Cloud Access Security Broker (CASB) Overview

Presenter

John Emerson

Director, Cloud Product Sales, US Federal, SI's and SP's

Date

5 April 2018

Symantec

Top Analysts Rate Symantec a CASB Leader

Forrester Wave

Source: November 2016, The Forrester Wave™: Cloud Security Gateways, Q4 2016
**Forrester evaluated Blue Coat in the evaluation, which was acquired by Symantec*

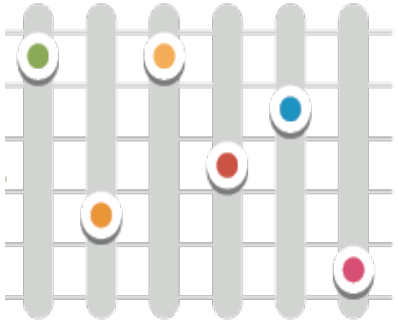
Gartner MQ

Source: Gartner, Inc., Magic Quadrant for Cloud Access Security Brokers, Steve Riley, Craig Lawson, November 30, 2017

Symantec CloudSOC™ Solution

Cloud App Visibility

Identify Shadow IT & monitor cloud usage at a granular level



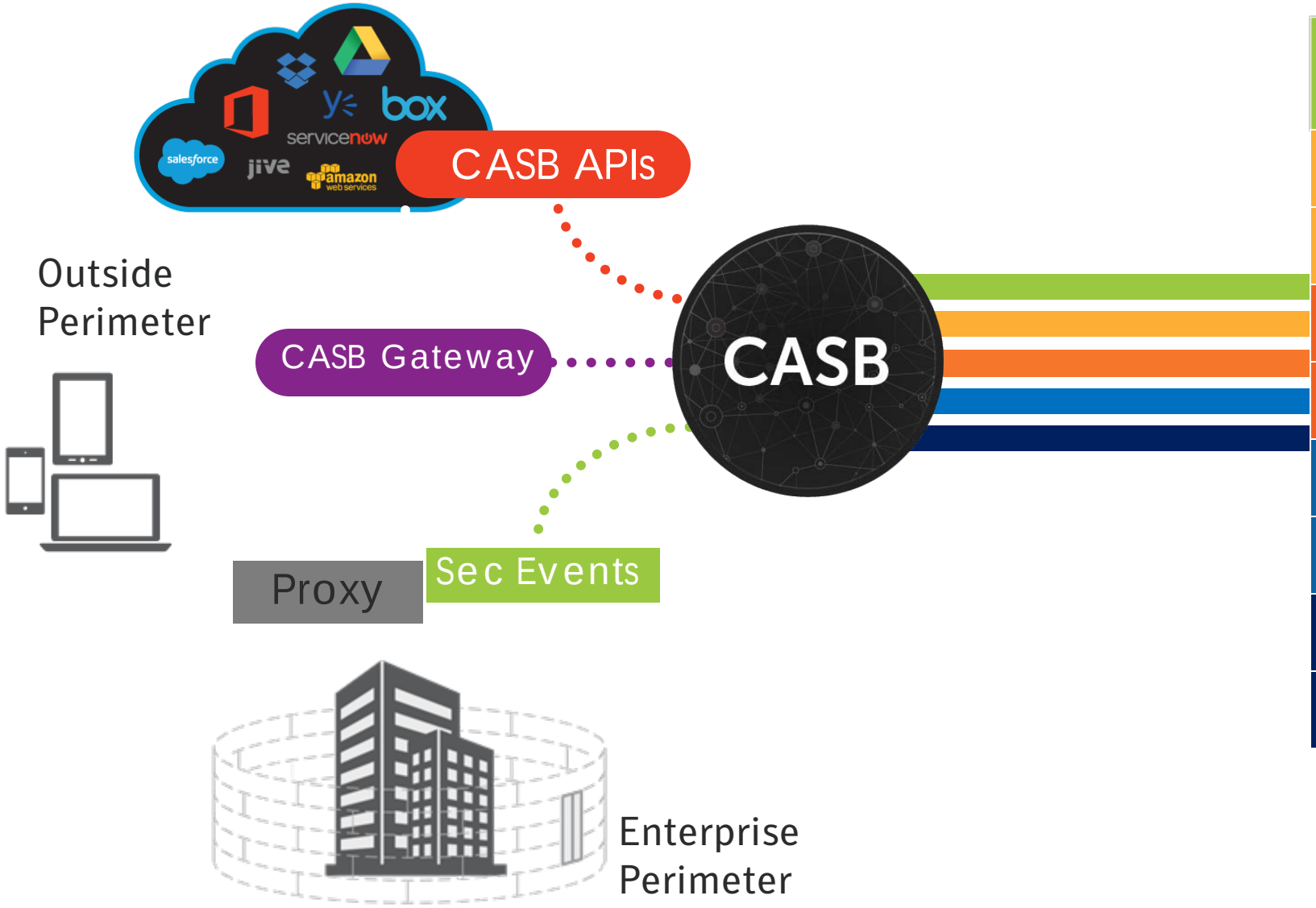
Data Security and Threat Protection

Govern sensitive data with granular controls and encryption/tokenization; Combat threats with user behavior analytics, malware analysis and incident response

Integration with Existing Technologies

Leverage and Integrate with existing technologies, including DLP, Web Proxies, 2 Factor Authentication, Endpoint Protection, and other capabilities

