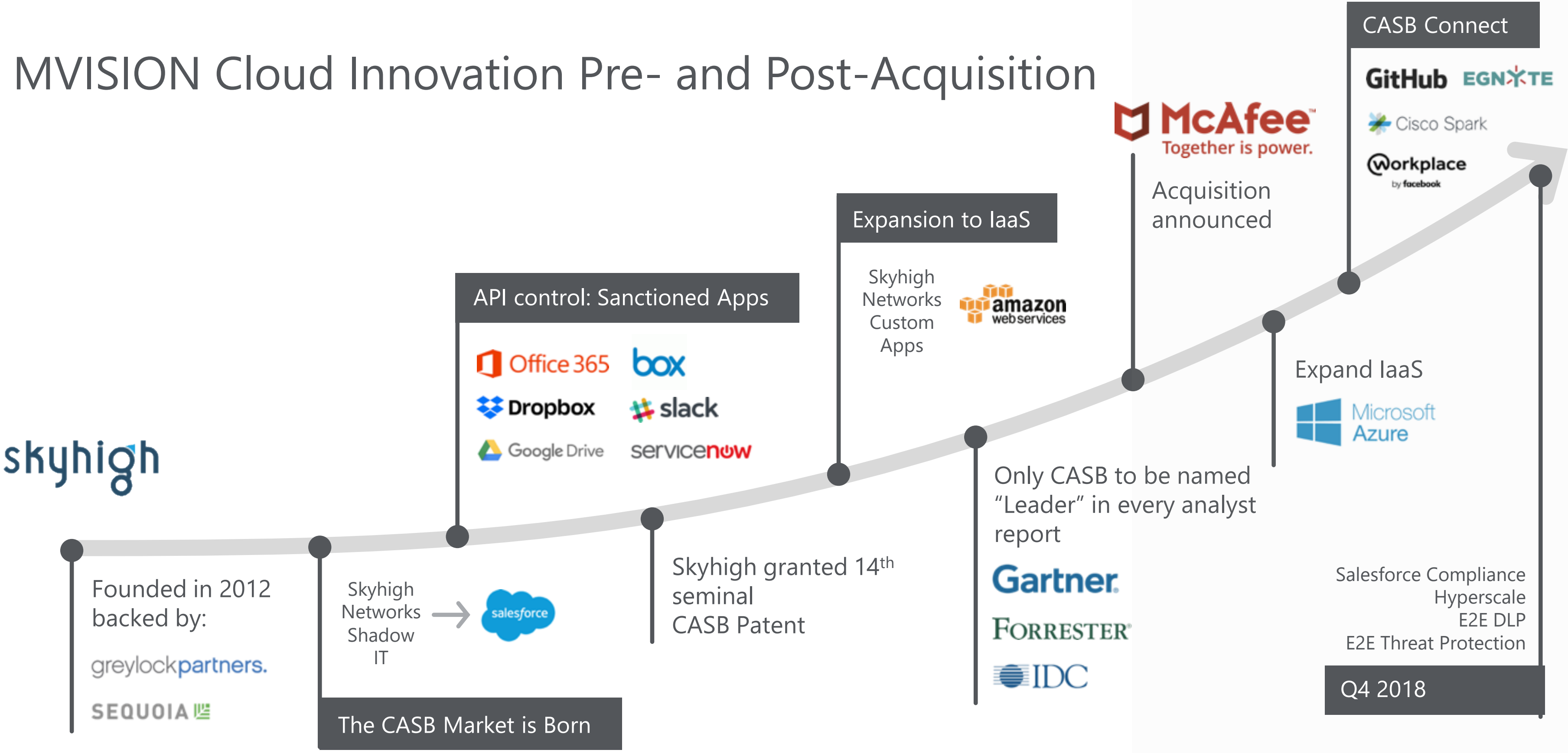
McAfee™
Together is power.

Security in the Age of Cloud

Kaushik Narayan

CTO, Cloud Business Unit

MVISION Cloud Innovation Pre- and Post-Acquisition



skyhigh

Founded in 2012 backed by:

greylockpartners.

SEQUOIA

Skyhigh Networks Shadow IT → salesforce

The CASB Market is Born

API control: Sanctioned Apps

Office 365, box, Dropbox, slack, Google Drive, servicenow

Skyhigh granted 14th seminal CASB Patent

Expansion to IaaS

Skyhigh Networks Custom Apps

amazon webservices

Only CASB to be named "Leader" in every analyst report

Gartner

Forrester

IDC

McAfee

Together is power.

