Netskope Introduction

Introductions and Agenda

- Introductions – roles / responsibilities
- Cloud services you're using
- Netskope overview
- Product demo
- Q&A / Next steps

Name Thomas Hedströmmer

Title Sr. SE Cloud Security

Email thomas.hedstrommer@netskope.com

Your Cloud Usage and Concerns

Cloud Services in Use or in Plan?

Data in the Cloud?

PCI

Intellectual Property

Design Documents

PII

PHI

Regulations, Standards, Other Requirements?

HIPAA

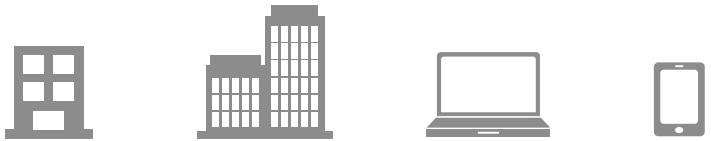
GLBA

GDPR

PCI-DSS

FINRA

Cloud Service Access (Who, Where, and How)?



Securing the Cloud

Top Cloud Security Concerns

Shadow IT
Risk of unapproved use of cloud services

Regulatory
Aligning cloud service use with regulatory requirements

Data Exposure
Risk of sensitive data loss via cloud services

Cloud Threats
Cloud services as targets and as attack vector

Gartner's Four Pillars of CASB

VISIBILITY

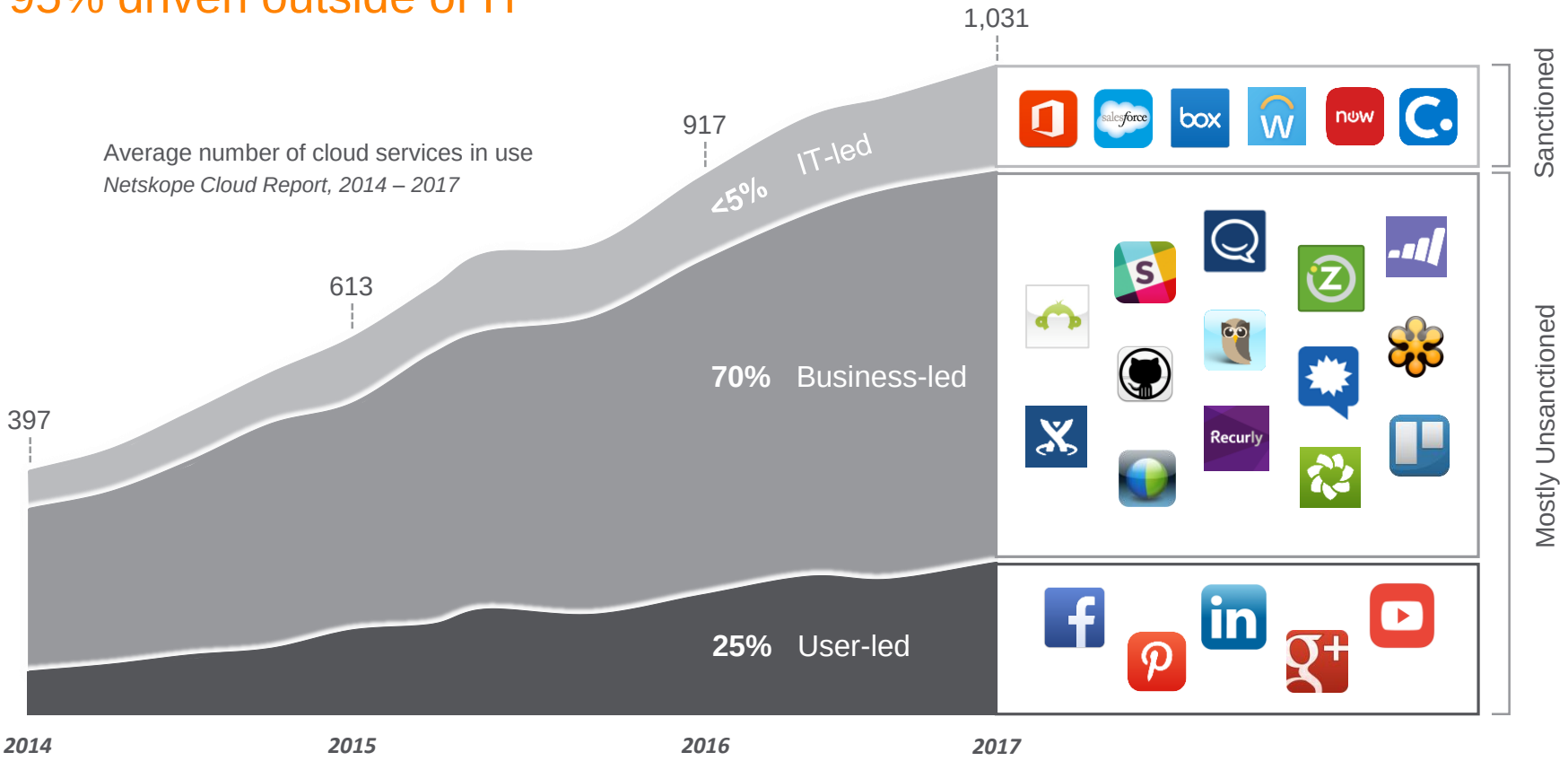
COMPLIANCE

DATA SECURITY

THREAT PROTECTION

Growth in Enterprise Cloud Services

95% driven outside of IT



How Users Access Cloud Services

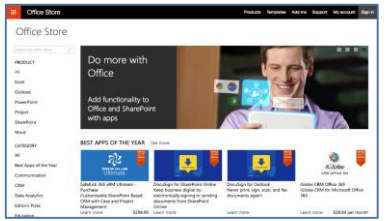
User locations and access methods determine appropriate CASB architecture