CASB Architecture



- Shadow IT Discovery & Controls
- Cloud Policy & Remediation
- Cloud DLP
- Cloud Intrusion Detection
- Cloud Malware Detection
- Cloud Incident Response
- Cloud Investigations
- Cloud Compliance
- Tokenization

Cloud Based Audit - Shadow IT Risk Assessment

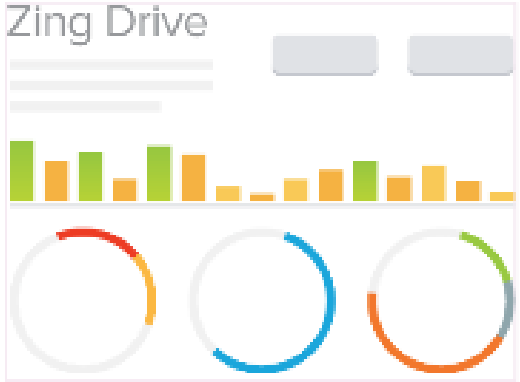
Based on logs and event info from ProxySG and other proxies and firewalls

Database of over 22,000 Applications Globally

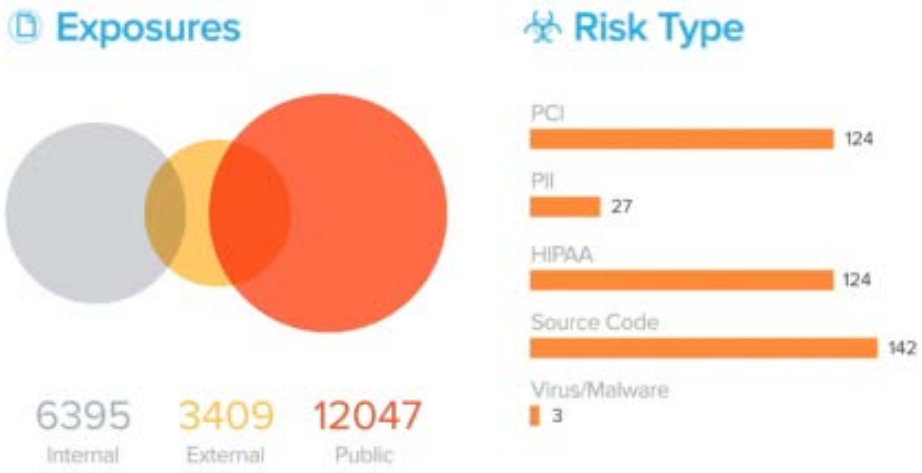
Analytics on your cloud app risks and compliance issues

App usage anomalies across your organization

What apps you should sanction and what apps you should block



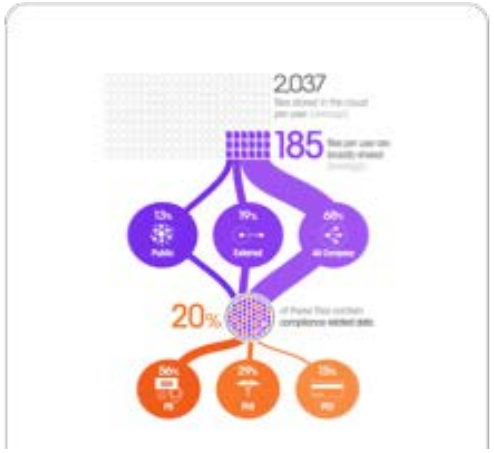
Shadow Data Risk Assessment

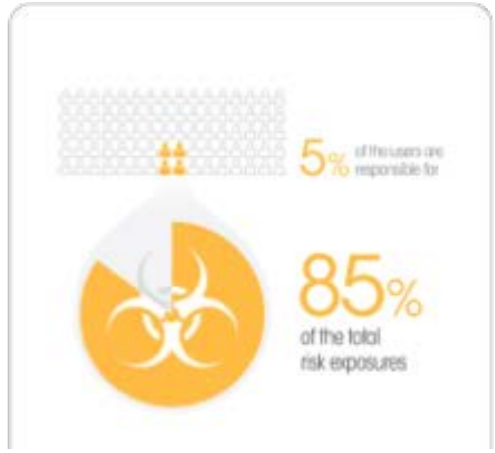


External and public content exposures, including compliance risks

Inbound risky content shared with employees (e.g. malware, IP, etc)

