

Cloud Access Security Broker (CASB) Overview

Presenter

John Emerson

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

Date

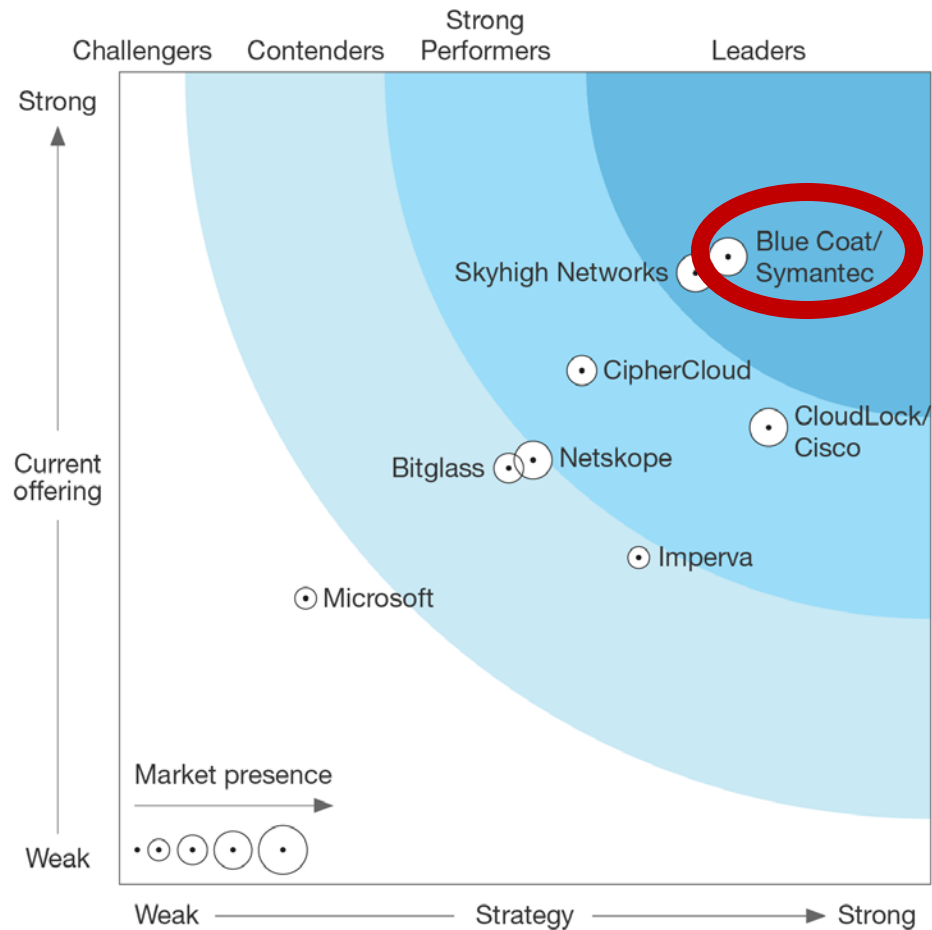
5 April 2018



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

The Forrester Wave is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

Gartner MQ



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

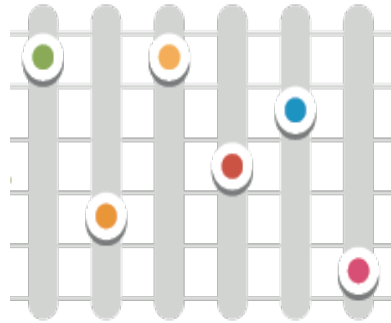
This Magic Quadrant graphic was published by Gartner, Inc. as part of a larger research note and should be evaluated in the context of the entire report. The Gartner report is available upon request from Symantec. Gartner does not endorse any vendor, product or service depicted in our research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Symantec CloudSOC™ Solution



