Symantec

Cloud Access Security Broker

Use Cases and Requirements

Whitepaper Series 01

Visibility

01 Identify on-prem and off-prem Shadow IT usage

Example View Shadow IT activity for users that may roam outside the corporate boundaries (e.g., firewall or SWG)

Requirements

- Analyze log files in virtually any format, including firewall, secure web gateway and endpoints, to uncover Shadow IT both on the corporate network as well as from off-network users
- Evaluate the security and compliance posture of both sanctioned apps and Shadow IT (i.e. PCI, HIPAA, GDPR, FISMA, PII, FERPA, and GLBA compliance).
- Customize risk rating of cloud apps based on customer-weighted security attributes and compliance certifications, and monitor overall company risk score
- Identify top users of risky cloud apps and resolve risk activity through coaching or intervention
- Compare apps with similar functionality side-by side and consolidate on the most secure option
- Generate comprehensive reports with executive summaries along with a list of discovered services and recommendations (e.g., overall corporate risk rating) for continuous monitoring

02 Automate Control of Shadow IT based on risk attributes

Example Restrict users from accessing cloud apps that have known vulnerabilities

Requirements

- Continuously updated cloud app database with rich risk information
- Dynamic network feed of app intelligence from CASB to Secure Web Gateway (SWG) or Firewall control points and management console.
- SWG that can enforce unified policy controls (on-prem and in the cloud) and report on cloud use based on dynamic CASB intelligence such as app type, risk attribute, and business readiness rating.
- Ability to block, redirect, and alert on policy violations enabling organizations to restrict unapproved cloud services while allowing access to those that meet organizational security guidelines.
- Unified user authentication between CASB and on-prem or cloud based Secure Web Gateway (chaining, etc.)

03 Monitor your organization's GDPR compliance in the cloud

Example Identify use of cloud apps that are not GDPR compliant

Requirements

- GDPR app risk rating based on a comprehensive set of GDPR-relevant cloud app security attributes
- Out of the box GDPR dashboards and reports to monitor whether cloud app usage aligns with GDPR regulations
- Perform vendor impact assessments and block use of GDPR non-compliant apps
- Identify data center locations (can find locations not included on self-published lists) via active traffic analysis of cloud apps, and enforce geography-based access controls
- Automated PII classification of content being uploaded and stored in cloud apps and services
- Remediation of risky exposures and ongoing policy enforcement to prevent leakage of PII content in the cloud (Cloud DLP)
- Encryption of personal data, such as PII, in cloud apps and services
- Rapid incident response to facilitate data breach notification requirements
- Extensive role-based access controls and custom reporting to provide correct access and visibility required by a Data Privacy Officer (e.g., four eyes principle)

04 Factor real-time cloud app breaches into Shadow IT analysis

Example Elevate the risk rating of a cloud app if it has experienced a breach in the last 90 days

Requirements

- Real-time cloud app breach data that is continuously updated and curated
- Dynamically update cloud app dashboards to reveal recent threat activity
- Ability to temporarily adjust cloud app risk ratings based on recent breaches
- Enforce policies and controls based on adjusted risk ratings

05 Identify over spend on cloud apps and services

Example Identify multiple instances of the same cloud app, that may pave the way for consolidation and cost optimization opportunities

Requirements

- Identify new instances of AWS or other cloud apps purchased outside of IT
- Compare apps with similar functionality side-by side and make smart choices that meet security and cost requirements
- Uncover and consolidate multiple accounts for the same cloud app
- Ability to discover all cloud accounts used across the corporate network, including personal accounts.
- Monitor cloud app usage relative to subscription license to identify overspend

06 Quickly investigate and respond to security incidents in the cloud

Example Get detailed visibility of what activity users were taking with a particular file leading up to a data breach

Requirements

- Extract and analyze granular detail from real-time HTTPS traffic, to identify user activity within a broad range of cloud apps and services
- Capture and process detailed user activity from API interfaces for sanctioned cloud apps and services, like Office365, Amazon Web Services and Google G-Suite
- Process consolidated log data with intuitive search and filtering functions to identify and explore incidents of interest, such as account takeovers, data exfiltration, and data destruction attempts.
- Generate custom reports that meets organizational requirements and schedules

01 Data Security

Identify and remediate risky data exposures in sanctioned apps

Example Identify any PII data that is being shared in my Office 365 account, and modify the sharing permissions to remove any public exposure