Risky users and user activities

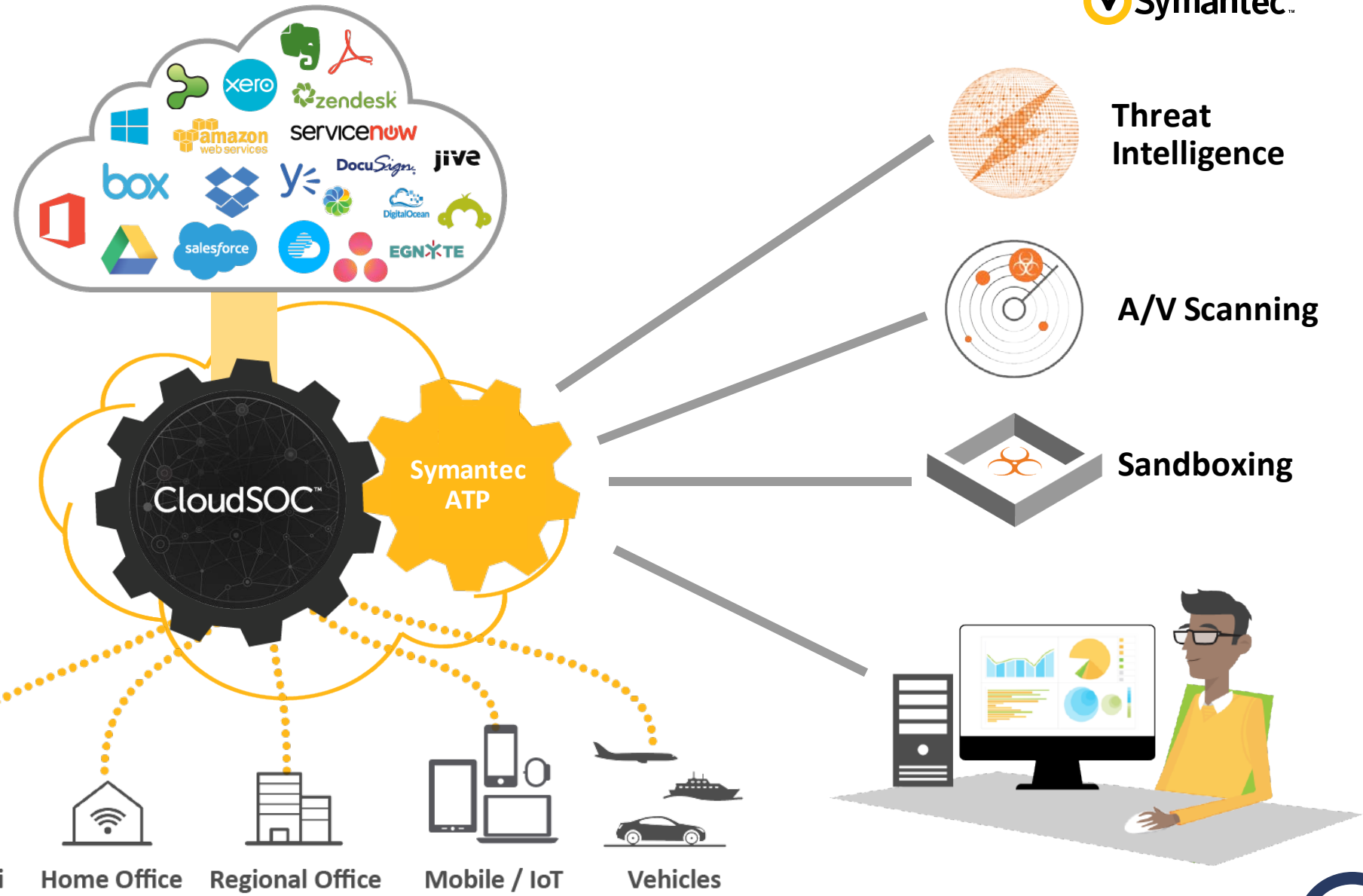




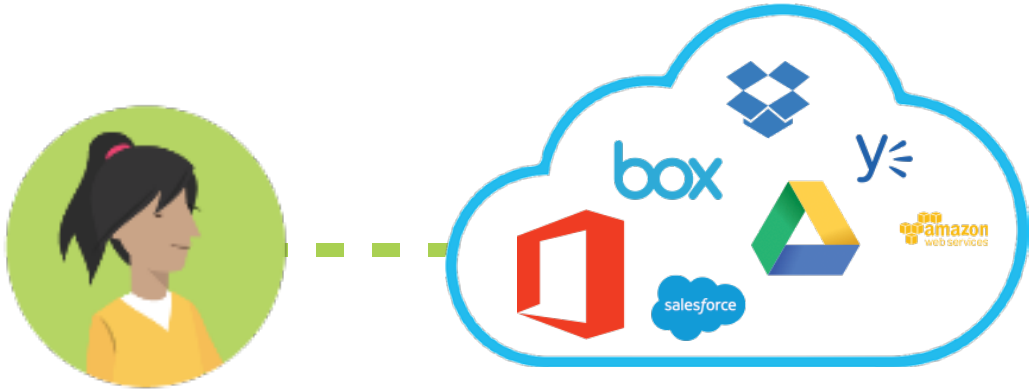
CloudSOC - integrated with Symantec Advanced Threat Protection (ATP)

- **Unique to Symantec – #1 Gartner Magic Quadrant (SEP), Best-of-Breed, Not Open Source**