Cloud App Visibility

Identify Shadow IT & monitor
cloud usage at a granular level



Data Security and Threat Protection

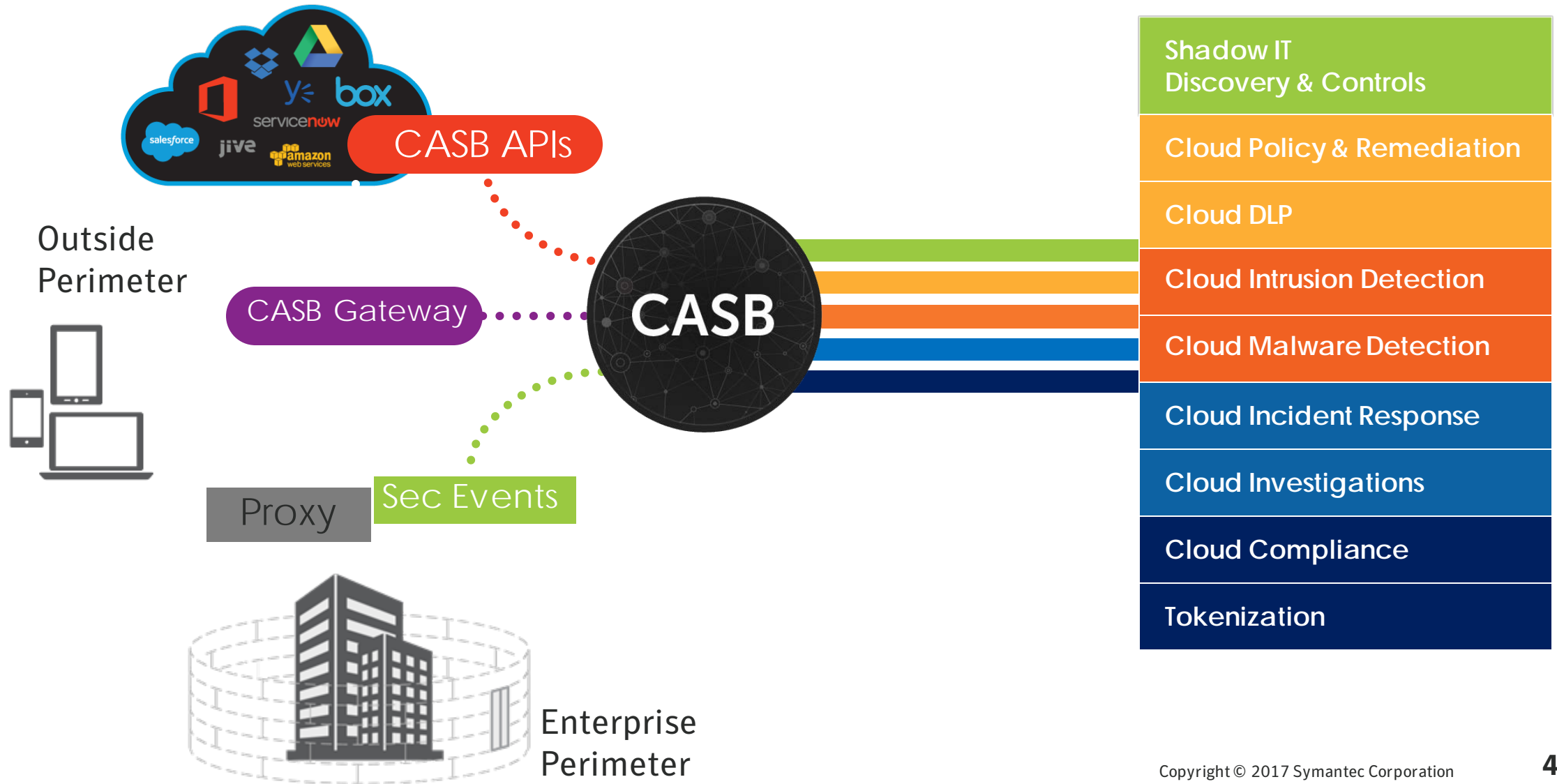
Govern sensitive data with granular
controls and encryption/tokenization;
Combat threats with user behavior
analytics, malware analysis and
incident response