Requirements

- Out of the Box data classifiers for a wide range of regulated and sensitive content, such as PII, PCI, PHI, and source code.
- Automated detection and granular policy enforcement for sensitive content uploaded to and created in cloud apps for email, file sharing, data repositories, and chat (requires extensive APIs and/or a proxy)
- Block high risk sharing of confidential data: to the public, external users, to entire organizations, and unsanctioned cloud accounts.
- DLP in the cloud based on machine-learning with predefined content and risk data classes, predefined terms, custom regular expressions, custom dictionaries.
- Ability to identify custom forms

02 Prevent data exfiltration from sanctioned corporate accounts to personal accounts.

Example Prevent users from downloading content from the corporate sanctioned Box account and uploading it to a personal Dropbox account.

Requirements

- Monitor both sanctioned and unsanctioned cloud app activity (requires CASB gateway with forward proxy architecture)
- Enforce policies that block employees from transferring confidential files from sanctioned corporate apps to their unsanctioned personal cloud accounts based on a range of criteria
- Ability to enforce different policies for personal and corporate instances of the same cloud service (e.g., a personal G-suite account vs. a corporate G-suite account).

03 Monitor and control cloud activity even when accessed from native apps and mobile devices

Example Identify DLP policy violations for users that leverage their native Salesforce app on their iPhone

Requirements

- Forward proxy support to monitor and control user activity and access to data via native endpoint applications for cloud apps.
- Integrate with active directory or single sign-on services to harmonize user groups when creating policies
- Define and enforce content-based and context-based policies to govern sensitive data inside and outside the organization
- Control sync actions and block downloads of confidential data to high risk endpoints such as unmanaged devices and endpoints with out-of-date browsers and operating systems.

04 Monitor and control all apps within Office 365 and G Suite

Example Identify and prevent DLP violations in Office 365 Outlook Email messages and enclosures as well as content stored in One Drive, which may be linked within email.

Requirements

- Support for all Microsoft Office 365 apps, including OneDrive, Outlook/email, Sites, Yammer, Teams, and Groups
- Support for all G Suite apps, including Drive, Gmail, Calendar, Hangouts, Sites, Vault, Contacts, and Admin
- Ability to scan these apps for DLP violations or malware, and remediate as appropriate

05 Automatically learn sensitive content types for monitoring and control

Example Automatically generate a data classification profile for a company-specific payroll document that cannot be shared outside the organization

Requirements

- Automatically classify documents based on document training-based machine learning
- Custom forms (regex)
- Leverage natural language processing and contextual analysis to identify types of documents not readily captured by regex matching, such as legal, health, etc.
- Enforce policies and controls based on these classifications
- Automate data classification with high accuracy and nearly zero false positives using document fingerprinting and similarity matching.
- Document fingerprinting-use data science algorithms to match a new document to a training set of documents to within a predetermined accuracy matching threshold. Fingerprinting is useful for identifying structured data within forms.
- Similarity matching-match content in newly scanned documents to a positive training set of documents, while ignoring documents that match a negative training set of documents. Matching is used when looking to identify sensitive content across multiple document types and formats, such as PDFs and PPTs.

06 Apply the same DLP controls across your enterprise both on-prem and in the cloud

Example Extend the same DLP policies for data stored in on-prem servers to data stored in cloud apps

Requirements

- Enable a central console for defining consistent policies and workflows across several channels, including on-prem storage, email, endpoint, network attach points and cloud
- Infuse the DLP console with rich insights from CASB including user risk assessments, threat trees and risky activities, and detailed cloud activity log information
- Native cloud-based DLP classification and analysis, avoiding inefficient backhauling of data (saving bandwidth and latency)
- Enhanced “cloud-specific” remediation options including the ability to “remove a shared link, update file permissions, remove an external collaborator, or delete or update collaborator permissions

07

Encrypt confidential data wherever it travels

Example Encrypt a sensitive document being uploaded to a corporate sanctioned cloud app, and subsequently restrict who may access this document after it is downloaded and shared

Requirements

- Granular and automated classification for content flowing in and out of cloud apps
- Comprehensive encryption triggered by data classification, protecting sensitive data in the cloud
- Ability to preserve encryption of content after it is downloaded from the cloud, and require user authentication to view content regardless of where it travels
- Revoke access to encrypted files at-will in the cloud and anywhere else they exist