Acquisition announced

Expand IaaS

Microsoft Azure

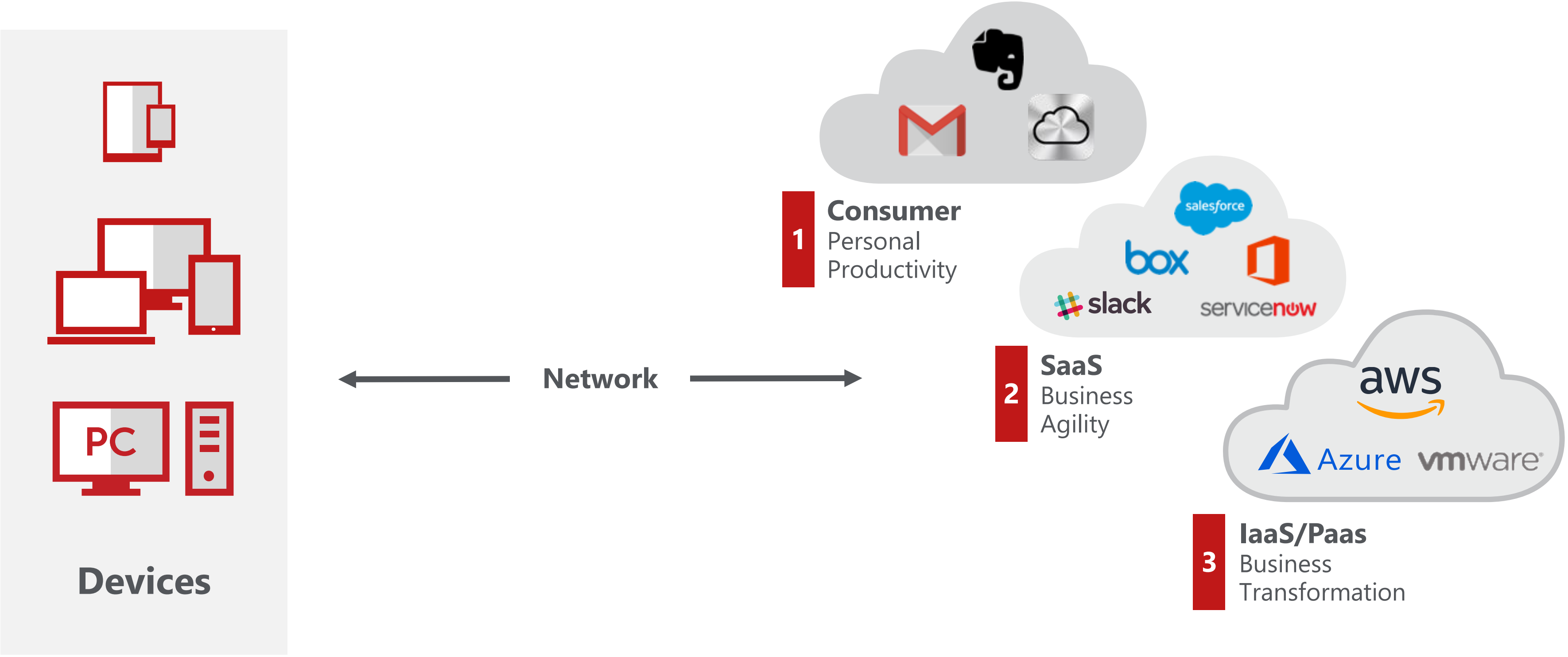
CASB Connect

GitHub, EGNYTE, Cisco Spark, Workplace by facebook

Salesforce Compliance
Hyperscale
E2E DLP
E2E Threat Protection

Q4 2018

Customer Drivers for Cloud Adoption



Devices

Network

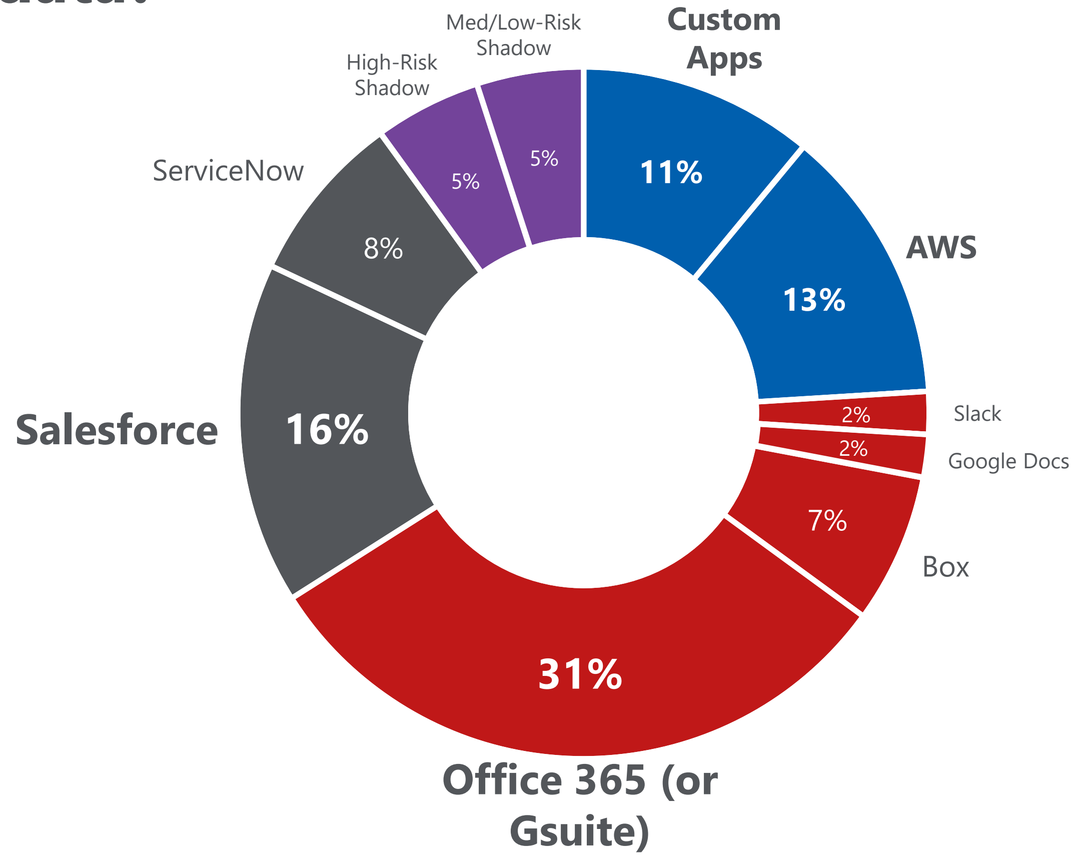
1 **Consumer**
Personal
Productivity

2 **SaaS**
Business
Agility

3 **IaaS/Paas**
Business
Transformation

Where is your sensitive data?

- 65% in top 5 SaaS apps
- 25% in IaaS/PaaS
- 10% in shadow/permitted

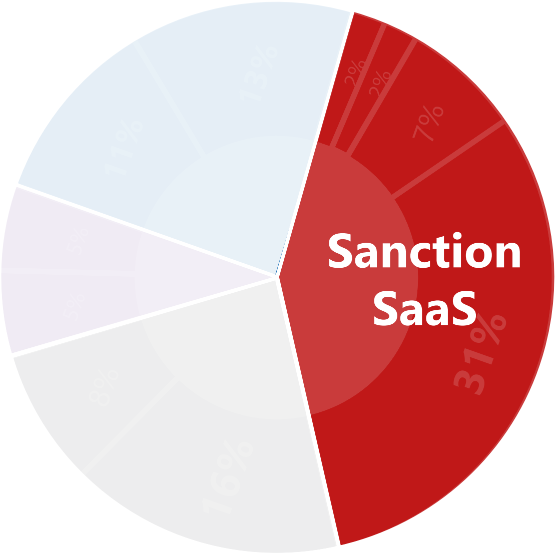


McAfee™

Together is power.

Enterprise SaaS

Sanctioned SaaS Use Cases



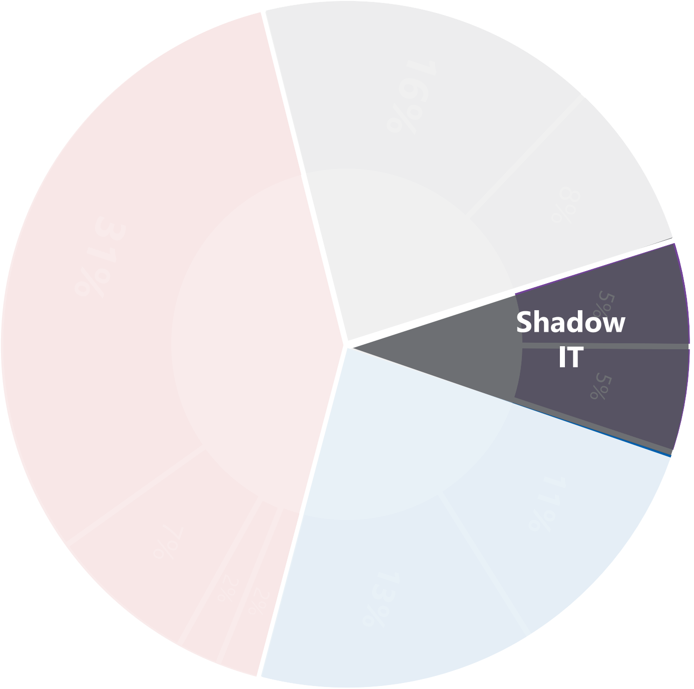
1. Data Protection
Prevent sensitive data from being stored and shared externally

2. Contextual Access Control
Block sync/download of corporate O365 data to personal devices

3. Advanced Threat Protection
Detect compromised accounts, insider/privileged threats, malware

Source: McAfee Cloud Adoption Report, Nov 2018

Shadow SaaS Use Cases



1. Discover & Govern
Discover & Coach on use of high risk

.