Integration with Existing Technologies

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

CASB Architecture



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

Database of over 22,000 Applications Globally



 **189** out of 421 services (45%) are at **medium or higher risk**

 **MOST USED SERVICES**
54 of these services

 **NEW APPS**
18 of these services

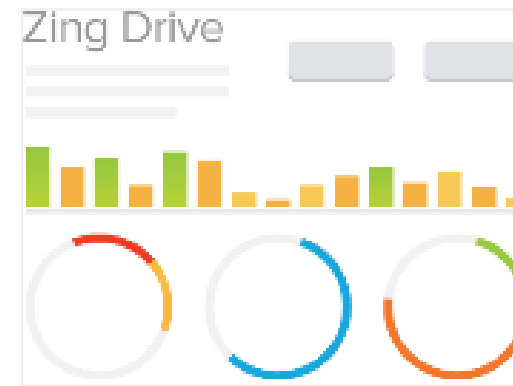
 **USERS**
1,189 of **2,230** users

 **CATEGORIES**
7 of **14** categories

Analytics on your cloud app risks and compliance issues



App usage anomalies across your organization



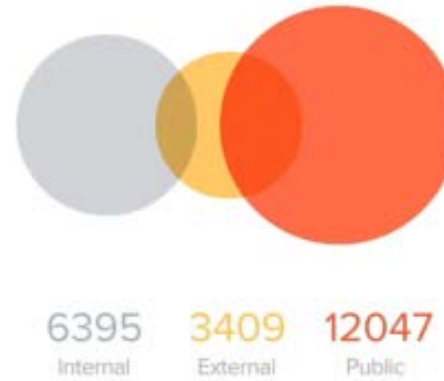
What apps you should sanction and what apps you should block



Shadow Data Risk Assessment



Exposures



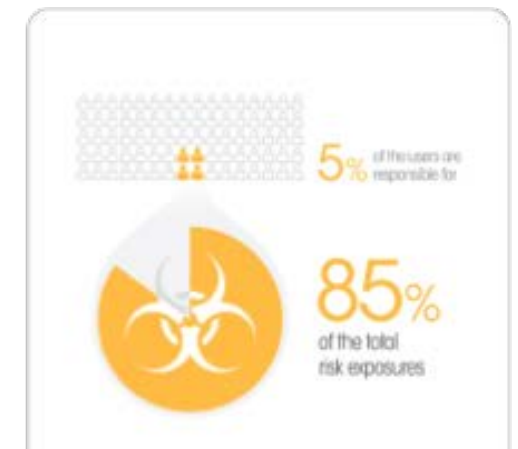
Risk Type



External and public content exposures, including compliance risks

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

Risky users and user activities



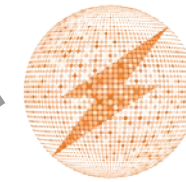
CloudSOC - integrated with Symantec Advanced Threat Protection (ATP)



