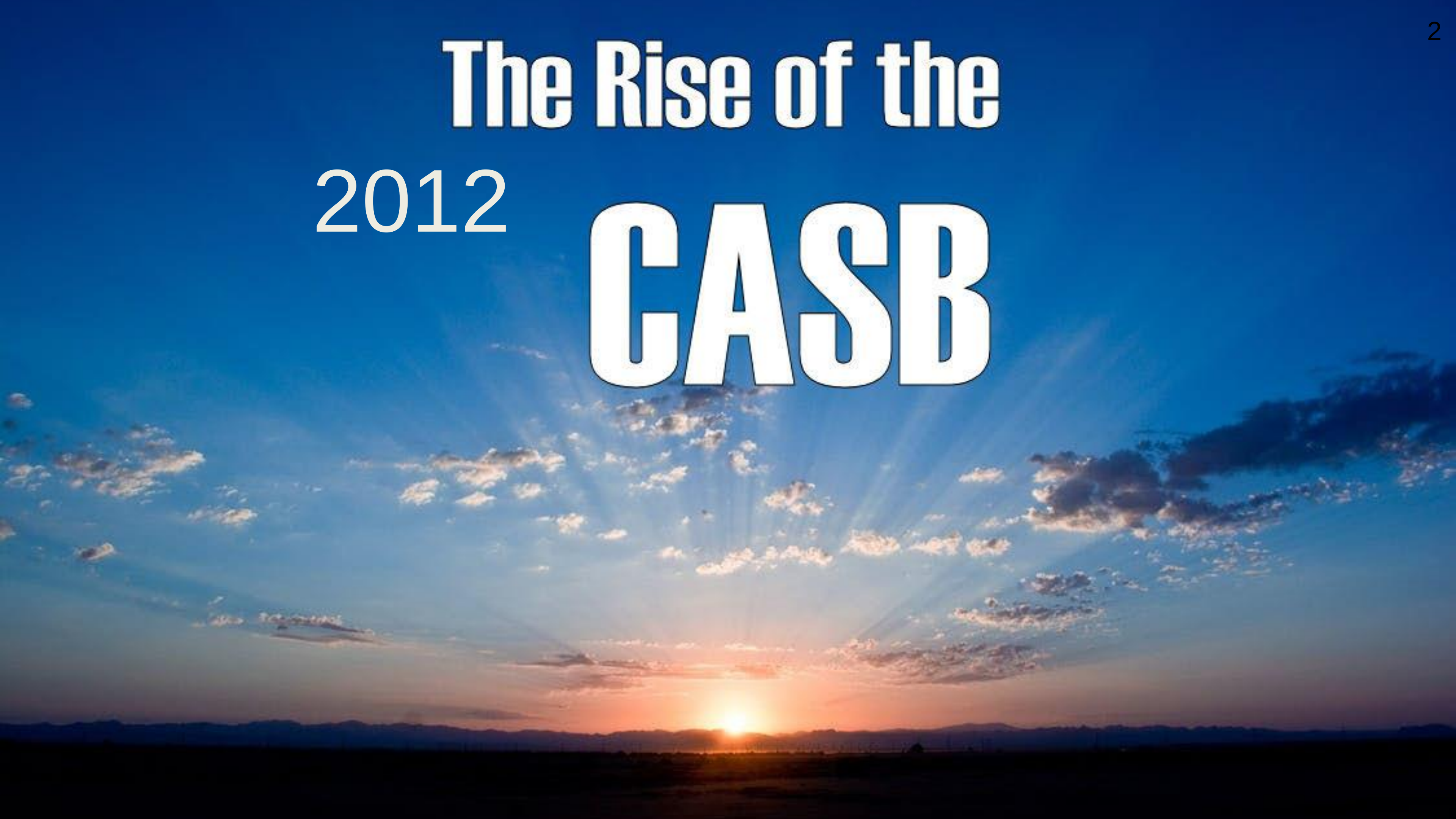
CASB

PvIB
Platform voor
InformatieBeveiliging

Martijn Duijm

bitglass



The Rise of the CASB

2012

While Shadow IT Grows . . .
Traditional IT Stalls

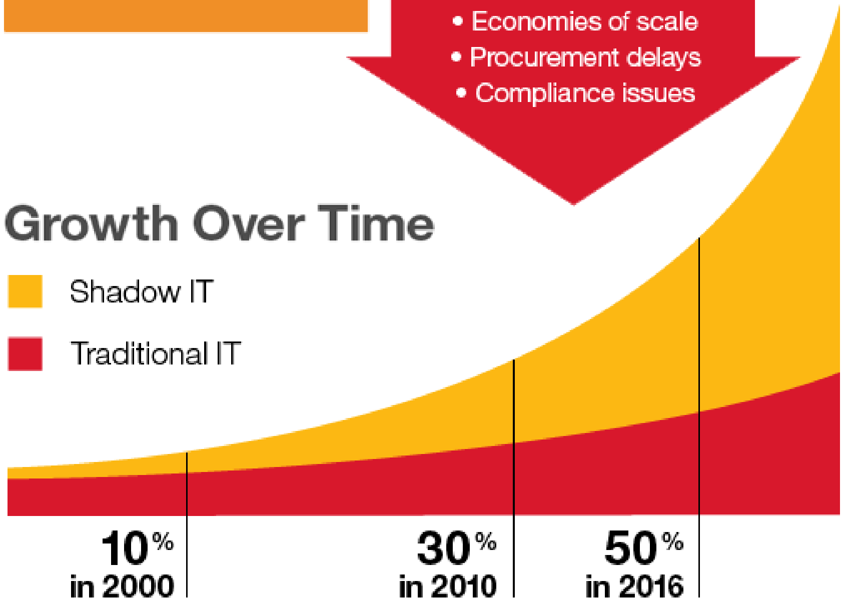
Shadow IT

- Fast innovation
- Low barriers to access
- Ample options
- Disruptive technologies
- BYOD/BYOA/BYOT
- Cloud options

Traditional IT

- Manageable
- Standardized
- Budget restricted
- Economies of scale
- Procurement delays
- Compliance issues

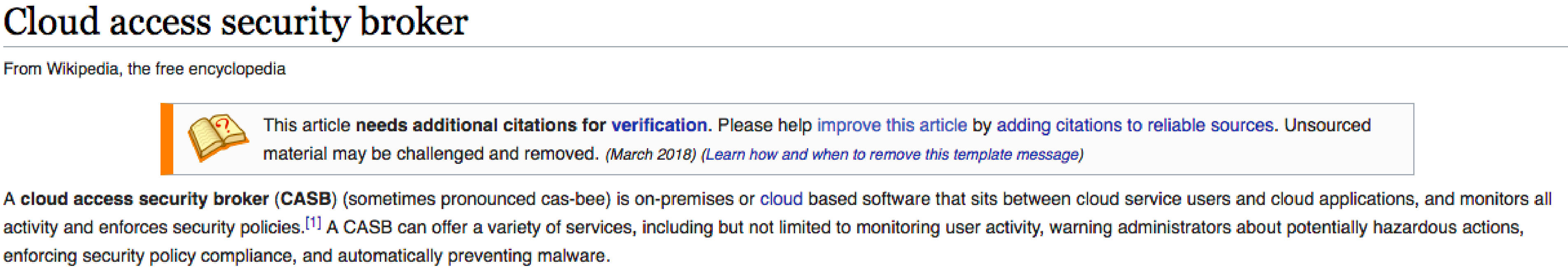
Growth Over Time



Cloud in numbers…

- **>1000 SaaS apps**
  used at a typical enterprise company
- **Up to 40%** of IT spend is
