Symantec™
A Division of Broadcom

Product Brief

CloudSOC Audit

Key Benefits

- **Uncover and Control Shadow IT:** Gain visibility into all the cloud apps used within your company and their detailed Business Readiness Ratings. Enforce access control, DLP, and threat protection with CloudSOC Gateway.
- **Make smart cloud app choices:** Compare cloud apps side-by-side, review risk attributes for the cloud and associated mobile app, consolidate on the most secure alternatives, and continuously monitor usage for compliance enforcement and cost containment.
- **Monitor risk and compliance:** Identify high-risk cloud and mobile apps and provide executive reports regarding your organization's risk profile tailored to your unique security requirements.
- **Integrate with Web Security:** Leverage integrations with Symantec Secure Web Gateways, including ProxySG and Web Security Service (WSS) to uncover Shadow IT in SWG traffic and apply granular policy controls to Shadow IT.

Overview

Symantec CloudSOC Audit discovers and monitors all the cloud apps being used in your organization and highlights any risks and compliance issues they may pose.

Provide visibility into Shadow IT usage Analyze logs from your proxy, firewall, and endpoints to identify the cloud services in use in your organization and provide an executive summary to IT and business decision makers. Our fully configurable, Flex log format interpreter can analyze almost any type of log file.

Identify Risky Apps

Identify risky SaaS, PaaS, and IaaS cloud apps and mobile apps in use based on hundreds of objective security attributes that can be customized to your organization's risk tolerance. Identify employees using these services, as well as how much they're using them. This intelligence can be used to coach BUs and users to select safe app alternatives and use them responsibly.

Control Access to High-Risk Cloud Apps

Block unapproved cloud services while allowing access to those that meet your security guidelines. Add apps from Audit to CloudSOC Gateway or use AppFeed integration with ProxySG and Web Security Services enables you to apply granular Shadow IT policy controls.

Enable Admin Data Visibility Via Role Based Access Controls (RBAC)

Control which admins can view activities on a specific subset of users.

Perform Risk Assessments on Cloud Services

Each service is measured against hundreds of objective security attributes, enabling you to perform side-by-side comparisons of functionally similar apps so you can select the most secure ones.

Consolidate Services and Reduce Costs

Comparing cloud services can help you make well-informed recommendations to business units to consolidate accounts, saving costs and reducing complexity.

Generate Automated and Custom Reports

Generate infographics and executive audit reports with the click of a button. Set up custom scheduled reports to be sent via email to critical stakeholders in the organization.

