netskope

20 Examples of Smart Cloud Security

The way people work has changed. Driven by the increasing use of cloud services and mobile devices, people now expect to be able to work at any time, from any place, and on any device. These changes are dramatically altering the network and security infrastructure in many organizations. Rather than staying with a legacy, hub-and-spoke network architecture, with offices interconnected over costly, dedicated links and remote users accessing centralized resources over VPN, more organizations are moving to a direct-to-web and direct-to-cloud model.

Furthermore, the underlying nature of the cloud and web is also changing, with static websites giving way to dynamically-generated and personalized web services as well as an ever-growing set of cloud services housing an organization’s critical applications and data. To keep pace with these changes, a fundamentally different approach to security is needed—an approach that allows organizations to address these changes head on with a unified cloud and web security platform that was designed from the start for today’s modern, distributed enterprise.

At Netskope, we call this **smart cloud security**. Smart cloud security is powered by four key capabilities:

Netskope Cloud XD

The brain behind Netskope, Cloud XD understands all inputs in extreme definition (XD) and performs big data analytics to eliminate blind spots and make policy enforcement simple across all cloud and web.

360º Data Protection

360º data protection uses data inspection techniques such as exact match, fingerprinting, and similarity hashes to protect your most valuable data assets. Through Cloud XD you only inspect what you have to — this means fewer false positives.

Advanced, Comprehensive Threat Protection

Detection engines combine real-time (e.g., pre-filters, AV, threat intelligence) and deep (e.g., cloud sandbox, heuristic analysis, ransomware and anomaly detection) protection to protect against the most sophisticated threats.

Unified, Cloud-native Platform

Provided in the industry's best user experience, Netskope was built in the cloud from the very beginning. Get best-of-breed CASB for SaaS and IaaS along with web security, all in one interface that hasn't been cobled together from several old platforms.

Smart cloud security provides critical capabilities such as governing access and activities in sanctioned and unsanctioned cloud services, securing sensitive data and preventing its loss, and protecting against internal and external threats.

GOVERN USAGE

SECURE DATA

PROTECT AGAINST THREATS

1 Prevent data exfiltration to any cloud service or website

For example, prevent the download of confidential content from a corporate-IT-led service such as Salesforce, Box, or even AWS S3 to a personal Dropbox or other file sharing service or website

Functional Requirements

See and control usage in both IT-led and business-led cloud services and any website

Detect sensitive data, e.g., "confidential"

Identify all unique content in motion and track its movement

Be aware of context, e.g., activities such as "upload" and "download"

Correlate users' identities (e.g., bob@netskope.com = bob123@yahoo.com = bobaran@gmail.com)

Differentiate between internal and external domains

Know corporate vs. personal accounts

Recognize and enforce differing policies between service instances, e.g., corporate and personal

Decrypt SSL and decode the unpublished API to understand the transaction

Surface data exfiltration activities in a user interface that is easy to understand

Deployment Requirements

Forward proxy (monitor and control)

2 Enforce different policies for personal and corporate instances of the same cloud service

For example, prevent the upload of regulated information (such as that beholden to FISMA, NERC, or PCI) to any Dropbox EXCEPT for the corporate- IT-led instance of Dropbox

Functional Requirements

Detect sensitive data, e.g., data beholden to FISMA, NERC, or PCI

Be aware of context, e.g., activities such as "upload" and "download"

Know corporate vs. personal accounts

Recognize and enforce differing policies between service instances, e.g., corporate and personal

See and control usage in both IT-led and business-led services

Decrypt SSL and decode the unpublished API to understand the transaction

Deployment Requirements

Forward proxy (monitor and control)

3 Quarantine malware in IT-led cloud services and en route to/from any cloud service and website

For example, detect, quarantine, and block malware being downloaded from and cloud service or website

Functional Requirements

Scan IT-led cloud services and quarantine malware

Inspect, detect, block, and remediate malware en route to/from all cloud services and websites

Decrypt SSL and decode the unpublished API to understand the transaction

Deployment Requirements

API (IT-led only)

Forward proxy

Reverse proxy (IT-led only, browser only)

4 Govern access to office 365 and other cloud services and websites by device ownership class

For example, offer web-based email access only to a BYOD device but full suite access to a corporate one

Functional Requirements

Understand different authentication protocols and federated identity across Office 365 and other cloud services

Enforce access and activity policies based on device attributes, including classification of “managed” and “unmanaged”

Decrypt SSL and decode the unpublished API to understand the transaction (for forward proxy)

Deployment Requirements

Forward proxy

Reverse proxy (IT-led only, browser only)