Web Browser

Sync Client

Mobile App

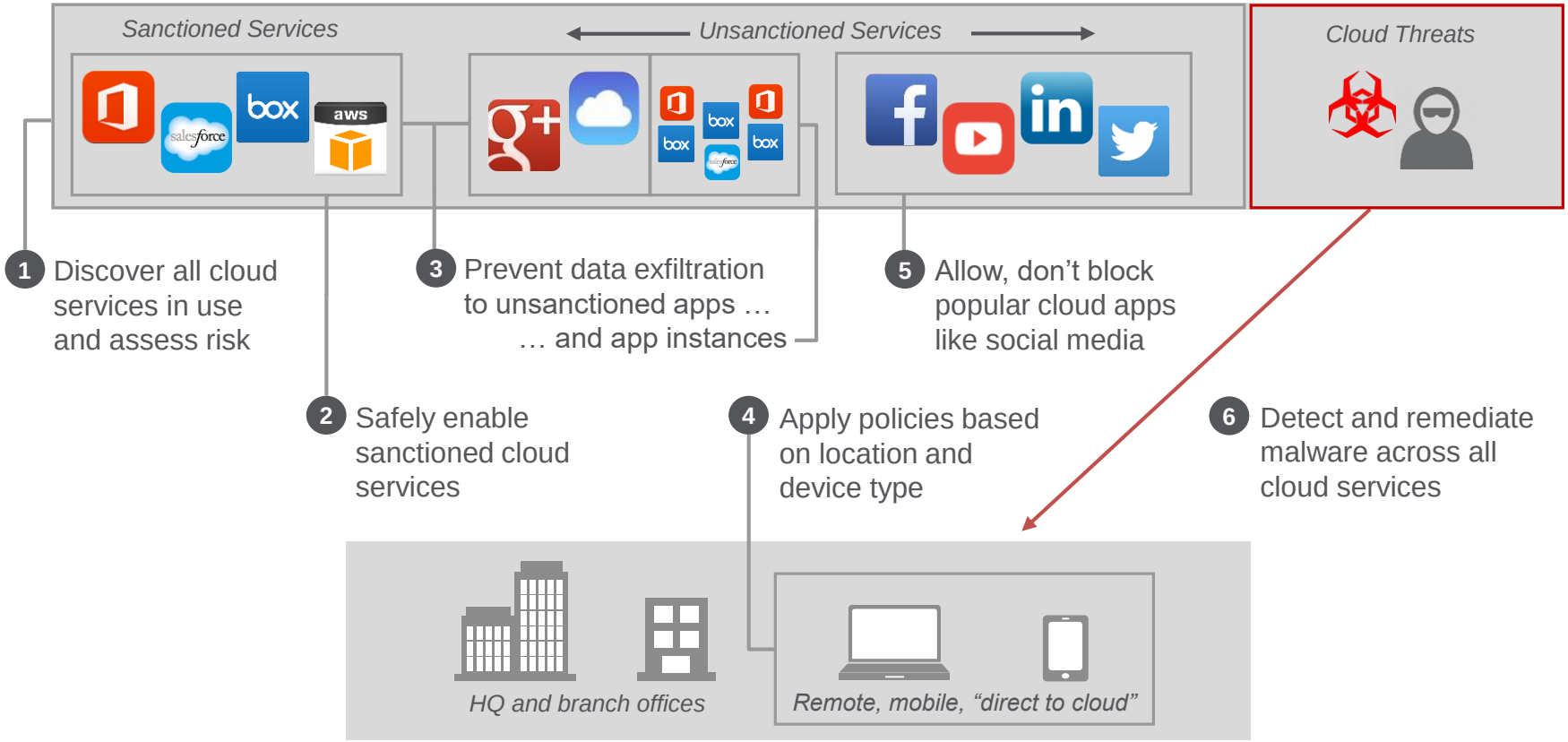
App Ecosystem



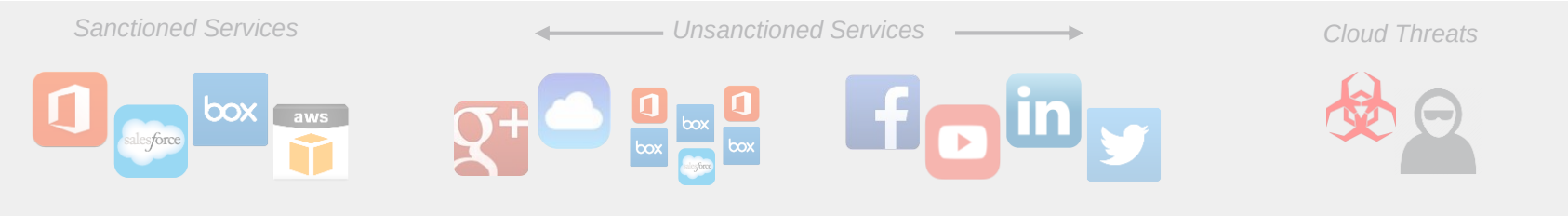
HQ **Branch**

Remote, Mobile, "Direct to Cloud"

Common Netskope Use Cases



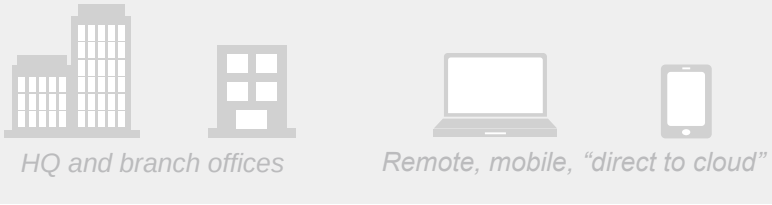
Netskope Solution Overview