- 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



Threat Intelligence



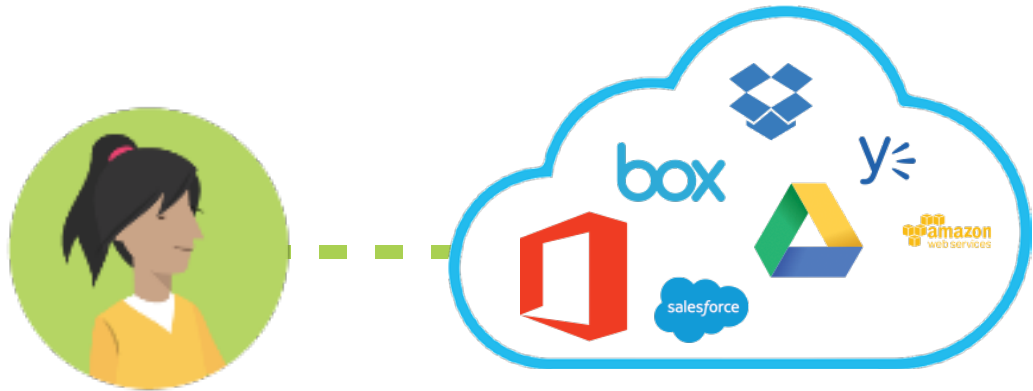
A/V Scanning



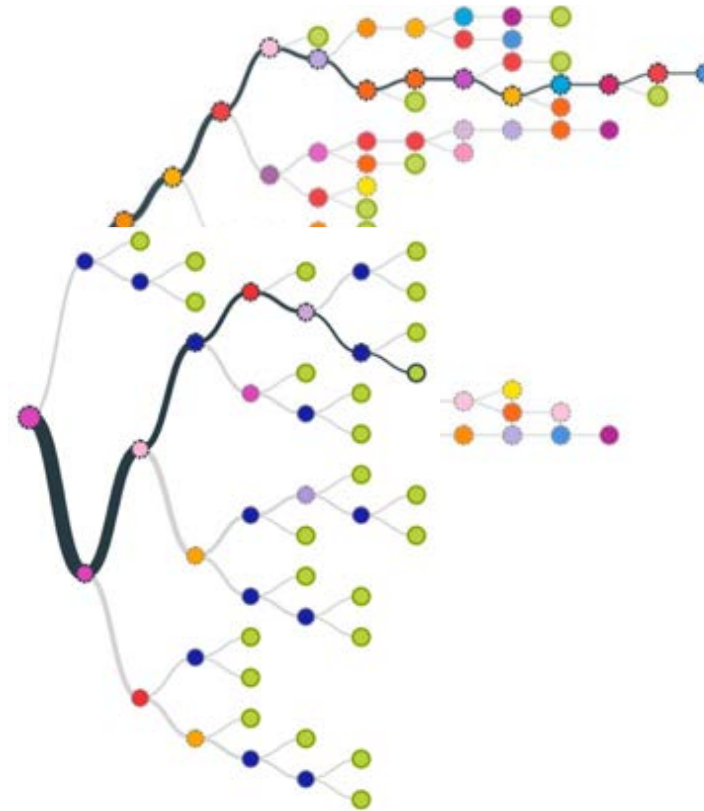
Sandboxing



User Behavior Analysis



suspicious activity

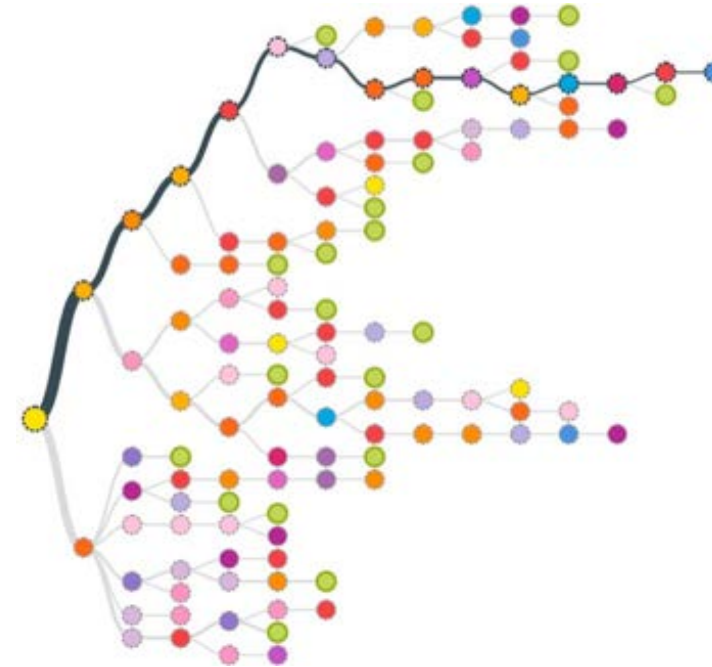
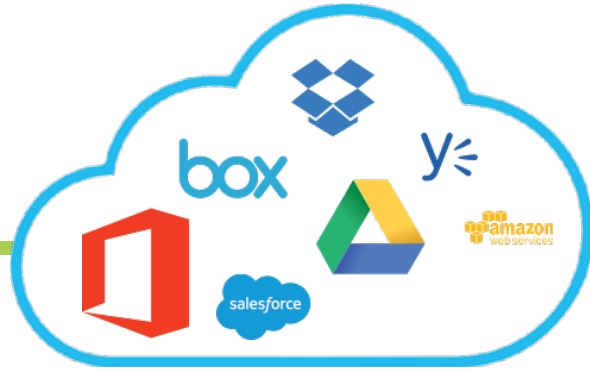


a unique graph for each individual

What happens when suspicious activity occurs for this user?

