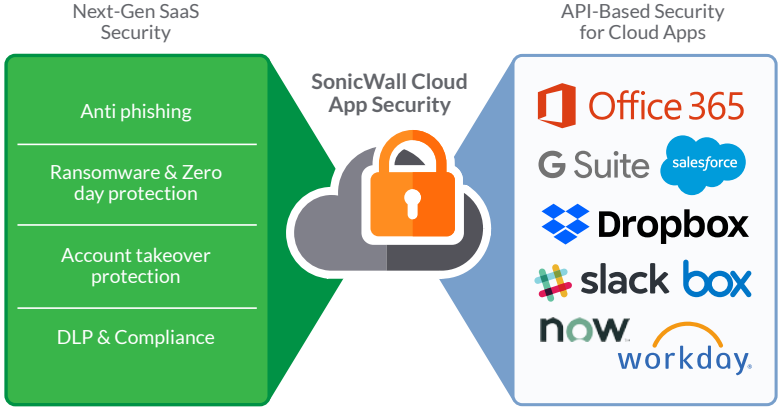
SONICWALL

SonicWall Cloud App Security

SonicWall Cloud App Security delivers next-gen security for SaaS applications such as Office 365 and G Suite, protecting email, data and user credentials from advanced threats while ensuring compliance in the cloud. If you are moving to the cloud, SonicWall provides best-in-class API-based security with low TCO, minimal deployment overhead and a seamless user experience.



Visibility: Identify all the cloud services (both sanctioned and unsanctioned) used by an organization's employees. This includes visibility of east-west traffic (cloud-to-cloud) as users can authenticate to unsanctioned apps using sanctioned IT such as Office 365.

Next-Gen Email Security: As email becomes the most popular SaaS app used, protecting this popular threat vector is key for SaaS security. The solution includes attachment sandboxing, advanced URL protection and Business Email Compromise (BEC) protection.

Advanced Threat Protection: Prevent malware propagation through apps such as OneDrive, Box and Dropbox with real-time anti-virus scanning for known threats and Capture ATP sandboxing for zero-days and unknown threats.

Data Security: Enforce data-centric security policies by offering granular access controls and preventing upload of sensitive or confidential files. The solution incorporates role-based policy tools, data classification, and loss prevention technologies to monitor user activity and block, or limit access.

Compliance: The solution collects extensive audit trail of every action, including real-time and historical events, and provides simple DLP templates to enforce policy controls and regulatory compliance in real time.

Benefits:

Next-Gen Email Security

- Stop ransomware, zero-days and targeted phishing email before they reach users' inbox
- Get advanced threat protection with attachment sandboxing and advanced URL protection
- Scan inbound, outbound and internal email in Office 365 and G Suite
- Block impersonation attacks using machine learning and artificial intelligence (AI)
- Retract malicious email from users' inboxes after delivery

Next-Gen SaaS Security (CASB)

- Gain granular visibility and control over sanctioned IT and shadow IT
- Get comprehensive coverage for both user-to-cloud and cloud-to-cloud traffic
- Prevent sensitive data uploads and unauthorized sharing of files
- Set consistent data security policies across sanctioned applications
- Protect against account takeovers (ATO), insider threats, compromised credentials
- Stop ransomware and zero-day malware propagation in the cloud
- Enforce regulatory compliance policies using simple DLP templates
- Identify breaches and security gaps by analyzing real time and historical events

Security Made Simple and Affordable

- Deliver a seamless user experience for access from any device and any location
- Eliminate point of failures, latency issues and the need to redirect traffic through a proxy
- Automate cloud application discovery when deployed with SonicWall NGFW
- Achieve low total cost of ownership (TCO) with fast deployment and ease of use

