SonicWall Cloud App Security

Securing cloud application usage through visibility and control

SonicWall Cloud App Security is a cloud service that provides CASB-like functionality, delivering real-time visibility and control of cloud application usage. Its comprehensive dashboard enables administrators to discover usage of risky applications, track user activity, and set app control (block/unblock) policies on sanctioned and unsanctioned applications to protect sensitive corporate data.

Shadow IT discovery

Leverage existing firewall log files to automate cloud discovery to identify applications being used and their risk posture

Real-time application visibility

Monitor usage in real-time with an intuitive dashboard view that provides details of applications being used, traffic volume, user activity and location of use

Application classification and control

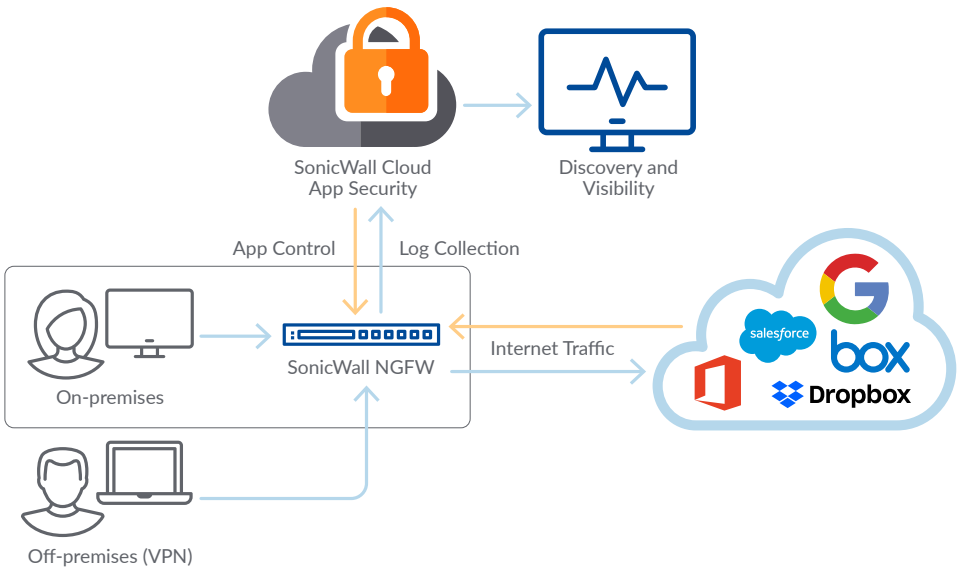
Classify unmanaged cloud applications into Sanctioned Apps (IT approved) or Un-Sanctioned Apps (Not IT approved), and set allow/block policies based on the application risk score

Benefits:

- Get real-time visibility into cloud application traffic, transaction volume and usage pattern
- Improve security posture by enforcing access policies to block risky applications
- Reduce shadow IT by discovering usage of sanctioned and unsanctioned IT applications
- Zero downtime deployment with SonicWall Capture Security Center

Overview

Cloud App Security is a cloud service that complements SonicWall next-generation firewalls (NGFW). By integrating with SonicWall NGFW, the Cloud App Security can leverage the existing network infrastructure to provide visibility into cloud usage.