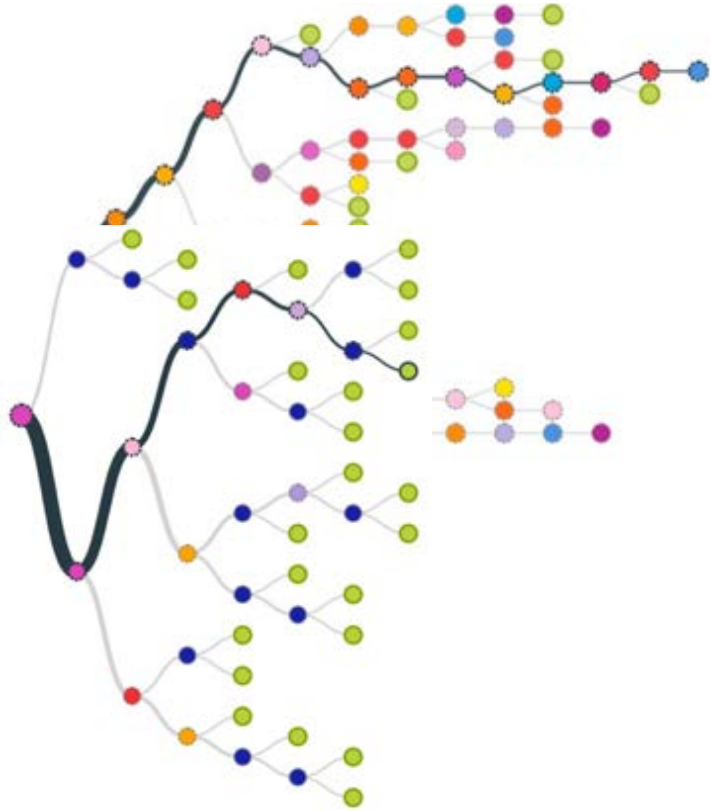
- Scan all content uploaded and stored in cloud apps
- Avoid sync & share distribution of malware
- Extend best-of-breed advanced malware protection to cloud content



User Behavior Analysis



suspicious activity



a unique graph for each individual

What happens when suspicious activity occurs for this user?

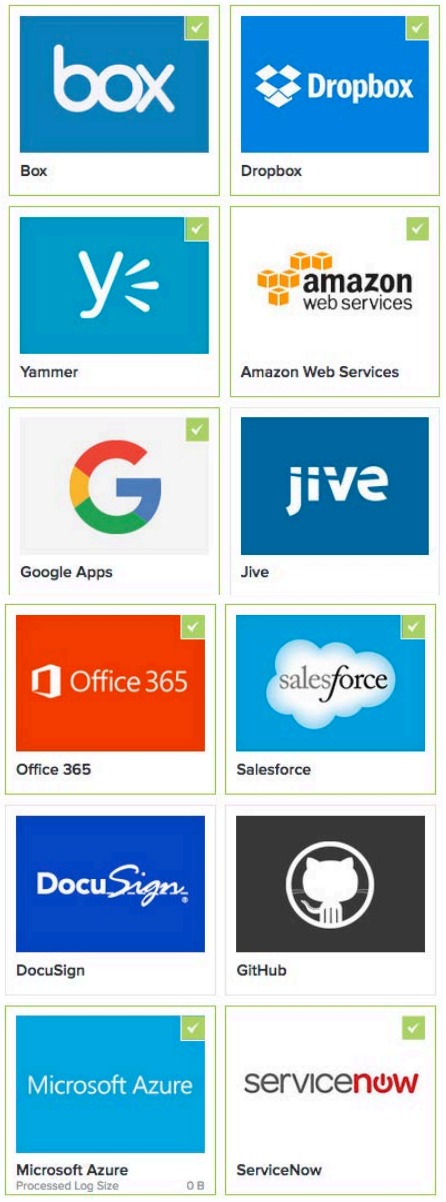
ThreatScore™

suspicious activity

ThreatScore™ based on severity of suspicious activity

- Actionable — visual drill down
- High accuracy — through User Behavior Analysis
- Automation — Leverage for policy enforcement