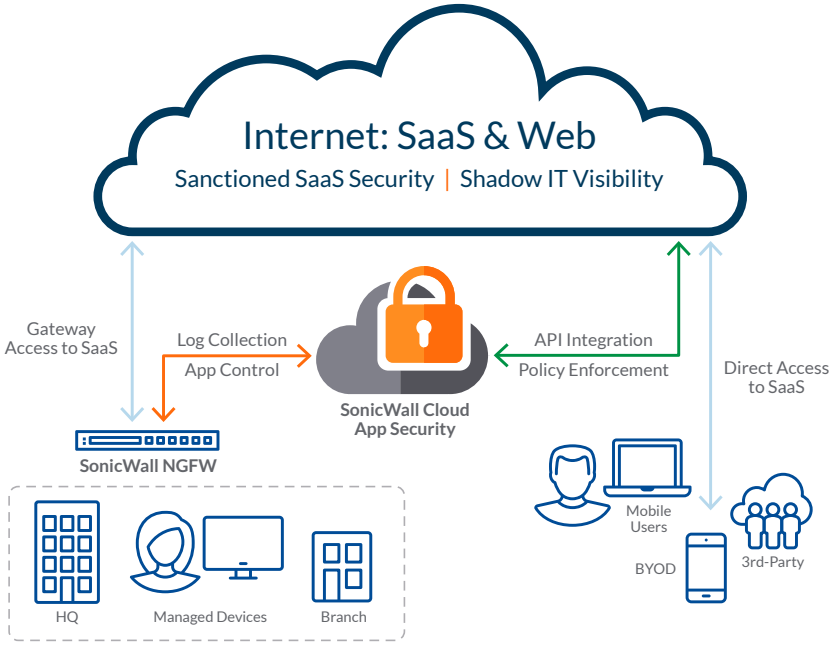
Solution Overview

SonicWall Solution Description

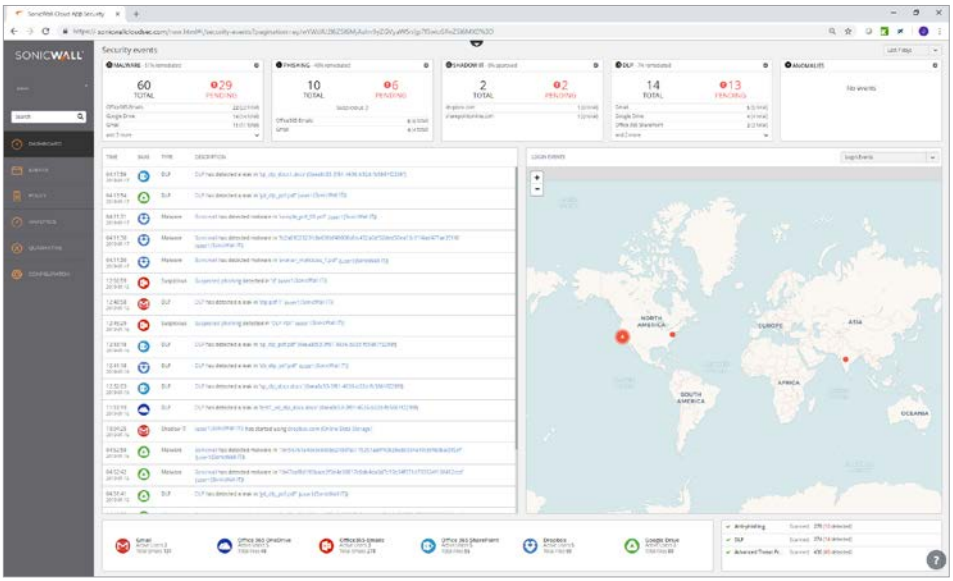
SonicWall Cloud App Security solution delivers out-of-band scanning of traffic to sanctioned and unsanctioned SaaS applications using APIs and traffic log analysis.

The solution seamlessly integrates with the sanctioned SaaS applications using native APIs, providing CASB functionalities- visibility, advanced threat protection, data loss prevention (DLP) and compliance. When deployed with SonicWall next-gen firewall (NGFW), Cloud App security offers shadow IT visibility and control for cloud usage on the network.

