

Risk & Compliance Jaarcongres
Donderdag **1 juni 2017**

Landgoed Groot Kievitsdal, Baarn

Thema:
Bestrijding Financial Economic Crime

www.riskcompliancejaarcongres.nl

RISK & COMPLIANCE

2017

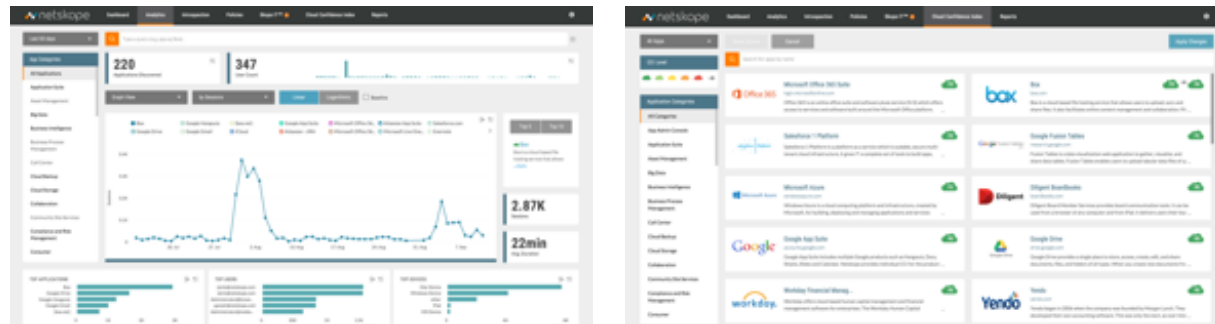
J A A R C O N G R E S



Netskope Product Overview

What We Do

- ▶ Discover apps and assess risk
- ▶ Safely enable sanctioned apps
- ▶ Govern all (i.e. unsanctioned) apps and data



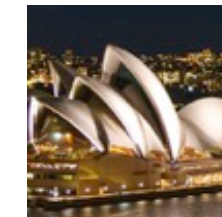
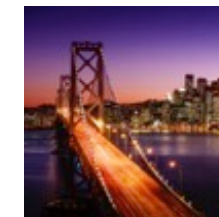
Customers

- ▶ Customers include some of the largest organizations across industries:

retail • financial services • healthcare • oil and gas • manufacturing • media • automotive
credit card processing • high tech • insurance • hospitality • consulting

Team

- ▶ 300+ employees globally, including North America, throughout Europe, and Asia-Pacific
- ▶ Early architects/executives from Palo Alto Networks, NetScreen, Cisco, McAfee, VMware
- ▶ 50+ patent claims granted



Investors

- ▶ \$131.4M from top venture firms in the world

ICONIQ

ACCEL
PARTNERS

LIGHTSPEED
VENTURE PARTNERS

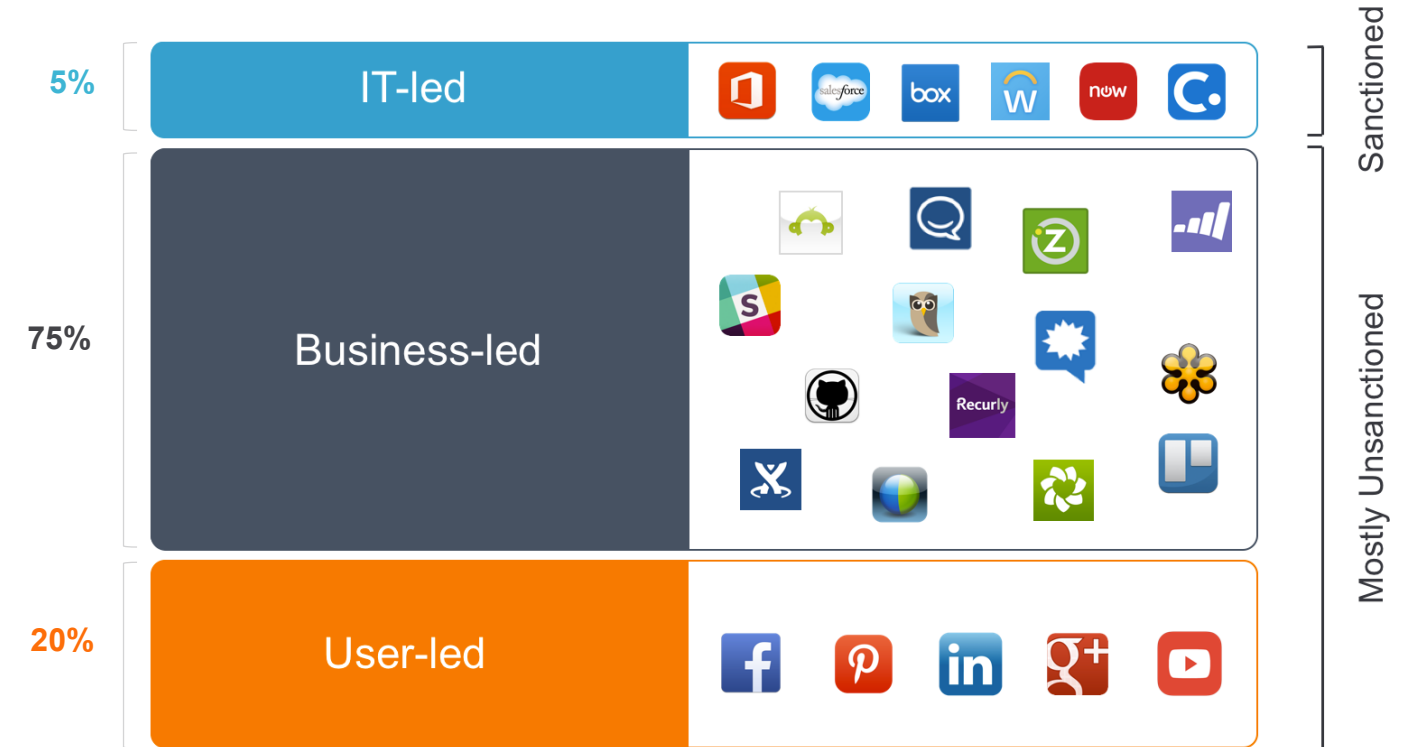
SC

THE SOCIAL+CAPITAL PARTNERSHIP

There are **22,000+**
enterprise cloud apps today (and growing)



977 apps on average, how do they get in?



95% of the apps are unknown by IT
Most apps are not enterprise-ready
End user is the new perimeter

Business data moving to cloud



Disruptive Trends

Rise of the API

Language of cloud is different than when legacy tools were built

The Everywhere Workplace

> 50% of all cloud usage occurs beyond your network

Browsers are “Losing” to Apps

> 50% of access comes from sync clients and apps, not browsers

Only by understanding these things can you gather a set of data rich enough solve the three primary CASB use cases