  Shadow IT (Unsanctioned apps)
- **65%** of organisations use Office365
- **Less than 50 percent** of organizations have deployed even the most basic cloud security tool – SSO. Only 47 percent of organizations sampled had a SSO tool in use.

So.. What is a CASB(ah)?



Cloud access security broker

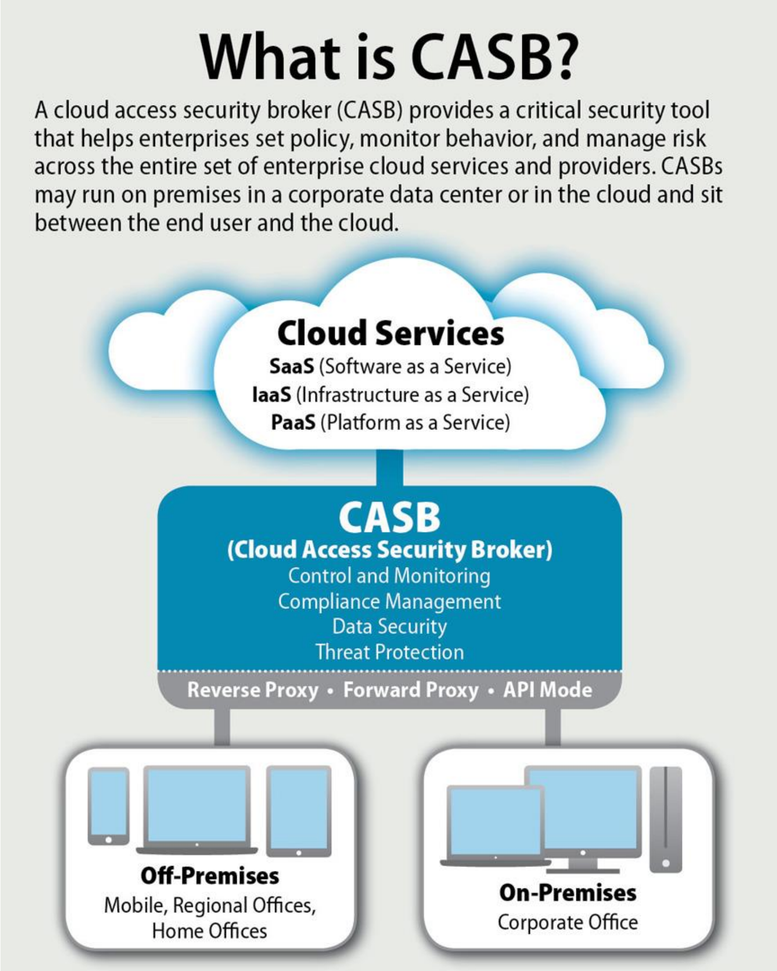
From Wikipedia, the free encyclopedia

This article **needs additional citations for verification**. Please help improve this article by adding citations to reliable sources. Unsourced material may be challenged and removed. *(March 2018) (Learn how and when to remove this template message)*