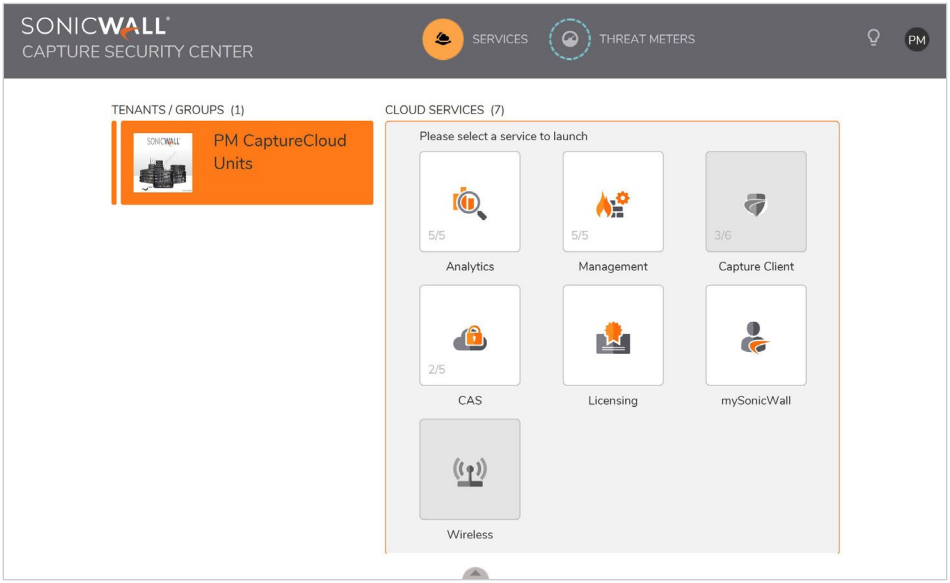


SonicWall NGFWs analyze and log all traffic entering and leaving the network. Logs generated for outbound traffic data do not clearly distinguish the cloud applications being used, and don't provide a risk score for each application used by employees.

For remote employees redirected through NGFW using VPN, the solution gathers additional details from these logs on the actions users take within cloud services. Cloud App Security processes log files from SonicWall NGFWs, and reveals which cloud services are in use by which users, data volumes uploaded to and downloaded from the cloud, and the risk and category of each cloud service. In effect, the Cloud App Security makes the existing infrastructure cloud-aware.

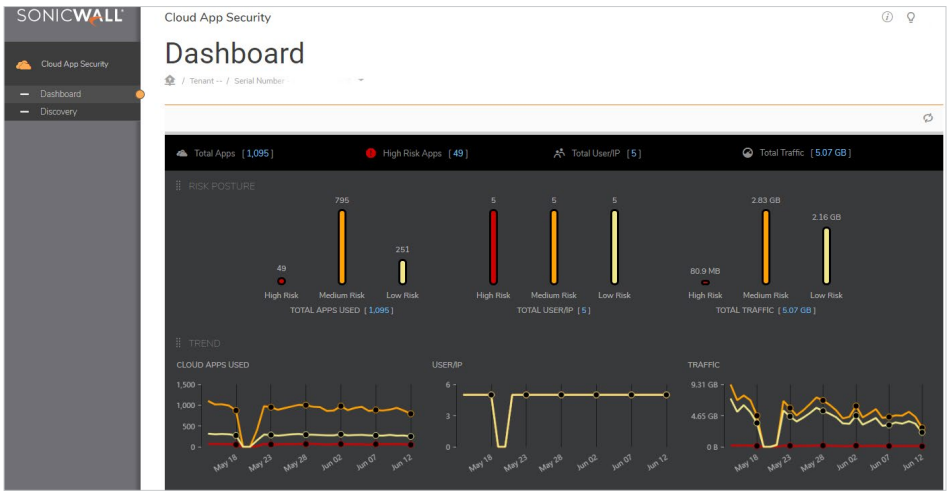
With employees increasingly using cloud applications for work, Cloud App Security enables administrators to detect gaps in security posture, classify cloud applications into sanctioned and un-sanctioned IT applications, and enforce access policies to block risky applications.

Cloud App Security is a critical part of SonicWall's vision to provide automated real-time breach detection and prevention capabilities for customers as they adopt cloud technologies. Delivered through the SonicWall Capture Security Center, our solutions work together to deliver a holistic security solution efficiently through, cloud-based management, reporting and analytics.