CASB Mitigation – API Based

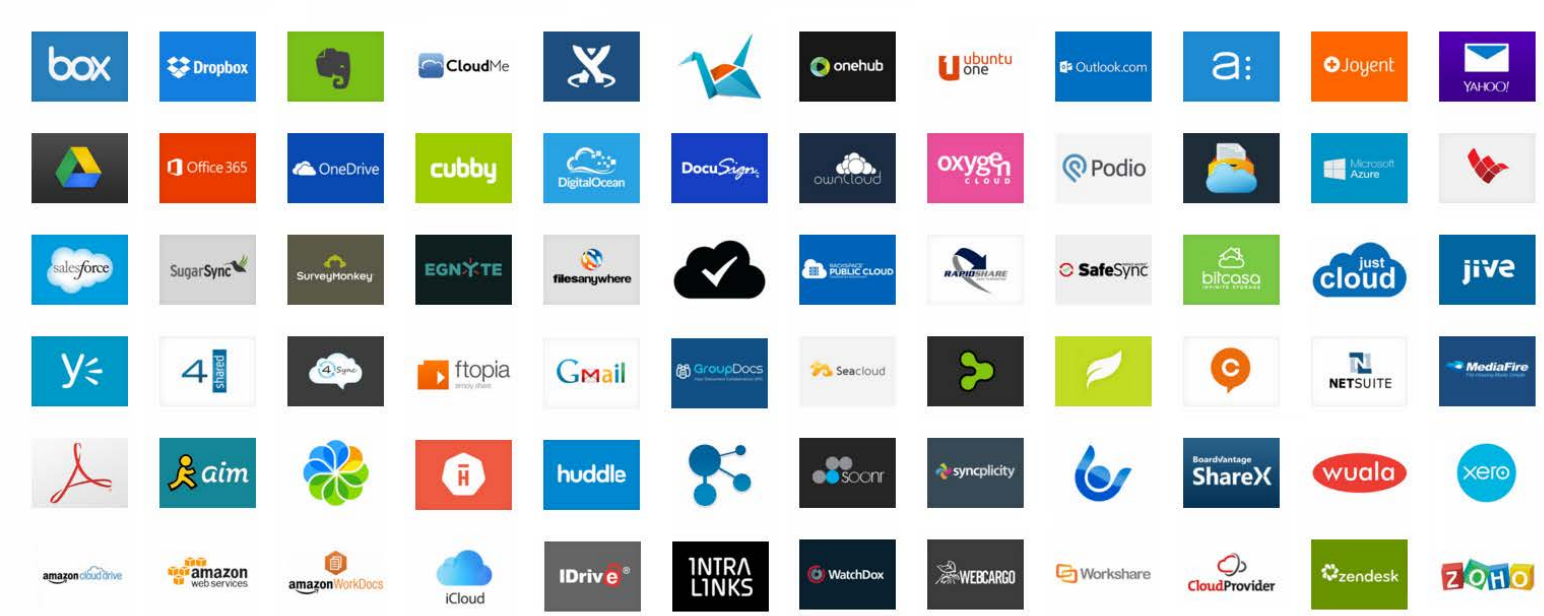


- API-based solutions that provide visibility and controls for sanctioned cloud applications
- Easy to on-board, minimal friction (just authenticate)
  - Help secure critical apps today, add additional capabilities down the road
- Standalone offering for each app providing:
  - Custom dashboard summarizing security metrics for that app
  - Identification and analysis of risky exposures based on advanced content analysis (PII, PCI, etc.)
  - Remediation of exposures through automated policies
  - Creation and enforcement of policies to govern sharing of sensitive data
- **15 Applications secured**

CASB Mitigation – Gateway Based

Over 175 applications secured – and growing rapidly

- Automated development allows rapid support of new Cloud applications



Granular Visibility

Real-time Enforcement

Broad Range of Cloud Apps

Monitor Unsanctioned & Personal Accounts

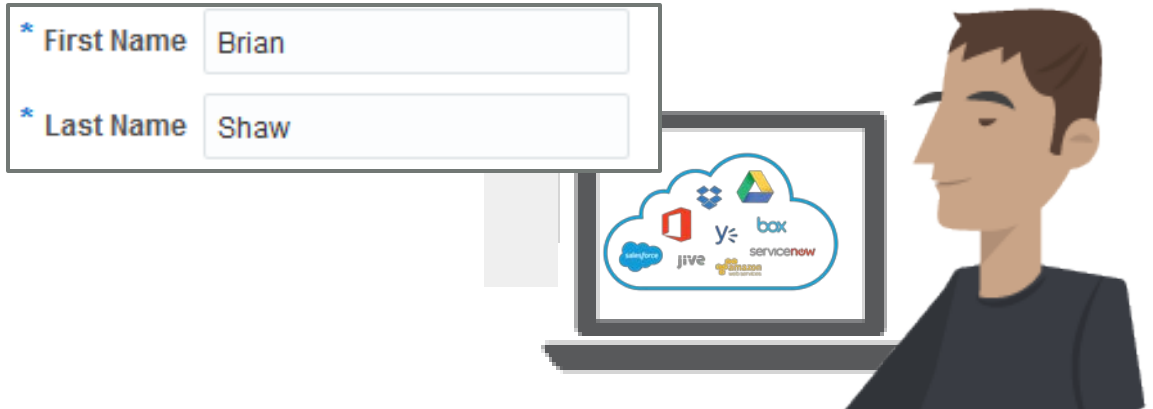
Support For Detect, Protect, Investigate Apps

Encryption and Tokenization

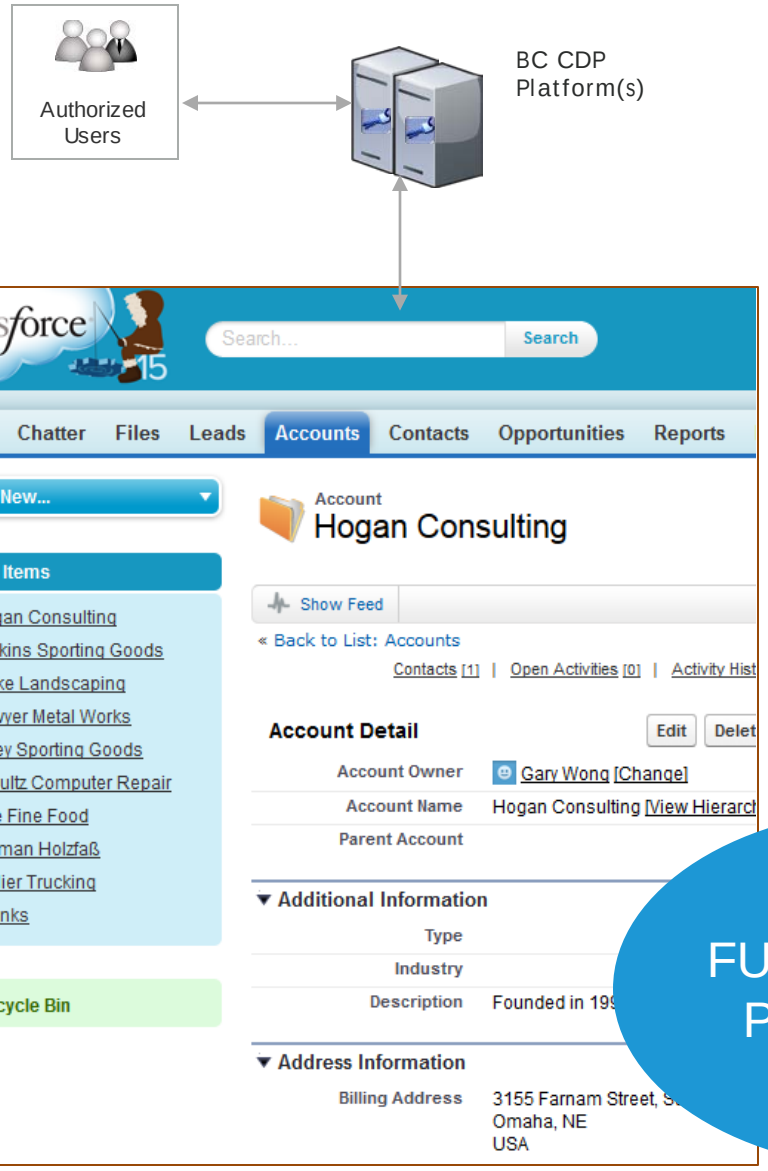
- Comply with Data Privacy and Security Regulations
- Field Level Tokenization & Encryption
  - At Rest, In Transit, In Use
  - Preserve SaaS App Functionality
- File Level Encryption