5 Monitor sensitive data in Amazon S3 buckets

For example, alert when PCI data is discovered in AWS S3 buckets

Functional Requirements

Cloud DLP that can scan S3 buckets

Specify all or individual S3 buckets

Incident management workflow

Deployment Requirements

API (IT-led only)

6 Monitor privileged accounts and prevent unauthorized activity in IaaS instances

For example, disallow creation, edit, or delete of cloud instances, "buckets," or "clusters"

Functional Requirements

Be aware of context, e.g., activities such as "create" and "edit" and objects such as "instances" and "buckets"

Determine identity and control usage by user, group, and other enterprise directory attributes

See and control usage in both IT-led and business-led services

Decrypt SSL and decode the unpublished API to understand the transaction

Deployment Requirements

API (IT-led only)

Forward proxy

7 Enforce an activity- or data-level policy across categories of cloud and web services

For example, block the download of personally-identifiable information (PII) from ANY HR service if the user is outside of the HR team

Functional Requirements

Be aware of context, e.g., activities such as “upload” and “download”

Correlate users’ identities (e.g., bob@netskope.com = bob123@yahoo.com = bobaran@gmail.com)

See and control usage in IT-led and business led cloud services and any website

Integrate with enterprise directory to enforce policies at a group or organizational unit level

Decrypt SSL and decode the unpublished API to understand the transaction

Deployment Requirements

Forward proxy

8 Monitor or control users' activities within Collaboration or Social Media without blocking those services

For example, block any financial employee from posting "guarantee" or "recommend" alongside a stock ticker or company name on any Collaboration or Social Media service like Slack or Twitter to comply with FINRA and other regulations

Functional Requirements

Integrate CASB with directory services to focus policy on a specific group, e.g., Investment Banking

Be aware of context, e.g., activities such as "view," "post," and "create"

See and control usage in both IT-led and business-led services

Detect data violations using advanced DLP features including regular expressions, custom keyword dictionaries, and Boolean operators to focus on specific risky activities (e.g., for FINRA) or to set policies for a specific group (e.g., Finance)

Decrypt SSL and decode the unpublished API to understand the transaction

Deployment Requirements

Forward proxy (monitor and control)

9 Enforce conditional activity-level policies

For example, block the uploading of sensitive content by a corporate 'insider' to any cloud service with a risky rating or any website

Functional Requirements

Be aware of context, e.g., activities such as "share"

See and control usage in IT-led and business-led cloud services and any website

Differentiate between internal and external domains

Enforce "set-it-once" policies across categories of services

Detect and enforce policies by IP address, network location, or geolocation

Integrate with enterprise directory to enforce policies at a group or organizational unit level

Decrypt SSL and decode the unpublished API to understand the transaction

Deployment Requirements

Forward proxy

Reverse proxy (IT-led only, browser only)

10 Enforce layered policies that include a “base” and “exception” policy

For example, prevent the upload of confidential data to ANY Cloud Storage service except corporate IT-led Google Drive

Functional Requirements

Support for policies with “allow” and “block” actions

Support for category-level policies

Differentiate between instances of cloud services

Deployment Requirements

Forward proxy

Reverse proxy (IT-led only, browser only)

11 Apply encryption based on conditional factors

For example, apply strong encryption with enterprise key management to confidential intellectual property such as next-generation product designs

Functional Requirements

Be aware of context, e.g., activities such as "upload"

See and control usage in both IT-led and business-led services

Apply strong encryption to sensitive content with enterprise key management

Integrate with KMIP-compliant, on-premises key manager

Decrypt SSL and decode the unpublished API to understand the transaction

Deployment Requirements

Forward proxy

Reverse proxy (IT-led only, browser only)

12 Detect and alert on user login anomalies

For example, detect users logging into a cloud service from two different locations with the same credentials, indicating a potentially compromised account

Functional Requirements

Correlate users' identities (e.g., bob@netskope.com = bob123@yahoo.com = bobaran@gmail.com)

See usage in both IT-led and business-led services

Use machine learning to detect cloud behavior anomalies

Detect IP addresses, network location, or geo-location

Decrypt SSL and decode the unpublished API to understand the transaction

Deployment Requirements

API (IT-led only)

Reverse proxy (IT-led only, browser only)

Forward proxy

13 Detect anomalies such as excessive downloads, uploads, or sharing within both IT-led and business-led services

For example, detect excessive download of sensitive customer data from Salesforce

Functional Requirements

Be aware of context, e.g., activities such as “download” and “share”

See and control usage in both IT-led and business-led services

Use machine learning and rules to detect anomalies that could signal risky behavior, non-compliance, data exposure, or even malware

