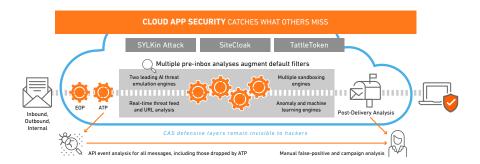# SONICWALL®

Cloud App Security

Full-suite protection for Office 365 and G Suite

As an integral component of the SonicWall Capture Cloud Platform, the SonicWall Cloud App Security (CAS) extends the most complete defense-in-depth security stack for Office 365 and G-Suite users. CAS helps stop targeted phishing and zero-day attacks that bypass Microsoft, Google and Secure Email Gateway security filters. Its API-based, multi-layered inline threat prevention system is invisible to hackers and enable full-suite protection for cloud email and SaaS applications. The solution easily deploys within minutes and employs a combination of machine learning, artificial intelligence and big-data analyses to provide powerful anti-phishing, attachment sandboxing, click-time URL analysis, impersonation and data leakage protection.

Business Benefits:

- Adopt cloud email and SaaS applications without fear
- Safe, productive users anytime, anywhere, and on any device
- IP and critical data protected
- Audit-ready, compliance
- Eliminate CAPEX of maintaining on-prem infrastructure
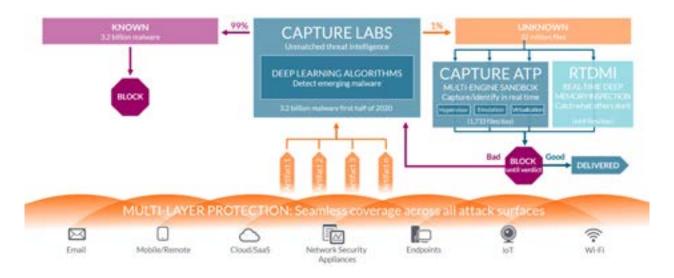
Operational Benefits:

- Deploy in minutes and secure with ease, granularity and zero user impact
- 100% API-based, nothing to install, no rerouting of traffic, no agent to deploy
- Apply policy in a consistent manner across all apps
- 100% visibility into every user, file, permission, and configuration change
- Visibility into all SaaS apps associated with user's Microsoft or G Suite account

CLOUD APP SECURITY CATCHES WHAT OTHERS MISS

SYLKin Attack   SiteCloak   TattleToken

Multiple pre-inbox analyses augment default filters

Two leading AI threat emulation engines   Multiple sandboxing engines

Real-time threat feed and URL analysis   Anomaly and machine learning engines

Inbound, Outbound, Internal   EOP   ATP   Post-Delivery Analysis

CAS defensive layers remain invisible to hackers

API event analysis for all messages, including those dropped by ATP   Manual false-positive and campaign analysis

Scan all email traffic and embedded content

CAS works seamlessly with Office 365 and G-Suite built-in security via API and scans any messages including inbound, outbound, and internal emails that bypasses preceding security filters. When using inline protection, no email, links and/or attachments can reach the inbox until CAS has scanned and determined they are 100% harmless. With a patented design that analyzes over 300 unique threat indicators, CAS spots and stops Business Email Compromise (BEC) and blocks targeted phishing, malware, zero-days, account takeover (ATO) and insider threats across your enterprise. It takes defensive actions before malicious content reaches user inboxes and before sensitive data leaks and alerts relevant personnel and products such as an admin, security analysts, EDR or SIEM about potential compromises for post-delivery remediation or recovery.

Security benefits:

- Catch phishing and zero-day attacks that Microsoft ATP and SEGs miss
- Block harmful messages, URLs and attachments from reaching the inbox
- Scan all emails preventing insider threats from compromised or trusted internal accounts
- Synchronous threat management via Capture Cloud Platform
- Visibility and control of data movements and prevent data leaks

Synchronous threat protection

Integration with the SonicWall Capture Cloud Platform security framework uniquely enables all SonicWall security solutions to work together for synchronous threat management. This allows CAS to leverage the SonicWall Capture ATP service, the only threat detection offering that combines multi-layer sandboxing, to analyze suspicious attachments and files. Threats revealed are used to create countermeasures at one part of the defense chain, which then immediately benefits all other parts of the defense ecosystem in real time. The entire process significantly reduces the window of exposure and false positives.