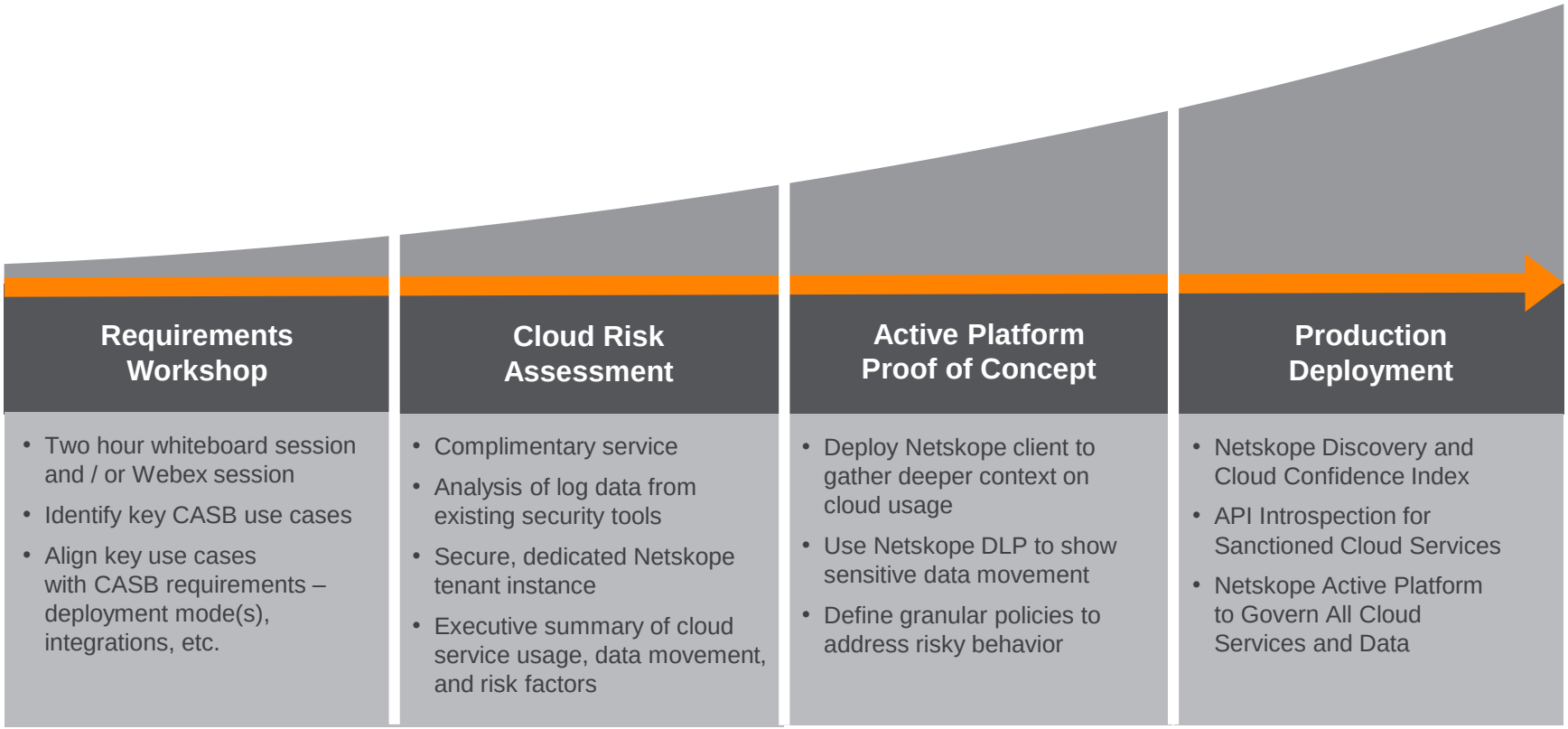
SSL Decryption at Scale

Discovery and risk assessment	Netskope Context Engine	Cloud data encryption
Granular policy control	Identity | App | Activity | Data	Anomaly detection and UBA
Advanced, enterprise DLP		Advanced threat protection