Threat Protection

01

Detect and take action on suspicious user activity that may indicate a malicious insider or a compromised account

Example If a user account shows an excessive number of downloads of sensitive content alert the security admin, and optionally block the user from accessing cloud apps

Requirements

- Leverage Machine Learning based User Behavior Analytics (UBA) to monitor each and every user account, and develop a dynamic user Threat Score based on that user’s risky activity

- Leverage both threshold based triggers and behavioral triggers for users to reduce false positives
- Create and enforce policies based on a user's unique ThreatScore that can alert, block upload/download, or quarantine users across a range of cloud apps and services to prevent data exposures and control access
- Provide threat attribution user activity visualization tree for rapid analysis and remediation of high risk issues

02 Identify and block malware and ransomware in cloud apps

Example Protect against malicious content that enter my corporate Office 365 environment from another cloud app

Requirements

- CASB API-based integration and inline gateway able to inspect email, file sharing, structured data, and chat communications for malware and high risk activity
- Detect, block, report and prevent proliferation of malicious files
- Identify, quarantine and block malware and VB macros (including their communication with Command & Control servers)
- Uses machine learning based algorithms, heuristics, and file reputation analysis for comprehensive A/V scanning with a world class threat intelligence database

03 Protect cloud accounts from advanced threats

Example Detect zero-day threats in corporate sanctioned cloud app accounts

Requirements

- Cloud sandboxing for analyzing unknown files to detect malware before uploading them to corporate cloud accounts.
- Scan content via API and Gateway (forward, reverse, mirror proxy) to identify advanced persistent threats regardless of the source of origin for that content (managed or unmanaged source device, external cloud app or account)

04 Identify and prevent complex data exfiltration attempts

Example Detect a continuous pattern of downloads from the corporate Office 365 account followed shortly by an upload to an unsanctioned personal account (Dropbox, for example) and alert security admin appropriately

Requirements

- Forward Proxy Gateway to monitor sanctioned and unsanctioned cloud activity, along with API
- Support for complex policies that identify a series of triggers in a predefined sequence that represent a potential data exfiltration attempt
- Pre-defined policies for common cases, as well as tools to customize policies based on customer specific use cases
- Ability to quickly identify and remediate incidents of concern

05 Monitor and control activities on personal IaaS instances from corporate devices

Example Monitor and control activities on personal AWS and Azure instances from corporate devices

Requirements

- Gateway and API support for IaaS services, such as Amazon Web Services, Microsoft Azure and Google Cloud Platform
- Prevent unauthorized activity in IaaS privileged accounts and restrict users from misconfiguring corporate AWS and Azure instances
- Safeguard AWS and Azure accounts from hackers and malicious insiders who try and use your infrastructure for their purposes leveraging user behavior analytics
- Identify and eliminate unsanctioned and malicious activities, virtual machines, and servers.]

06 Dynamically step-up authentication for risky transactions

Example Dynamically enforce multi-factor authentication for transactions when a user's sThreatScore goes above 80 out of a 100 [or a designated critical threshold].

Requirements

- Dynamically identify risky transactions based on user behavioral patterns, access to sensitive content or a custom defined set of transactions
- Define and enforce granular policies based on risky transactions that trigger stepped up authentication
- Pause a session while verifying the user's identity and resume the session upon confirmation

Symantec CloudSOC™
Cloud Access Security Broker

Where to start?

A free shadow IT risk assessment

The first step towards securing your organization's cloud usage is to request a Shadow IT Risk Assessment to uncover all apps running on your extended network. This will also give you an opportunity to see the Symantec Audit in action through a 30-day free trial.

go.symantec.com/shadow-it

A free shadow data risk assessment

The next step towards securing your organization's cloud usage is to request a Shadow Data Risk Assessment to uncover and classify all Shadow Data stored and shared within your selected cloud app. You will also get temporary access to the CloudSOC dashboard, which will give you an opportunity to see the Securlet in action.

go.symantec.com/shadow-data

About CloudSOC

The Data Science Powered™ CloudSOC platform empowers companies to confidently leverage cloud applications and s ervices while staying safe, secure and compliant. A range of capabilities delivers the full life cycle of cloud application security, including auditing of shadow IT, real-time detection of intrusions and threats, protection against intrusions and compliance violations, and investigation of historical account activity for post-incident analysis.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit **www.symantec.com** or connect with us on **Facebook**, **Twitter**, and **LinkedIn**.

Symantec™

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com