Decrypt SSL and decode the unpublished API to understand the transaction

Deployment Requirements

API (IT-led only)

Forward proxy

Reverse proxy (IT-led only, browser only)

14 Monitor or control advanced or cross-service activities in real time

For example, “Edit in Box,” “Save to Dropbox” from Slack, or enforce which services can integrate and share data with your G Suite

Functional Requirements

Be aware of context, e.g., activities such as “edit,” “sync,” and “save”

See and control usage in both IT-led and business-led (including ecosystem) apps

Identify and control integration with ecosystem services

Decrypt SSL and decode the unpublished API to understand the transaction

Deployment Requirements

Forward proxy (monitor and control)

15 Find and protect sensitive data embedded in images

For example, find and stop patient data embedded in an x-ray image being uploaded to a personal cloud servicecloud service

Functional Requirements

Cloud DLP with OCR (Optical Character Recognition) capability

Ability to scan IT-led cloud services with OCR-supported cloud DLP

Ability to apply OCR to cloud traffic to and from business-led cloud services

Deployment Requirements

API (IT-led only)

Forward proxy

Reverse proxy (IT-led only, browser only)

16 Block and quarantine zero-day malware in the cloud and web

For example, detect and quarantine new strains of malware present in IT-led cloud services and block this type of malware enroute to and from all cloud services and websites

Functional Requirements

Support for cloud-based inspection with dynamic analysis using a cloud-based sandbox

Support for multiple threat intelligence mechanisms including external and internal

Support quarantine workflows that are malware-centric

Deployment Requirements

API (IT-led only)

Forward proxy

Reverse proxy (IT-led only, browser only)

17 Recover from cloud-based ransomware infections

For example, alert when a ransomware infection has taken place and provide a seamless workflow to recover from the infection

Functional Requirements

Use 70 different signals to identify unauthorized encryption

Integration with cloud storage apps like OneDrive to enable "roll-back" functionality

A streamlined UI to enable an intuitive workflow for rolling back infected content to pre-infected state

Deployment Requirements

API (IT-led only)

18 Prevent data infiltration involving new employees

For example, block new employees from uploading confidential data from their previous employer to their new company's IT-led cloud service

Functional Requirements

Integrate "new employee" policy with enterprise directory

Use custom keyword dictionary to delineate sensitive competitor documents

Decrypt SSL and decode the unpublished API to understand the transaction

Deployment Requirements

API (IT-led only)

Forward proxy

Reverse proxy (IT-led only, browser only)

19 Protect against password email abuse

For example, block passwords being sent via any webmail app

Functional Requirements

Cloud DLP with custom keyword dictionaries to incorporate any variation of keyword that may signal that a password is being shared

Cloud DLP support for business-led webmail accounts (hundreds)

Support for category-level policies with specific support for webmail

Decrypt SSL and decode the unpublished API to understand the transaction

Deployment Requirements

Forward proxy

Reverse proxy (IT-led only, browser only)

20 Monitor or control users' activities (even when they are accessing cloud services from a mobile or desktop app or sync client)

For any of the real-time use cases that require a forward proxy, support should be extended to mobile apps, desktop apps, and sync clients

Functional Requirements

Inspect and control cloud traffic even when it originates from a mobile or desktop app or sync client

See and control usage in both IT-led and business-led services

Enforce policy action such as block, coach, or justify in real time

Decrypt SSL and decode the unpublished API to understand the transaction (for forward proxy)

Deployment Requirements

Forward proxy (monitor and control)

GOVERN USAGE

Govern access to office 365 and other cloud services and websites by device ownership class

Monitor privileged accounts and prevent unauthorized activity in IaaS instances

Monitor or control users' activities within Collaboration or Social Media without blocking those services

Monitor or control advanced or cross-service activities in real time

Protect against password email abuse

Monitor or control users' activities even when they are accessing cloud services from a mobile or desktop app or sync client

SECURE DATA

Prevent data exfiltration to any cloud service or website

Enforce different policies for personal and corporate instances of the same cloud service

Monitor sensitive data in Amazon S3 buckets

Enforce an activity- or data-level policy across categories of cloud and web services

Enforce conditional activity-level policies

Enforce layered policies that include a "base" and "exception" policy

Apply encryption based on conditional factors

Find and protect sensitive data embedded in images

PROTECT AGAINST THREATS

Block or remediate malware in IT-led and en route to/from business-led cloud services

Detect and alert on user login anomalies

Detect anomalies such as excessive downloads, uploads, or sharing within both IT-led and business-led services

Block and quarantine zero-day malware in the cloud and web

Recover from cloud-based ransomware infections

Prevent data infiltration involving new employees

netskope