Log-based discovery | API connector | All Mode Architecture | Reverse proxy | Forward proxy



Getting Started with Netskope



Customers

Thank You!

Thomas Hedströmmer
Thomas.hedstrommer@netskope.com

Team

- 350+ employees globally, including North America, Europe, and Asia-Pacific
- Early architects/founders from Palo Alto Networks, NetScreen, Cisco, McAfee, VMware
- First comprehensive CASB patents. 40+ patent claims across four categories

netskope

The leader in cloud security

Partners

- Strong technology integration and services partnerships

box · Microsoft Gold Partner · Google · Dropbox · salesforce · TITUS · okta · Ping Identity · IBM Radar

Investors

- $131.4M from top Silicon Valley VCs
- Early investors in Atlassian, Box, Cloudera, Nimble Storage, Yammer

ICONIQ · ACCEL PARTNERS · LIGHTSPEED VENTURE PARTNERS · S+C THE SOCIAL+CAPITAL PARTNERSHIP

Leading Companies Using Netskope

The Fortune 1	The top automaker in the world	Top 3 global hotel chain
3 of the top 5 global retailers	The most valuable bank in the world	Top 3 U.S. oil and gas company
Largest equipment manufacturer in the world	The largest insurance company in the world	Top 3 global apparel manufacturer

Discover All Cloud Services in Use and Assess Risk

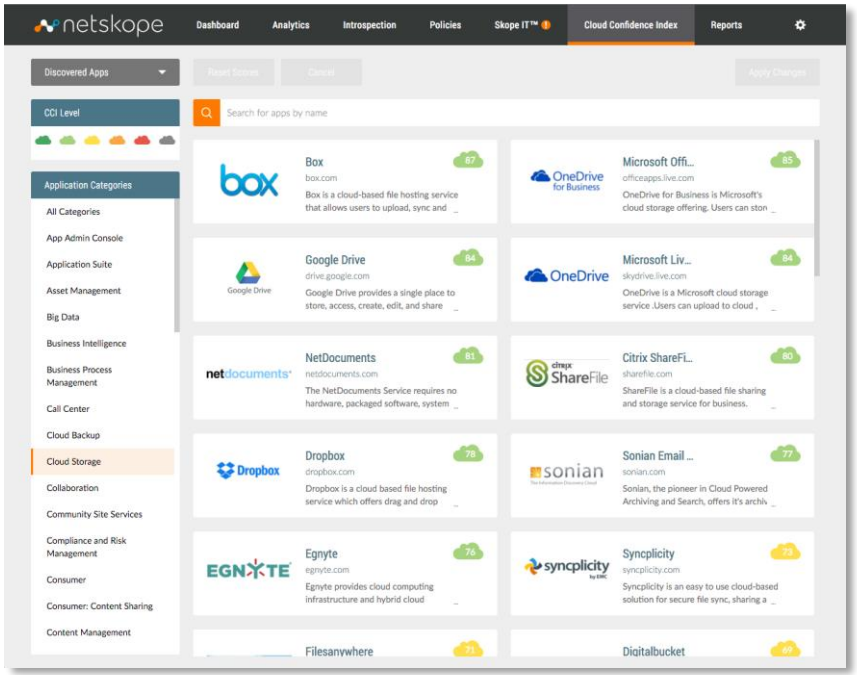
Functional requirements

- Find all cloud services in use
- Report on cloud service enterprise-readiness using 45+ criteria
- Assess risk based on cloud service readiness coupled with cloud usage and user behavior
- Compare and consolidate redundant services