Three Primary Cloud Security Use Cases

1

Discover
shadow IT

2

Govern and secure
sanctioned apps

3

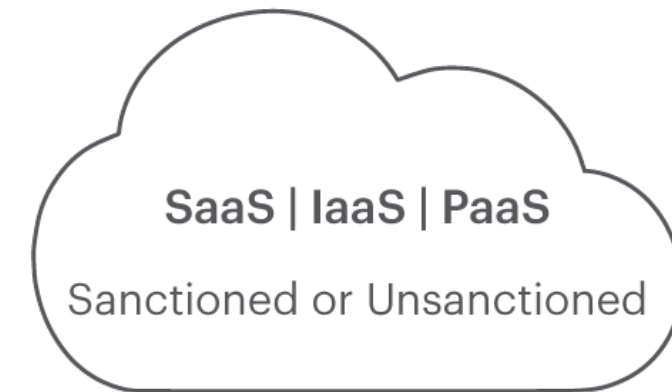
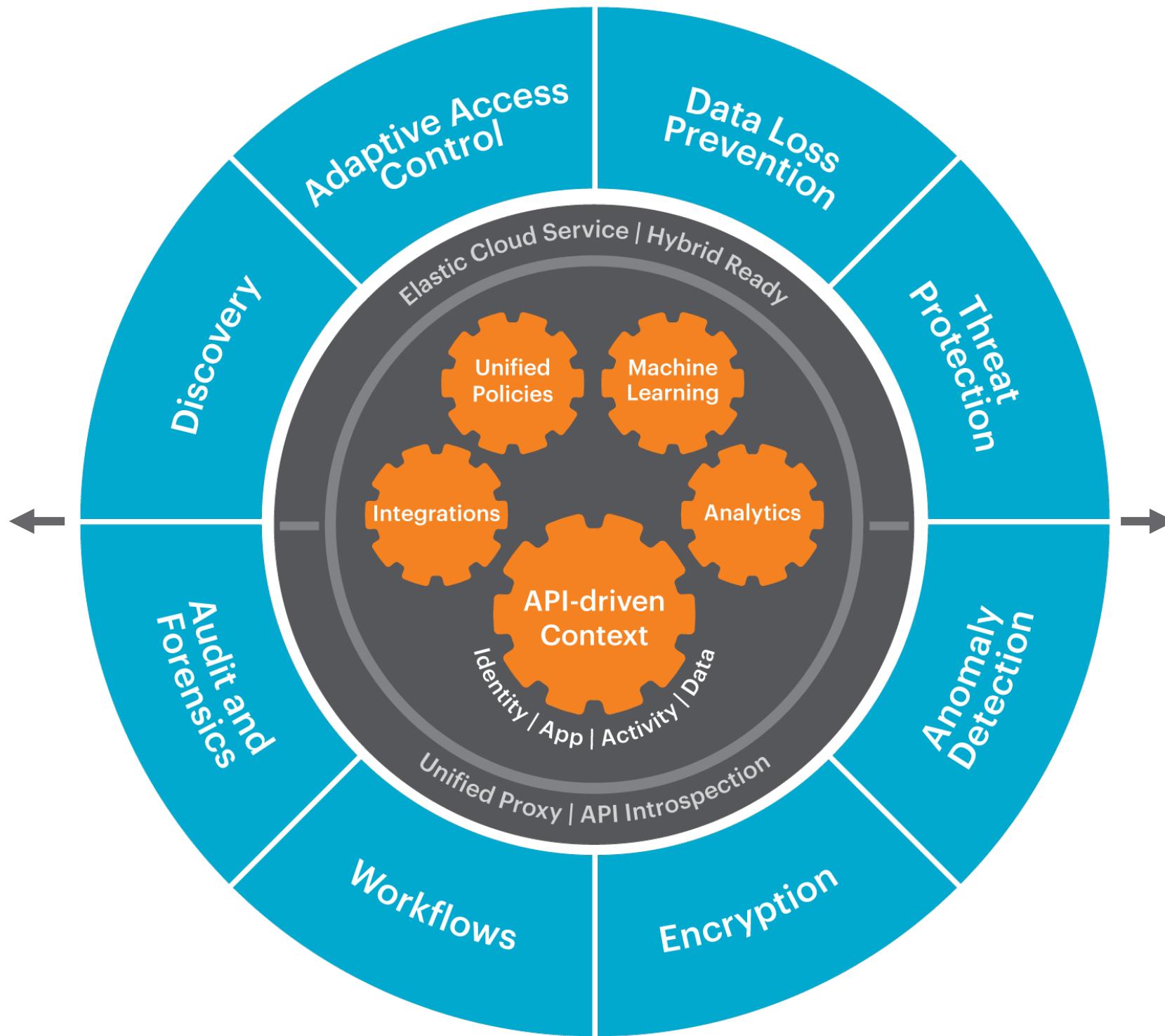
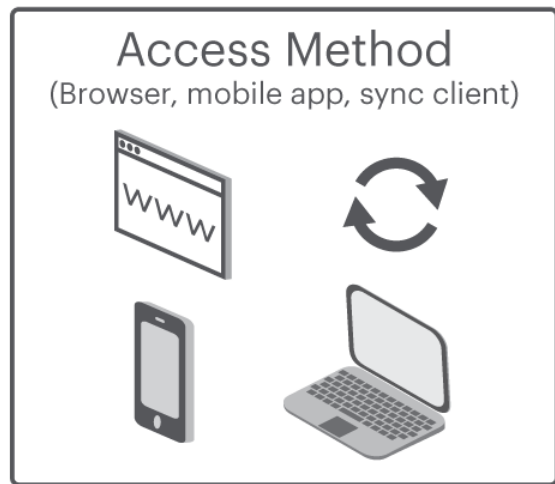
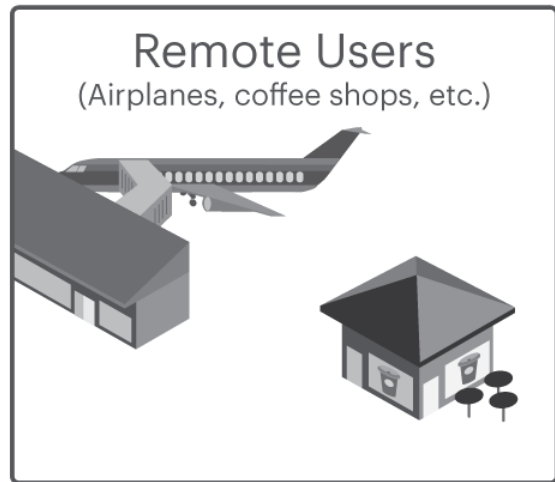
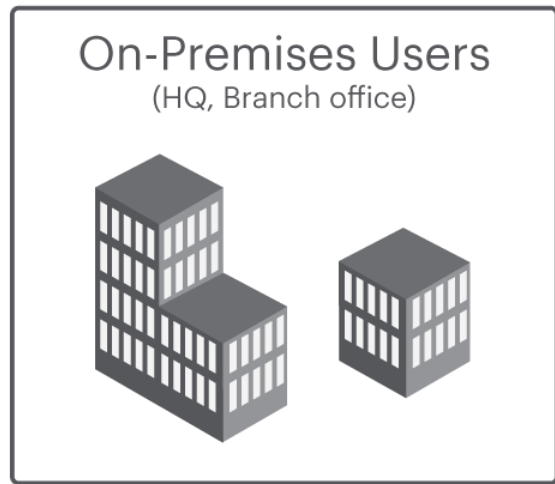
Govern and secure
all apps

How?

Logs

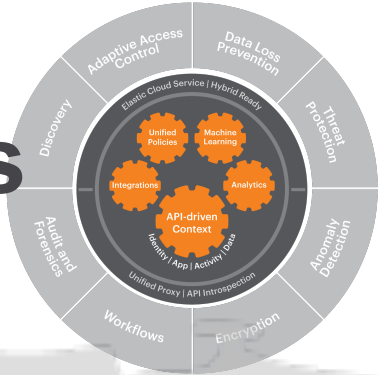
In-line and/or out-of-band

In-line

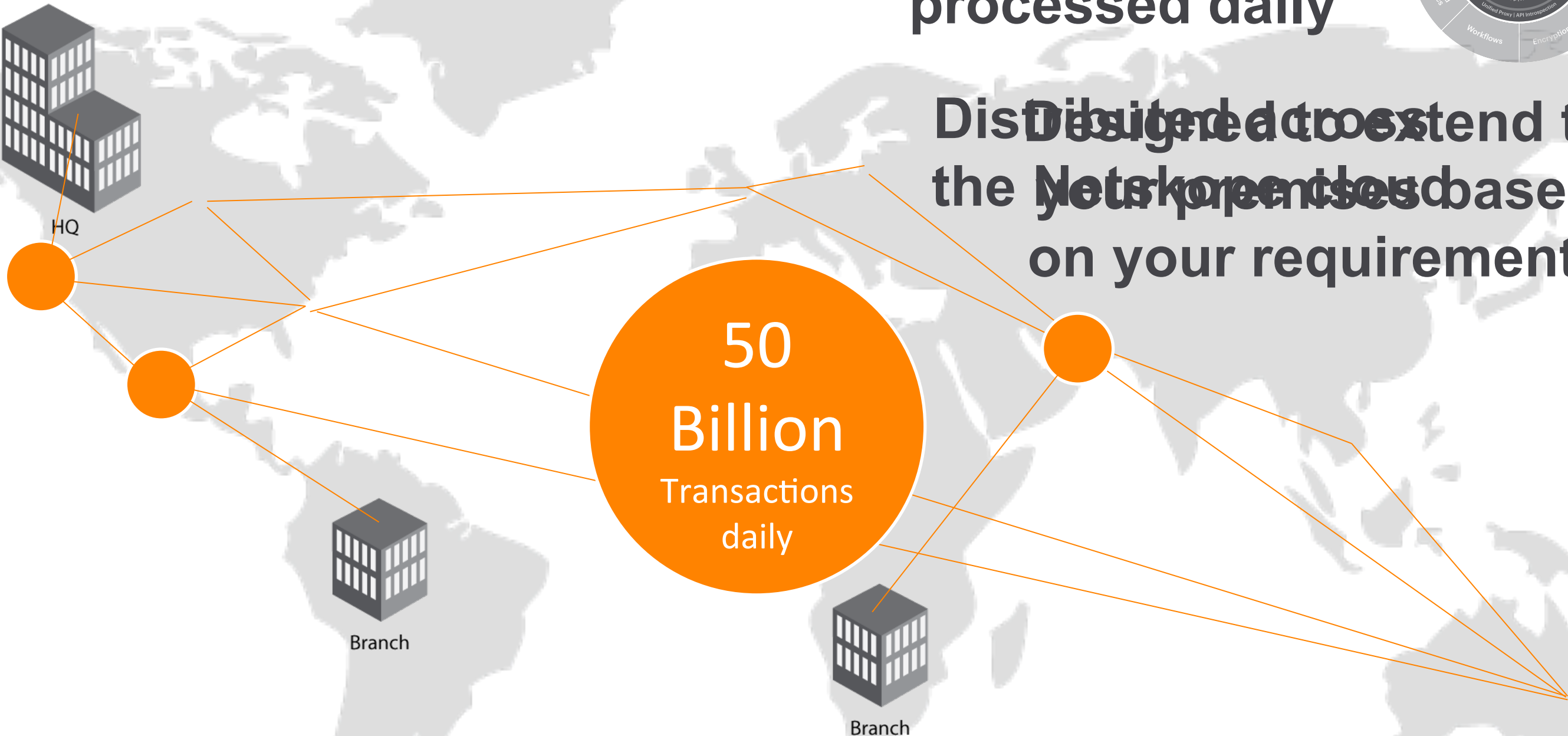


Elastic cloud services

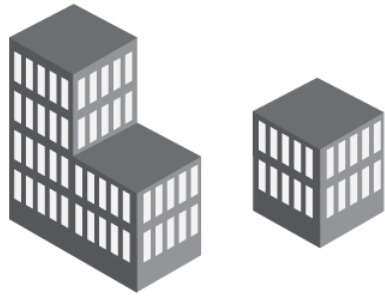
50 billion transactions
processed daily



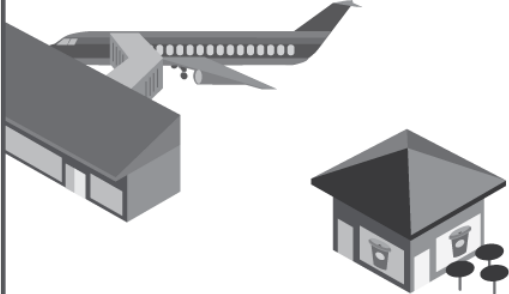
Designed to extend to
the Netskope cloud based
on your requirements