A **cloud access security broker** (**CASB**) (sometimes pronounced cas-bee) is on-premises or cloud based software that sits between cloud service users and cloud applications, and monitors all activity and enforces security policies.[1] A CASB can offer a variety of services, including but not limited to monitoring user activity, warning administrators about potentially hazardous actions, enforcing security policy compliance, and automatically preventing malware.

Cloud Access Security Broker, AH!

CASB ? What ?



What is CASB?

A cloud access security broker (CASB) provides a critical security tool that helps enterprises set policy, monitor behavior, and manage risk across the entire set of enterprise cloud services and providers. CASBs may run on premises in a corporate data center or in the cloud and sit between the end user and the cloud.

Cloud Services

SaaS (Software as a Service)
IaaS (Infrastructure as a Service)
PaaS (Platform as a Service)

CASB

(Cloud Access Security Broker)

Control and Monitoring
Compliance Management
Data Security
Threat Protection

Reverse Proxy • Forward Proxy • API Mode

Off-Premises
Mobile, Regional Offices, Home Offices

On-Premises
Corporate Office

Gartner's Vision on CASB

visibility

apps, data, users & devices

compliance

apps, data, users & devices

data protection

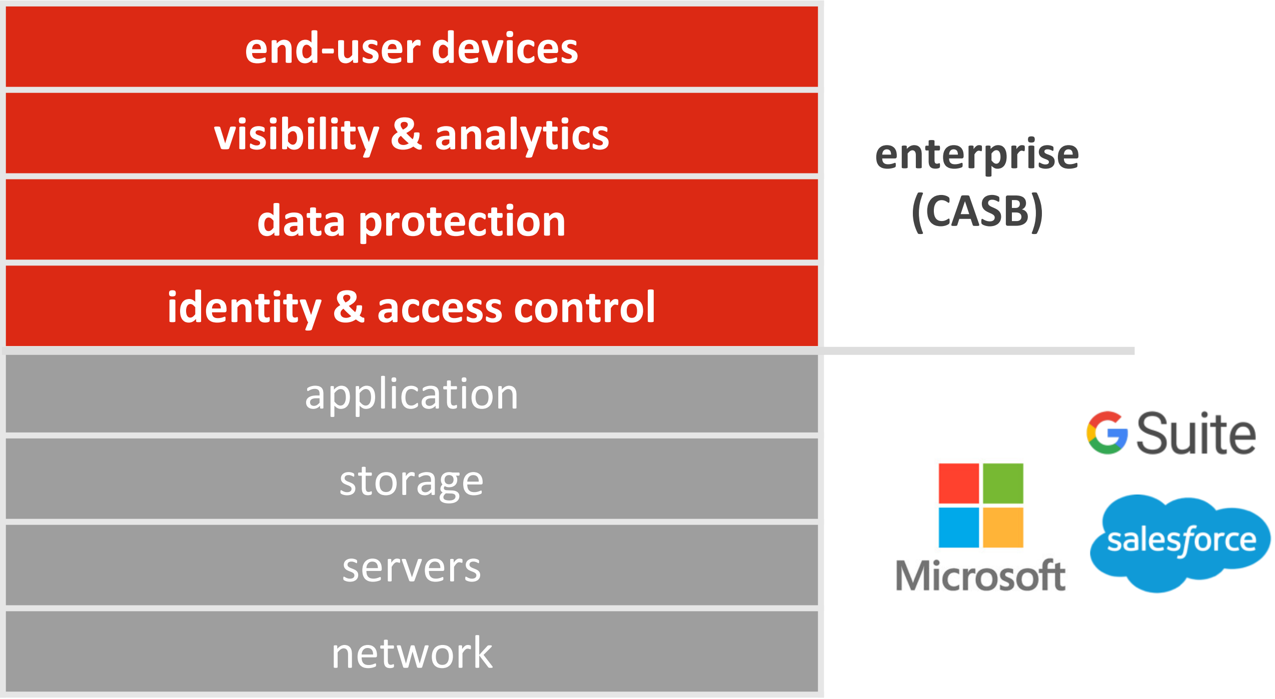
in the cloud, at access, and on devices

threat protection

malware, APT, hijack

So why the need for a CASB?

enterprises can't rely solely on native app security



end-user devices

visibility & analytics

data protection

identity & access control

application

storage

servers

network

enterprise (CASB)

Cloud Service Adoption

- https://www.gartner.com/newsroom/id/3591417
- By 2019, total public cloud services spending rise to $13.6 billion
- The highest growth (SaaS) with a 28.5 percent increase in 2017