ThreatScore™

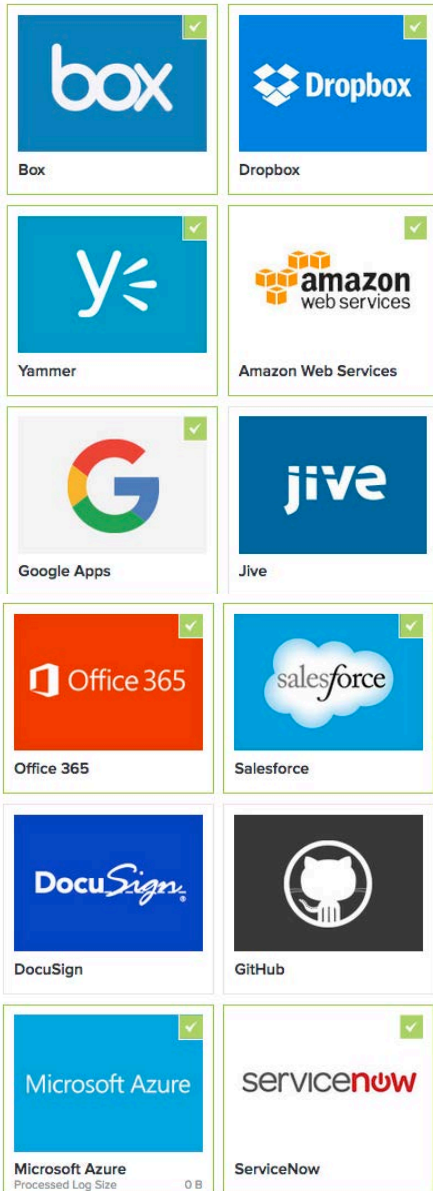
suspicious activity



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

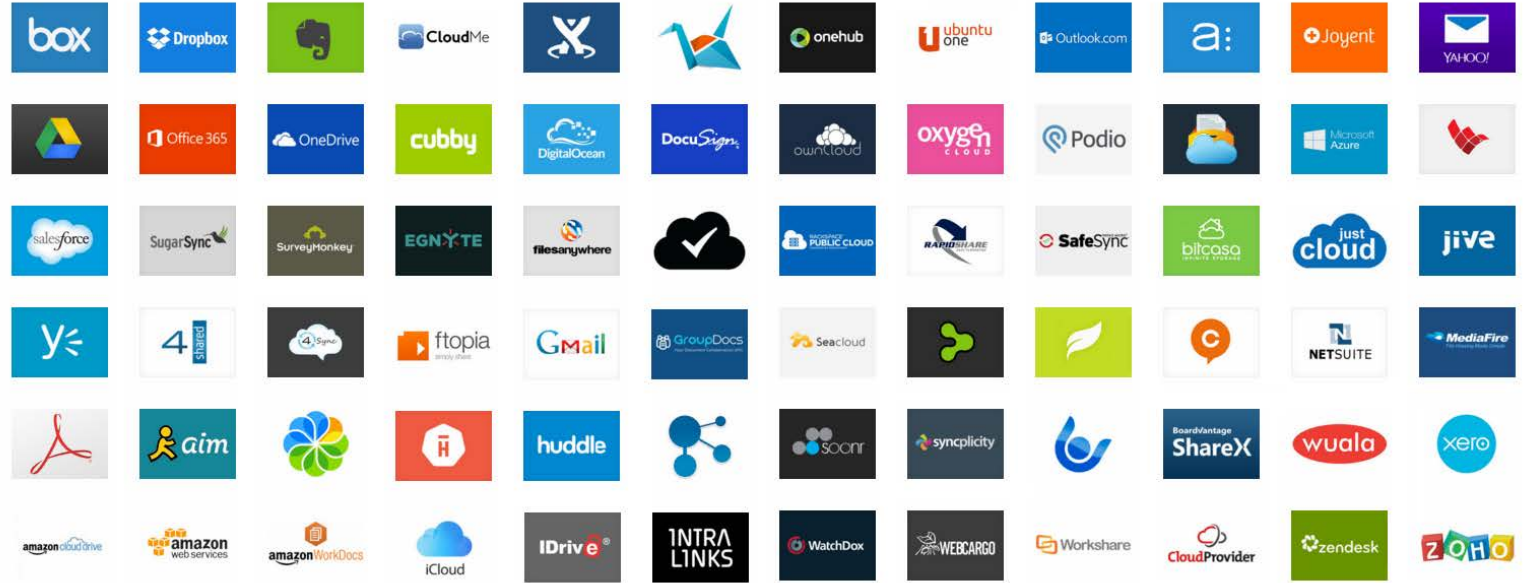


- API-based solutions that provide visibility and controls for sanctioned cloud applications
- Easy to on-board, minimal friction (just authenticate)
 - Help secure critical apps today, add additional capabilities down the road
- Standalone offering for each app providing:
 - Custom dashboard summarizing 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

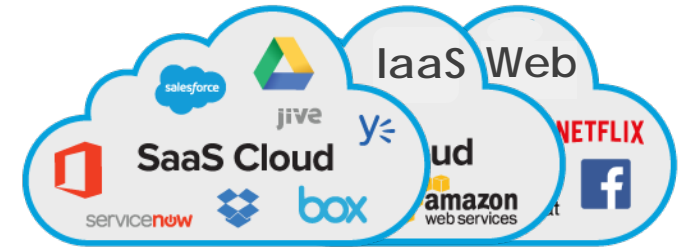
Broad Range of Cloud Apps

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



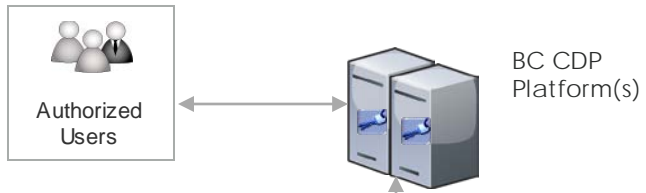
* First Name	간갑갈갯갈갯갯갯갯갯갯갯
* Last Name	갯갯갯갯갯갯갯갯갯갯갯갯

* First Name	Brian
* Last Name	Shaw



Cloud Data Protection User Experience

Info Stored & Processed in the Cloud



Account: Hogan Consulting

Account Owner: Gary Wong [Change]

Account Name: Hogan Consulting [View Hierarchy]

Parent Account

Additional Information

Type	
Industry	
Description	Founded in 19...