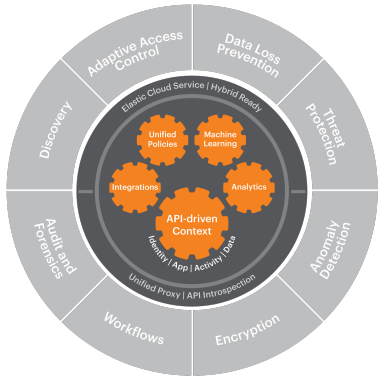
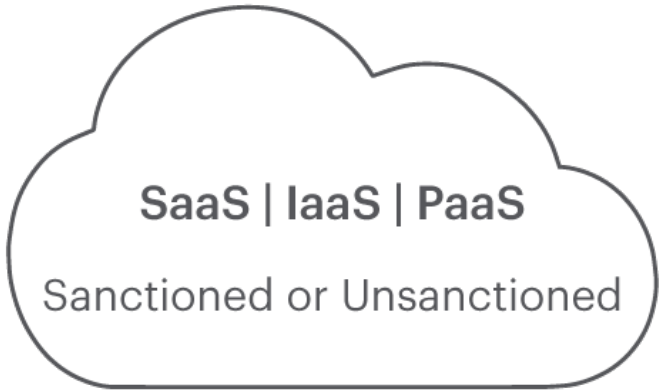
On-Premises Users
(HQ, Branch office)



Remote Users
(Airplanes, coffee shops, etc.)



























Access Method
(Browser, mobile app, sync client)



Unified proxy



	Access method	Discover	Govern usage	Secure data	Protect against threats	
 Logs		 				NEAR REAL-TIME
 API introspection						
 Reverse proxy						REAL-TIME
 Forward proxy		 	 	 	 	



Browser, remote, mobile and desktop apps, sync clients



Browser and remote



Browser

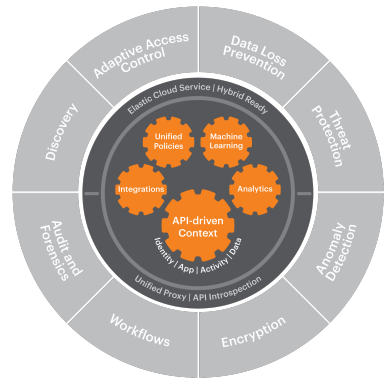


Sanctioned

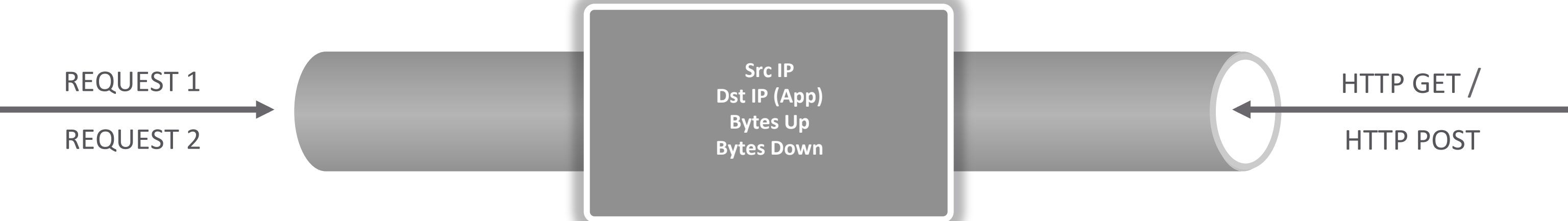


Unsanctioned

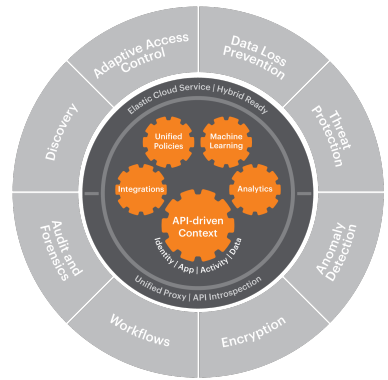
Core Platform



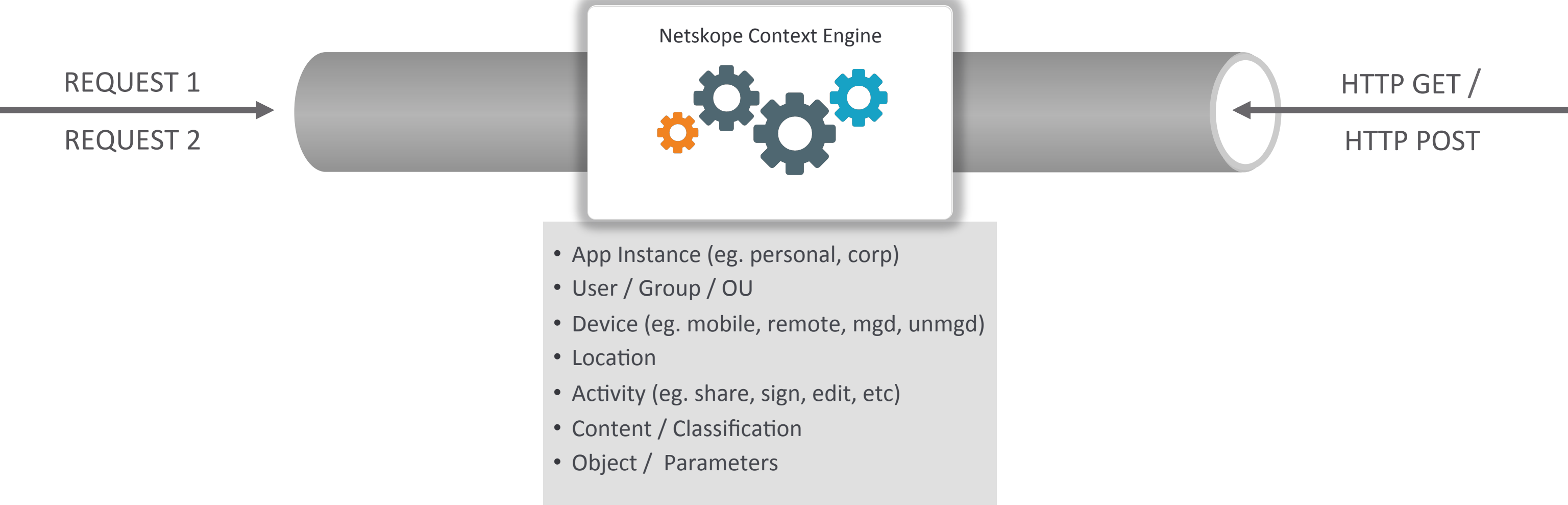
How legacy systems see traffic



Core Platform

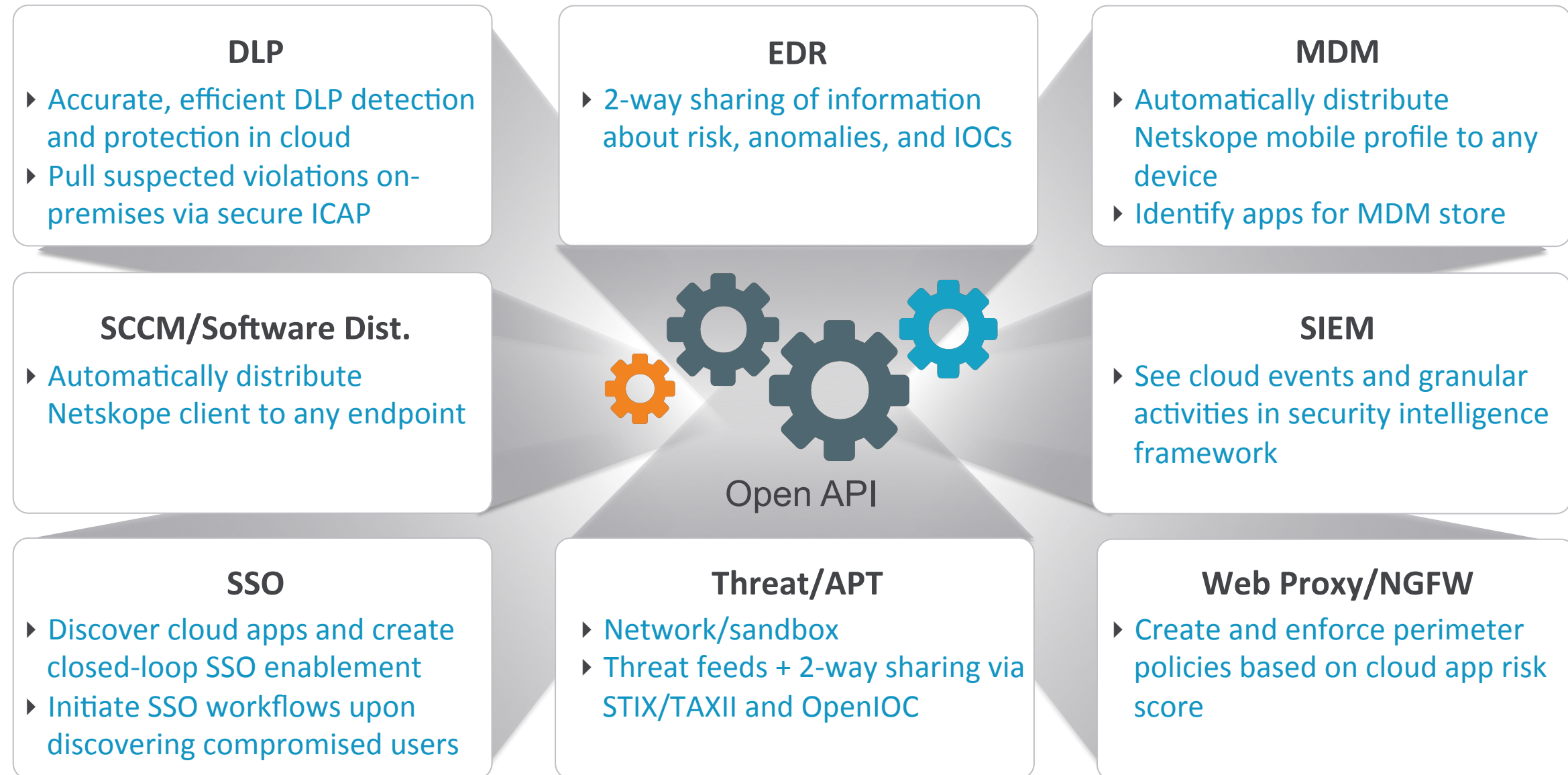
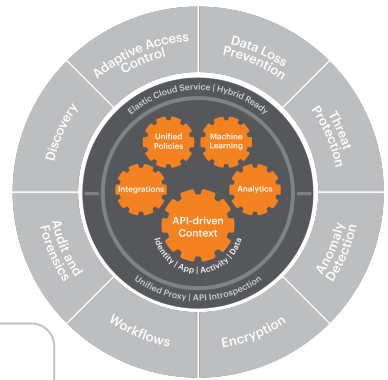