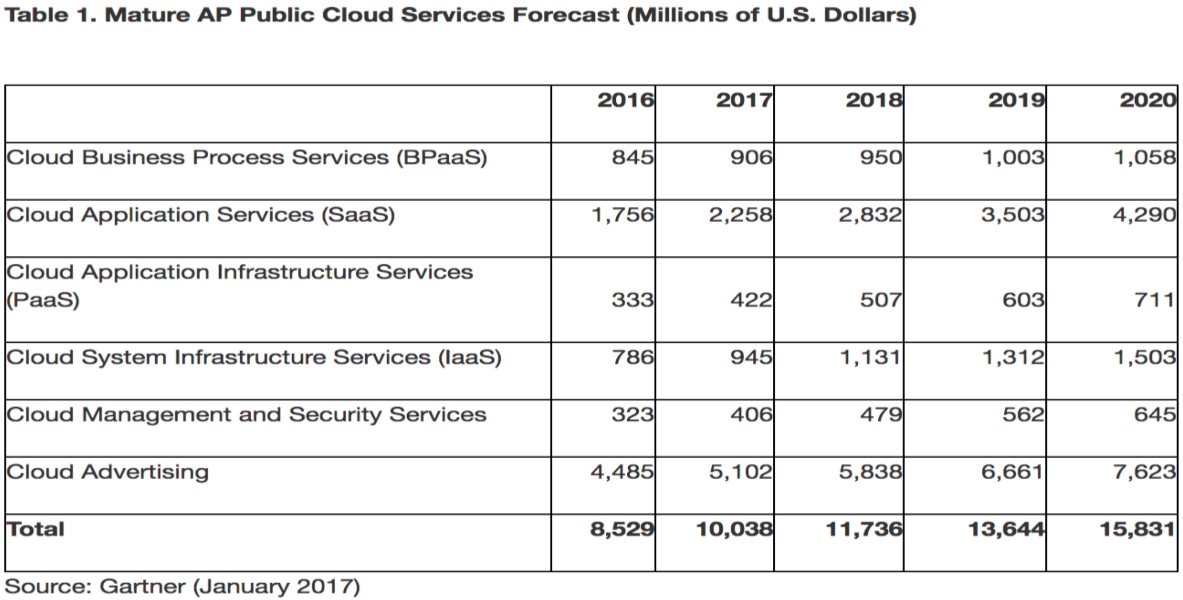


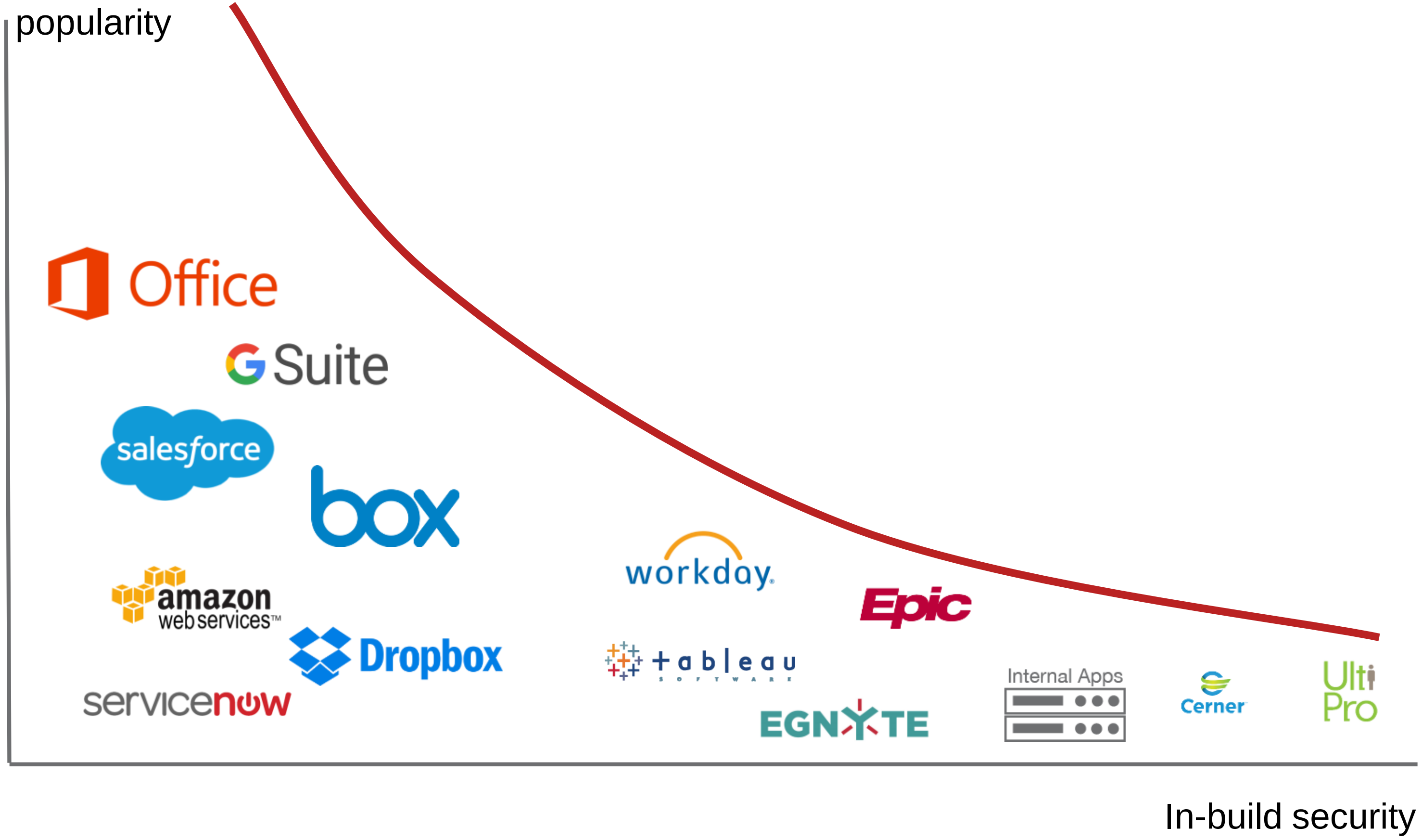
Table 1. Mature AP Public Cloud Services Forecast (Millions of U.S. Dollars)