2. Conditional Access Control
Activity and Instance based access control

3. Data Loss Prevention
Prevent data exfiltration to medium risk services.

Source: McAfee Cloud Adoption Report, Nov 2018

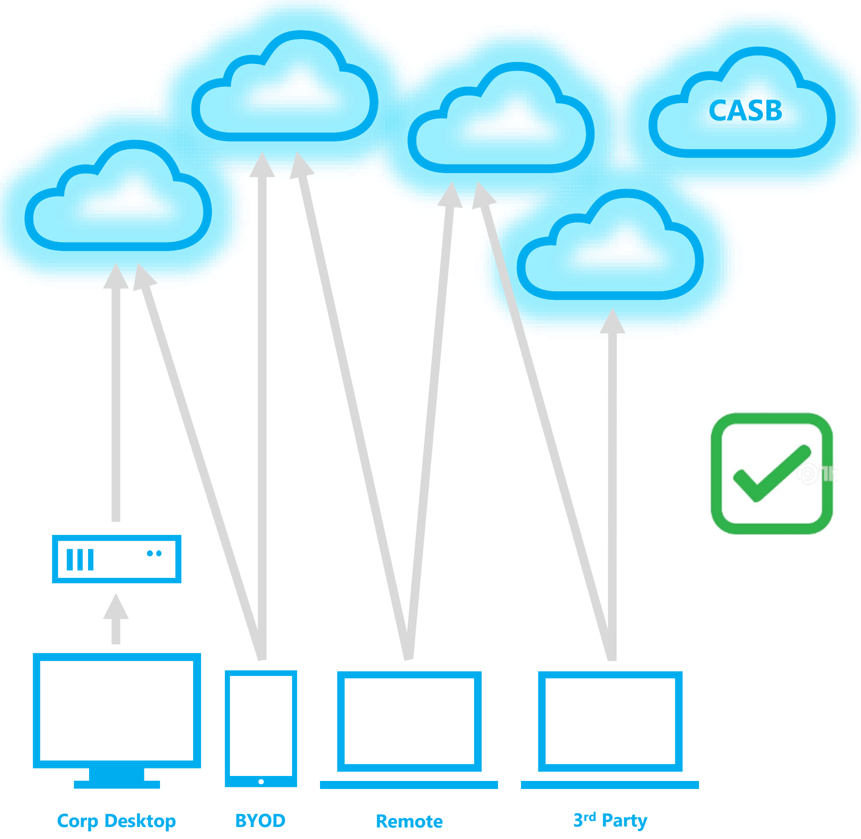
Key Considerations for SaaS Security

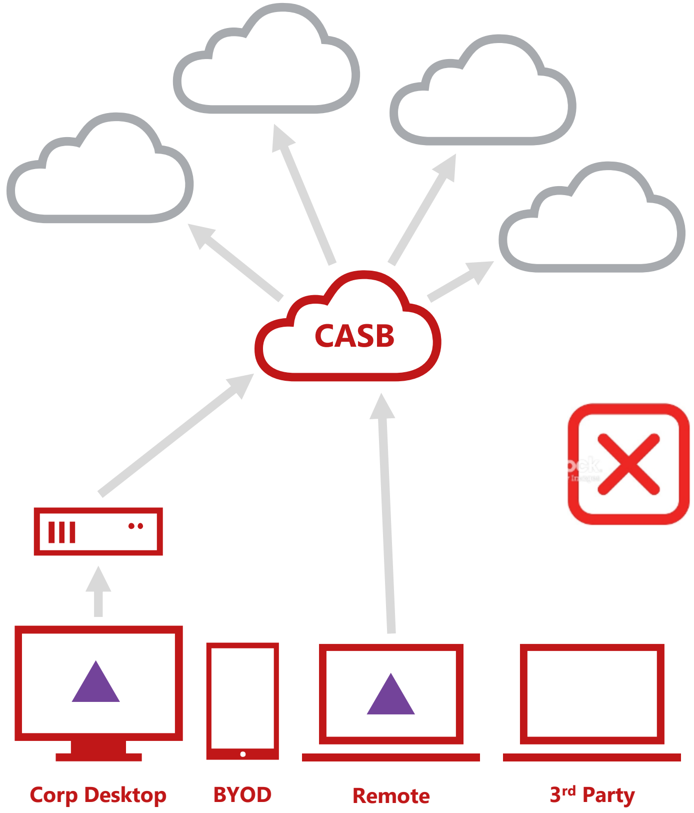
- Frictionless solutions are key to success

- Operational integration with Enterprise Data Protection stack

- Coverage for all SaaS applications including long tail.

Frictionless Controls : Cloud Native Brokering





Microsoft's position on network intermediation for O365*

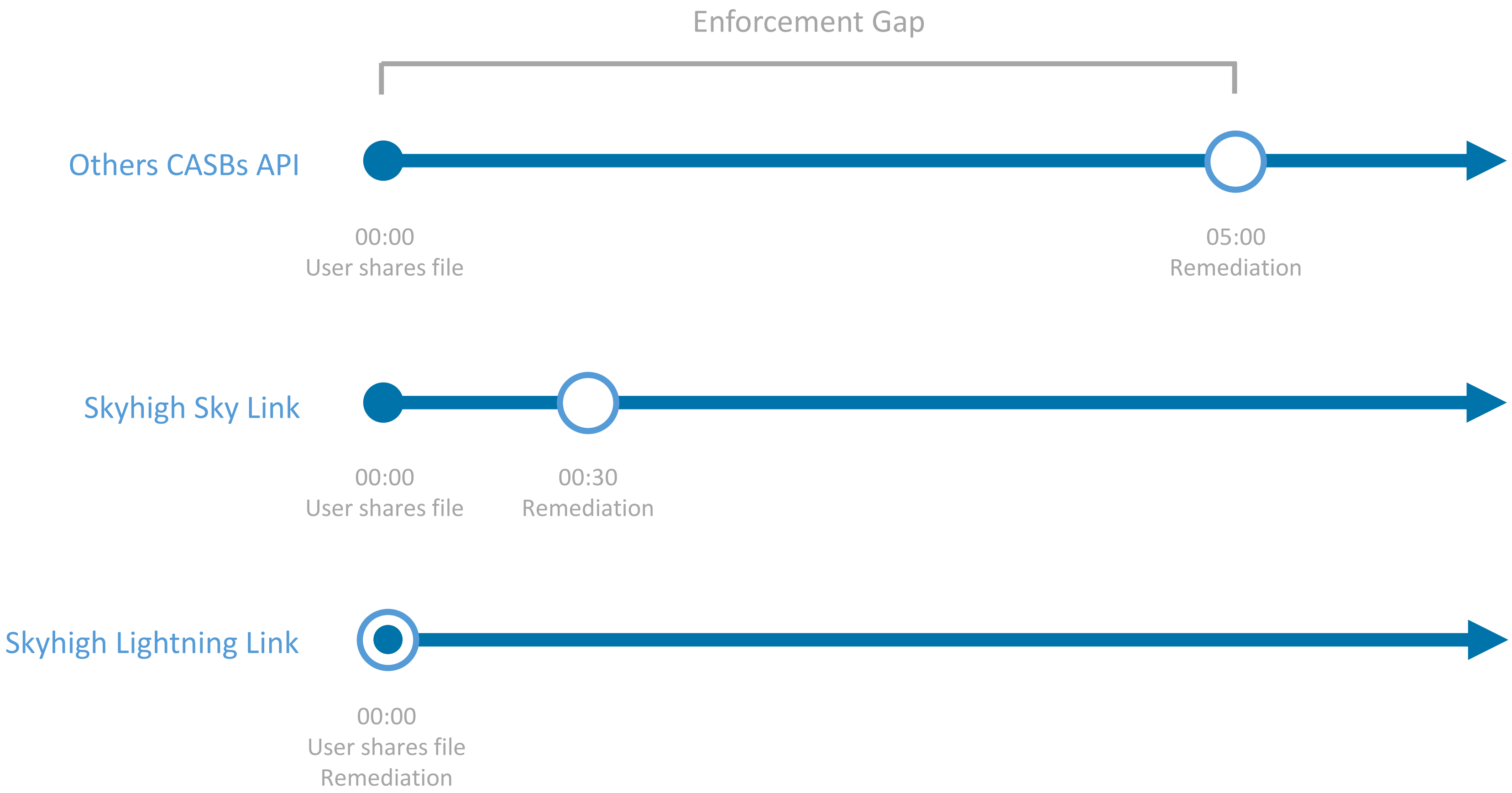
1. Microsoft support requires proxies to be turned off For MSFT to provide support, they require proxies to be turned off before they can handle the case.

2. Terms of use violation Proxies intercepting/decrypting network requests cause changes to O365 protocols & data streams which violate the terms of use

3. No guarantee of compatibility Except for public O365 APIs, Microsoft will make changes to O365 without informing proxy solution providers

Source : https://support.microsoft.com/en-us/help/2690045/using-third-party-network-devices-or-solutions-with-office-365