Feature Summary

Email Protection
- In-line threat protection
- Policy-based configuration
- Machine-learning for anti-phishing
- Anti-spoofing
- Office 365 EOP Anti-Spam augmentation
- Brand impersonation protection
- User impersonation detection
- Business Email Compromise (BEC) protection
- Page emulation analysis
- URL rewriting and click-time analysis
- Attachment sandboxing

- Post-delivery search, quarantine and remediation
- Post-detection alerts
- Forensic analysis
- Analytics
- Reporting dashboard
- One-click deployment

SaaS Security
- Account takeover (ATO) and insider threats protection
- Zero-day malware protection
- Active-form analysis
- Shadow SaaS Monitoring

Data Security
- Date leak protection (DLP)
- Policy-based Office 365 message encryption
- Data classification

Compliance
- Compliance templates
- Audit-ready reports
- Compliance enforcement

SONICWALL®

LICENSING AND PACKAGING

SonicWall Cloud App Security	Basic	Advanced
Cloud App Licensed[1]	Office 365 or G Suite	O365 Suite or G Suite, Box, Dropbox
ML-based Anti-Phishing	Yes	Yes
Capture ATP[2] for email attachments	Yes	Yes
Advanced URL Protection	Yes	Yes
Click-time Protection	Yes	Yes
Capture ATP[2] for files stored in SaaS	Yes	Yes
Account Takeover Protection	Yes	Yes
Data Leak Protection	No	Yes
Office Message Encryption integration	No	Yes

[1] Both packages include the choice of Office 365(email, OneDrive, and SharePoint) or G Suite (Gmail and Google Drive. Advanced also includes support for DropBox, and Box.
[2]SonicWall Capture ATP includes Real-Time Deep Memory Inspection™ (RTDMI™)

Product	SKU
SONICWALL CLOUD APP SECURITY ADVANCED 5 - 24 USERS 1 YR	02-SSC-2122
SONICWALL CLOUD APP SECURITY ADVANCED 25 - 49 USERS 1 YR	02-SSC-2128
SONICWALL CLOUD APP SECURITY ADVANCED 50 - 99 USERS 1 YR	02-SSC-2132
SONICWALL CLOUD APP SECURITY ADVANCED 100 - 249 USERS 1 YR	02-SSC-2136
SONICWALL CLOUD APP SECURITY ADVANCED 250 - 499 USERS 1 YR	02-SSC-2140
SONICWALL CLOUD APP SECURITY ADVANCED 500 - 999 USERS 1 YR	02-SSC-2144
SONICWALL CLOUD APP SECURITY ADVANCED 1000 - 4999 USERS 1 YR	02-SSC-2148
SONICWALL CLOUD APP SECURITY ADVANCED 5000 - 9999 USERS 1 YR	02-SSC-2152
SONICWALL CLOUD APP SECURITY ADVANCED 10000+ USERS 1 YR	02-SSC-2156
SONICWALL CLOUD APP SECURITY BASIC 5 - 24 USERS 1 YR	02-SSC-2124
SONICWALL CLOUD APP SECURITY BASIC 25 - 49 USERS 1 YR	02-SSC-2130
SONICWALL CLOUD APP SECURITY BASIC 50 - 99 USERS 1 YR	02-SSC-2134
SONICWALL CLOUD APP SECURITY BASIC 100 - 249 USERS 1 YR	02-SSC-2138
SONICWALL CLOUD APP SECURITY BASIC 250 - 499 USERS 1 YR	02-SSC-2142
SONICWALL CLOUD APP SECURITY BASIC 500 - 999 USERS 1 YR	02-SSC-2146
SONICWALL CLOUD APP SECURITY BASIC 1000 - 4999 USERS 1 YR	02-SSC-2150
SONICWALL CLOUD APP SECURITY BASIC 5000 - 9999 USERS 1 YR	02-SSC-2154
SONICWALL CLOUD APP SECURITY BASIC 10000+ USERS 1 YR	02-SSC-2158

Multi-year SKUs and support contracts are also available. For a complete list, please contact your preferred reseller or SonicWall Sales.

Internet Browsers

Microsoft® Internet Explorer 11.0 or higher and latest version of Microsoft Edge, Mozilla Firefox, Google Chrome and Safari.

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

SONICWALL®