	2016	2017	2018	2019	2020
Cloud Business Process Services (BPaaS)	845	906	950	1,003	1,058
Cloud Application Services (SaaS)	1,756	2,258	2,832	3,503	4,290
Cloud Application Infrastructure Services (PaaS)	333	422	507	603	711
Cloud System Infrastructure Services (IaaS)	786	945	1,131	1,312	1,503
Cloud Management and Security Services	323	406	479	562	645
Cloud Advertising	4,485	5,102	5,838	6,661	7,623
Total	**8,529**	**10,038**	**11,736**	**13,644**	**15,831**

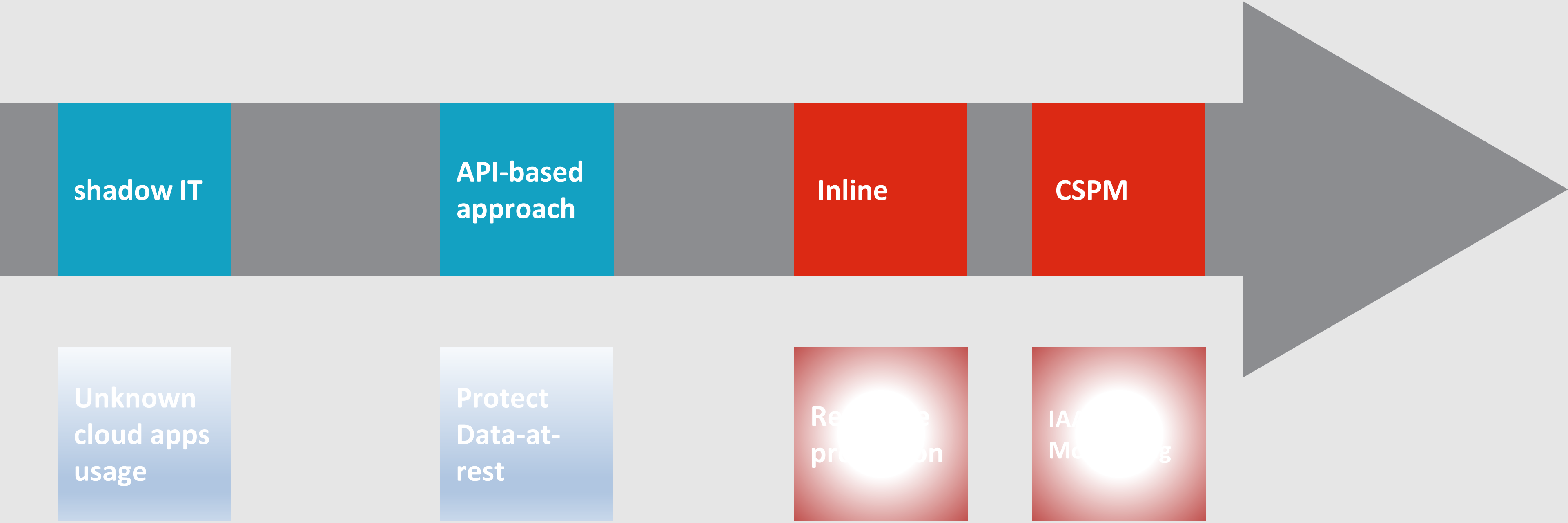
Source: Gartner (January 2017)

- ”… indicators that migration of application and workloads from on premises data centers to the cloud, as well as development of cloud ready and cloud native applications, are fueling growth in the cloud space," said Sid Nag research director at Gartner.
- "Software vendors will continue to shift investments from on-premises license-based software to cloud-based offerings."