Architectural considerations

- Out-of-band options include log-based discovery and TAP mode

- Forward proxy modes provide deeper context for advanced discovery



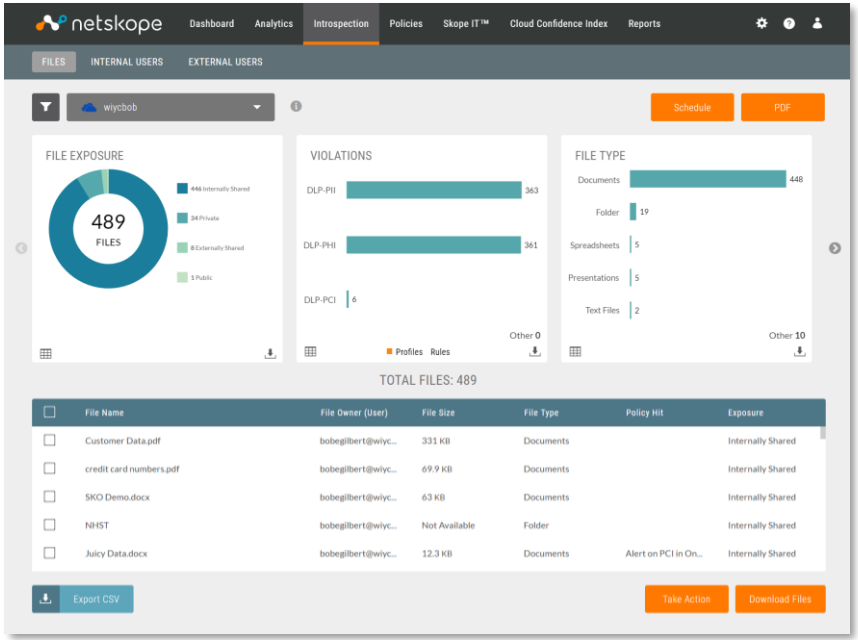
Safely Enable Sanctioned Cloud Services

Functional requirements

- Identify sensitive data in sanctioned services
- Understand how cloud service and data is being used
  - Data shared publicly or outside of company?
  - Inappropriate access by internal users?
- Protect against malware

Architectural considerations

- Can be deployed with out-of-band API connector
- Inline options for real-time visibility and control



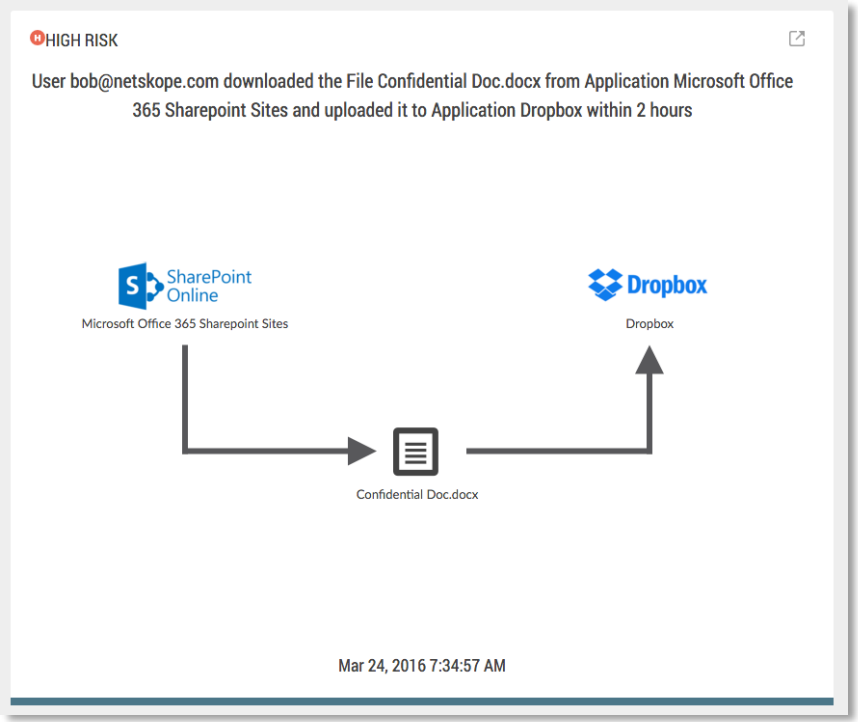
Prevent Data Exfiltration to Unsanctioned Apps and App Instances

Functional requirements

- Visibility into activities across sanctioned and unsanctioned cloud services
- Ability to differentiate cloud service instances
  - For example, corporate Box instance vs. personal Box instances
- Detect sensitive data across all cloud services
- Correlation of events across multiple cloud services

Architectural considerations

- Granular control of unsanctioned cloud services requires forward proxy



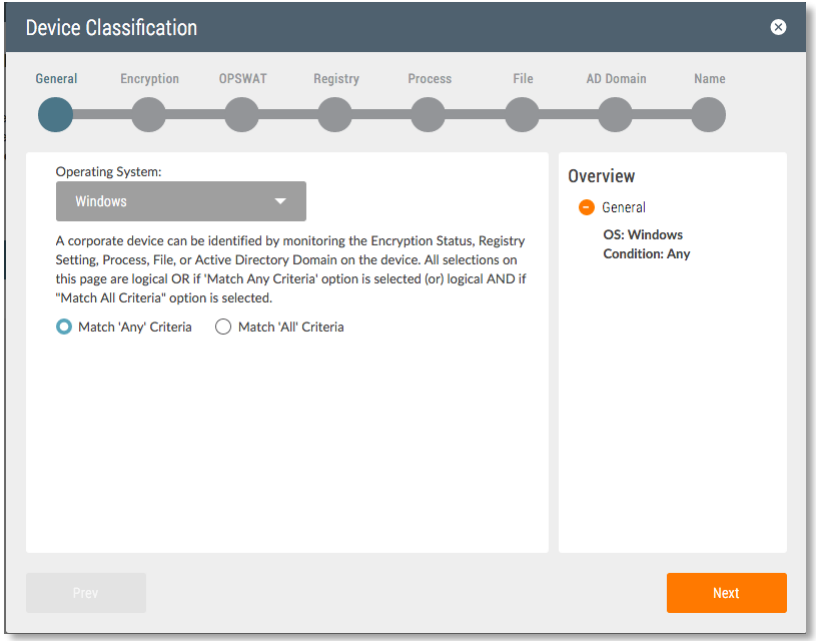
Apply Policies Based on Location and Device Type