The solution empowers IT departments to roll out SaaS applications without compromising on security and compliance. Administrators can set consistent policies across all the SaaS applications deployed within the organization from a single console. Use available DLP and compliance reporting templates to quickly close security gaps and set custom policies to fulfill business and regulatory needs. Whether you have a few hundred users or hundreds of thousands of employees distributed across the globe, the solution can scale to meet your needs without the need to install and manage hardware.



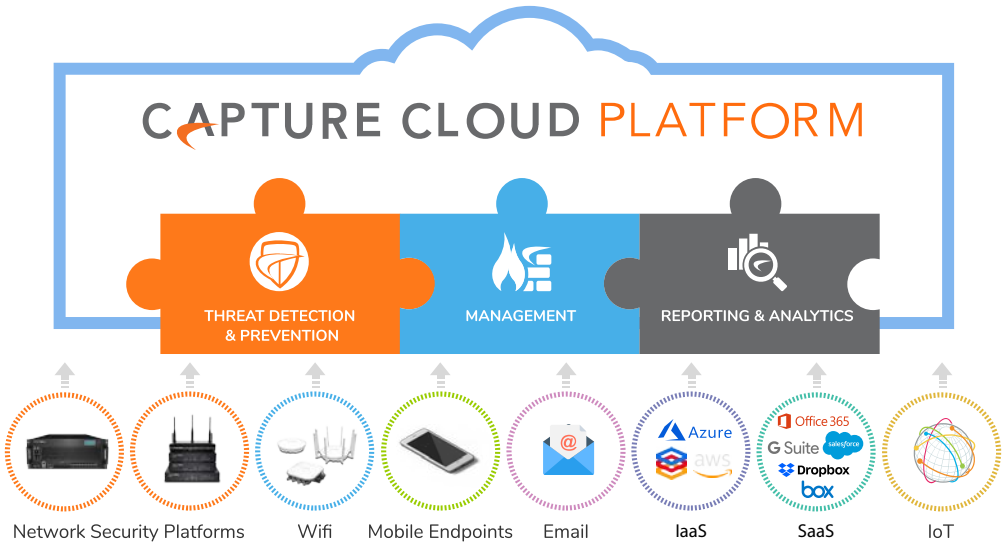
API-based SaaS security that delivers CASB functionalities



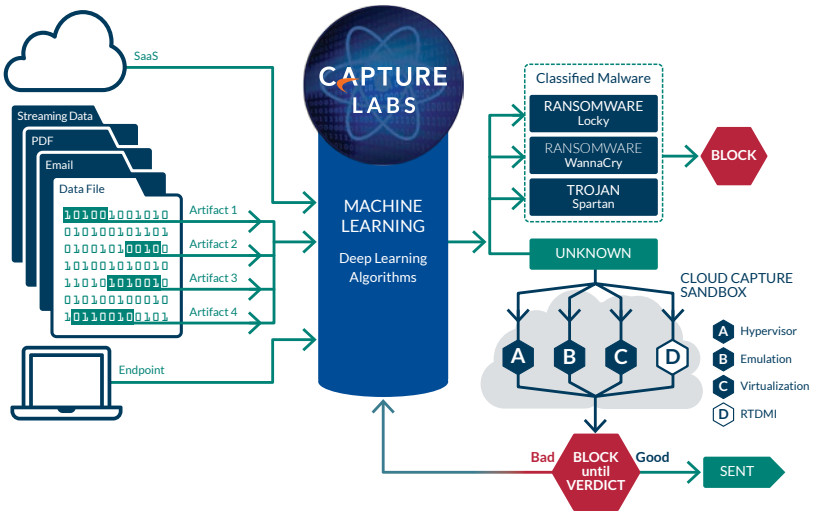
The real-time dashboard enables administrators to monitor usage of risky applications, track user activity, transaction volume and location from which the application is being used. The solution ensures safe adoption of SaaS applications without impacting employee productivity.