How Netskope see traffic



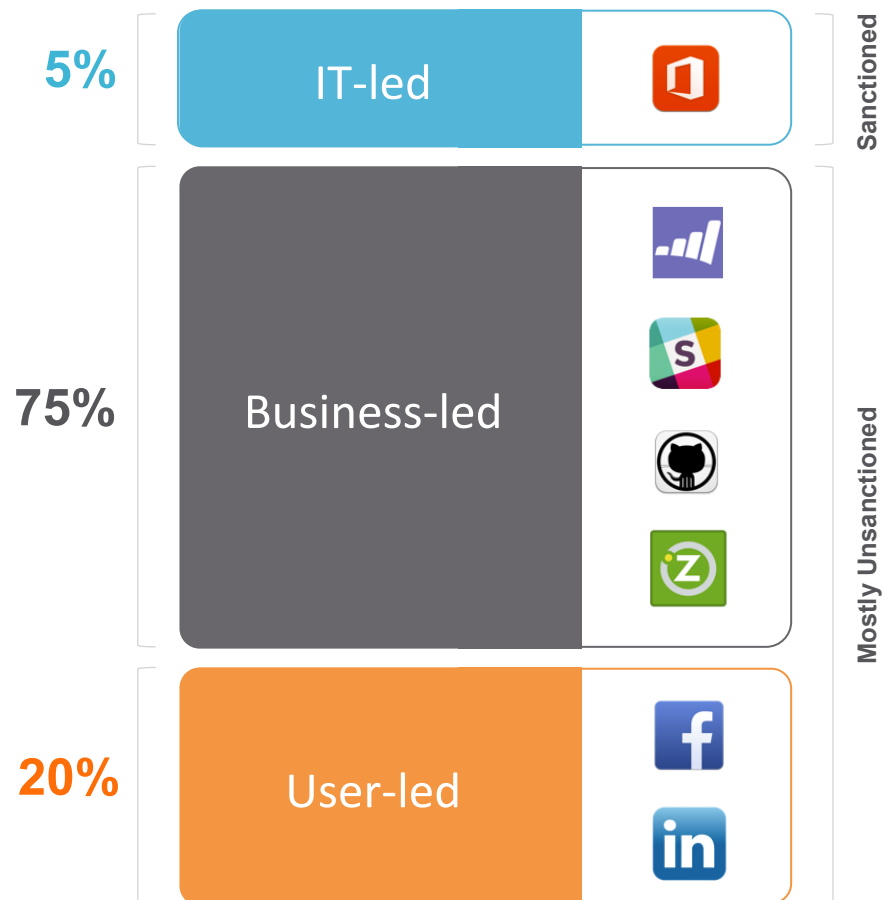
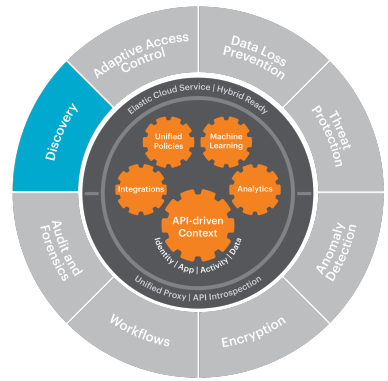
Security Ecosystem Integrations

Purpose-built, two-way integrations



Discovery

Find all cloud usage and quantify risk



- Find all apps in use and see who is using them
- Understand inherent and activity-based risk
- Automate your vendor assurance process

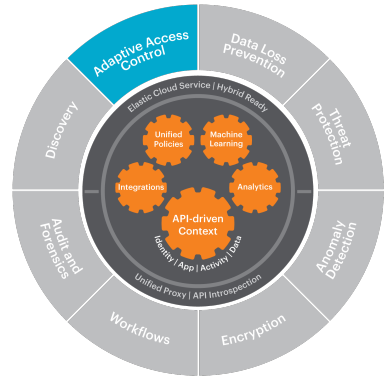
Netskope Cloud Confidence Index™

Adapted from CSA's Cloud Controls Matrix

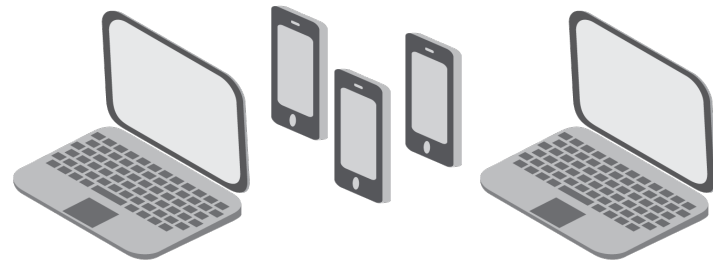
- ▶ Certifications and Standards
- ▶ Data Protection
- ▶ Access Control
- ▶ Auditability
- ▶ DR and Business Continuity
- ▶ Legal and Privacy
- ▶ Vulnerabilities and Exploits

Adaptive Access Control

Granular, post-authorization, control of apps

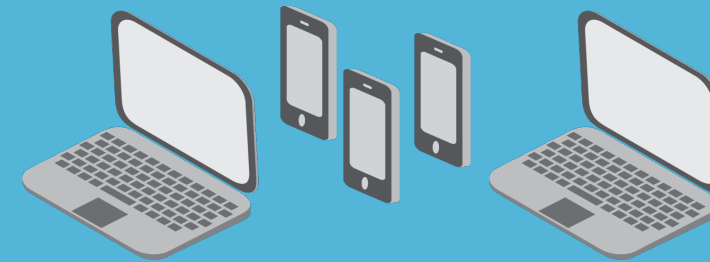


Example: Granular policies for managed or unmanaged devices



Unmanaged Device

- Block browser-based and/or mobile access from any unmanaged device
- Allow contractors or partners to view content, but block downloading

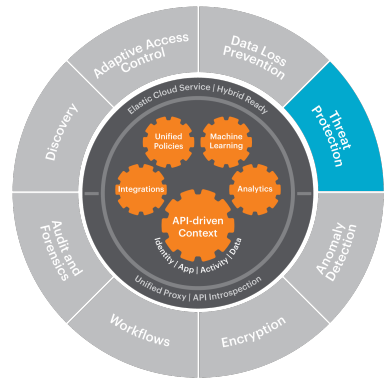


Managed Device

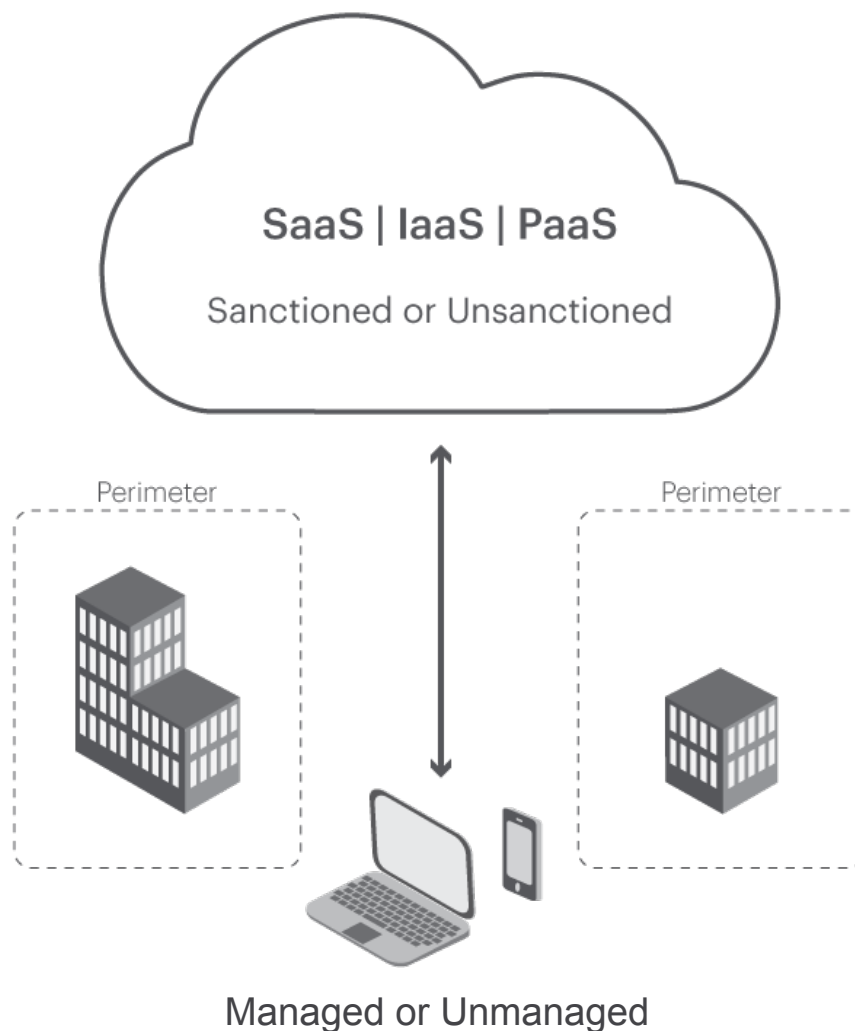
- Allow employees to view sensitive content on a managed device, but block downloading
- Quarantine and tombstone files suspected to be malicious

