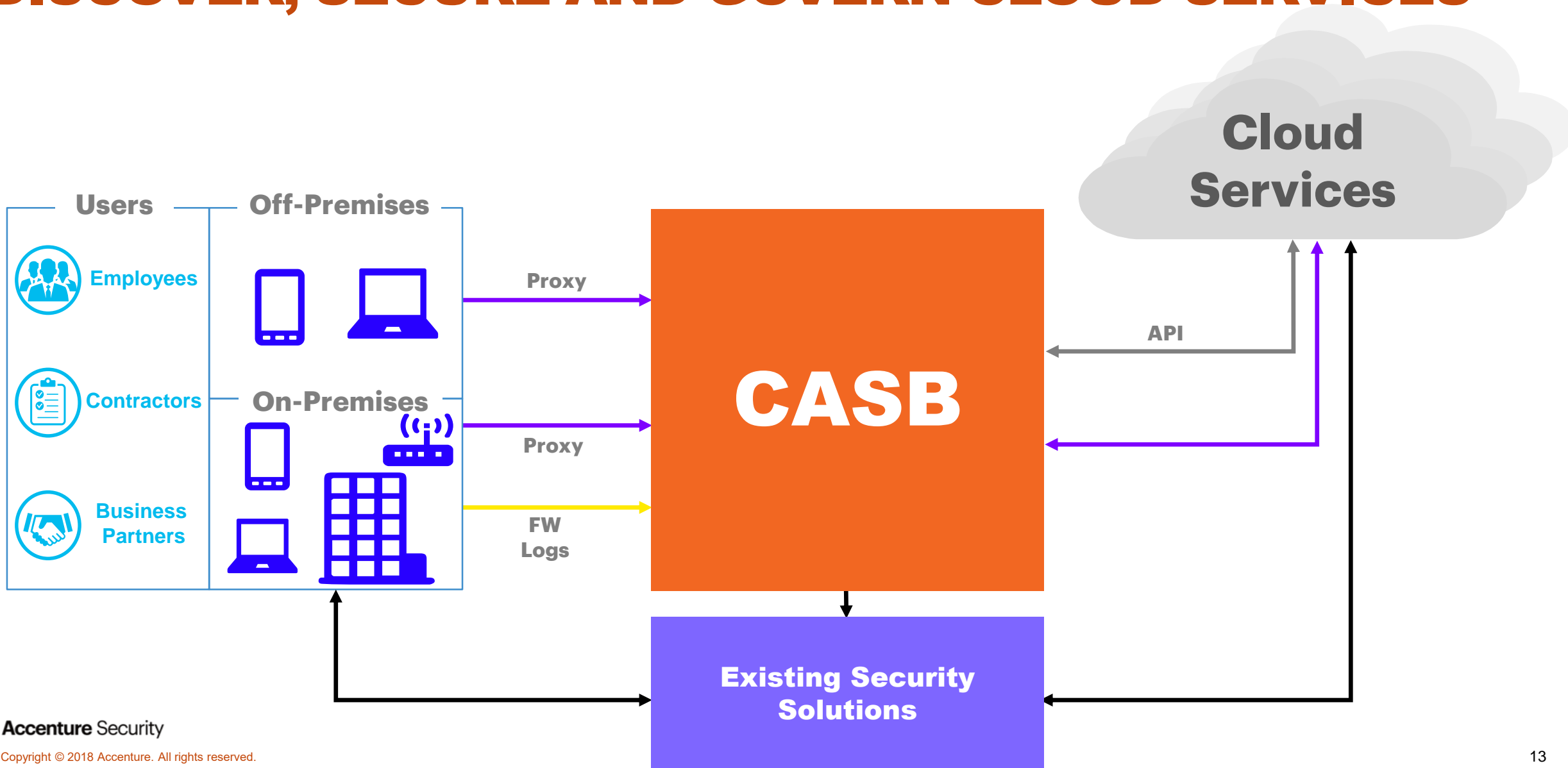
AS YOU EXTEND TO THE CLOUD, CASBS CAN ADDRESS GAPS IN SECURITY ...