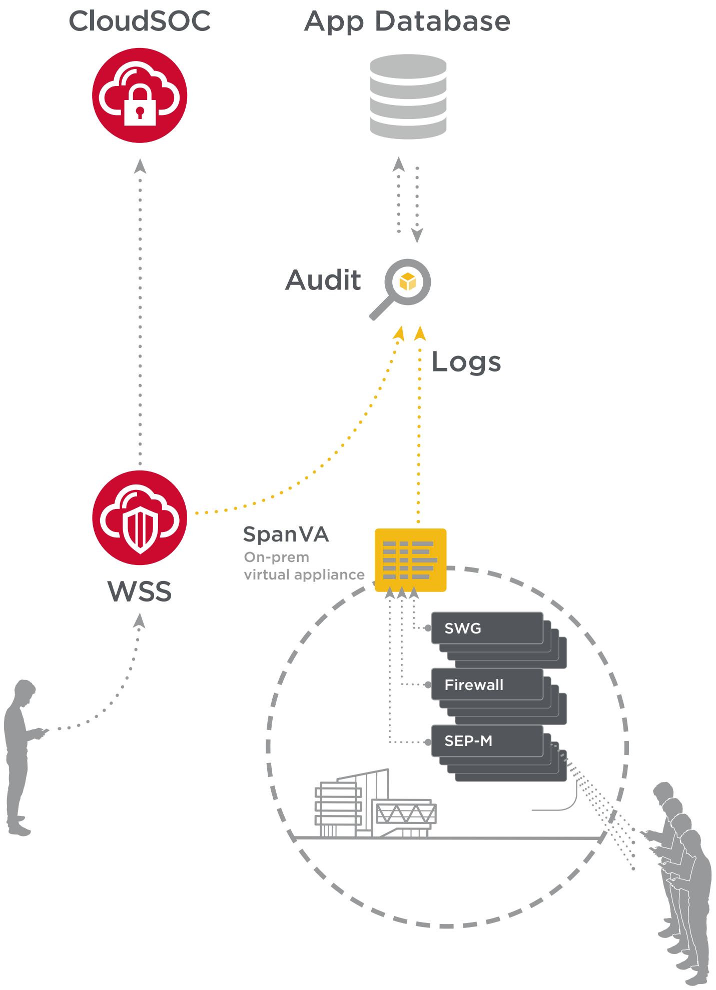
Key Features

- **Shadow IT Risk Assessment:** Find and monitor all cloud apps used in your organization and highlight any risk and compliance issues.
- **Business Readiness Rating:** Automatically rate the security of each cloud app and associated mobile apps discovered in your organization, based on hundreds of objective metrics, including security mechanisms and compliance certifications.
- **Customized Ratings:** Weight individual risk attributes to provide a customized BRR for each app based on your organization's unique risk requirements.
- **Comparative Analysis:** Find alternatives to high-risk apps and enables you to perform intuitive side-by-side comparisons.
- **Usage Analysis:** Reveal how frequently each cloud app is used and by whom, identifying opportunities for streamlining and cost reduction. Identify "New" apps employees have introduced that may be risky.
- **Advanced Visualization:** Quickly zoom into the information with easy-to-use filters, pivot views, and time scale adjustments.
- **Cloud Services Risk Assessment Report:** Generate a comprehensive report with executive summaries along with a list of discovered services and recommendations.
- **Access Enforcement Policies:** Allow remediation at the proxy or firewall through blocking of non-IT approved apps.
- **Admin Single Sign-On:** Enjoy Single Sign-On (SSO) between Audit and WSS.

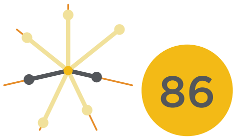
Specifications

Feature	Description
Log File Formats	Flex Universal Log Format enables ingestion of almost any log file type (proxy, firewall, endpoint, malware, etc.) into CloudSOC Audit.
Log Ingestion Modes	Log ingestion modes include web uploads, SpanVA for continuous monitoring, SCP, SFTP, and S3.
Log File Anonymization	Tokenize user-identifiable information before it is sent to CloudSOC Audit using SpanVA, an optional virtual appliance.
User Directory Synchronization	Synchronize users from LDAP or AD into CloudSOC using the SpanVA (optional) Directory Sync feature.
UBA and Threat Intelligence Feeds	Perform User Behavioral Analysis (UBA) on firewall, SIEM, endpoint, and proxy logfiles to identify and rate threats to cloud apps leveraging advanced data science.
Data Export Formats	Readily export data for offline analysis and processing in CSV format or REST API.
Dashboards and Reports	• Create customizable dashboards with customizable widgets and predefined widgets. • Generate infographics and executive audit reports at the click of a button. • Schedule delivery of customized reports via email to critical stakeholders in the organization.
App Classification Types	Automatically classify apps as cloud hosting, collaboration, social network, security email, search engine, file sharing, storage, VoIP, instant messaging, expense management, identity management, workforce management, IT services management, CRM, digital certificates, domain registrar, cloud hosting, PaaS, development, analytics, personal finance, or online productivity suite.
App Business Readiness Rating Attributes	Cloud apps are rated high, medium and low risk according to customizable security attributes, including: compliance, data protection, admin controls, access control, service characteristics, business characteristics, and informational.

How CloudSOC Audit Works

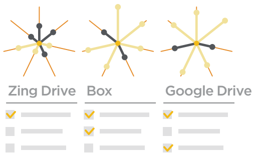


01 Analyze



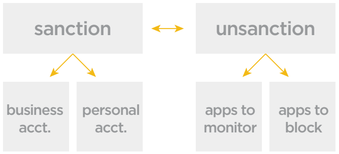
Business Readiness Rating for tens of thousands of cloud apps including hundreds of risk attributes and features required for compliance

02 Compare



Cloud and mobile app security risks, features, cost, and so on

03 Choose



Apps to sanction, which to monitor, and which to block

04 Monitor and Control

Automated reporting and CloudSOC Gateway

Integrations

Symantec Secure Web Gateways (ProxySG/WSS)

Apply granular policy controls to Shadow IT from the proxy management console and streamline deployment through unified authentication, UI integration, and automatic WSS log ingestion by CloudSOC Audit.

Single Sign-On Solutions

Integrates seamlessly with any third-party single sign on solutions based on SAML.

Active Directory (LDAP)

Enable user mapping for tracking user activity and identifying high-risk users.

Symantec Endpoint Manager (SEP-M)

Uncover Shadow IT used on managed endpoints outside of your network perimeter.

For more product information: broadcom.com