Integrated with SonicWall Capture Cloud Platform

SonicWall Cloud App Security is a cloud native security service architected using the capture cloud platform and delivered through Capture Security Center. SonicWall's Capture Cloud Platform delivers cloud-based threat prevention and network management plus reporting and analytics for organizations of any size. The platform consolidates threat intelligence gathered from multiple sources including our award-winning multi-engine network sandboxing service, Capture Advanced Threat Protection, as well as more than 1 million SonicWall sensors located around the globe. And Capture Security Center provides a single pane of glass management and administrators can easily create both real-time and historical reports on network and cloud activity.



To protect SaaS applications, SonicWall Cloud App Security leverages SonicWall Capture Cloud Platform, which combines the global security intelligence of the Capture Threat Network and the advanced threat prevention of the multi-engine Capture ATP sandbox. This approach enables SonicWall to extend our real-time automated breach prevention capabilities into the SaaS environments, empowering organizations to move to the cloud. Native APIs directly integrate with cloud services enabling the solution to scan files in apps such as OneDrive or Dropbox using Capture ATP service with Real-Time Deep Memory Inspection™ (RTDMI™), stopping ransomware and zero-days from entering the network.



SONICWALL®

Comprehensive Security for Office 365 & G Suite

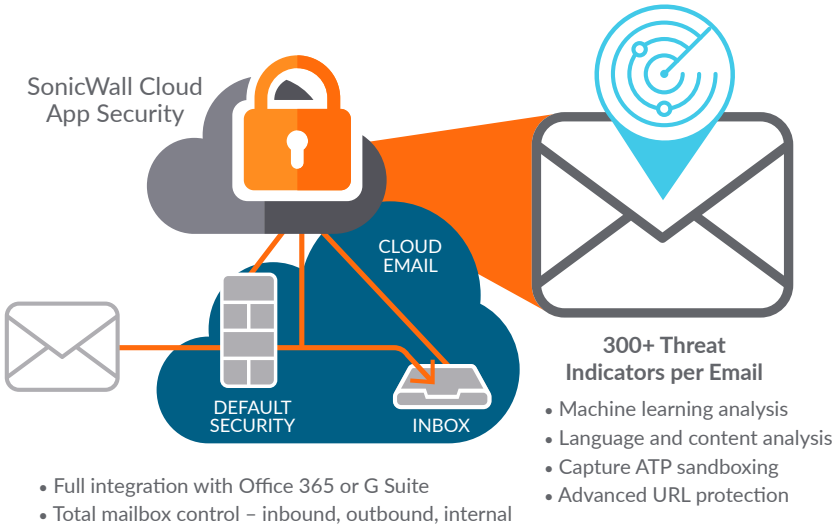
Next-Gen Security for Cloud Email

SonicWall Cloud App Security includes next-gen email security designed for cloud email platforms. Typically, when organizations move their email to the cloud, they either rely exclusively on the email provider's built-in security or supplement it with a traditional MTA proxy. External mail gateways, however, may not be sufficient to detect and block today's threats.

In addition to traditional email security layers of SPF, DKIM and DMARC checks, as well as URL filtering by leveraging three major data sources for URL blacklists, Cloud App Security's unique architecture provides protection that is impossible for an external gateway solution:

- Adds a layer of advanced threat protection: Cloud App Security blocks phishing messages missed by Office 365 and G Suite. The solution utilizes machine learning, artificial intelligence and big-data analysis to provide powerful anti-phishing, attachment sandboxing, advanced URL protection and impersonation protection.
- Monitors inbound, outbound and internal email: Cloud App Security's SaaS integration can scan and quarantine every email before it reaches the user's inbox, whether it is coming from outside the organization or from a compromised internal account.
- Scans historical messages for threats: On first connect, Cloud App Security scans historical messages (even closed accounts) for potential breaches or compromised accounts.
- Global Email Retraction: Malicious messages can be edited or retracted at any time, whether they are malicious, contain confidential information or due to an employee's accidental reply-all.

Because Cloud App Security's email protection is applied before the inbox but after the native Microsoft or Google filters (as well as any external MTA gateway that might be deployed), its machine-learning algorithms are uniquely tuned to identify threats that they miss. Cloud App Security is also able incorporate the results of the native scans into its own detection algorithms.