... AND EXTEND YOUR SECURITY CAPABILITIES TO THE CLOUD TOO



CASBS PROVIDE A FLEXIBLE ARCHITECTURE TO DISCOVER, SECURE AND GOVERN CLOUD SERVICES



THE CLIENT SOUGHT TO IMPROVE SECURITY

**BY REVIEWING CLOUD SECURITY REQUIREMENTS
AND PROACTIVELY ADDRESS SECURITY GAPS**



GATHER PROXY DATA

SENT IT TO CASB

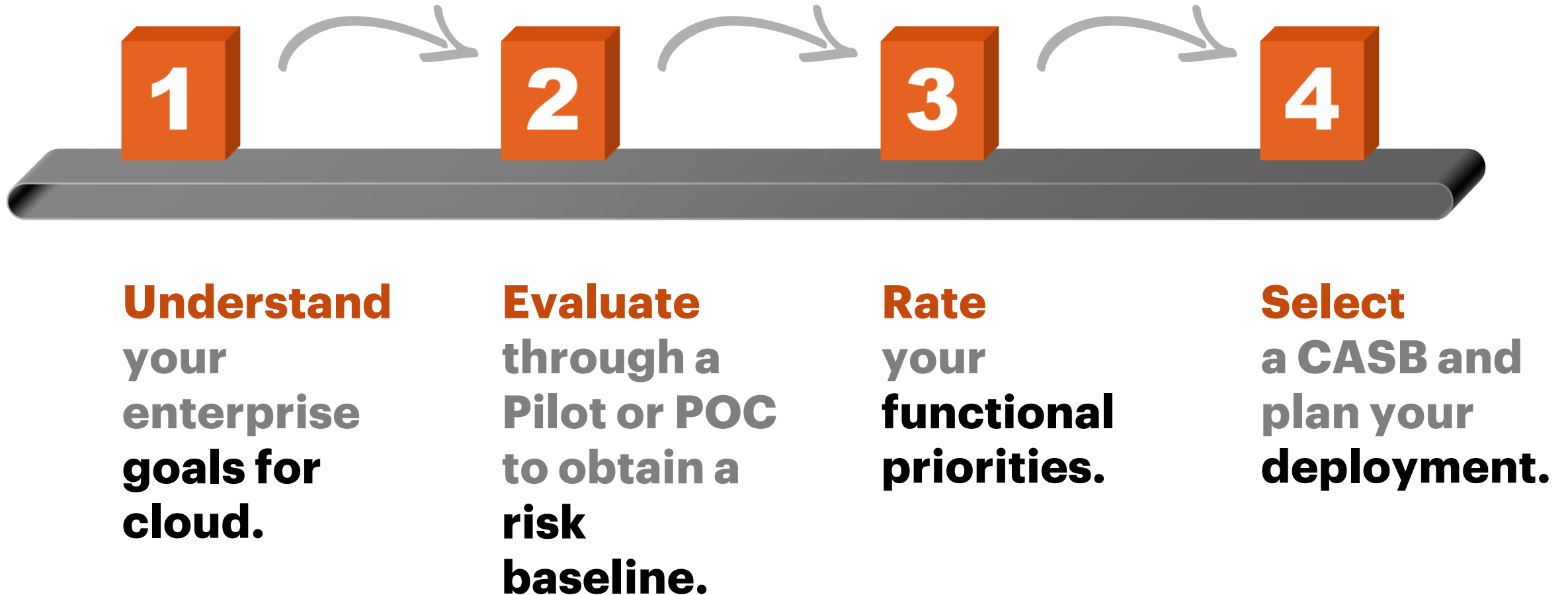
ANALYZE DATA

DETERMINE RISK

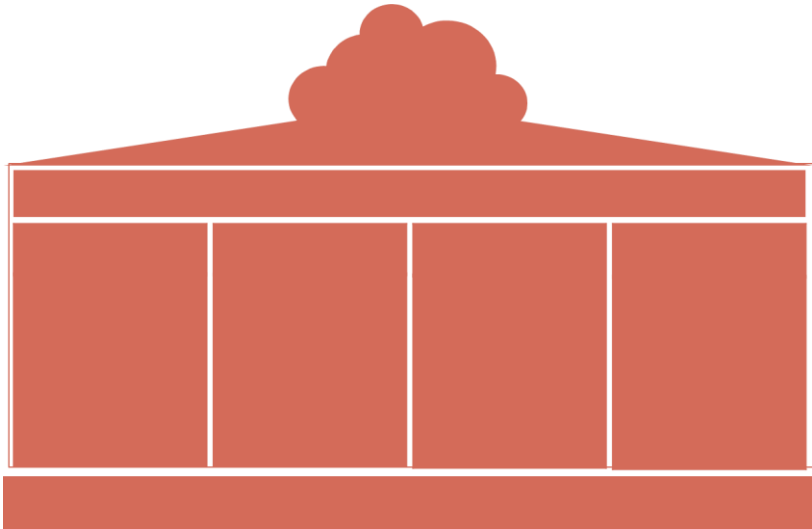
ROADMAP



GET STARTED AND SEE WHAT OPTION WORKS FOR YOUR ENVIRONMENT



FINALLY, THINK ABOUT THE CYBER DEFENSE OPERATING MODEL



How does the operating model include CASB?





ACCENTURE SECURITY

Contact:
Akis Giouchas, akis.giouchas@accenture.com