Frictionless Controls : Realtime API controls



Enforcement Gap

Others CASBs API

00:00
User shares file

05:00
Remediation

Skyhigh Sky Link

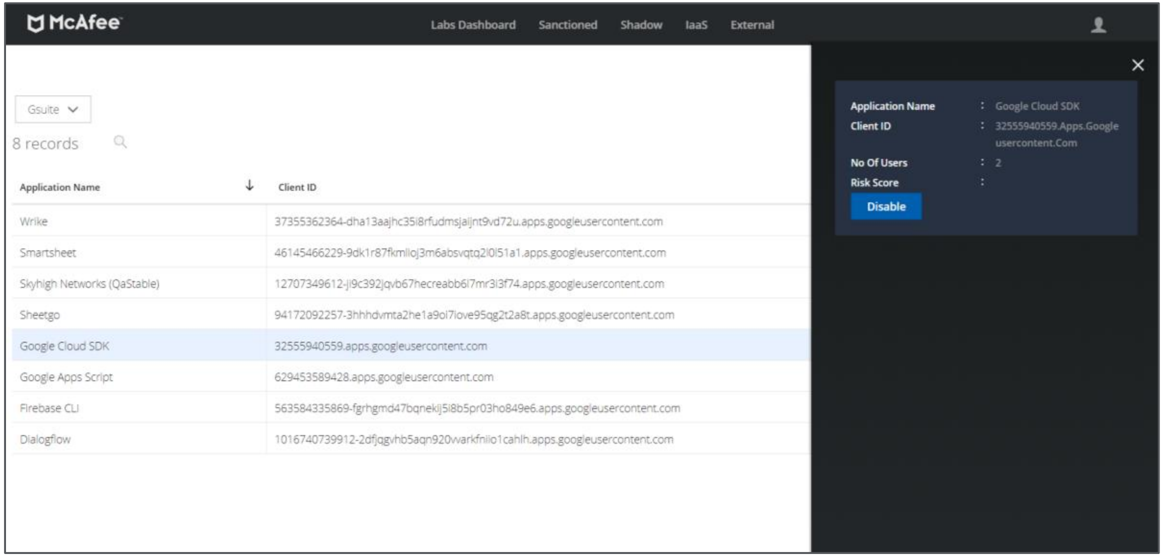
00:00
User shares file

00:30
Remediation

Skyhigh Lightning Link

00:00
User shares file
Remediation

Frictionless Controls - Marketplace controls via Connected App Firewall



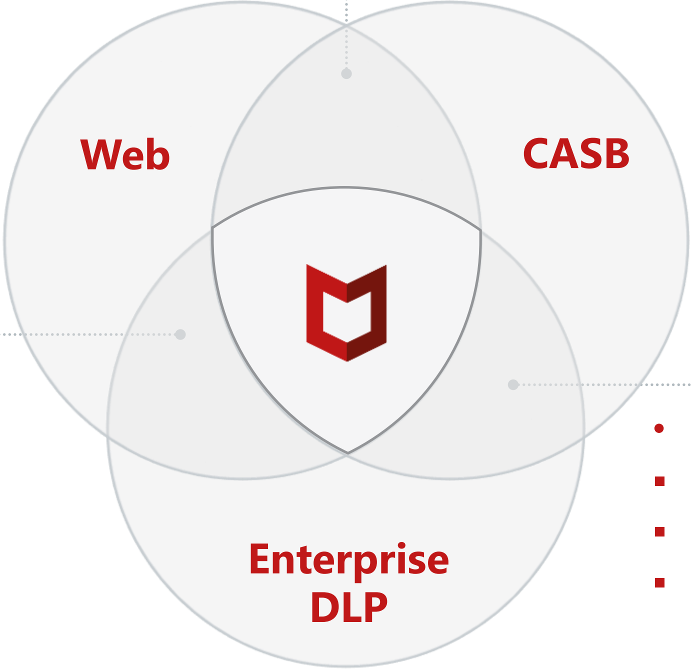
8 records

Application Name	Client ID
Wrike	37355362364-dha13aajhc35i8rfudmsjaijnt9vd72u.apps.googleusercontent.com
Smartsheet	46145466229-9dk1r87fkmlioj3m6absvqtq2l0l51a1.apps.googleusercontent.com
Skyhigh Networks (QaStable)	12707349612-ji9c392jqvb67hecreabb6l7mr3i3f74.apps.googleusercontent.com
Sheetgo	94172092257-3hhhdvmta2he1a9oi7iove95qg2t2a8t.apps.googleusercontent.com
Google Cloud SDK	32555940559.apps.googleusercontent.com
Google Apps Script	629453589428.apps.googleusercontent.com
Firebase CLI	563584335869-fgrhgmd47bqnekij5i8b5pr03ho849e6.apps.googleusercontent.com
Dialogflow	1016740739912-2dfjqgvhb5aqn920warkfniio1cahlh.apps.googleusercontent.com

Application Name : Google Cloud SDK
Client ID : 32555940559.Apps.Googleusercontent.Com
No Of Users : 2
Risk Score :

- Control exfiltration of data from sanctioned apps to unsanctioned marketplace apps. For e.g. Sales reporting apps connected to SF.com.
- Control malicious marketplace applications from exploiting your SaaS instance. For e.g. High risk Gsuite apps.

End to End Data Protection

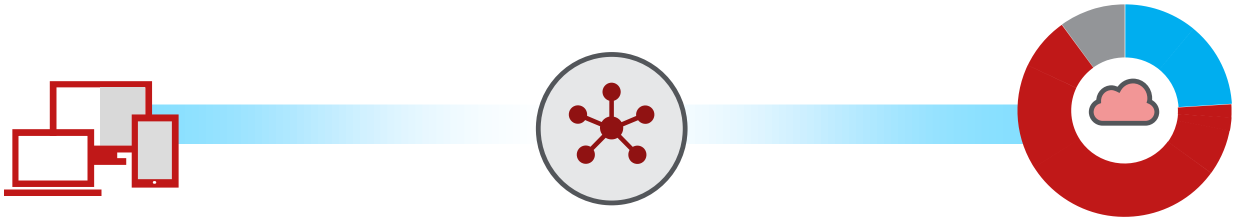


- "Any Cloud" Protection
- Inline CASB controls
- MCP for mobile protection
- Threat protection for Unsanctioned Cloud

- Pervasive Data Protection
- Cloud Native or Hybrid Services
- Inline DLP & ICAP support
- Endpoint & Network Coverage

- Unified Management
- Unified Policies
- Unified Reporting
- Endpoint & Cloud Coverage

End to End Data Protection



Device

Network

Cloud

Device-centric controls
(DLP, device control, encryption, threat protection, etc.)

Network-centric controls
(Web protection, DLP, threat protection, etc.)

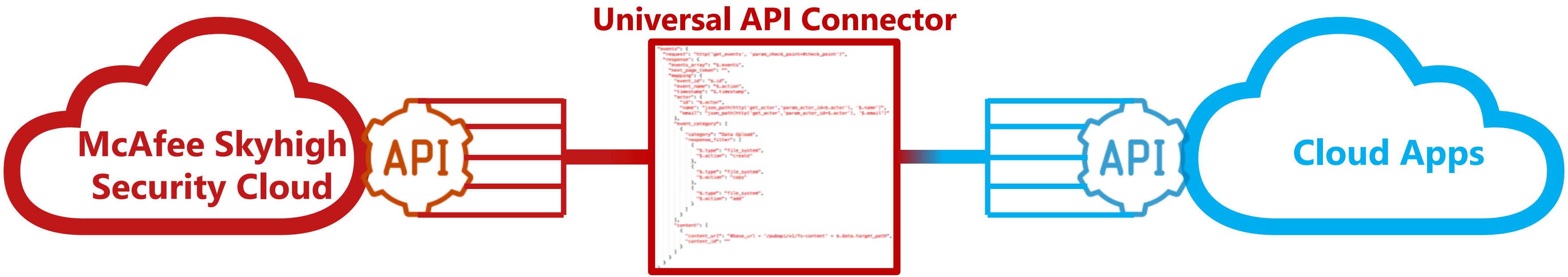
Cloud-native controls
(DLP, configuration management, threat protection, etc.)

End-to-end Policy

Unified Incident Management

SAAS Coverage : Security Long Tail SaaS

CASB Connect



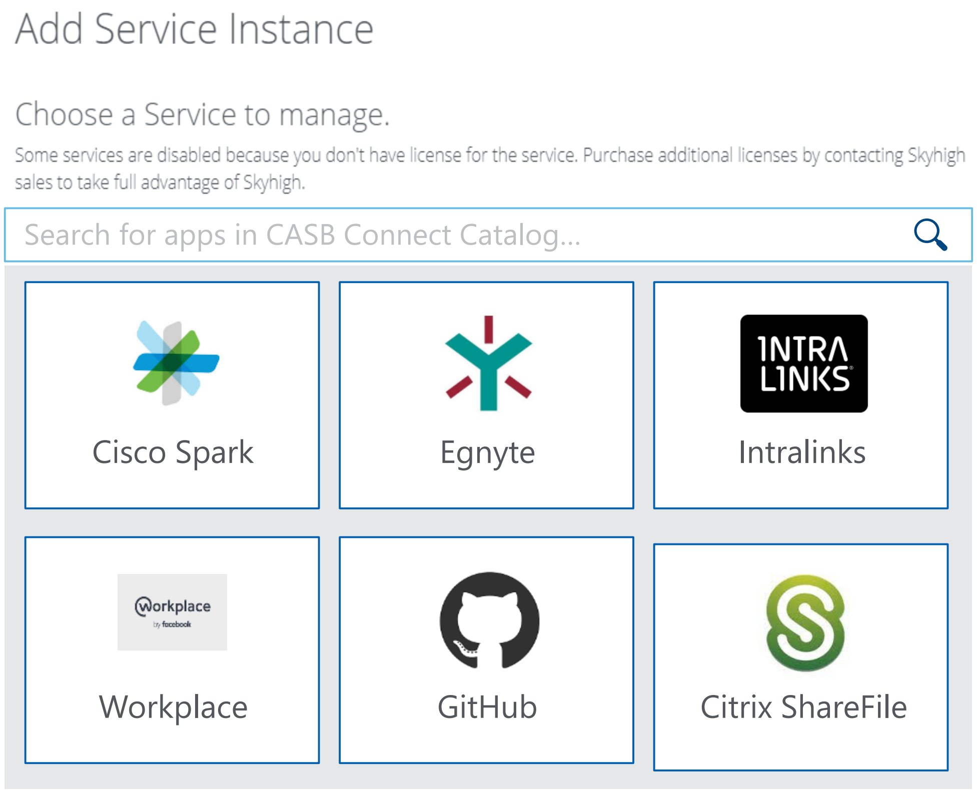
```
"events": {
  "request": "http('get_events', 'param_check_point=#check_point')",
  "response": {
    "events_array": "$.events",
    "next_page_token": "",
    "mapping": {
      "event_id": "$.id",
      "event_name": "$.action",
      "timestamp": "$.timestamp",
      "actor": {
        "id": "$.actor",
        "name": "json_path(http('get_actor','param_actor_id=$.actor'), '$.name')",
        "email": "json_path(http('get_actor','param_actor_id=$.actor'), '$.email')"
      },
      "event_category": [
        {
          "category": "Data Upload",
          "response_filter": [
            {
              "$.type": "file_system",
              "$.action": "create"
            },
            {
              "$.type": "file_system",
              "$.action": "copy"
            },
            {
              "$.type": "file_system",
              "$.action": "add"
            }
          ]
        }
      ],
      "content": [
        {
          "content_url": "#base_url + '/pubapi/v1/fs-content' + $.data.target_path",
          "content_id": ""
        }
      ]
    }
  }
},
```