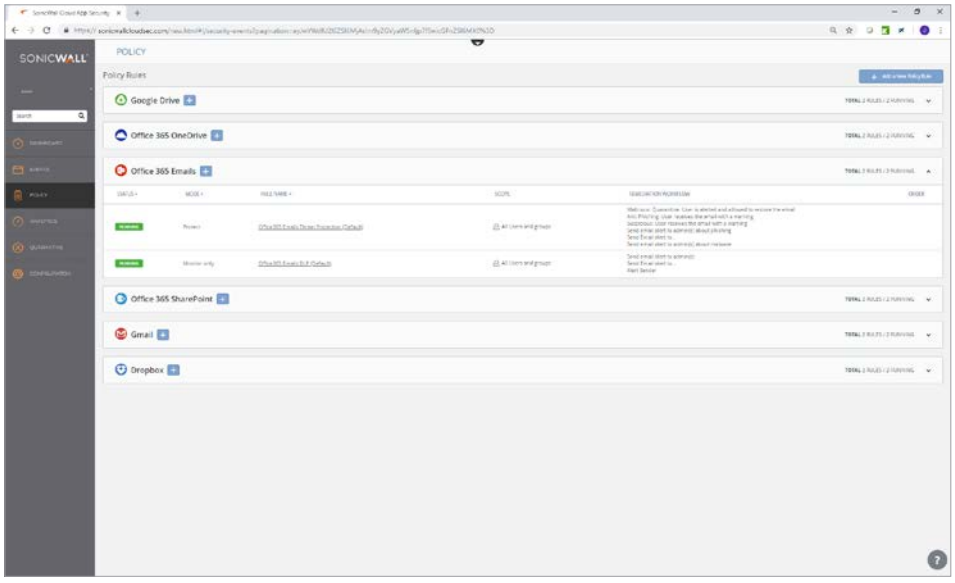
Virtual in-line protection stops malicious messages before they reach users' inbox

Next-Gen Security for the complete productivity suite

Cloud App Security offers complete, defense-in-depth security for Office 365 or G Suite. Whether you use email, share drives, IMs or the full collaboration environment, the solution helps you:

- Prevent phishing and malware from propagating within your organization or spreading to your customers and partners.
- Check every file for malicious content using Capture ATP sandboxing and active-content analysis to quarantine threats before they are downloaded by your users.
- Identify confidential information and apply cloud-aware policies that keep it within a organization or work group. Your users can harness the full power of cloud-based productivity suite while automated work flows enforce regulatory compliance, ensuring PCI, HIPAA, PII or other confidential data is not shared externally.

Comprehensive protection for the complete cloud office suite



Every SaaS app has a completely different policy engine, each with its own rules and enforcement capabilities. Sonicwall's solutions maps these across the sanctioned SaaS apps, and provides more granular controls. This way, Cloud App Security enables you to create a single policy that is applied in a consistent manner across the apps.

In addition, the context-aware policies make it possible to create enforcement workflows that inform the user of the issue, offer policy-safe options, and audit responses above and beyond what the built-in permissions controls in each SaaS ordinarily allow.

SaaS Security

To secure SaaS usage within organizations, SonicWall Cloud App Security provides:

Sanctioned IT Security – Directly integrate with cloud services using APIs for advanced threat protection and data loss prevention within SaaS environments.

Shadow IT Visibility and Control – Seamless integration with SonicWall NGFW for automated cloud application discovery and risk assessment using traffic log analysis.