The Evolving Cloud Landscape



CASB – 2012 -> 2018



shadow IT

API-based approach

Inline

CSPM

Unknown cloud apps usage

Protect Data-at-rest

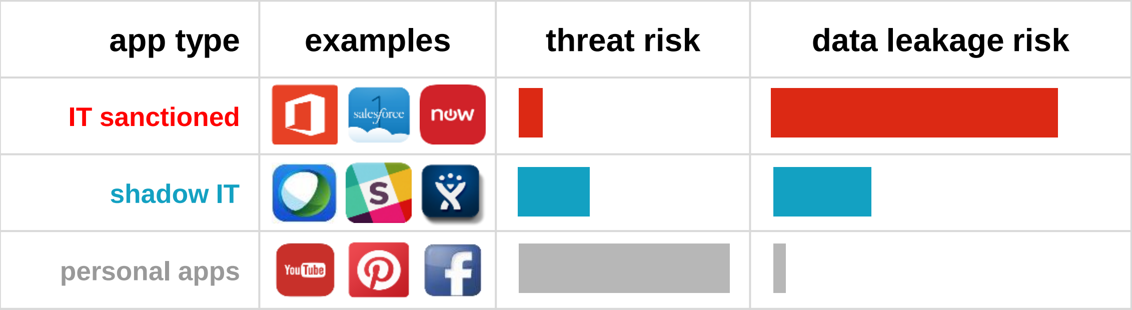
Real-time protection

IAAS Monitoring

Shadow IT

IT departments have lack of visibility

- thousands of enterprise cloud apps today (and growing)
- 95% of apps are not sanctioned by IT
  - many of which are unknown to IT
- most apps are not enterprise ready



app type	examples	threat risk	data leakage risk
IT sanctioned	salesforce now	█	████████████
shadow IT	S	███	████
personal apps	YouTube	█████████	▏

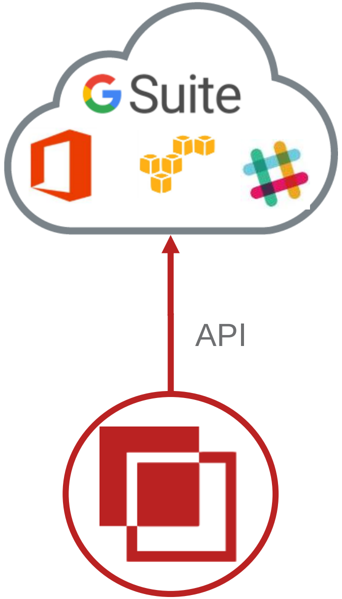
API monitoring

CASB connects to a cloud service

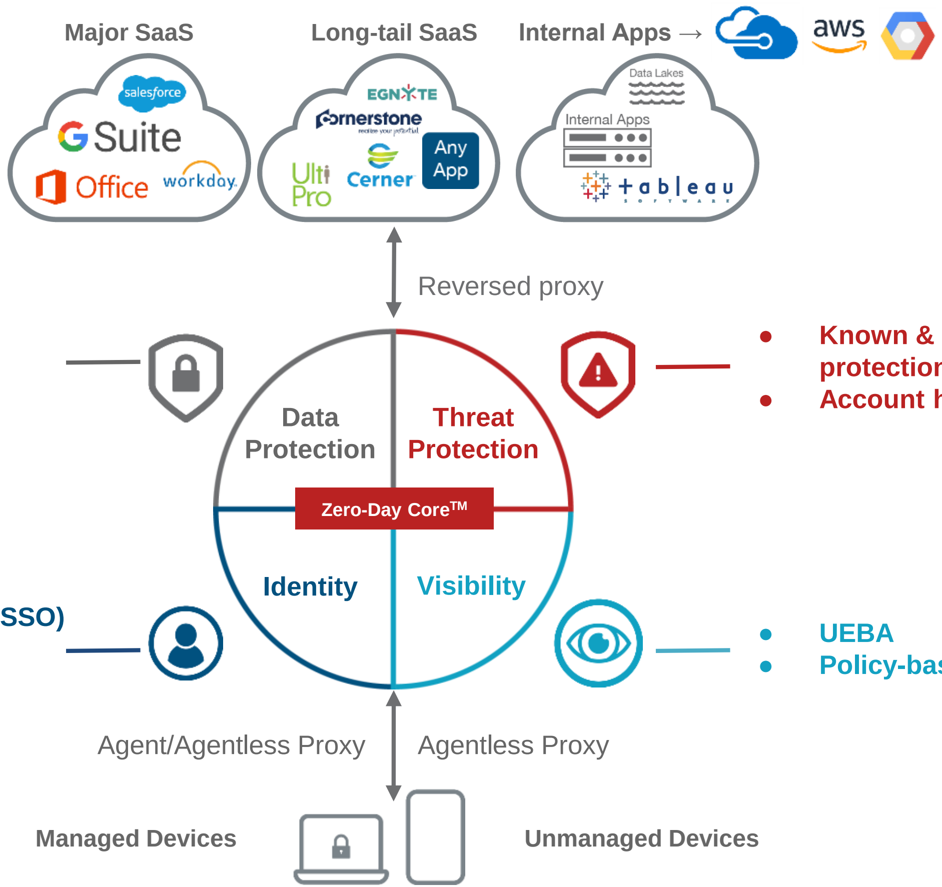
Perpetual Incremental Crawling Based on Changes Every 5 Min