CDP

* First Name	갇갘갚갚갘갰倆企伂佑갆각
* Last Name	갇갘감개갖갖倆企伂作갆각



Cloud Data Protection User Experience



FUNCTIONALITY PRESERVED

Info Stored & Processed in the Cloud

Comparison – Architecture

Method	Benefits	Detriments	Notes
Upload Logs	• Easy to implement • Comprehensive – shows all activity on the Network	• Historical data only, not real time • No mitigation; informational only	• Best solution to characterize recent application usage
API	• Easy to implement – just Authenticate • Catches all data in the Cloud, including historical • Fix any problem that is enabled via API (break links, move files, etc.) • No traffic steering	• Not real time (but lag typically minor) • Moderately difficult to support new applications	• Great first step for mitigation, as it's easy to get started
Forward Proxy	• Easy to support new applications • Block or alert in real time	• Implementation "moderately easy" • Requires traffic to be steered – proxy chaining, PAC files, agents, etc. • No historical information	• Good bang for the buck, as typically secures a large number of applications
Reverse Proxy	• No traffic steering • Block or alert in real time	• Implementation "moderately difficult" • Very difficult to support new applications • Brittle - can break when application changes • Limited scope – typically transactional only, no email if tokenization/encryption • No historical information	• Typically reserved for most strategic applications requiring tokenization or encryption

Full Integration of all Market Leaders - #1 in All Markets

ProxySG

SWG

DLP

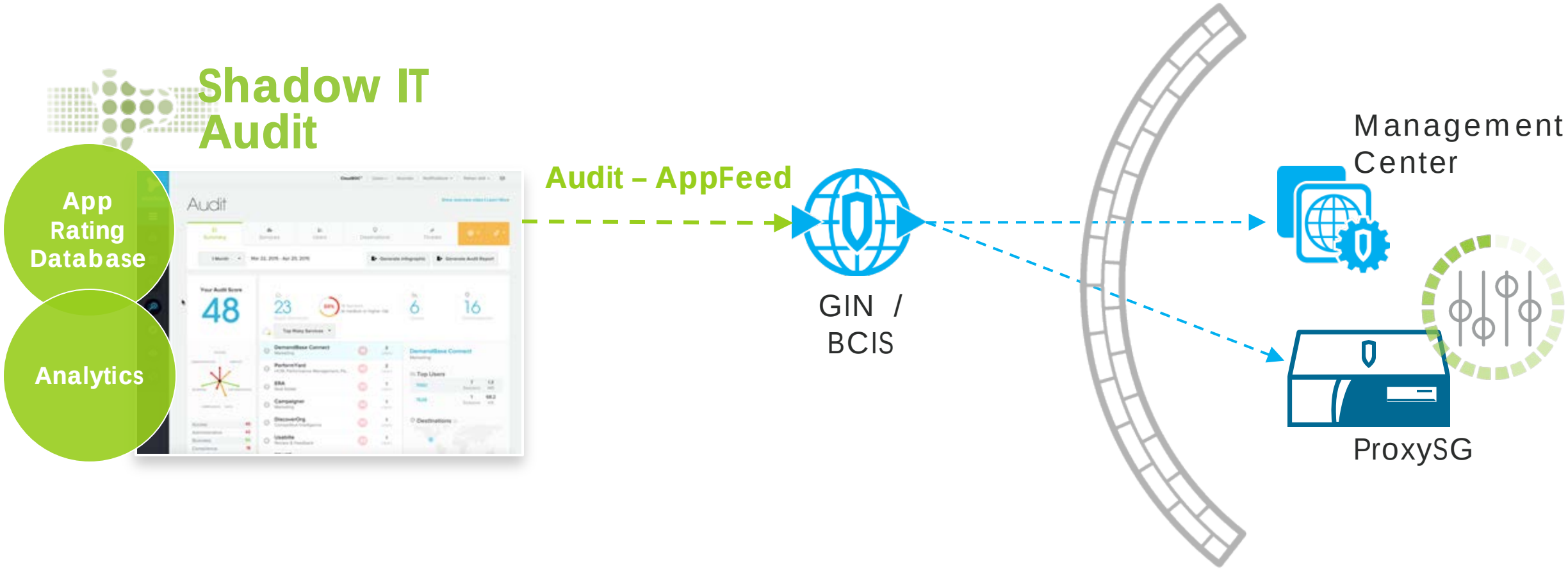
EPP

CloudSOC™

CASB

15,000 SWG customers + 2,100 DLP customers

Audit DataFeed (aka “AppFeed”)