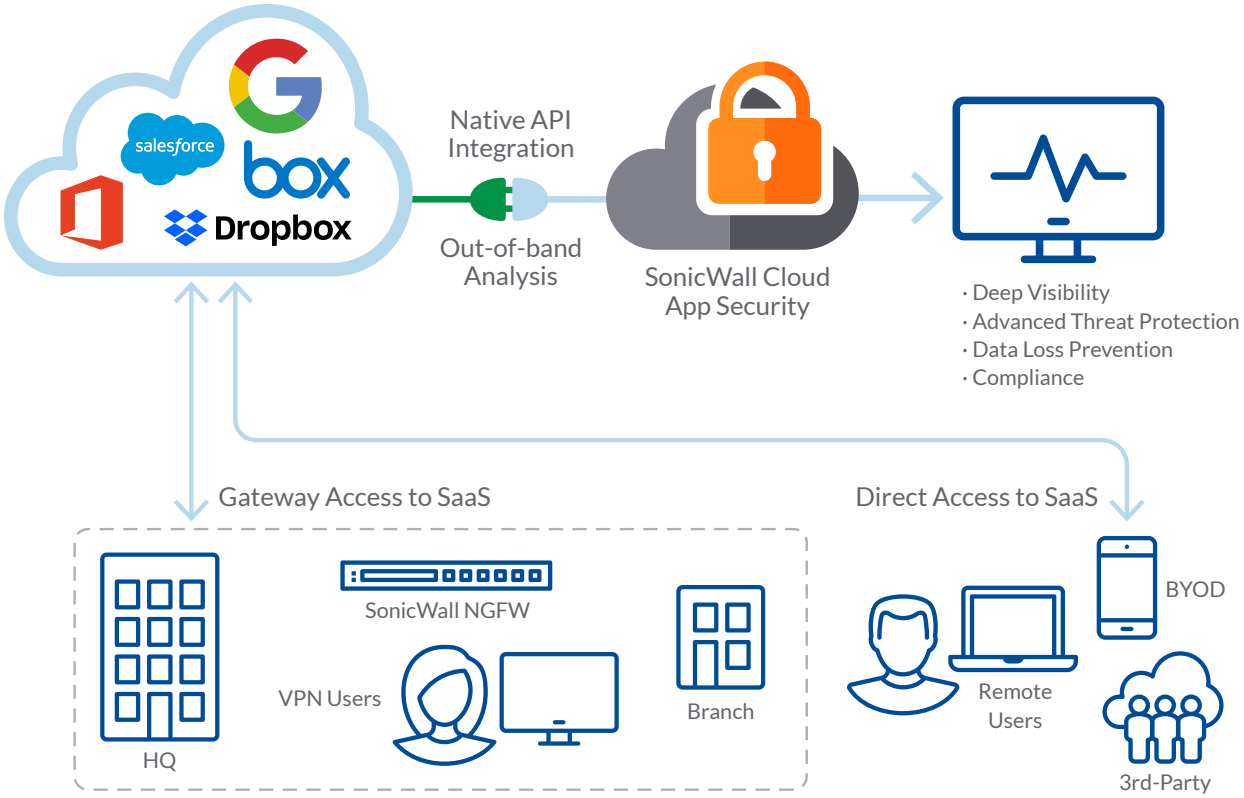
Sanctioned IT Security

When adopting SaaS applications such as Box and Dropbox, the responsibility to ensure security for data still resides with the organization and not the cloud service provider (CSP). This information is often disclosed in the fine print and the CSPs are not accountable for data leakage or malware infection and propagation. Hence organizations decide to use these applications, they must consider deploying a solution that can inspect the data in the cloud applications.

Only API-based solutions can inspect data at rest within SaaS apps since inline proxy-based solutions inspect only the data uploaded to the cloud from behind a firewall. Since many organizations already have a large volume of data stored in the cloud, APIs are used to enforce policies on this data. Other capabilities are only possible when connecting directly to an app via API include the ability to scan security configuration settings within the app and suggest changes that bolster security, as well as the ability to scan the sharing permissions on files and folders to assess the risk of third-party and external access to corporate data.

The solution provides deep visibility, advanced threat protection using Capture ATP sandbox and data loss prevention for SaaS applications such as cloud-based email alongside file sharing and cloud storage apps like Google G Suite and Microsoft Office 365.