API framework and toolkit for native integration

Only 2 hours to complete with no coding required

Adopted by over 25 Cloud apps in just one month

SAAS Coverage : CASB Connect Catalog (API + Inline)



Add Service Instance

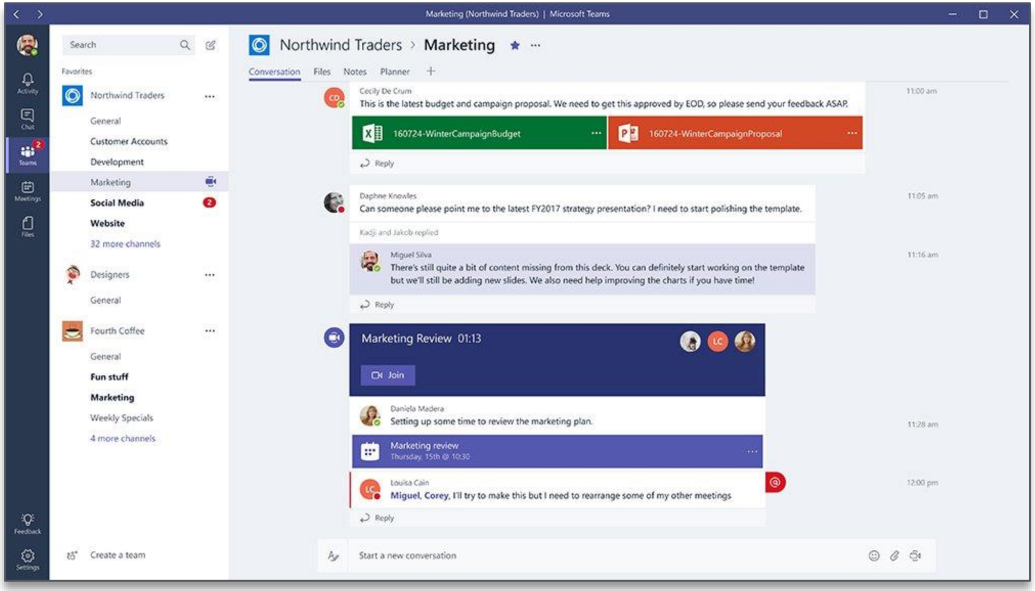
Choose a Service to manage.

Some services are disabled because you don't have license for the service. Purchase additional licenses by contacting Skyhigh sales to take full advantage of Skyhigh.

Search for apps in CASB Connect Catalog...

- Largest catalog of SAAS services
  - Single pane of all sanctioned services supported by Skyhigh
  - Business goals (use cases)
  - Shadow metrics
  - Ownership of integration
- Validating user inputs while enabling API access.
- Submit new app requests

SaaS Security - Day Zero Microsoft Teams Support



Cecily De Crum 11:00 am
This is the latest budget and campaign proposal. We need to get this approved by EOD, so please send your feedback ASAP.

Daphne Knowles 11:05 am
Can someone please point me to the latest FY2017 strategy presentation? I need to start polishing the template.

Kadji and Jakob replied

Miguel Silva 11:16 am
There's still quite a bit of content missing from this deck. You can definitely start working on the template but we'll still be adding new slides. We also need help improving the charts if you have time!

Daniela Madera 11:28 am
Setting up some time to review the marketing plan.

Louisa Cain 12:00 pm
Miguel, Corey, I'll try to make this but I need to rearrange some of my other meetings

- Extend DLP policies to Microsoft teams for both files and messages.
- Scan existing Microsoft Teams accounts to identify compliance issues.
- Extend Conditional Access policies to Microsoft Teams.
- Apply EUBA to Microsoft Teams.

McAfee™

Together is power.

Enterprise IaaS/PaaS

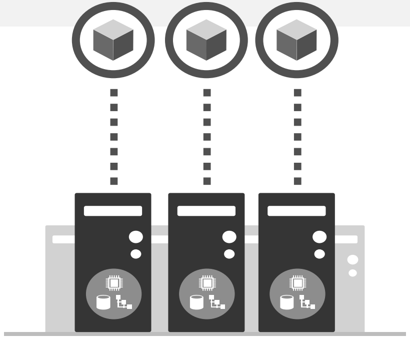
Enabling Cloud Native Architectures

Cloud Native Architectures

What is Different ?

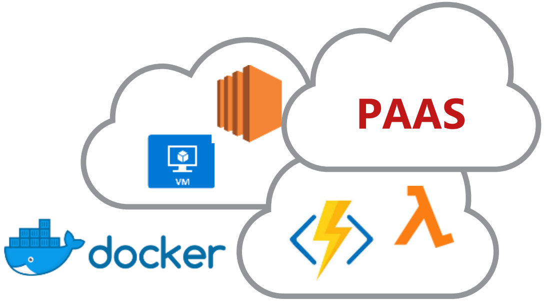
Traditional Applications

- Tight coupling between infrastructure and apps
- Siloed infrastructure, operations, and dev teams
- Security is custom and technical controls based



Cloud Native

- Loosely coupled apps and micro-services
- Service-focused DevOps
- Security is standard and specification based



Enterprise IaaS/PaaS Use Cases

1. Managing Drift
Identify IaaS resources with security settings that are non-compliant

2. Advanced Threat Protection
Detect compromised accounts, privileged user threats, malware.

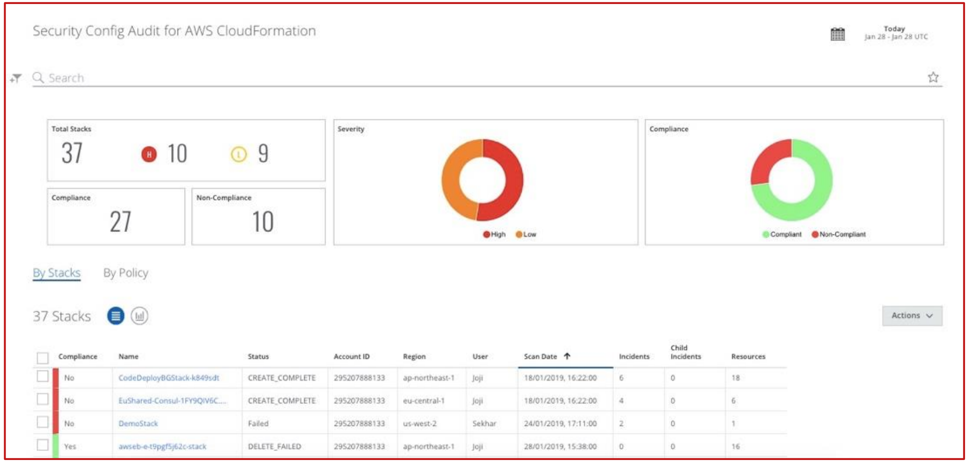
3. Sensitive Data Visibility
Manage risk of sensitive information/data.

Source: McAfee Cloud Adoption Report, Nov 2018

Key Considerations for Enterprise IaaS/Paas Security

- Developer/Devops centric models are key to success.
- Multi Cloud & Hybrid Cloud support.
- Information risk driving context and priority.