Functional requirements

- Determine source and destination locations of cloud service usage
- Ability to classify device type
- Coverage of all access methods
  - Browser, sync client, and mobile app
- Apply granular policies based on location, device classification and access method

Architectural considerations

- Must be deployed inline using forward or reverse proxy



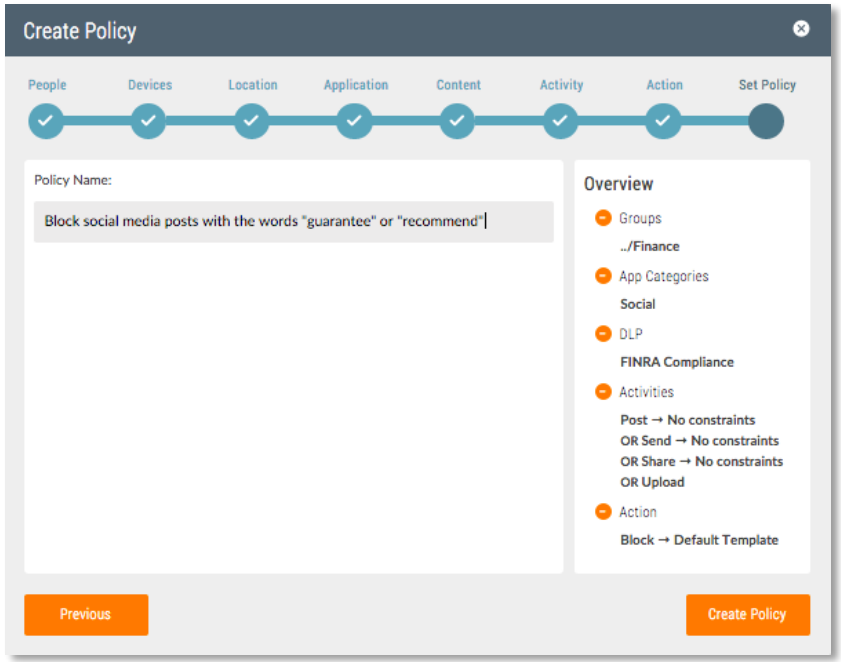
Allow, Don’t Block Popular Cloud Apps like Social Media

Functional requirements

- Support for category-level policies such as ‘social media’
- See activity-level detail across all cloud services
- DLP engine that can identify specific content tied to activities in unsanctioned cloud services
- Use context including activity and data to define policies that carve out specific risky activities

Architectural considerations

- Granular control of unsanctioned cloud services requires forward proxy



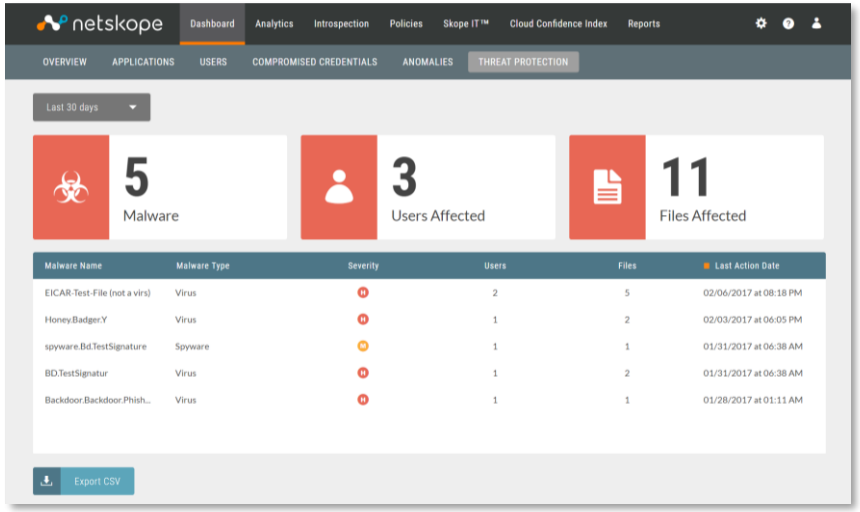
Detect and Remediate Malware Across All Cloud Services