Intelligence of 22,000+ Apps

Don’t Just Discover Shadow IT, Control IT

Gain Shadow IT Analysis

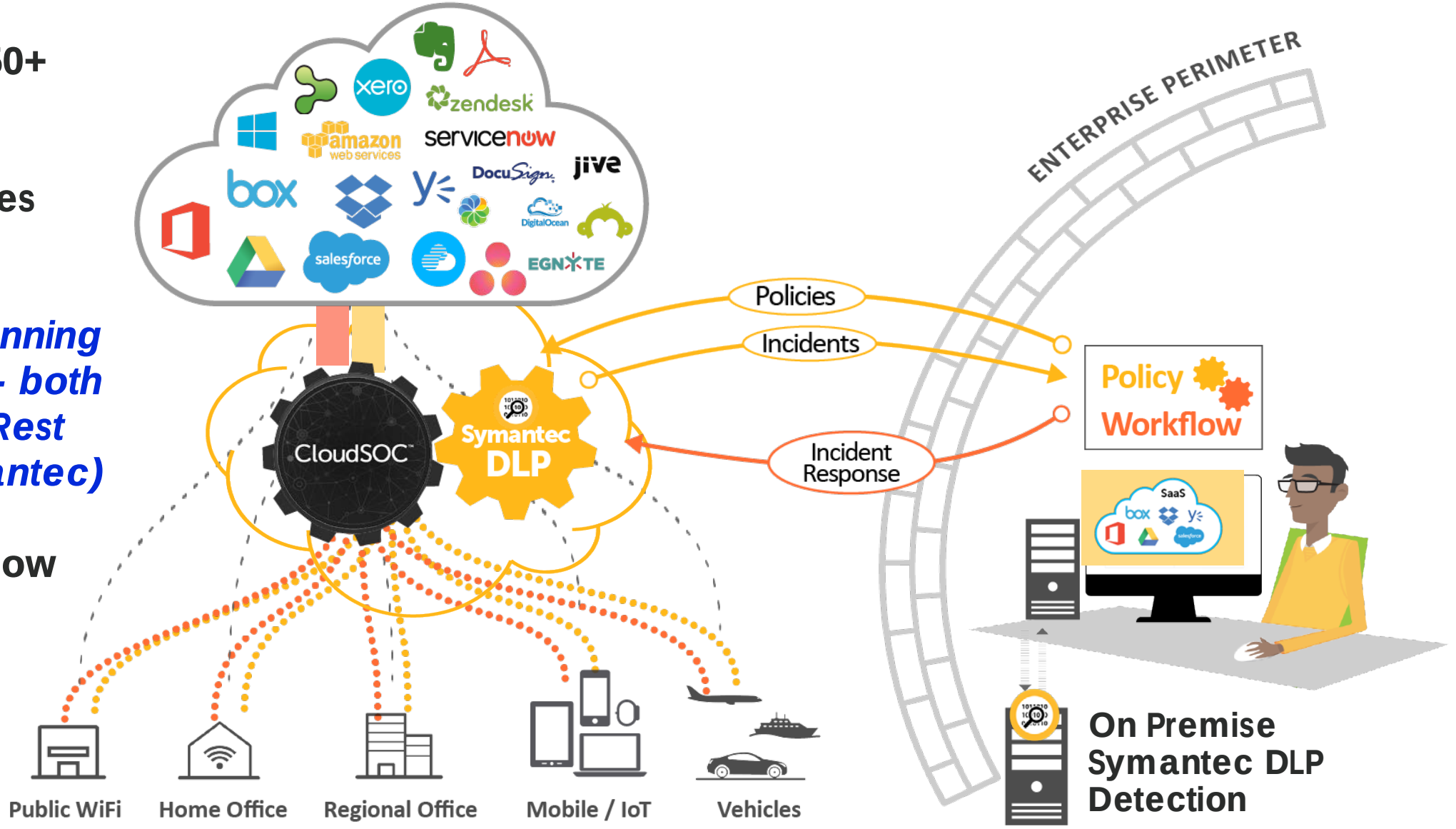
Symantec DLP Scanning for Cloud Applications

Extend DLP to 150+ Cloud Apps

Apply DLP Policies to Cloud

Perform DLP Scanning on Cloud Email - both In Flight and At Rest (Unique to Symantec)