Integrating Security Into The DevOps Process



Security Config Audit for AWS CloudFormation

Today
Jan 28 - Jan 28 UTC

Search

Total Stacks
37 H 10 L 9

Compliance
27

Non-Compliance
10

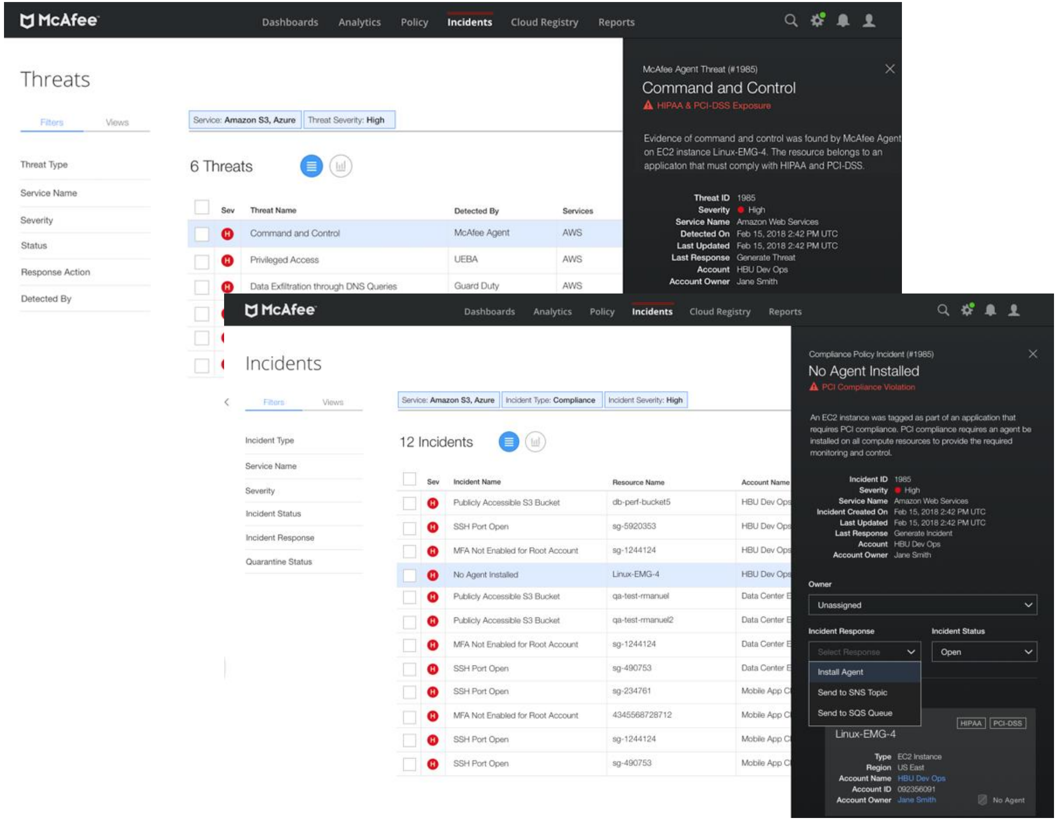
By Stacks By Policy

37 Stacks

□	Compliance	Name	Status	Account ID	Region	User	Scan Date ↑	Incidents	Child Incidents	Resources
□	No	CodeDeployBGStack-k849sdt	CREATE_COMPLETE	295207888133	ap-northeast-1	Joji	18/01/2019, 16:22:00	6	0	18
□	No	EuShared-Consul-1FY9QIV6C...	CREATE_COMPLETE	295207888133	eu-central-1	Joji	18/01/2019, 16:22:00	4	0	6
□	No	DemoStack	Failed	295207888133	us-west-2	Sekhar	24/01/2019, 17:11:00	2	0	1
□	Yes	awseb-e-t9pgf5j62c-stack	DELETE_FAILED	295207888133	ap-northeast-1	Joji	28/01/2019, 15:38:00	0	0	16

- Compliance protection on CloudFormation templates and Landing Zone scripts
- Prevent misconfigurations from being deployed as opposed to correctly them after the fact
- Integrate with DevOps Tools

Multi-Cloud & Hybrid Cloud Coverage



Threats

Threat Type
Service Name
Severity
Status
Response Action
Detected By

Service: **Amazon S3, Azure** | Threat Severity: **High**

6 Threats

	Sev	Threat Name	Detected By	Services
□	H	Command and Control	McAfee Agent	AWS
□	H	Privileged Access	UEBA	AWS
□	H	Data Exfiltration through DNS Queries	Guard Duty	AWS

McAfee Agent Threat (#1985)

Command and Control

⚠ HIPAA & PCI-DSS Exposure

Evidence of command and control was found by McAfee Agent on EC2 instance Linux-EMG-4. The resource belongs to an applicaton that must comply with HIPAA and PCI-DSS.

Threat ID	1985
Severity	● High
Service Name	Amazon Web Services
Detected On	Feb 15, 2018 2:42 PM UTC
Last Updated	Feb 15, 2018 2:42 PM UTC
Last Response	Generate Threat
Account	HBU Dev Ops
Account Owner	Jane Smith

Incidents

Incident Type
Service Name
Severity
Incident Status
Incident Response
Quarantine Status

Service: **Amazon S3, Azure** | Incident Type: **Compliance** | Incident Severity: **High**

12 Incidents

	Sev	Incident Name	Resource Name	Account Name
□	H	Publicly Accessible S3 Bucket	db-perf-bucket5	HBU Dev Ops
□	H	SSH Port Open	sg-5920353	HBU Dev Ops
□	H	MFA Not Enabled for Root Account	sg-1244124	HBU Dev Ops
□	H	No Agent Installed	Linux-EMG-4	HBU Dev Ops
□	H	Publicly Accessible S3 Bucket	qa-test-rmanuel	Data Center E
□	H	Publicly Accessible S3 Bucket	qa-test-rmanuel2	Data Center E
□	H	MFA Not Enabled for Root Account	sg-1244124	Data Center E
□	H	SSH Port Open	sg-490753	Data Center E
□	H	SSH Port Open	sg-234761	Mobile App C
□	H	MFA Not Enabled for Root Account	4345568728712	Mobile App C
□	H	SSH Port Open	sg-1244124	Mobile App C
□	H	SSH Port Open	sg-490753	Mobile App C

Compliance Policy Incident (#1985)

No Agent Installed

⚠ PCI Compliance Violation

An EC2 instance was tagged as part of an application that requires PCI compliance. PCI compliance requires an agent be installed on all compute resources to provide the required monitoring and control.

Incident ID	1985
Severity	● High
Service Name	Amazon Web Services
Incident Created On	Feb 15, 2018 2:42 PM UTC
Last Updated	Feb 15, 2018 2:42 PM UTC
Last Response	Generate Incident
Account	HBU Dev Ops
Account Owner	Jane Smith

Owner: Unassigned

Incident Response: Select Response

- Install Agent
- Send to SNS Topic
- Send to SQS Queue

Incident Status: Open

HIPAA | PCI-DSS

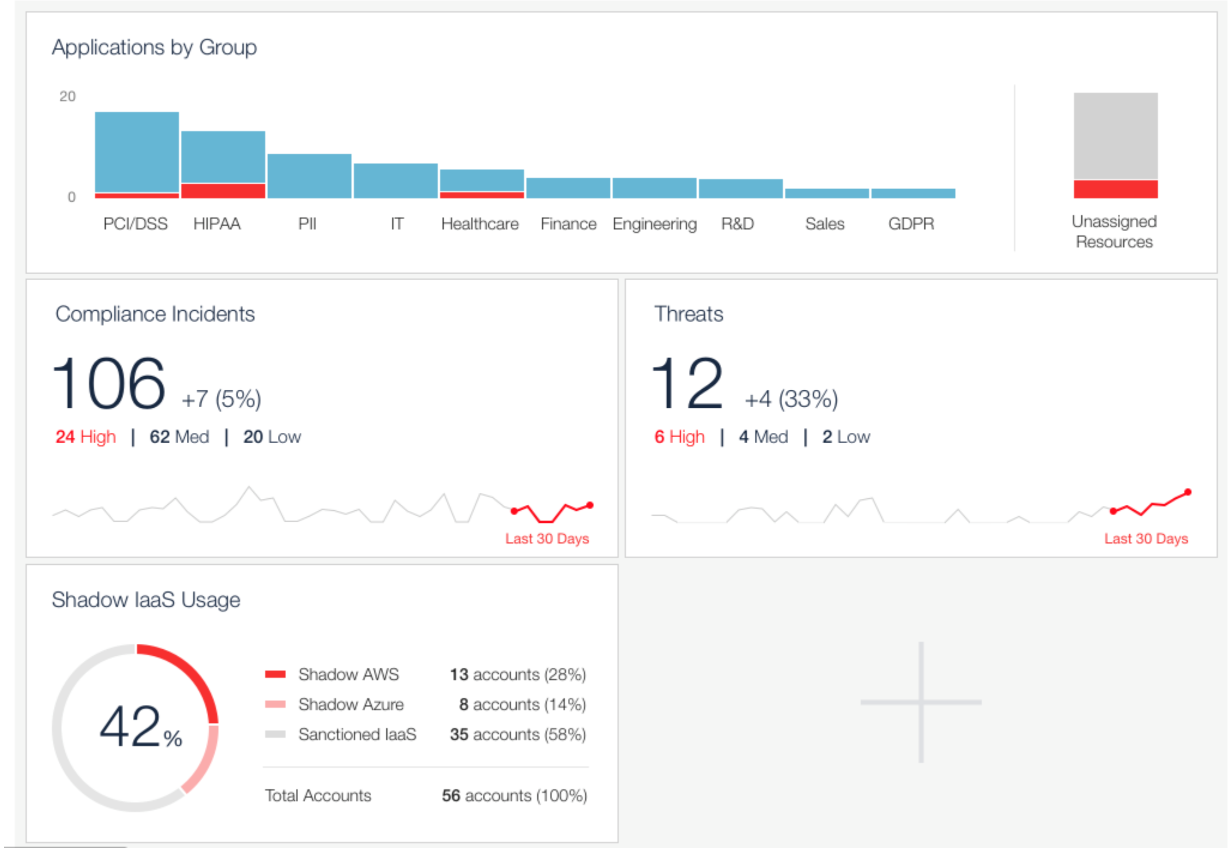
Linux-EMG-4

Type	EC2 Instance
Region	US East
Account Name	HBU Dev Ops
Account ID	092356091
Account Owner	Jane Smith

No Agent

- Seamless workflow for discovery of compute resources and recommendations for agent deployment.
- Server workload threat protection via Mcafee Server Protection Suite.
- Single console for all Threat protection – UEBA, Malware, Workloads

Tying Information Risk to Drift and Threat.