Threat Protection

Comprehensive threat protection for cloud services



See “direct to cloud” traffic



Netskope Context Engine

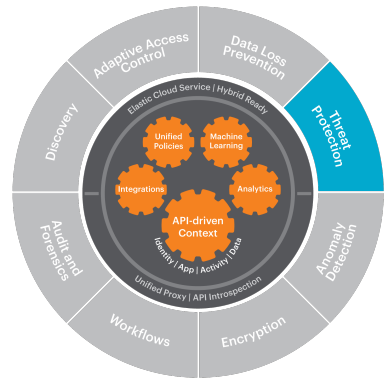


Netskope uses context to find indicators of compromise:

- Unauthorized encryption
- File entropy
- Abnormal volume of changes
- Etc.

Threat Protection

Comprehensive threat protection for cloud services



Network Intelligence

- ▶ 40+ threat feeds
- ▶ Proprietary intelligence curated by dedicated threat researchers

Anomaly Detection

- ▶ User & entity behavior analytics
- ▶ Compromised credentials

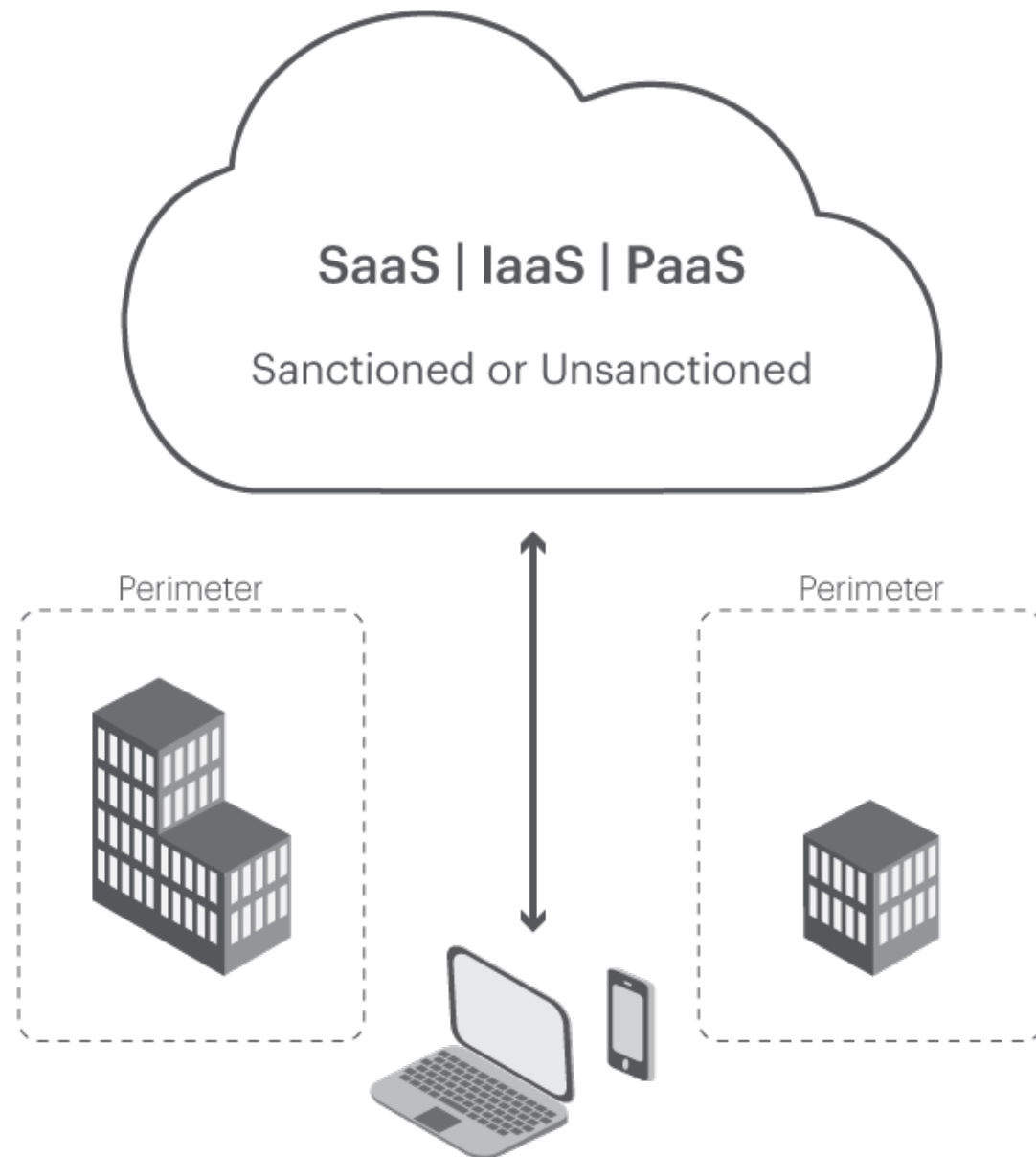
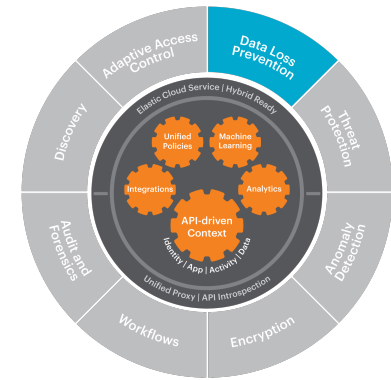
Anti-malware

- ▶ Multi-engine powered detection
- ▶ Flexible, policy based

← Machine Learning: Both heuristics and rules-based →

Cloud Data Loss Prevention

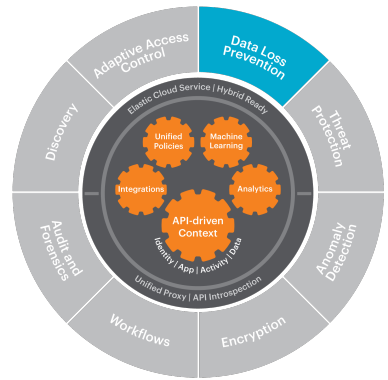
Prevent sensitive data leakage with accuracy and precision



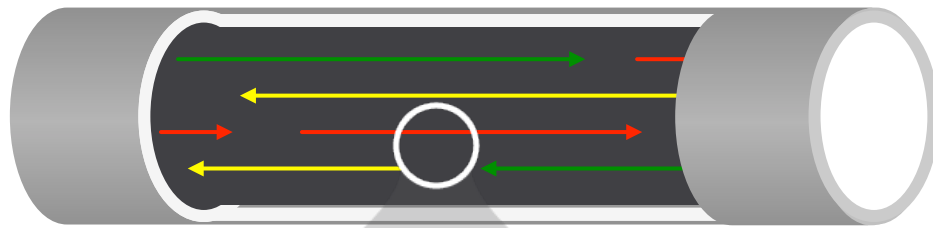
Since more than 50% of cloud traffic occurs beyond the corporate network, existing, on-premises DLP solutions are unable to inspect that content

Cloud Data Loss Prevention

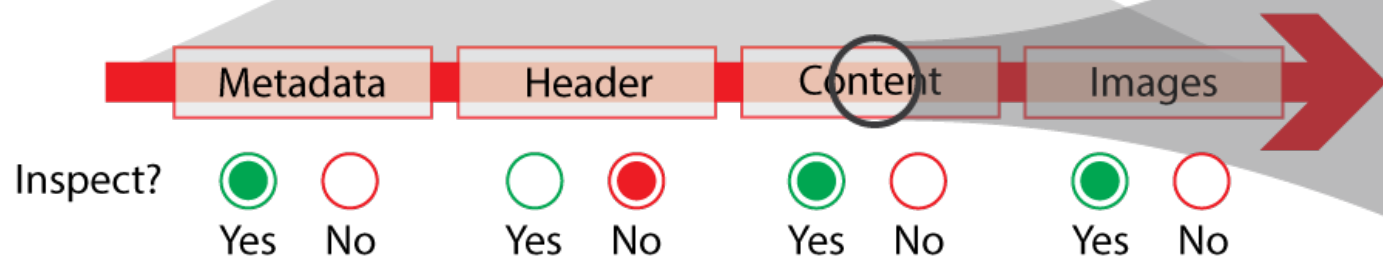
Prevent sensitive data leakage with accuracy and precision



Understanding transactions (decoded APIs) provides context so you can inspect the right traffic



Go deeper into each transaction to inspect content at a granular level



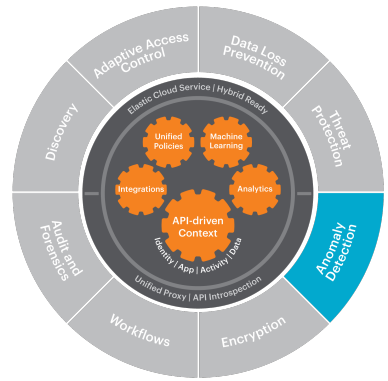
Inspect the right content

Use Best-in-class DLP to pinpoint sensitive information and reduce false positives