Address Information

Billing Address	3155 Farnam Street, S Omaha, NE USA
-----------------	---

Account: 각각각객儼企併濫踏扶樊鋏...

Account Owner: Gary Wong [Change]

Account Name: 각각각객儼企併濫踏扶樊鋏...

Parent Account

Additional Information

Type	
Industry	
Description	각각각객儼企併濫踏扶樊鋏...

Address Information

Billing Address	각각각객儼企併濫踏扶樊鋏...
-----------------	-----------------

FUNCTIONALITY PRESERVED

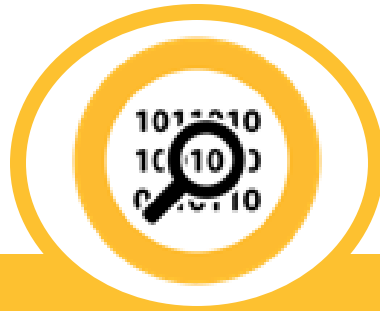
Comparison – Architecture

Method	Benefits	Detriments	Notes
Upload Logs	<ul style="list-style-type: none">• Easy to implement• Comprehensive – shows all activity on the Network	<ul style="list-style-type: none">• Historical data only, not real time• No mitigation; informational only	<ul style="list-style-type: none">• Best solution to characterize recent application usage
API	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Not real time (but lag typically minor)• Moderately difficult to support new applications	<ul style="list-style-type: none">• Great first step for mitigation, as it's easy to get started
Forward Proxy	<ul style="list-style-type: none">• Easy to support new applications• Block or alert in real time	<ul style="list-style-type: none">• Implementation “moderately easy”• Requires traffic to be steered – proxy chaining, PAC files, agents, etc.• No historical information	<ul style="list-style-type: none">• Good bang for the buck, as typically secures a large number of applications
Reverse Proxy	<ul style="list-style-type: none">• No traffic steering• Block or alert in real time	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Typically reserved for most strategic applications requiring tokenization or encryption