Applications by Group

Compliance Incidents

106 +7 (5%)

24 High | 62 Med | 20 Low

Threats

12 +4 (33%)

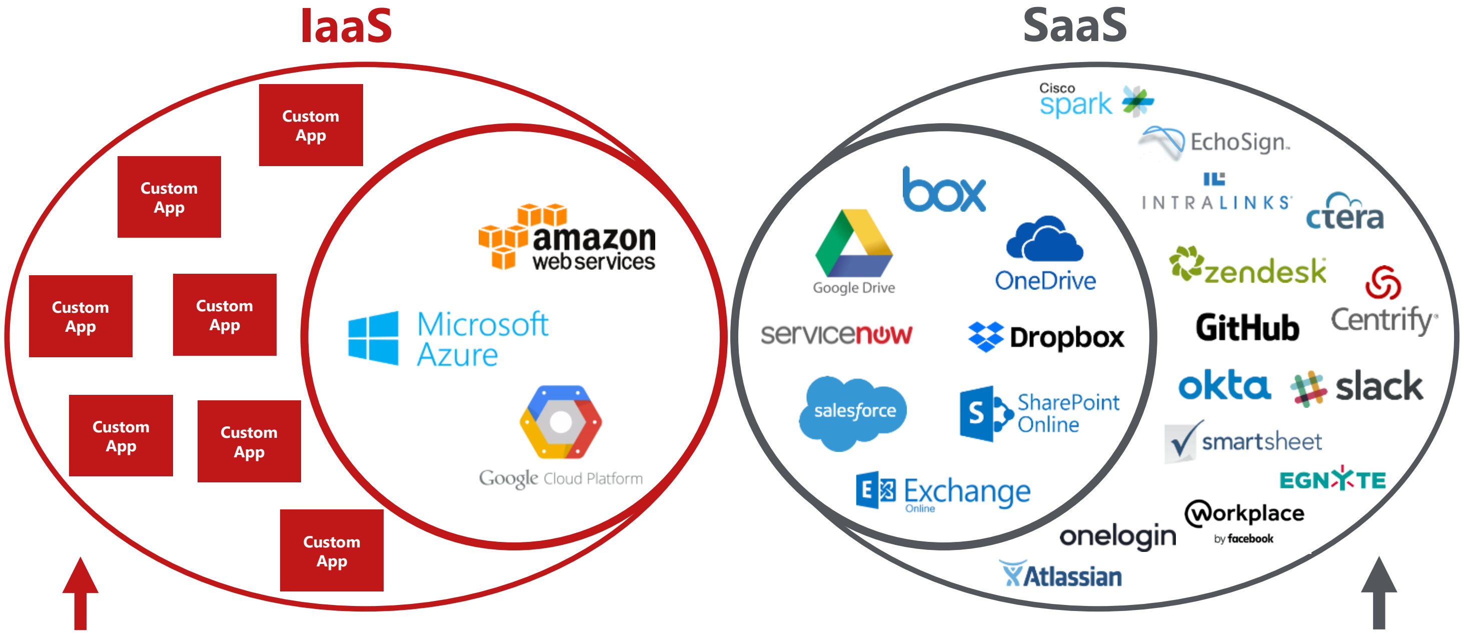
6 High | 4 Med | 2 Low

Shadow IaaS Usage

42%

🟥	Shadow AWS	13 accounts (28%)
▨	Shadow Azure	8 accounts (14%)
▨	Sanctioned IaaS	35 accounts (58%)
	Total Accounts	56 accounts (100%)

Comprehensive Security for the Cloud

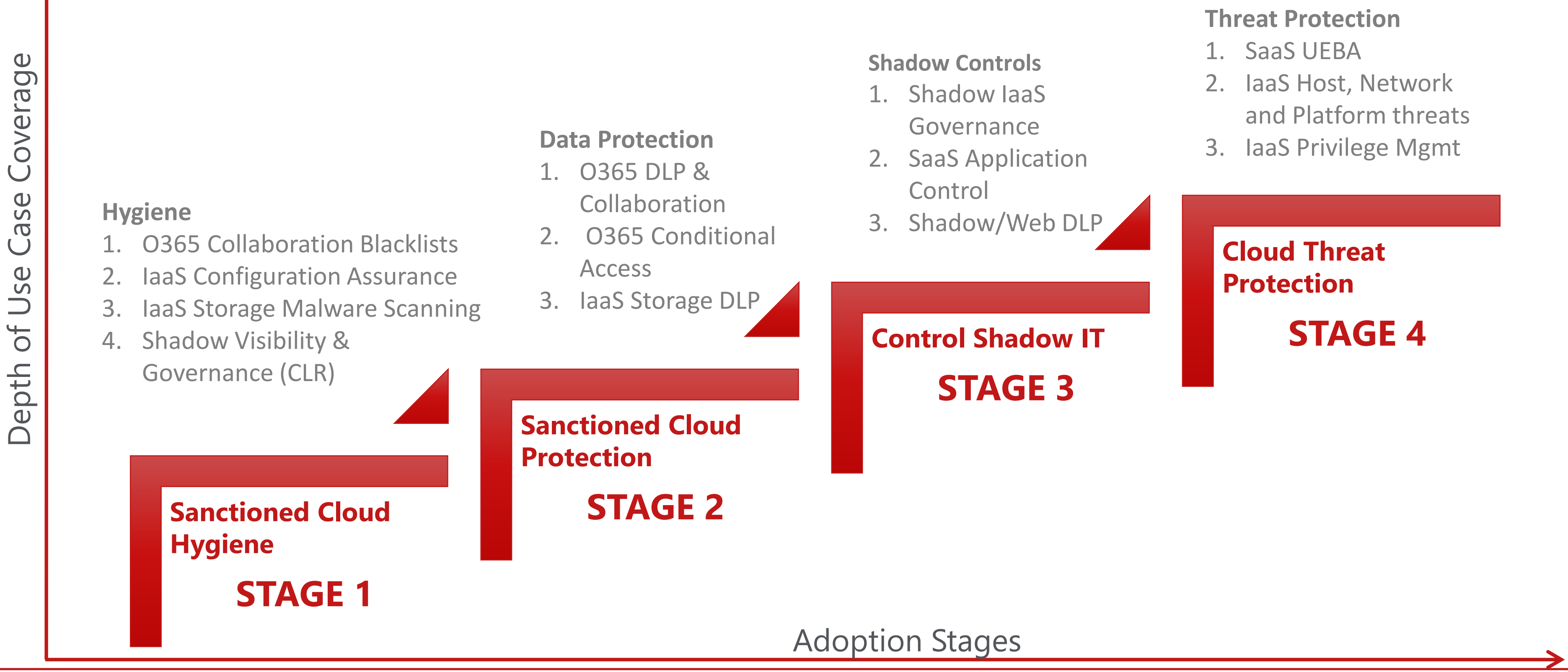


Support for Custom Apps

SaaS Catalog

Operational Simplification & Automation

Prescriptive Adoption Methodology



Depth of Use Case Coverage

Hygiene

1. O365 Collaboration Blacklists
2. IaaS Configuration Assurance
3. IaaS Storage Malware Scanning
4. Shadow Visibility & Governance (CLR)