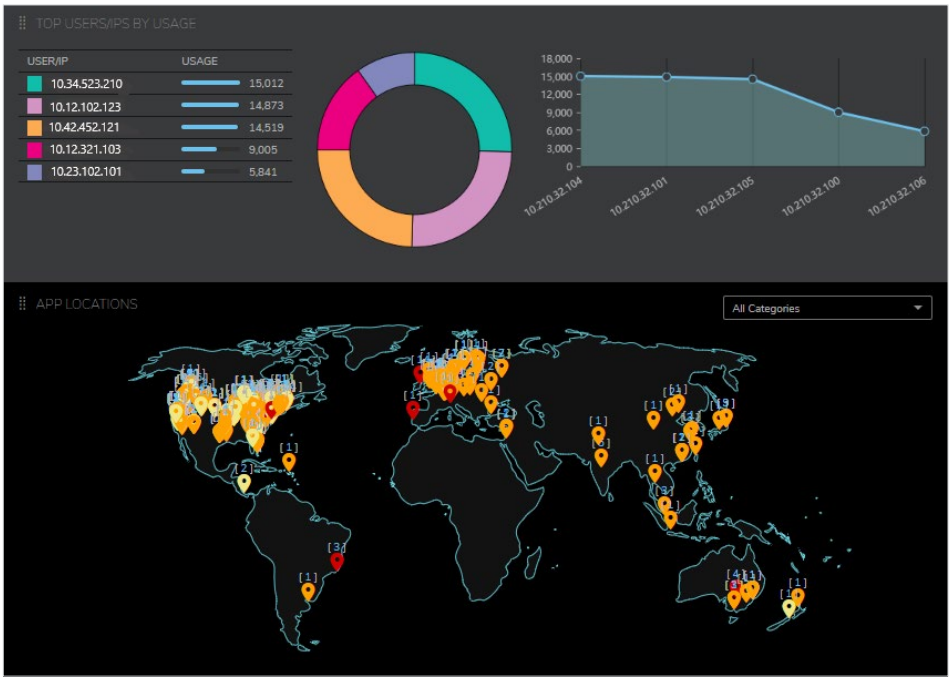


Real Time Visibility

The real-time dashboard enables administrators to monitor usage of risky applications, track user activity, transaction volume and location from which the application is being used. The solution ensures safe adoption of SaaS applications without impacting employee productivity, and at a low total cost of ownership.



The dashboard view provides administrators the real-time visual representation of applications being used, traffic volume, user activity and location of use.



For Discovered Applications, the dashboard displays by Traffic, Users, and Usage the Top 10:

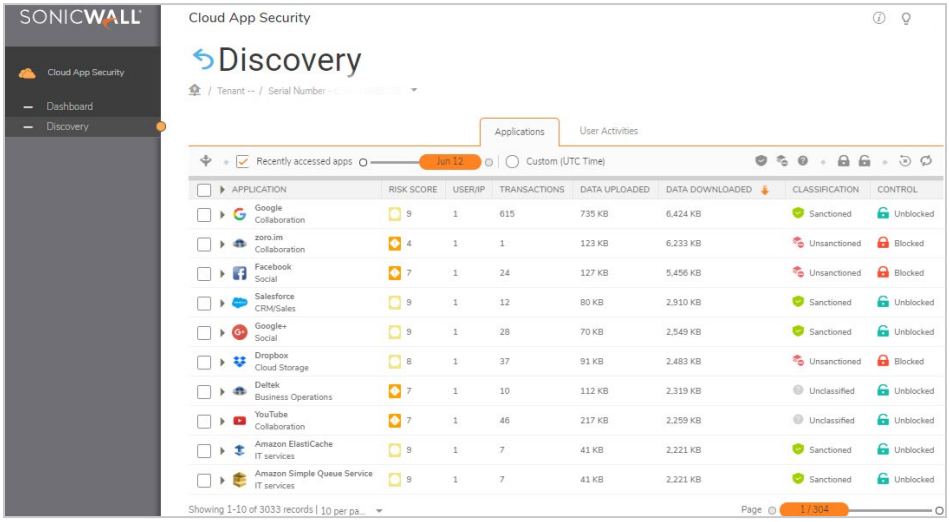
- Applications
- Categories
- Risk Levels (10-8 -> Low Risk, 7-4 -> Medium Risk, 3-1 -> High Risk)