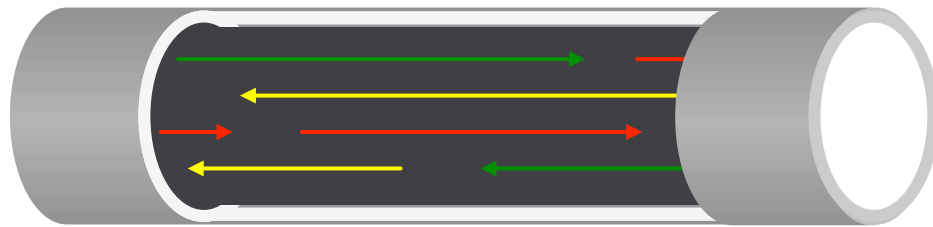
- Exact match
- Fingerprinting
- Proximity
- Boolean expressions
- Global data identifiers
- Natural language processing
- Custom keyword dictionaries

Anomaly Detection

Identify unusual data movement and user activity



Netskope Context Engine



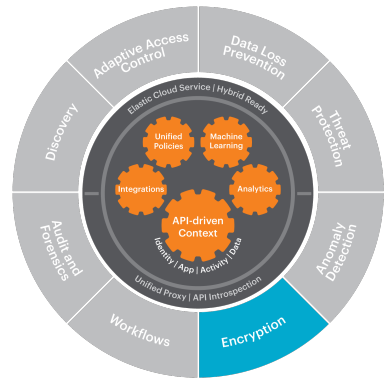
Netskope uses context to see anomalous behavior based on:

- Activities
- Geo
- User behavior
- App history (i.e., abnormal file movement)
- Etc.

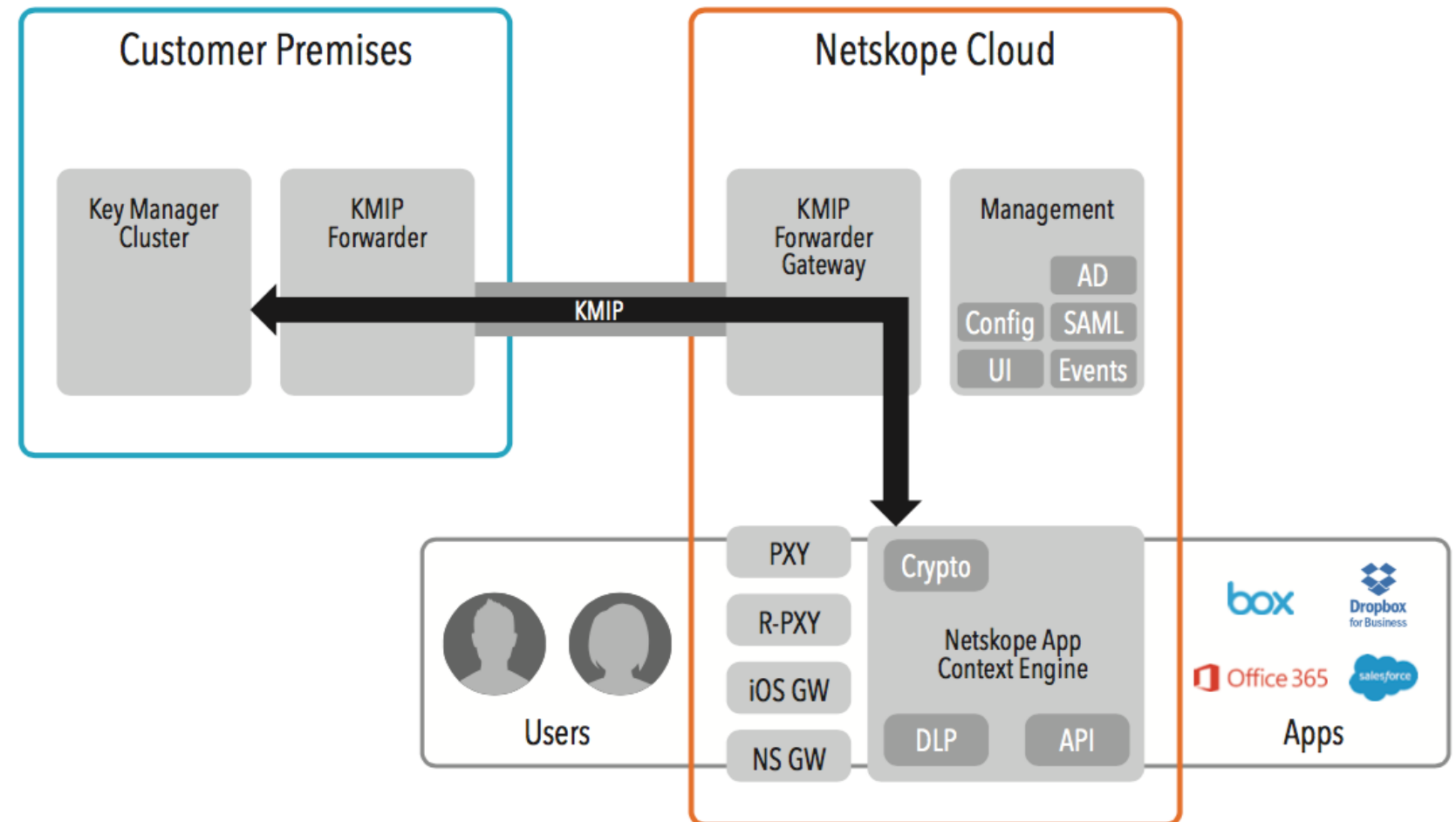
Go beyond coarse-grained details

- Allow security teams to see more than just anomalous access
- Get as detailed as seeing sensitive data moving from sanctioned to unsanctioned apps

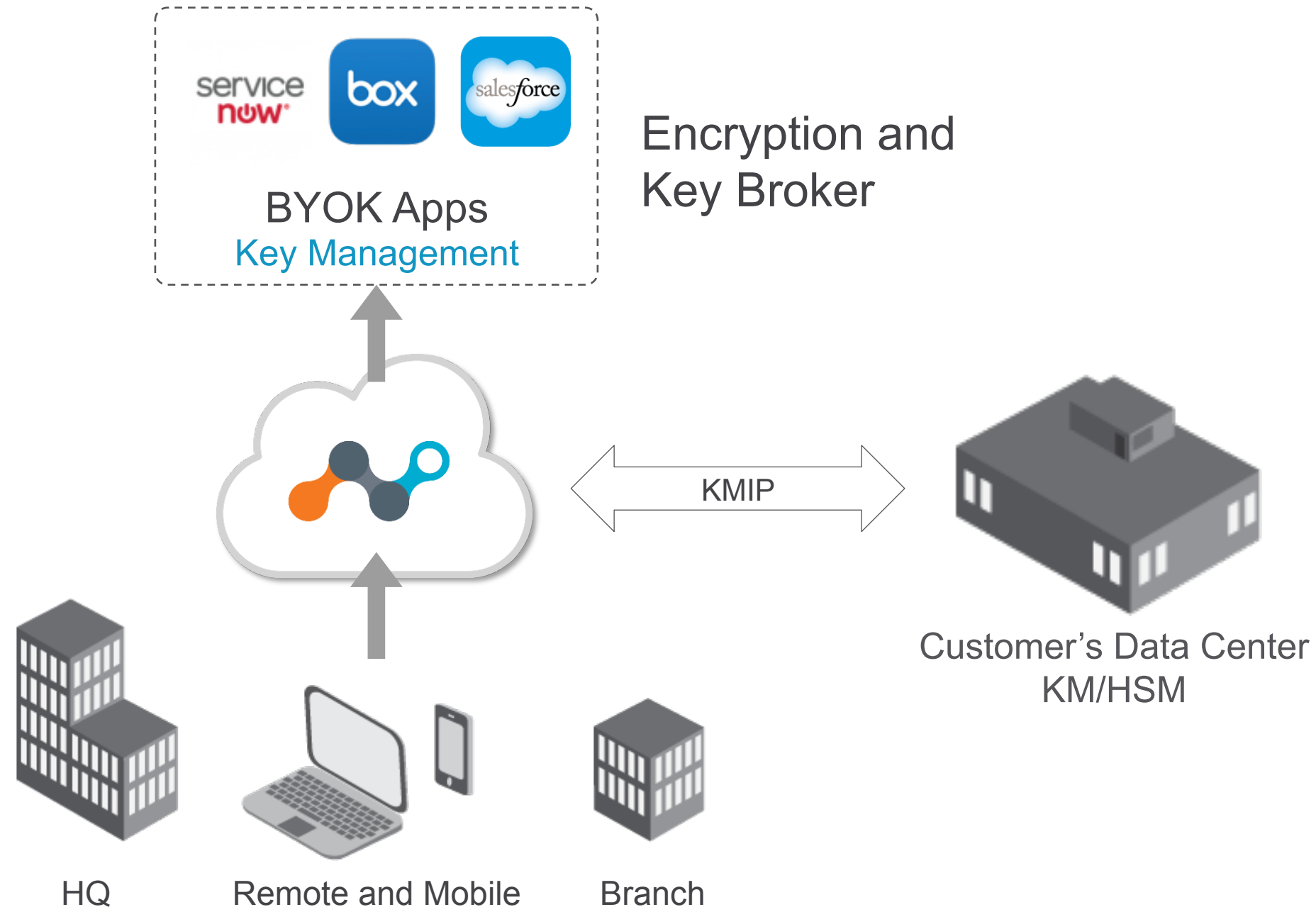
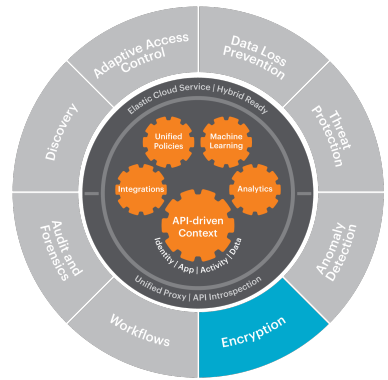
Unstructured Data Encryption