Functional requirements

- Multi-layered detection engines
  - Static AV, heuristic, dynamic analysis, and more
- Detect malware in real-time en route to and from any cloud service
- Inspect sanctioned cloud services for malware
- Automated remediation capabilities to quarantine detected malware and reverse malware fan-out effect

Architectural considerations

- API connector for sanctioned services
- Forward proxy required for real-time inspection across all cloud services



Netskope Context Engine

Legacy systems
CASB 1.0

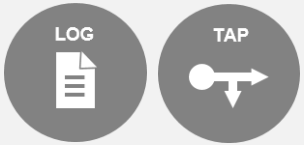
- URL
- Source/destination IP address
- Bytes transferred

- Geo-location
- User / Group / OU
- Device (managed, unmanaged, mobile)
- Client software (OS, browser, app)
- Cloud service
- Instance (corporate, personal, partner)
- Activity (edit, share, sign, etc.)
- Content

Netskope

Comparing CASB Architectures

Cloud Service Discovery

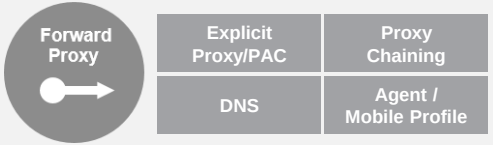


- Out-of-band deployment
- Provides high-level visibility into cloud service usage
- No cloud service policy control
- Couple cloud service discovery with cloud service risk assessment

Secure Sanctioned Cloud Services

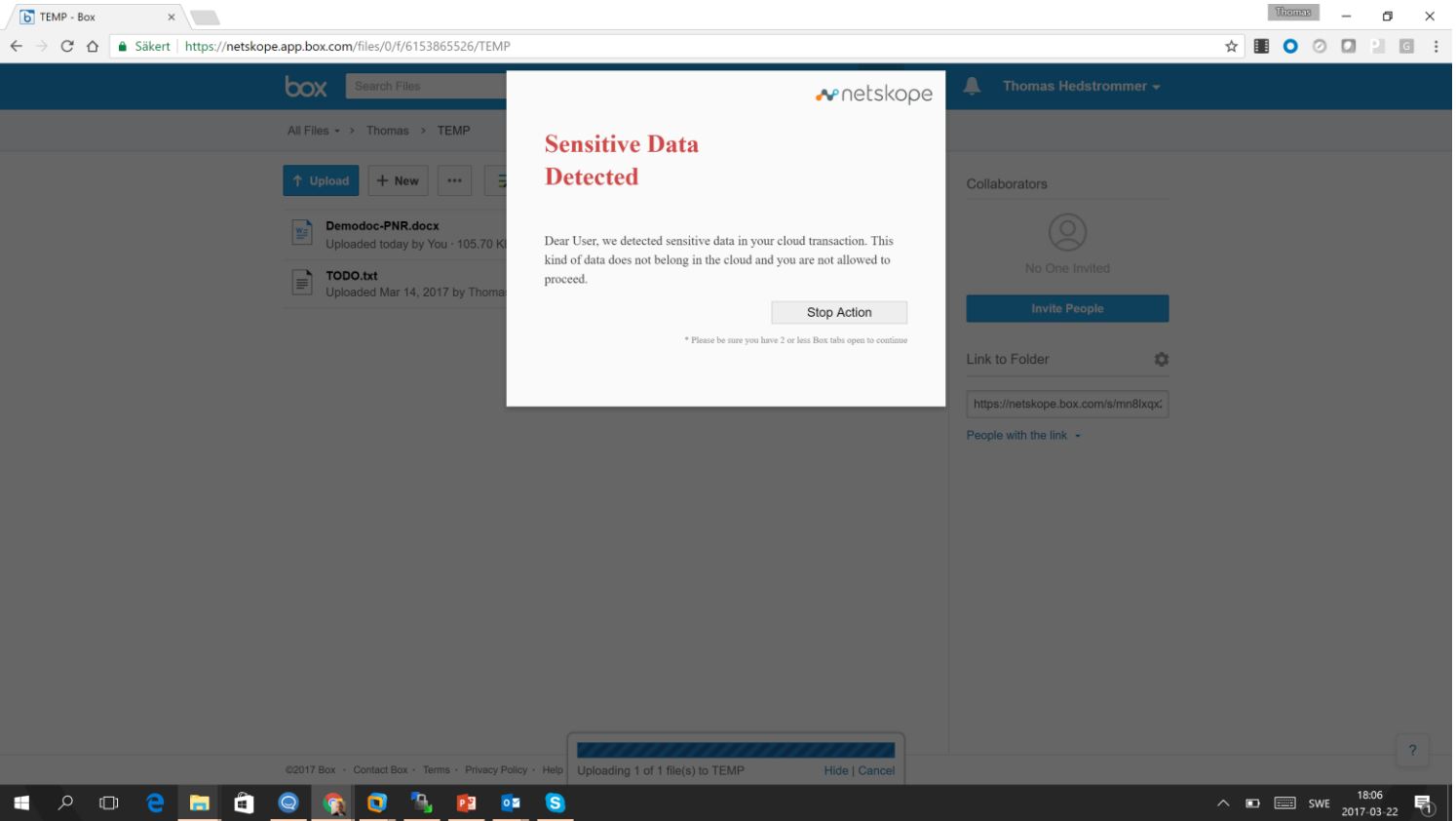
- API Introspection
  - Secure sanctioned cloud services with near real-time content inspection and policy control
- Reverse Proxy
  - Real-time policy control for sanctioned cloud services
  - Only covers browser access