Leverage Workflow Integrations



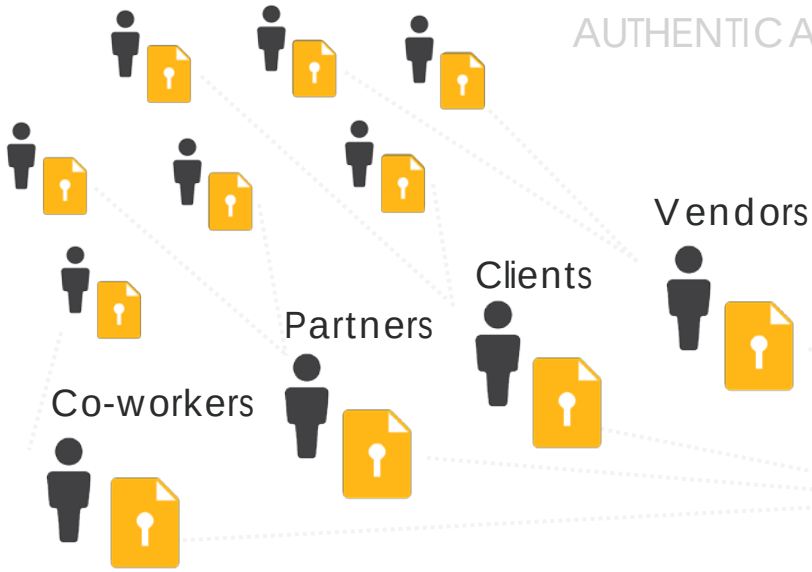
Data-Centric Security

- Per File Encryption
- Per Device Posture Check
- Granularly Revocable Files
- Native Mobile App and Desktop App Support

DATA CLASSIFICATION

AUTHENTICATION

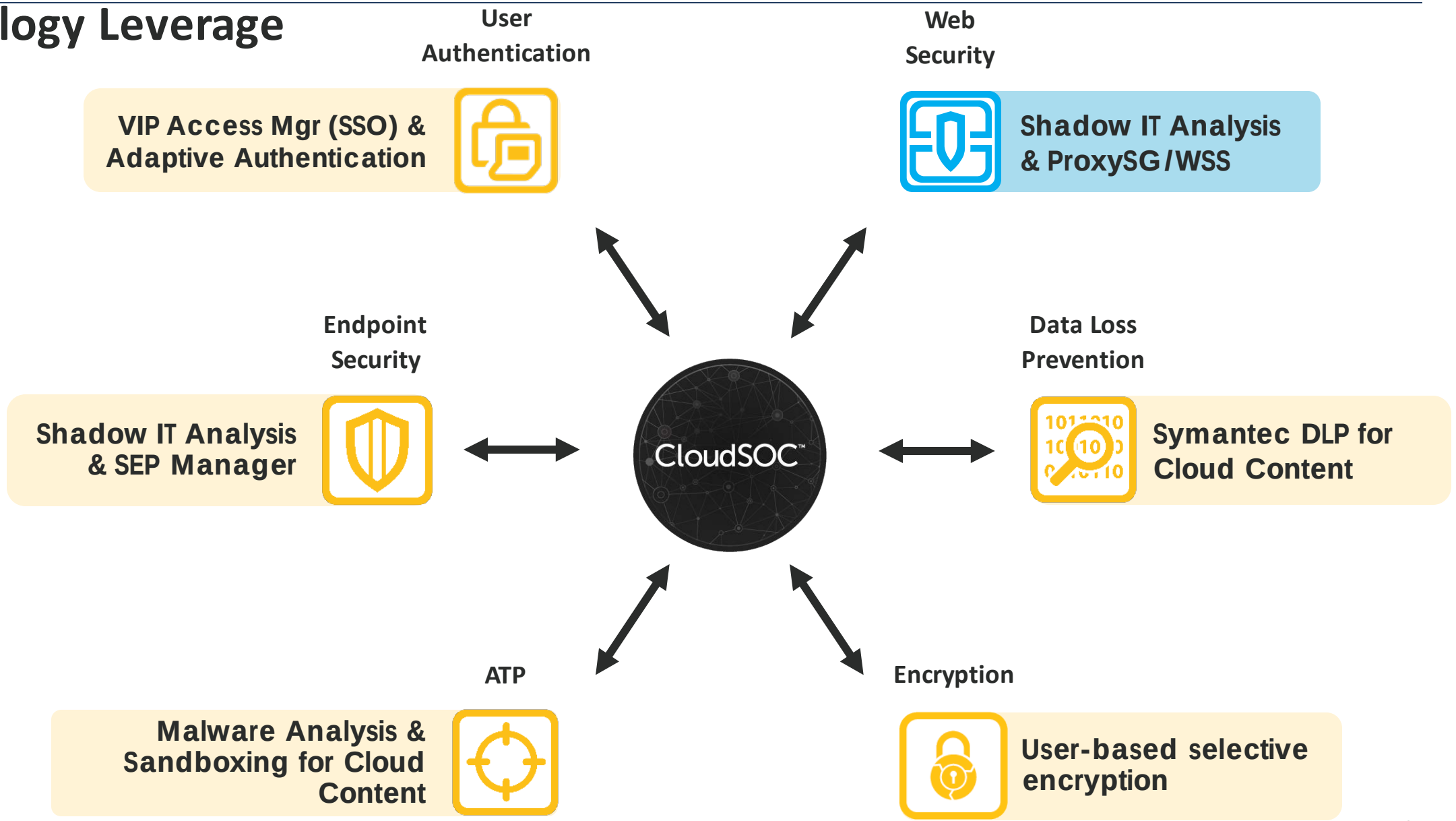
ENCRYPTION



ENTERPRISE PERIMETER

18

Technology Leverage



John Emerson

John_Emerson@Symantec.Com