Gotcha’s and Pitfalls

- No real time security
- Limited set of applications



Inline security



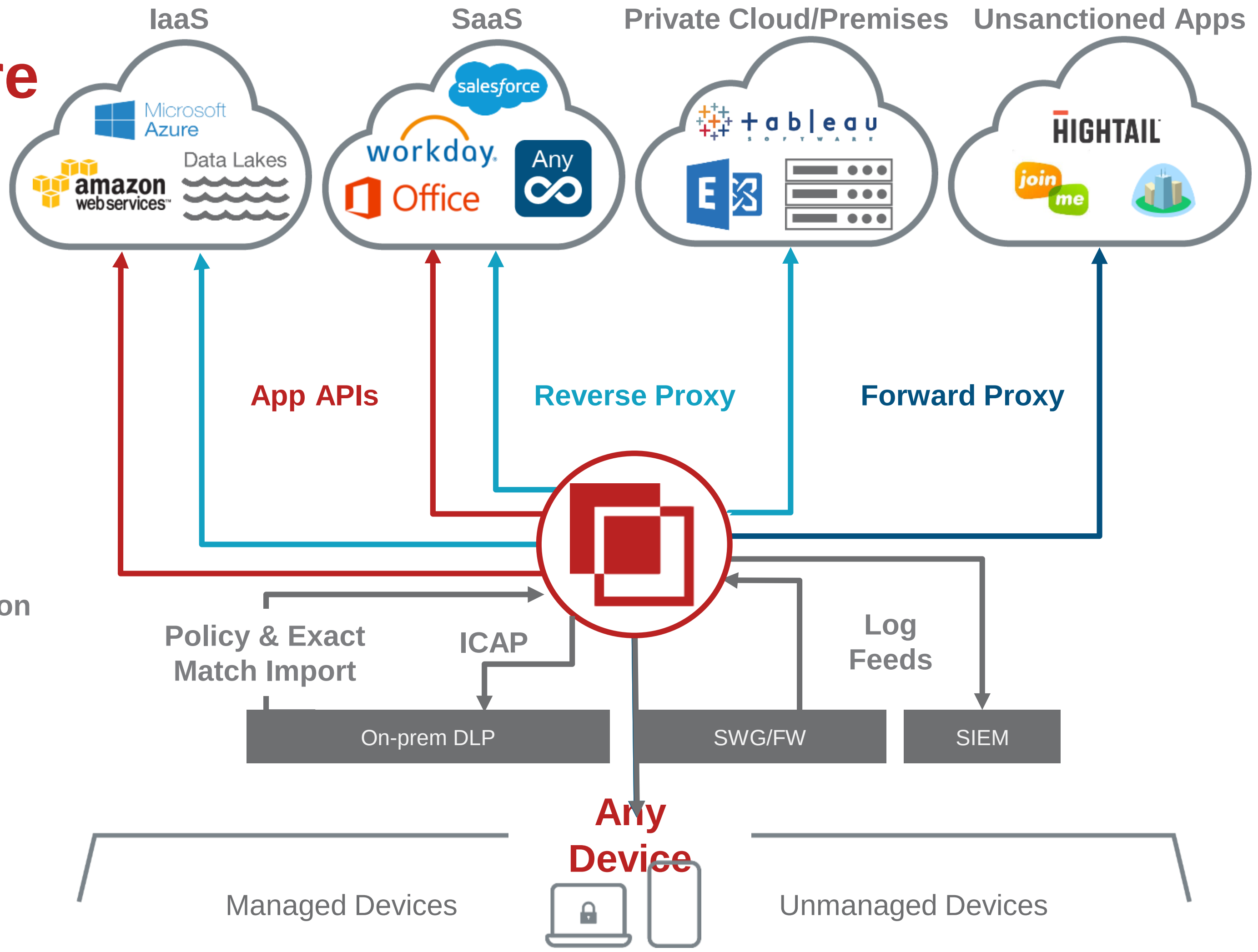
- Contextual access control
- DLP w/ adv. remediation
- Field and file encryption

- Known & Zero-day malware protection
- Account hijack protection

- Integrated Single Sign-On (SSO)
- Step-up multi-factor auth
- Session management