Sanctioned Cloud Hygiene

STAGE 1

Data Protection

1. O365 DLP & Collaboration
2. O365 Conditional Access
3. IaaS Storage DLP

Sanctioned Cloud Protection

STAGE 2

Shadow Controls

1. Shadow IaaS Governance
2. SaaS Application Control
3. Shadow/Web DLP

Control Shadow IT

STAGE 3

Threat Protection

1. SaaS UEBA
2. IaaS Host, Network and Platform threats
3. IaaS Privilege Mgmt

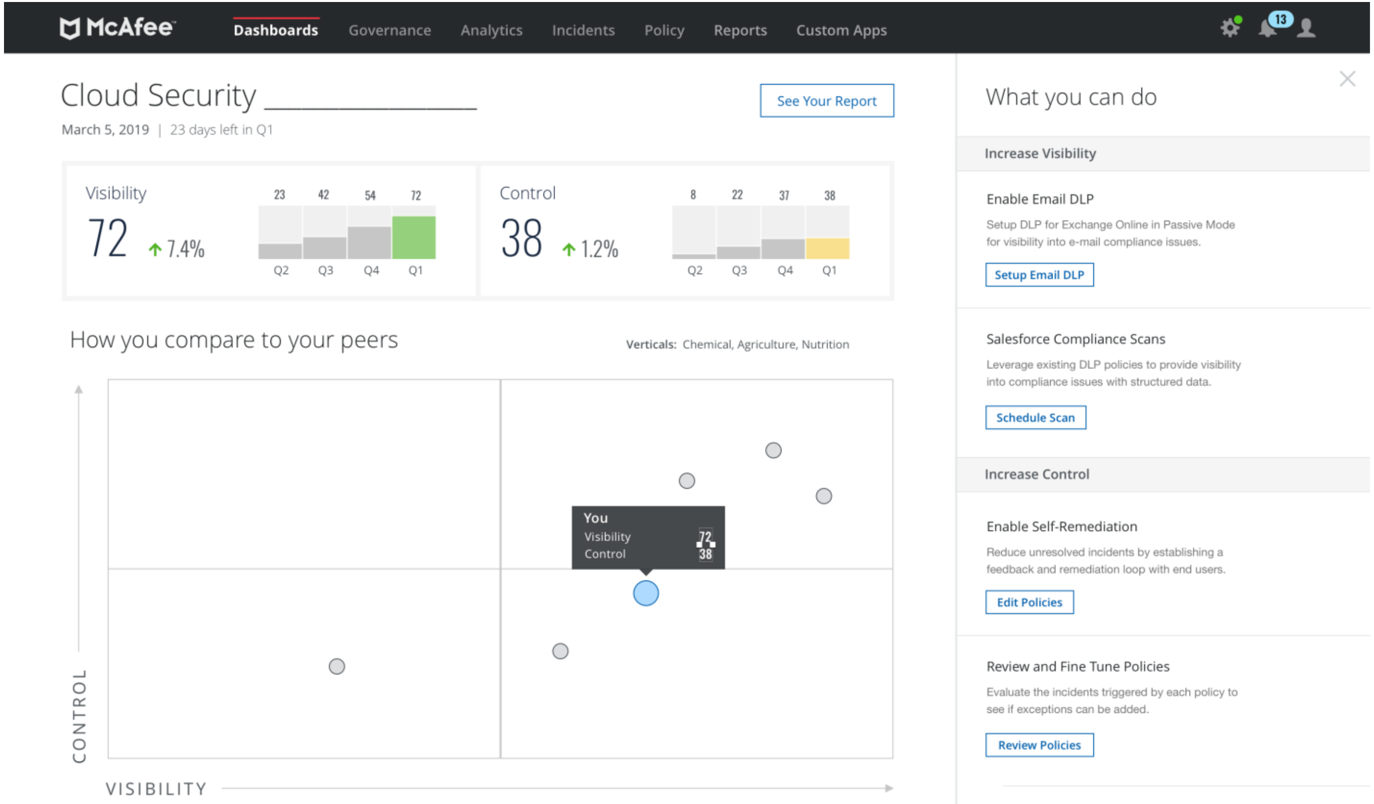
Cloud Threat Protection

STAGE 4

Adoption Stages

Operational Simplification & Automation

Customer cloud maturity and value reporting



Cloud Security ______________

March 5, 2019 | 23 days left in Q1

How you compare to your peers

Verticals: Chemical, Agriculture, Nutrition

What you can do

Increase Visibility

Enable Email DLP

Setup DLP for Exchange Online in Passive Mode for visibility into e-mail compliance issues.

Salesforce Compliance Scans

Leverage existing DLP policies to provide visibility into compliance issues with structured data.

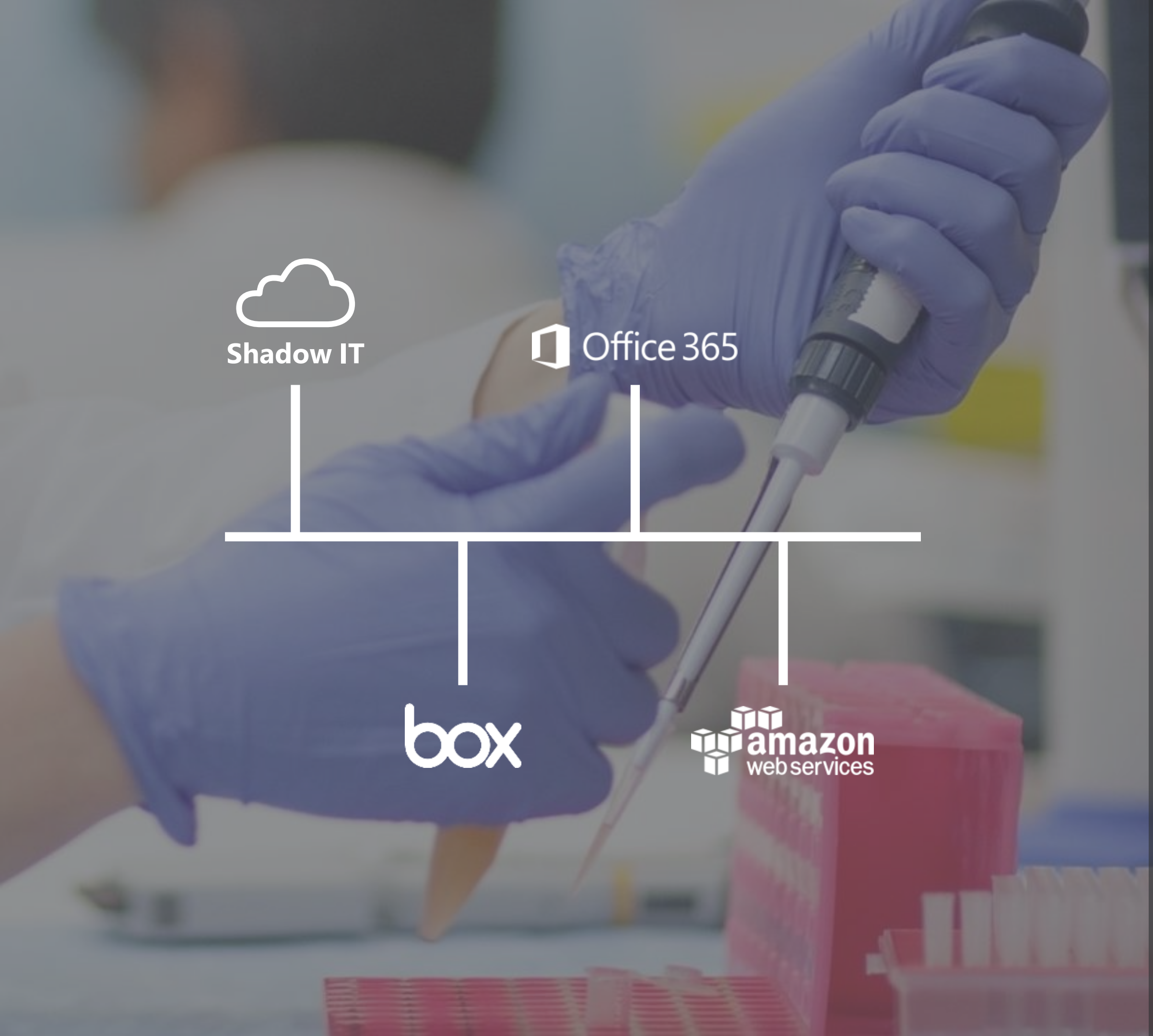
Increase Control

Enable Self-Remediation

Reduce unresolved incidents by establishing a feedback and remediation loop with end users.

Review and Fine Tune Policies

Evaluate the incidents triggered by each policy to see if exceptions can be added.



AstraZeneca

McAfee (Skyhigh) customer since 2014

65,000 Employees

Why McAfee Skyhigh Security Cloud

- Collaboration Control
- Data Loss Prevention
- Governance

Project Champion

- Jeff Haskill (Group CSO)
  - Won CSO50 Award for use of Skyhigh to accelerate business

Atrium Health

65,000 Employees

Why MVISION Cloud

- Governance of cloud services
- Comprehensive cloud security (on path to CASB+WG+DLP)
- Microsoft-recommended approach to Office365 data security

MVISION Cloud

Cloud Security that Accelerates Business

FOR MORE INFORMATION: Kaushik_Narayan@mcafee.com