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



SWG



DLP



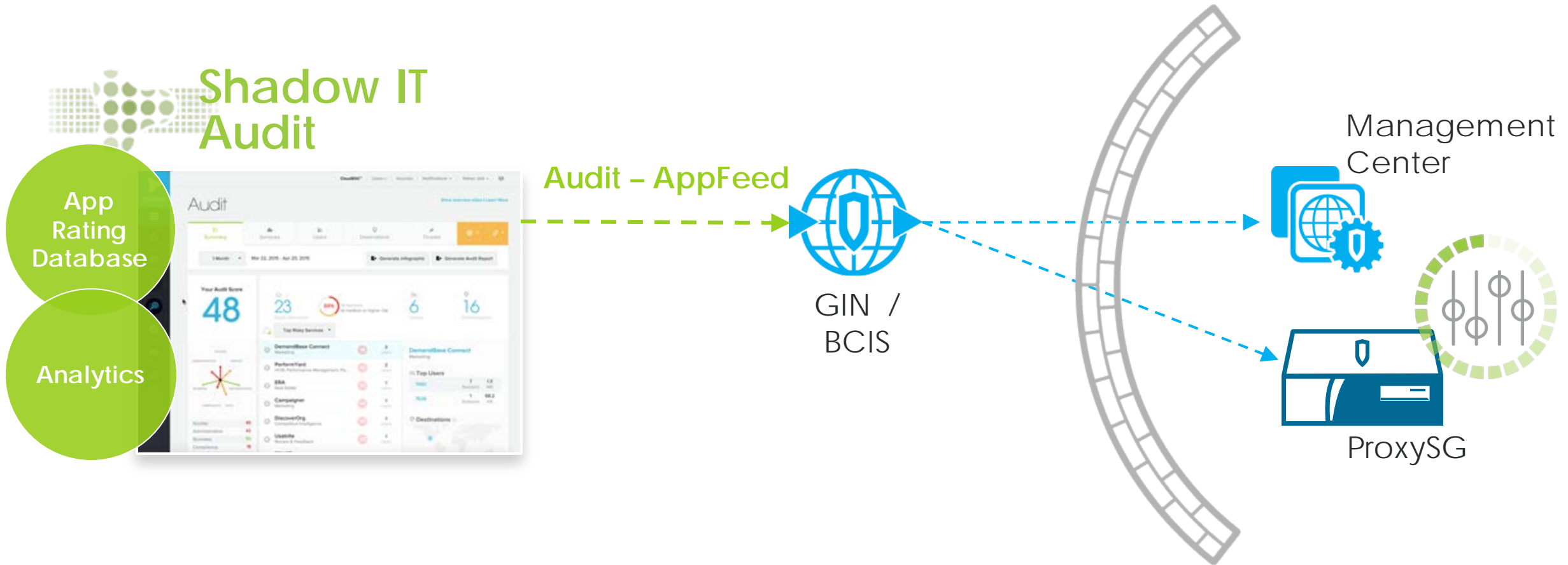
EPP



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

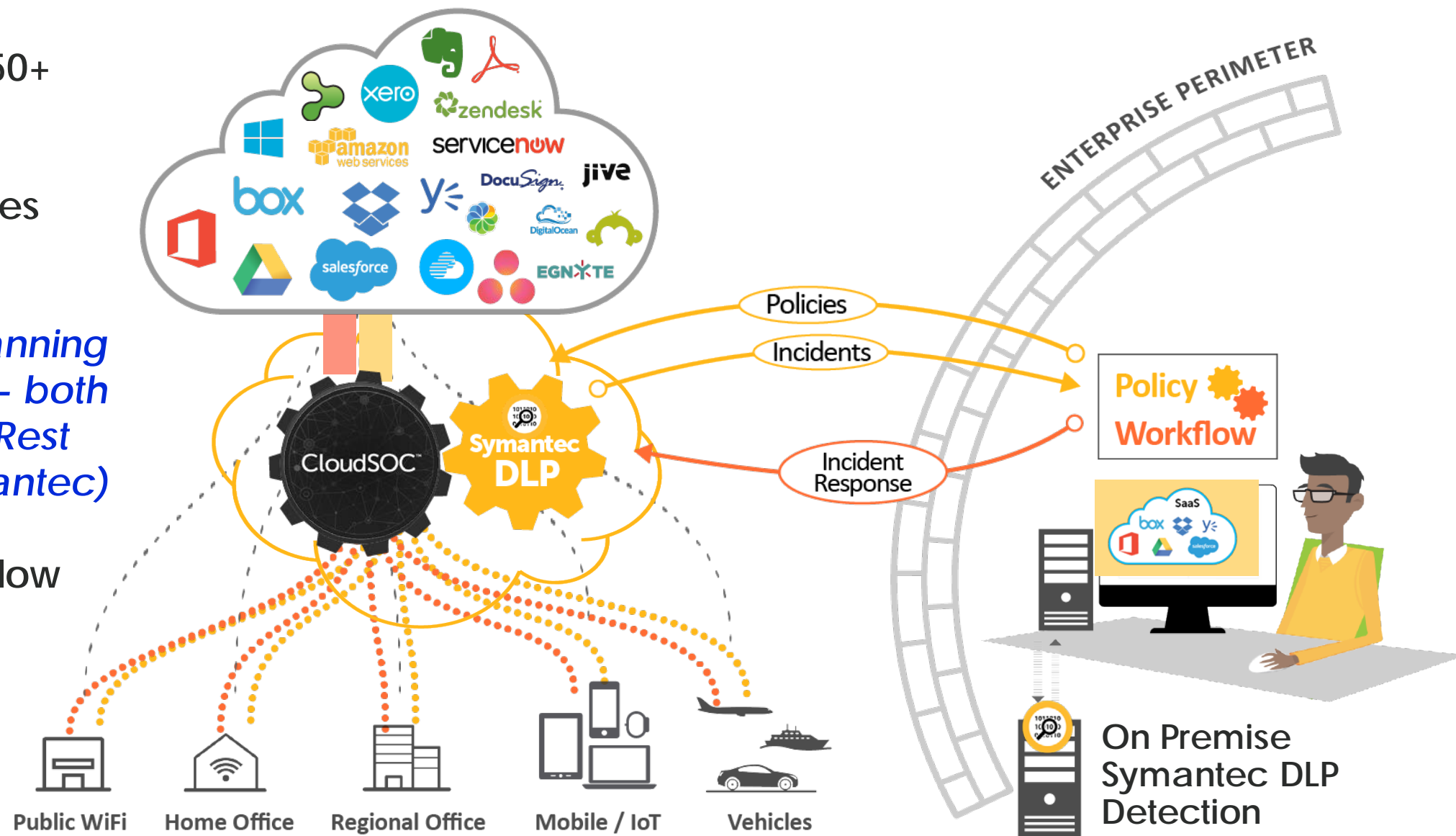
Symantec DLP Scanning for Cloud Applications