The dashboard also displays real-time views of:

- Number and type of cloud applications being used, highlighting those with a High Risk level
- Number of users accessing cloud applications, highlighting those at High, Medium, and Low Risk
- Amount of data being used by cloud applications, highlighting those at High, Medium, and Low Risk

Discovery and Control

Cloud App Security provides a complete view of cloud services being used on the network. This feature delivers comprehensive discovery and reporting on shadow IT services using an exclusive reputation database of cloud-based services maintained by SonicWall. Discovered applications are assigned a risk score derived from an algorithm based on reputation, and security and compliance certifications. IT administrators can classify applications based on the risk score as Sanctioned or Unsanctioned IT applications for use. Through Capture Security Center, the solution empowers administrators to set block/unblock policies and control Sanctioned and Unsanctioned IT applications on the network.



The discover view displays details about both the cloud applications accessed within your organization and the user activities.

Users can choose either the Application view or the User view to review the following information

- **Application:** the name of the cloud application.
- **User List:** IP addresses of the users who have accessed the application, how much data was uploaded to and downloaded from the application.
- **Application Details:** detailed information about the cloud application, including its category, the company who created it, and other related information.
- **Risk Score:** Risk Score assigned to the cloud application based on SonicWall's proprietary threat assessment algorithms.
- **Users:** number of users who have accessed the application.
- **Transactions:** number of transactions performed with the application
- **Data Uploaded/Downloaded:** amount of data uploaded/downloaded to the application
- **Classification:** the classification of the application: Unclassified (this is the default), Sanctioned, or Unsanctioned.
- **Control:** whether the application is Blocked or Unblocked

Feature Summary

Feature	Benefits
Real-Time Dashboard	Get real-time, visual representation of applications being used, traffic volume, user activity and location of use
App Discovery	Automate cloud application discovery by leveraging your SonicWall firewall log files to identify shadow IT activities on the network
App Risk Assessment	Make informed decisions to block/unblock applications based on the risk assessment
App Classification and Control	Classify applications into Sanctioned or Unsanctioned apps, and set policies to block risky applications

Capture Security Center licensing and packaging

Capture Security Center (CSC)					
Licensing tier		CSC Management Lite	CSC Management	CSC Management and Reporting	CSC Analytics
Licensing requirement	Available to customers with active AGSS/CGSS subscription	AGSS/CGSS	AGSS/CGSS	AGSS/CGSS	AGSS/CGSS
Management	Single Pane of Glass	✓	✓	✓	–
	Backup/Restore	✓	✓	✓	–
	Task scheduling	–	✓	✓	–
	Group firewall management	–	✓	✓	–
	Inheritance - forward/reverse	–	✓	✓	–
	Zero touch	–	✓	✓	–
	Offline firewall signature downloads	–	✓	✓	–
	Workflow	–	✓	✓	–
Reporting	Live monitor, Summary dashboards	–	–	✓	–
	Download Reports: Applications, Threats, CFS, Users, Traffic, etc.	–	–	✓	–
	Scheduled reporting	–	–	✓	–
Analytics	Analytics (30-day retention)	–	–	–	✓
	Cloud App Security (30-day retention)	–	–	–	✓

Capture Security Center Analytics ordering information

Product	SKU
SonicWall Capture Security Center Analytics for NS*a* 2600 to 6650 and NSv 200 to 400 1yr	02-SSC-0391
SonicWall Capture Security Center Analytics For TZ Series, NSv 10 to 100 1yr	02-SSC-0171

Cloud App Security is available with the Capture Security Center Analytics bundle. Click here for more information.
To learn more about Cloud App Security visit our website or contact SonicWall sales here.

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 businesses in over 150 countries, so you can do more business with less fear.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

Datasheet-CloudAppSecurity-US-KJ-MKTG2770