Govern Sanctioned and Unsanctioned Cloud Services



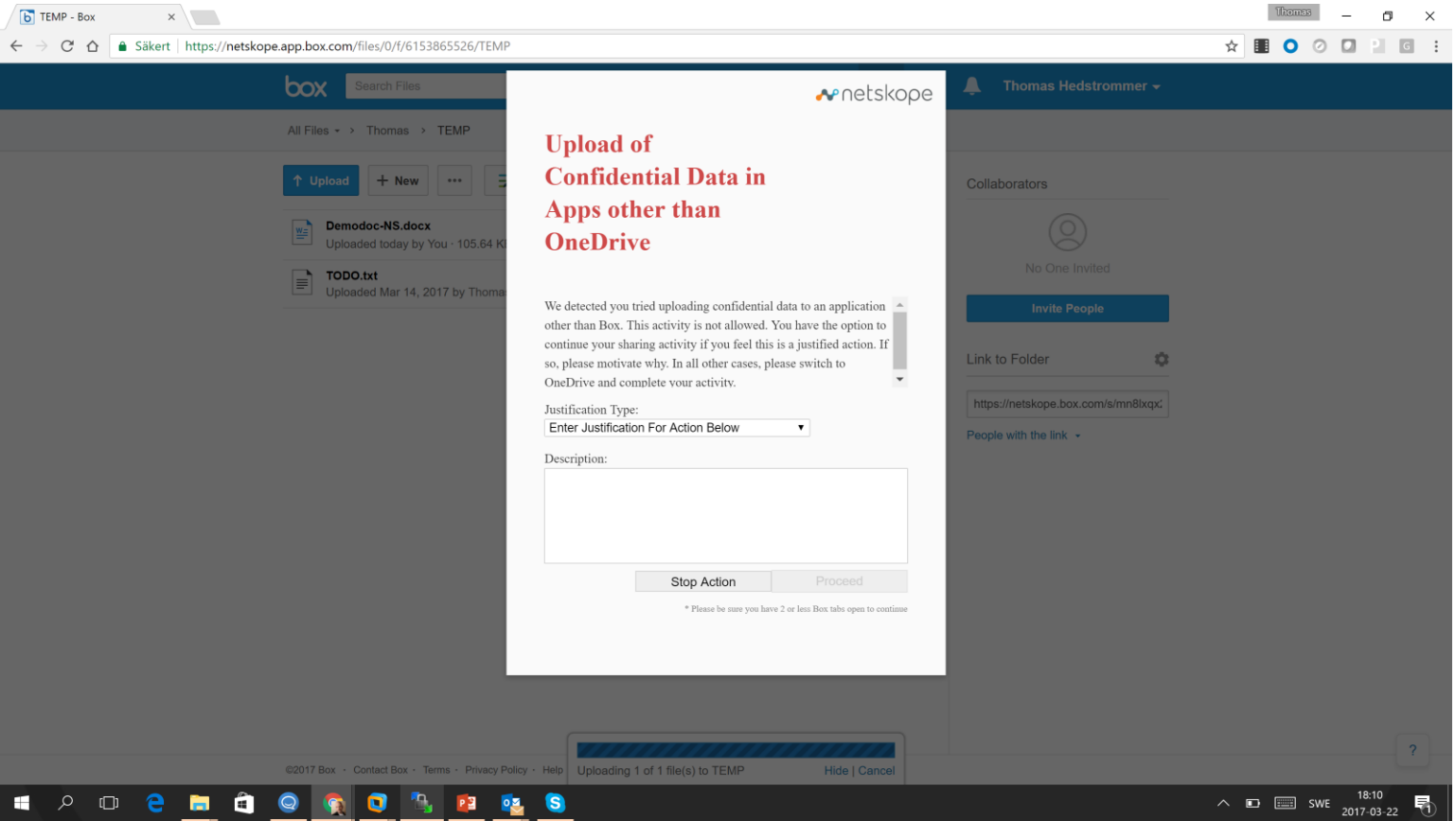
- Real-time policy control for all cloud services
- Visibility into remote and mobile, “direct-to-cloud” traffic
- Covers browsers, mobile apps, and sync clients

Use DLP to stop Personal Information Entering the Cloud



In this example a file containing Swedish Person nr has been dragged & dropped into Box.

Use DLP to coach users when they are trying to upload confidential materials



In this example a file containing Netskope Internal Only has been dragged & dropped into Box.