- Strong AES 256-bit encryption while you retain full control of the keys
- Supports integration with on-premises, KMIP-compliant key management server cluster
- Netskope encryption can also be deployed as a cloud-based, fault-tolerant FIPS 140-2 Level 3 key management with HSM

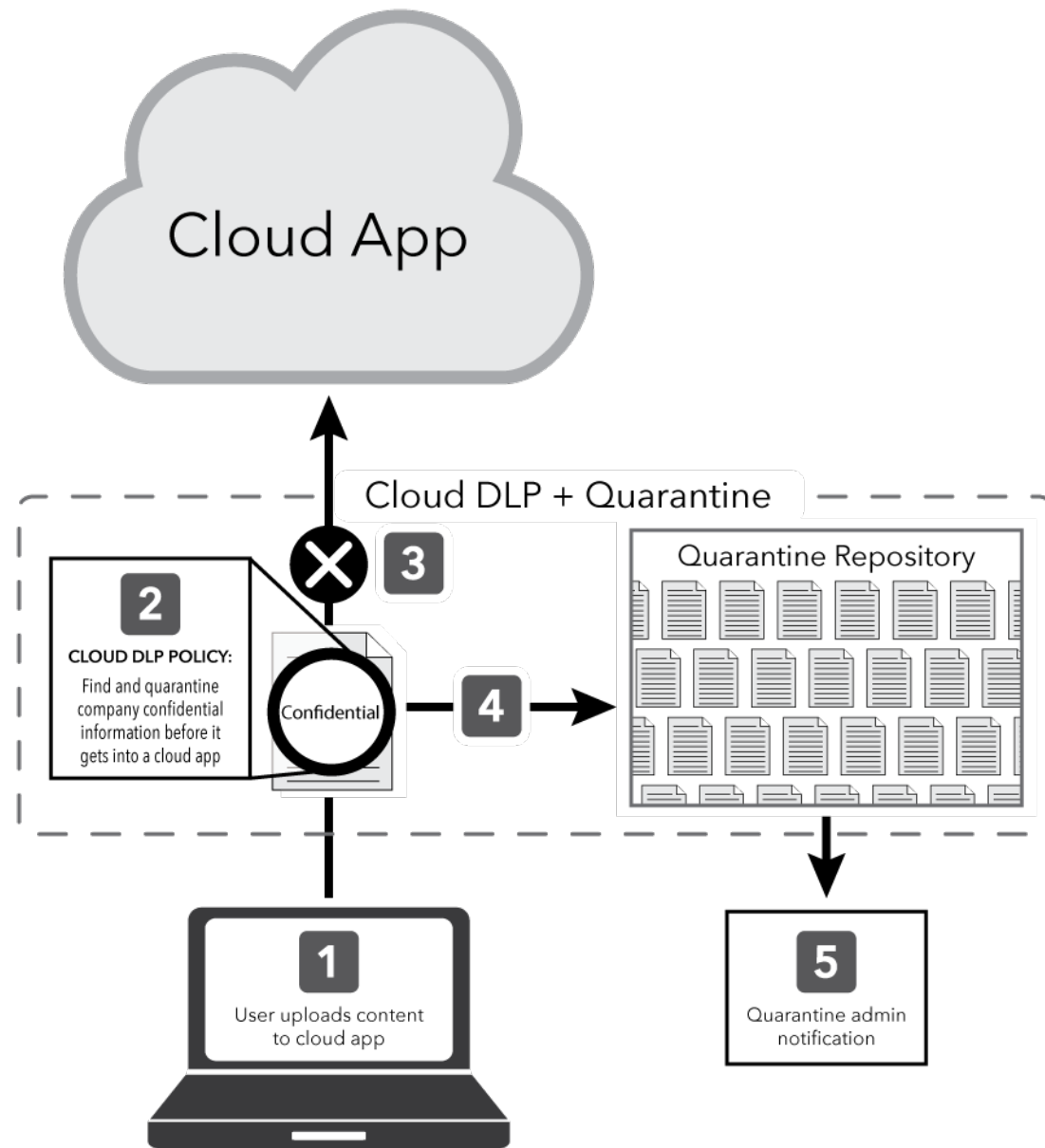
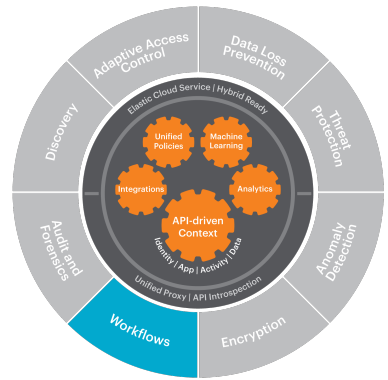


Structured Data Encryption



- Unified Data Governance across growing list of providers offering BYOK
- Customer, not Netskope, to own the keys -> KMIP!

Workflows

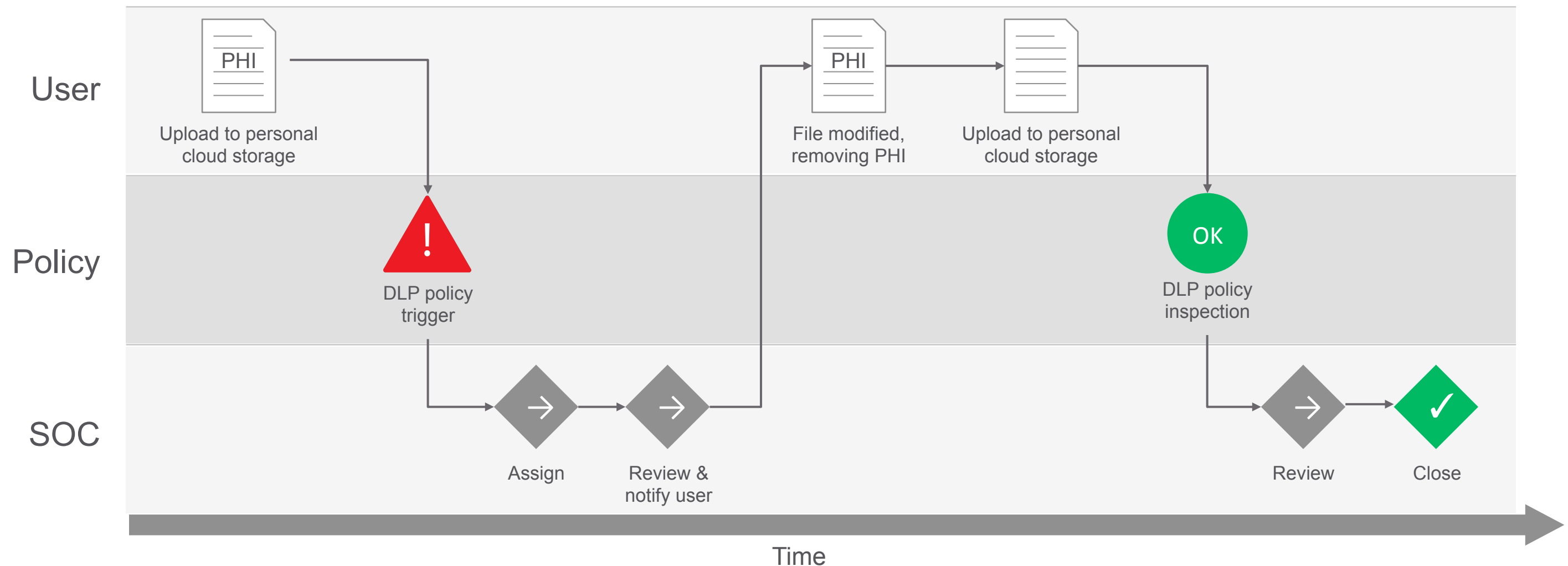
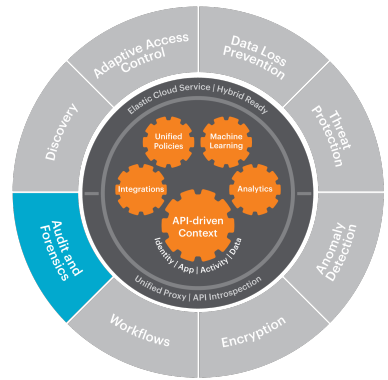


Key Use Cases

- Automated, customizable coaching messages to educate users and drive compliant behavior
- Integrated quarantine and legal hold workflows support security and legal review processes

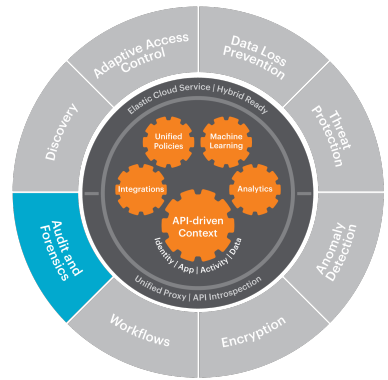
Audit and Forensics

Real-time access to rich cloud usage data



Audit and Forensics

Real-time access to rich cloud usage data



FORENSICS

INCIDENT DETAIL

HISTORY

06/10/16 02:46 AM (Latest) Introspection

Preview ⓘ

Number	EXPJohn	Smith	4111-1111-1111-1111	2/4
Number	EXPJane	Smith	4111-1111-1111-1111	2/4
Number	EXPJohn	Smith	4111-1111-1111-1111	2/4
Number	EXPJane	Smith	4111-1111-1111-1111	2/4

