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.

**Uncover Shadow IT**
Gain visibility into all the cloud apps used within your company and their detailed Business Readiness Ratings™.

**Monitor risk and compliance**
Identify high-risk cloud apps and provide executive reports regarding your organization’s risk profile tailored to your unique security requirements.

**Make smart cloud app choices**
Compare cloud apps side-by-side, consolidate on the most secure alternatives, and continuously monitor usage for compliance enforcement and cost containment.

**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.
CloudSOC Audit

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 SaaS apps
Identify risky cloud apps in use based on 100+ 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. AppFeed integration with ProxySG and WSS enables you to apply granular Shadow IT policy controls directly from the proxy management console.

Identify risks in cloud app traffic
Uncover threats in firewall, proxy and endpoint logfiles using User Behavior Analytics (UBA) and advanced data science.

Perform risk assessments on cloud services
Each app is measured against 100+ 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.

Customize app Business Readiness Ratings by weighting individual risk attributes (i.e., compliance certifications).
How Audit Works

The Audit application ingests logs from firewalls and other security proxy devices to perform its Shadow IT analysis. In order to meet privacy needs and regulations, customers can also anonymize and compress log information with Symantec’s on-prem virtual appliance SpanVA, prior to log streaming. Logs are processed and results are available in the CloudSOC Audit App.

01 Analyze

Business Readiness Rating for ten’s of thousands of cloud apps incl. 100+ risk attributes and features req’d for compliance

02 Compare

app security risks, features, cost, etc.

03 Choose

which apps to sanction, which to monitor, and which to block

04 Monitor

with automated reporting

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 3rd 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.
## Key Features

<table>
<thead>
<tr>
<th>Shadow IT Risk Assessment</th>
<th>Find and monitor all cloud apps used in your organization and highlight any risk and compliance issues.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Readiness Rating™</td>
<td>Automatically rate the security of each cloud app discovered in your organization, based on 100+ objective metrics, including security mechanisms and compliance certifications.</td>
</tr>
<tr>
<td>Customized Ratings</td>
<td>Weight individual risk attributes to provide a customized BRR for each app based on your organization’s unique risk requirements.</td>
</tr>
<tr>
<td>Comparative Analysis</td>
<td>Find alternatives to high-risk apps and enables you to perform intuitive side-by-side comparisons.</td>
</tr>
<tr>
<td>Usage Analysis</td>
<td>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.</td>
</tr>
<tr>
<td>Advanced Visualization</td>
<td>Quickly zoom into the information with easy-to-use filters, pivot views, and time scale adjustments.</td>
</tr>
<tr>
<td>Cloud Services Risk Assessment Report</td>
<td>Generate a comprehensive report with executive summaries along with a list of discovered services and recommendations.</td>
</tr>
<tr>
<td>Access Enforcement Policies</td>
<td>Allow remediation at the proxy or firewall through blocking of non-IT approved apps.</td>
</tr>
<tr>
<td>Admin Single Sign-On</td>
<td>Enjoy Single Sign-On (SSO) between Audit and WSS.</td>
</tr>
</tbody>
</table>

## Specifications

<table>
<thead>
<tr>
<th>Log File Formats</th>
<th>Flex Universal Log Format enables ingestion of almost any log file type (proxy, firewall, endpoint, malware, etc.) into CloudSOC Audit.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Ingestion Modes</td>
<td>Log ingestion modes include web uploads, SpanVA for continuous monitoring, SCP, SFTP, and S3.</td>
</tr>
<tr>
<td>Log File Anonymization</td>
<td>Tokenize user-identifiable information before it is sent to CloudSOC Audit using SpanVA, an optional virtual appliance.</td>
</tr>
<tr>
<td>User Directory Synchronization</td>
<td>Synchronize users from LDAP or AD into CloudSOC using the SpanVA (optional) Directory Sync feature.</td>
</tr>
<tr>
<td>UBA and Threat Intelligence Feeds</td>
<td>Perform User Behavioral Analysis (UBA) on firewall, SIEM, endpoint, and proxy log files to identify and rate threats to cloud apps leveraging advanced data science.</td>
</tr>
<tr>
<td>Data Export Formats</td>
<td>Readily export data for offline analysis and processing in CSV format or REST API.</td>
</tr>
<tr>
<td>Dashboards and Reports</td>
<td>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.</td>
</tr>
<tr>
<td>App Classification Types</td>
<td>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.</td>
</tr>
<tr>
<td>App Business Readiness Rating Attributes</td>
<td>Apps are rated high, medium and low according to over 100 customizable security attributes, including: compliance, data protection, admin controls, access control, service characteristics, business characteristics, and informational.</td>
</tr>
<tr>
<td>Cloud Traffic Destinations</td>
<td>Destinations are trackable by city, country, number of services, number of sessions, KB uploaded, KB downloaded, number of users and number of platforms.</td>
</tr>
</tbody>
</table>
Get better security with less complexity

Deploy a cloud security solution that integrates with your existing security infrastructure. A Symantec solution with CloudSOC provides greater security coverage, reduces operational complexity, and provides an optimal user experience.

About CloudSOC

Data Science Powered® Symantec CloudSOC platform empowers companies to confidently leverage cloud applications and services while staying safe, secure and compliant. A range of capabilities on the CloudSOC platform deliver the full life cycle of cloud application security, including auditing of shadow IT, real-time detection of intrusions and threats, protection against data loss 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.

For more info on Symantec CloudSOC CASB and its industry leading integrations with Symantec Enterprise Security Systems, visit go.symantec.com/casb