- UEBA
- Policy-based remediation

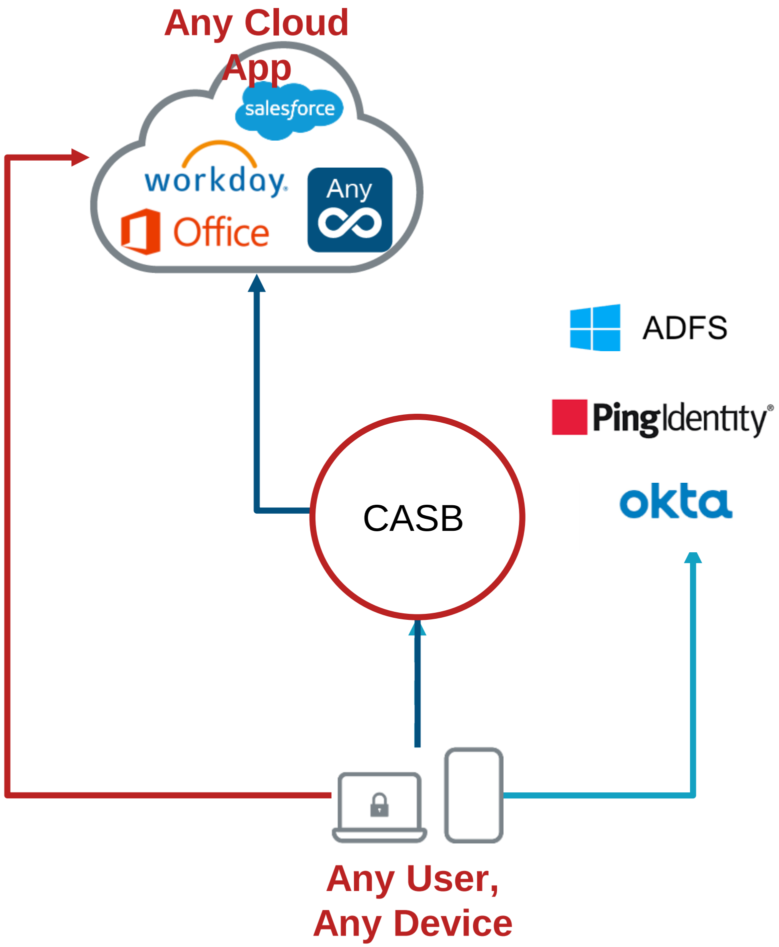
Architecture



1	API
2	Reverse Proxy
3	Forward Proxy
4	Enterprise Integration

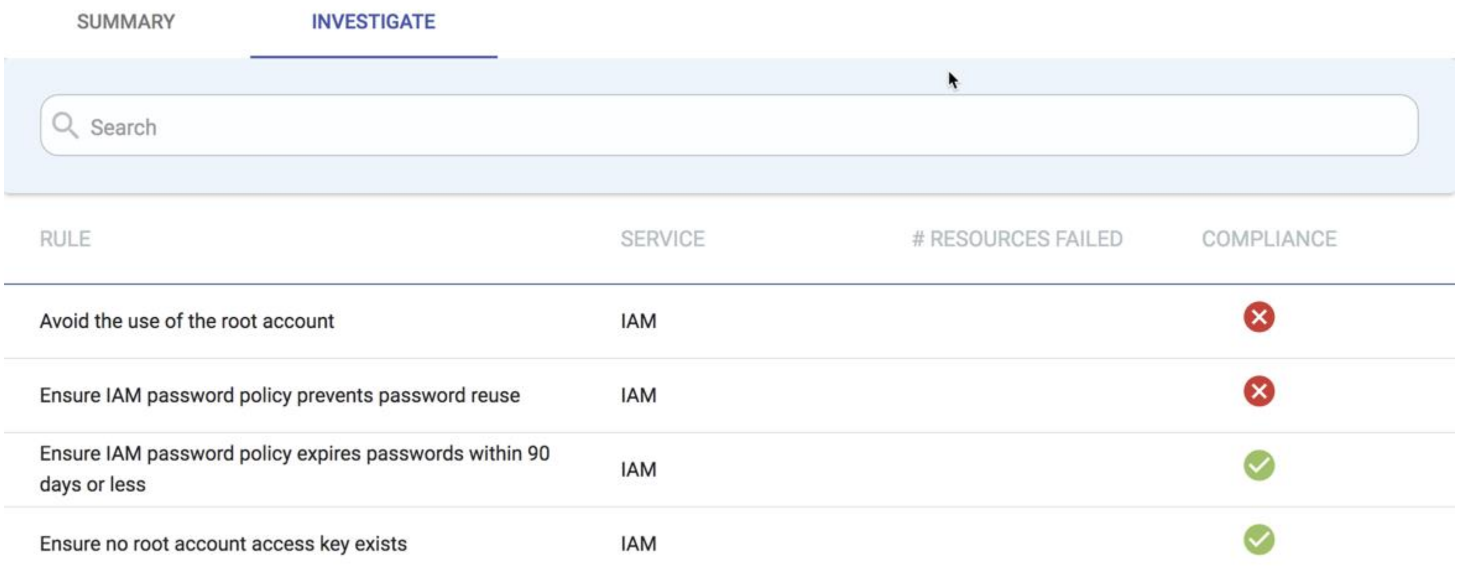
Authentication Flow

1	User connects directly to app
2	User redirected to CASB then to IdP
3	User redirected back to CASB; proxied to app



Continuous IaaS Configuration Monitoring (CSPM)

- Scanning configuration based on industry benchmarks (HIPAA, CIS Benchmark, SOC 2, etc)
- Scored report to determine compliance violations per service / instance / bucket
- Provide remediation documentation and advice
- Ability to create fully customized templates and rules for flexible reporting and alerting



RULE	SERVICE	# RESOURCES FAILED	COMPLIANCE
Avoid the use of the root account	IAM		✗
Ensure IAM password policy prevents password reuse	IAM		✗
Ensure IAM password policy expires passwords within 90 days or less	IAM		✓
Ensure no root account access key exists	IAM		✓

https://www.esecurityplanet.com/mobile-security/casb.html