FORENSICS

INCIDENT DETAIL

HISTORY

INCIDENT

OBJECT

APPLICATION

Incident ID: ⓘ 781012343786336

Parent Incident ID: 781012343786336

Timestamp: 06/10/16 02:46 AM (Latest)

Type: Introspection

Activity: Introspection Scan

User: admin@nammazone.com

DLP Profile: DLP-PCI

DLP Policy: Alert on PCI violations in Google [

Violations: 200

Access Method: API Connector

Connection Id: 721637216950934016

Object ID: 0B3aTkk0E8Yf2VDFwbzhtdjFsRl

Object Name: ⓘ inci_1063586828305808_conten

Object Type: File

File Type: text/plain

File Size: 8.62 KB

Forensic File Size: 8.62 KB

File Owner: admin@nammazone.com

Exposure: Private

MD5: caa24f9b078f12178de96ba548c

Application: Google Drive

Instance ID: nammazone.com

App Category: Cloud Storage

URL: doc-00-8o-docs.googleuserconter

CCL: high

Activity: Introspection Scan

AppSession ID: 721637328177690016

USER

SOURCE

DESTINATION

User: admin@nammazone.com

Device: other

OS: unknown

Location: unknown

Timezone: unknown

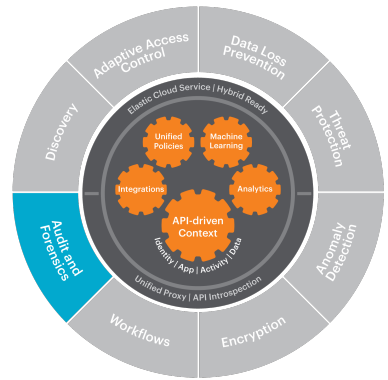
IP: 216.58.194.161

Location: Mountain View

Region: California

Audit and Forensics

Real-time access to rich cloud usage data



FORENSICS INCIDENT DETAIL HISTORY

Show Events: ☒ Intropection ☒ Inline ☒ Activity Feed ☒ Version Log ☒ Incident Audit

Timestamp	Type	User	Activity	DLP Profile	Violations	Action	Go To
06/10/16 11:22 AM	Incident Audit	ddorosin@netskope....	Status : New → In Pr...				
06/10/16 11:22 AM	Incident Audit	ddorosin@netskope....	Assignee : None → d...				
06/10/16 11:22 AM	Incident Audit	ddorosin@netskope....	Status : New → In Pr...				
06/10/16 02:46 AM	Activity Feed	admin@nammazone....	Intropection Scan				
06/10/16 02:46 AM	Activity Feed	admin@nammazone....	Intropection Scan				
06/10/16 02:46 AM	Intropection	admin@nammazone....	Intropection Scan	DLP-PCI			
06/10/16 02:43 AM	Version Log	admin@nammazone....	0B3aTkk0E8Yf2aDV...				

Complete incident history:

- Policy violations (including re-scans)
- Incident assignment and status updates
- Associated user activities

Forensic Incident ...



Thank you!



Walmart operates a chain of hypermarkets, discount department stores and grocery stores. They are the world's largest company by revenue, ranks #1 on the Fortune 500, and is the world's largest private employer.

Challenges:

- ▶ Need to safely enable sanctioned apps, including Box, Microsoft Office 365, and Slack
- ▶ Need to find and protect PCI and PII and manage incidents

Solution:

- ▶ Netskope Introspection for all apps
- ▶ Netskope Threat Protection
- ▶ Netskope Cloud DLP
- ▶ Netskope Professional Services
- ▶ Netskope Advanced Discovery

Benefits:

- ▶ Safely enable Slack, Microsoft Office 365, Box, and others
- ▶ Protect PCI and PII and manage incidents
- ▶ Monitor external collaborators in cloud services
- ▶ Detect and remediate malware in sanctioned apps
- ▶ Find and understand cloud apps in use

Williams-Sonoma is a multi-channel specialty retailer of high quality products for the home. It is one of the largest e-commerce retailers in the USA with some of the best known brands in home furnishings.

Challenges:

- ▶ Understand cloud apps in use and assess risk
- ▶ Need to report on app risk to business unit executives

Solution:

- ▶ Netskope N5000 Secure Cloud Appliance
- ▶ Netskope Advanced Discovery

Benefits:

- ▶ Greater visibility and risk assessment of cloud apps in use
- ▶ Provide reports on risky app usage for compliance



Stearns Holdings, LLC, is the parent company of Stearns Lending, LLC, a leading provider of mortgage lending services in the wholesale, retail, correspondent, and strategic alliance sectors throughout the USA.

Challenges:

- ▶ Prevent data leakage into unsanctioned Box instances
- ▶ Allow users access to broader set of apps while controlling risky activities
- ▶ Prevent spread of malware from unsanctioned apps to sanctioned apps

Solution:

- ▶ Netskope Active Platform
- ▶ Netskope Cloud DLP
- ▶ Netskope Encryption
- ▶ Netskope Threat Protection
- ▶ Netskope Introspection for Office 365

Benefits:

- ▶ Differentiate between Box instances and apply granular controls
- ▶ Allow unsanctioned apps, but control risky activities
- ▶ Understand and control user activities and data in Office 365
- ▶ Inline inspection of content for malware



The Charles Schwab Corporation is an American brokerage and banking company based in San Francisco, CA. It operates in four major divisions: investing, wealth management, banking, and trading.

Challenges:

- ▶ Understand risk profile of sanctioned and unsanctioned apps
- ▶ Control data movement in Salesforce.com

Solution:

- ▶ Netskope for Salesforce.com
- ▶ Netskope Advanced Discovery

Benefits:

- ▶ Monitor for inappropriate sensitive data being uploaded to Salesforce.com
- ▶ Control access by users with compromised credentials to Salesforce.com
- ▶ Reduce app redundancy

Hospital Corporation of America (HCA) is an American for-profit operator of healthcare facilities. One of the nation's leading providers of healthcare services with 250 hospitals in the USA and UK.

Challenges:

- ▶ Shadow IT sprawl
- ▶ Unmanaged access of Office 365 and Salesforce presented security and compliance risks
- ▶ No visibility into data sharing from unsanctioned services
- ▶ Lack of protection from cloud threats

Solution:

- ▶ API Introspection for all apps Netskope covers
- ▶ Netskope Cloud DLP
- ▶ Netskope Appliance
- ▶ Netskope Threat Protection

Benefits:

- ▶ Safely enable Microsoft Office 365 and Salesforce
- ▶ Visibility and control of shadow IT
- ▶ Protect sensitive data from loss
- ▶ Detect and remediate malware found in cloud



Lilly is a global healthcare leader that unites caring with discovery to make life better for people around the world. Founded more than a century, Lilly employs 41,000 people and markets products in 120 countries.

Challenges:

- ▶ Control shadow IT without having to do it app-by-app
- ▶ Rolling out Office 365 and Box, but needs to ensure appropriate treatment of sensitive data

Solution:

- ▶ Netskope Active Platform
- ▶ Netskope Cloud DLP
- ▶ Netskope for Office 365
- ▶ Netskope for Box

Benefits:

- ▶ Safely enable Box and Microsoft Office 365
- ▶ Comply with regulations
- ▶ Protect sensitive data from loss
- ▶ Visibility and control of shadow IT



Accell Group focuses internationally on the mid-range and higher segments of the market for bicycles, and bicycle parts and accessories. Accell and its subsidiaries employ 3,000 people in 18 countries.

Challenges:

- ▶ Need to comply with international data protection regulations
- ▶ Need visibility and control of all apps in use
- ▶ Need to protect sensitive data from loss

Solution:

- ▶ Netskope Active Platform
- ▶ Netskope Professional Services

Benefits:

- ▶ Safely enable Microsoft Office 365
- ▶ Comply with regulations, including the EU GDPR
- ▶ Protect intellectual property from loss
- ▶ Visibility and control of shadow IT



iRobot was founded in 1990 by three MIT graduates who designed war robots. In addition to robots for police and military, they build a range of autonomous home cleaning solutions such as Roomba.

Challenges:

- ▶ Need to protect intellectual property in cloud services

Solution:

- ▶ Netskope for Microsoft Office 365
- ▶ Netskope Threat Protection for Microsoft Office 365

Benefits:

- ▶ Visibility into and control over data exfiltration or unauthorized sharing of IP
- ▶ Malware detection and remediation in Microsoft Office 365



AA is a UK-based company that offers roadside assistance service. Company segments include roadside assistance, insurance services, and driving services. It is the UK's largest motoring organization.

Challenges:

- ▶ Govern access from unmanaged devices for remote, mobile work force
- ▶ Protect sensitive data from loss
- ▶ Safe enablement of Microsoft Office 365
- ▶ Visibility and control over Shadow IT

Solution:

- ▶ Netskope Active Platform
- ▶ Netskope Cloud DLP

Benefits:

- ▶ Granular access policies for mobile workforce on unmanaged devices
- ▶ Limit Microsoft Exchange email to “view only” from mobile devices
- ▶ DLP for all apps, including unsanctioned cloud storage apps, to prevent sensitive data from loss

Aankomende Congressen

BEHAVIORAL RISK

2017

C O N G R E S S



28 november 2017 te Baarn

RISKCONGRES

PublicValues

2018



5 april 2018 Den Haag

Hartelijk dank voor uw komst

en tot ziens bij ons

Risk & Compliance Jaarcongres 2018

RISK & COMPLIANCE

J A A R C O N G R E S

2017