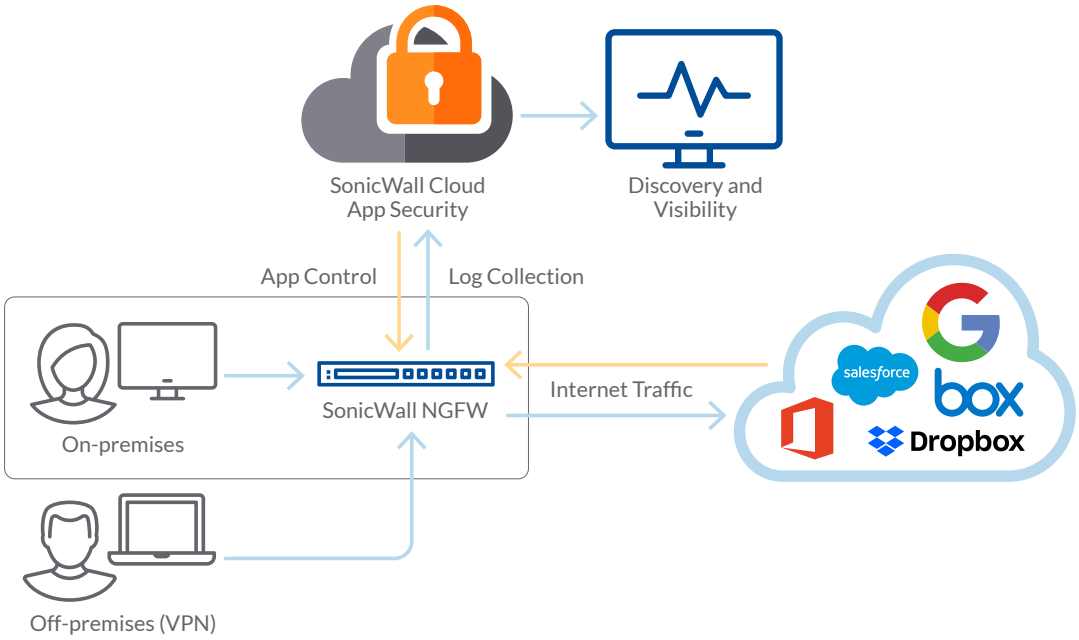
SonicWall Cloud App Security analyzes all traffic (log events, user activities, data files and objects, configuration state etc.) and enforces the necessary security policies through direct integrations with native APIs of the cloud service. Since the solution leverages native APIs, the solution does not use a proxy or sit in-line between the user and the cloud. This enables the solution to provide coverage for sanctioned apps regardless of the user's device or network. In addition, the API-based approach allows for easy deployment, granular control, and zero impact to the user experience.



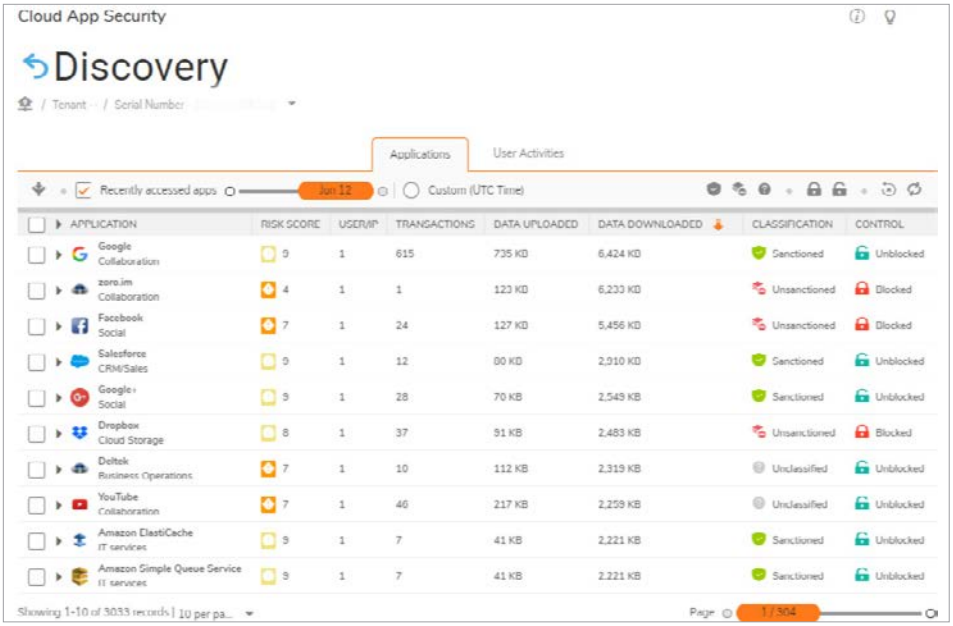
Secure sanctioned SaaS applications

Shadow IT Visibility and Control

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.