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

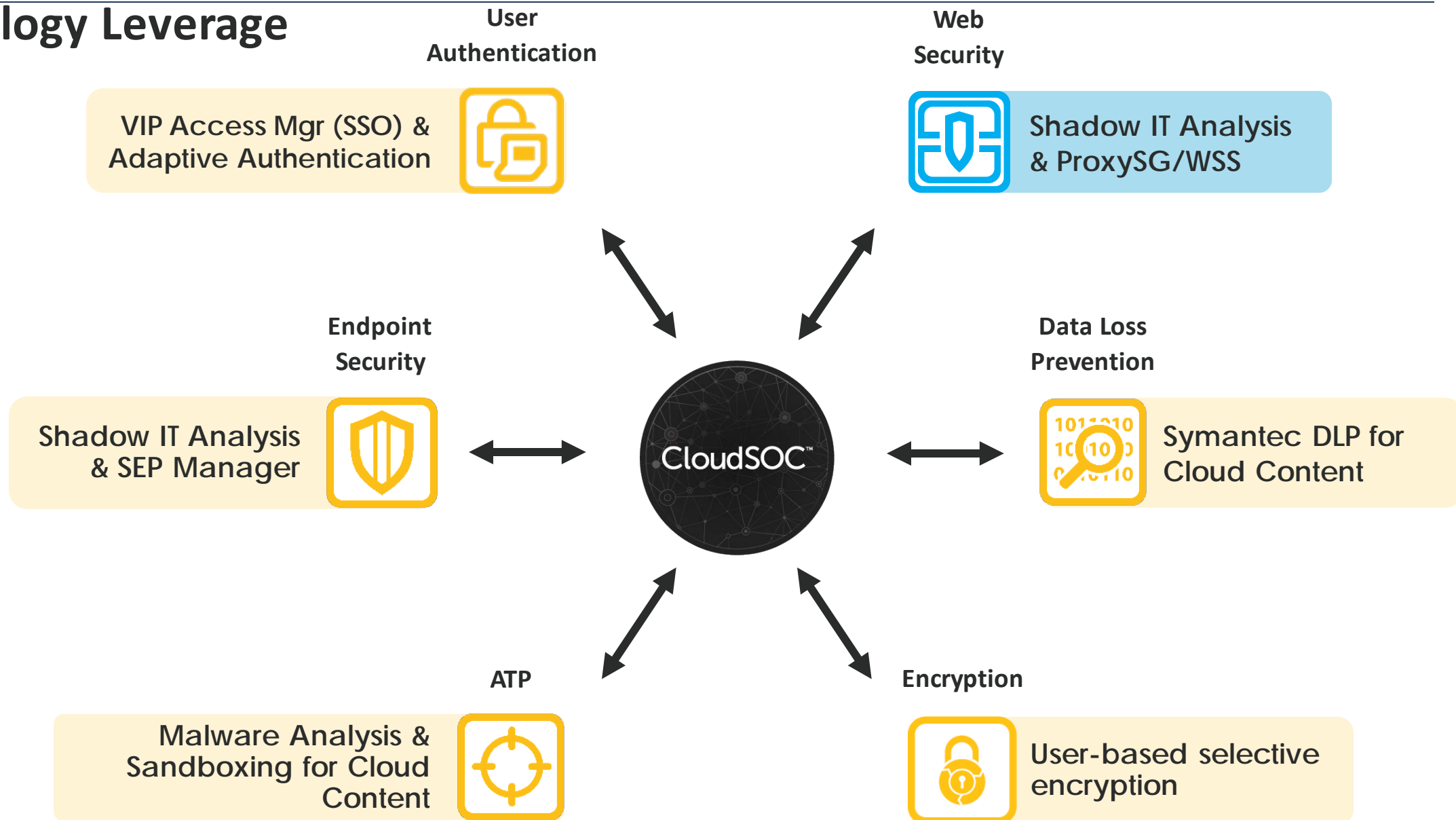


Data-Centric Security

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



Technology Leverage





John Emerson

John_Emerson@Symantec.Com