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

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

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.
**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

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

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

**Compliance**
- Compliance templates
- Audit-ready reports
- Compliance enforcement
LICENSING AND PACKAGING

<table>
<thead>
<tr>
<th>SonicWall Cloud App Security</th>
<th>Basic</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud App Licensed‡</td>
<td>Office 365 or G Suite</td>
<td>O365 Suite or G Suite, Box, Dropbox</td>
</tr>
<tr>
<td>ML-based Anti-Phishing</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Capture ATP² for email attachments</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Advanced URL Protection</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Click-time Protection</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Capture ATP² for files stored in SaaS</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Account Takeover Protection</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Data Leak Protection</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Office Message Encryption integration</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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™)

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.