Discover shadow IT in your network



SonicWall Cloud App Security discovers and reports on risky 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 Shadow IT activities on the network.

Features

FEATURE		BENEFIT
Visibility	Cloud Application Discovery	Automate cloud application discovery by leveraging your SonicWall firewall log files to identify shadow IT activities on the network
	Cloud Usage Visibility	Get real-time, visual representation of applications being used, traffic volume, user activity and location of use
	Application Risk Assessment	Make informed decisions to block/unblock applications based on the risk assessment
	Event Monitoring	Monitor every action, including real-time and historical events, made in your SaaS environment
Next-Gen Email Security	Anti-Phishing	Stop targeted phishing attacks that are designed to evade default security offered Office 365 or G Suite
	Anti-Spoofing	Protect your corporate brand and users from email fraud and impersonation attacks
	Attachment Sandboxing	Block malicious email attachments from reaching your users inbox
	Advanced URL protection	Ensure users are protected from malicious embedded URLs
Advanced Threat Protection	Zero-day Malware Protection	Prevent malware from being stored and propagated through apps such as Box, Dropbox, OneDrive and G Drive
	Account Takeover Protection	Safeguard SaaS credentials by detecting anomalous user behavior, permission violations, or configuration changes
Data Security	Data Classification	Identify sensitive or confidential data and apply policies across SaaS applications to control how that information can be shared.
	Data-centric Access Control	Manage file permissions based upon the user's role and the type of data the file contains
	Remediation workflows	Ensure that securing data does not affect business through real time enforcement
Compliance	Compliance templates	Reduce administrative overhead by using simple compliance templates to meet requirements for SOX, PCI, HIPAA and GDPR
	Audit trail	Access historical event data for retrospective compliance auditing as well as real time reporting
	Policy enforcement	Enforce compliance in real-time with each SaaS to control access permissions, move files, block and edit email, and communicate with both users and administrators

SonicWall Cloud App Security	CLOUD APP SECURITY - BASIC	CLOUD APP SECURITY - ADVANCED
Unified Cloud Management (Capture Security Center)	●	●
Supported Cloud Apps	Select 1 SaaS App (Office 365 or G Suite)	Choose up-to 10 SaaS Apps
Anti-Phishing for O365 Mail or Gmail	●	●
Capture ATP* for Email Attachments	●	●
Advanced URL Protection	●	●
Capture ATP* for files stored in SaaS	●	●
Account Takeover Protection	●	●
Data Loss Protection	—	●
Shadow IT Visibility**	—	●

SonicWall Capture ATP includes Real-Time Deep Memory Inspection™ (RTDMI™)
***Requires SonicWall NGFW*

Partner Enabled Services

Need help to plan, deploy or optimize your SonicWall solution? SonicWall Advanced Services Partners are trained to provide you with world class professional services.

About SonicWall

SonicWall has been fighting the cybercriminal industry for over 27 years defending small and medium businesses, enterprises and government agencies worldwide. Backed by research from SonicWall Capture Labs, our award-winning, real-time breach detection and prevention solutions secure more than a million networks, and their emails, applications and data, in over 215 countries and territories. These organizations run more effectively and fear less about security.

© 2019 SonicWall Inc. ALL RIGHTS RESERVED. SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.
Datasheet-CloudAppSecurity-US-VG-MKTG5359

SONICWALL®

Connection we solve IT

Contact an Account Manager for more information.
1.800.800.0014 ■ www.connection.com/Sonicwall