SONICWALL

SOLUTION BRIEF

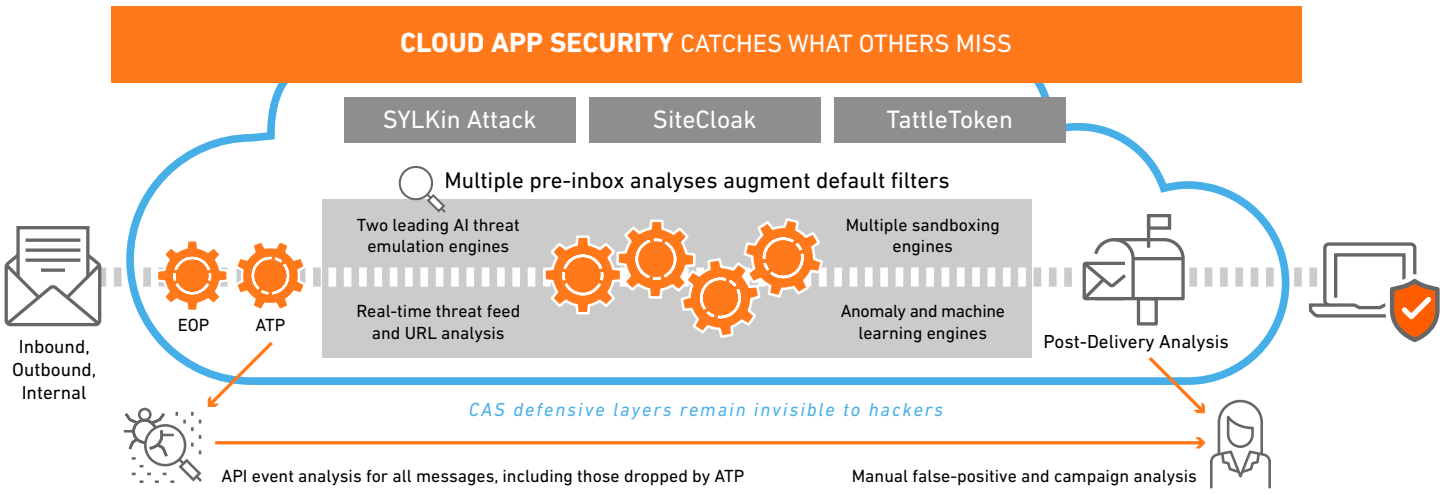
SonicWall Cloud App Security for Office 365

Protect Office 365 from the inside

SonicWall Cloud App Security (CAS) offers complete, defense-in-depth security for Office 365, whether cloud email, OneDrive, or the full suite. If your organization is making the transition from on-premise applications to the cloud, CAS offers the best way to ensure seamless security.

CAS connects to your Office 365 environment via API and scans for threats after your existing security but before the inbox. It is laser-focused on advanced attacks while also filtering out spam and greymail. It deploys instantly with the only one-click, cloud-enabled platform with no need for a proxy, appliance or endpoint agent.

> *"We use Cloud App Security as an added security layer for Microsoft 365 email. It's easy to configure and catches threats that Microsoft 365 does not."*
>
> *— Robert Dick, IT Manager, Lekker Food Distributors*



CLOUD EMAIL SECURITY

In-line Threat Protection	No email, links and/or attachments can reach the inbox until CAS has scanned and determined they are 100% harmless.
Scans all emails	Examines any inbound, outbound and internal emails that EOP and ATP miss.
Policy-based Configuration	Provides custom policy workflows to manage threats and run in 3 possible modes – Protect Inline, Detect and Prevent or Monitor Only.
Machine Learning for Anti-Phishing	Employs multiple machine-learning models trained on attacks that evade Office 365 and G-Suite and analyzes over 300 indicators of phishing per message, even when the hackers try to change its characteristics.
Anti-Spoofing	Protects corporate brand and users from email fraud and impersonation attacks.
Brand Impersonation Protection	Detects email that might spoof the domain, images, the language or just the look and feel of the most likely spoofed companies on the internet.
User Impersonation Detection	Knows employees by name and role, making it possible to identify messages that are attempting to impersonate a real person.
Business Email Compromise Detection	Uses multi-factor spoof detection data and advanced contextual analysis for identifying messages that might exploit human nature to reveal confidential information. Tight integration with the inbox makes it possible to interact with the user to second-guess suspicious conversations--"Do you trust this sender?"
Page Emulation Analysis	Goes beyond domain reputation checks and file analysis by examining the pathway and resulting pages to look for phishing design and behavior.
URL rewriting and time-of-click analysis	Blocks malicious URLs before they are delivered to the user's inbox. It can disarm the URL, making it non-clickable. Then, it replaces the URL with a text warning ("embedded URL removed for security reasons") and redirects the link to the inspection service for time-of-click analysis protection.
Attachment Sandboxing	Blocks malicious email attachments from reaching your users 'inbox.
Post-delivery Protection	Retracts malicious messages, removing it from the user's inbox after initial delivery.
Post-detection Alerts	Alerts relevant personnel and products such as an admin, analyst, EDR or SIEM about potential compromises for remediation or recovery.
Forensic Analysis	Shows timeline of steps malware took as it detonated in the SonicWall Capture ATP sandbox. This exportable visualization of advanced malware forensics comes in the form of a bar chart with insights into process, registry, and Network/HTTP events.
Analytics	Monitor every action, including real-time and historical events, made in your SaaS environment.
Reporting Dashboard	CAS custom report queries are flexible, and context based. Search by sender, subject, recipient or attachment name speeds up the pace of a forensic search.
Email- native education opportunities	Automated emails alert end users to threats, provide key details into the malicious message, and provide a link to further reading about phishing attacks.

"We use SonicWall Cloud App Security in addition to O365 Email Security to ensure that as much spam and phishing as possible will be caught before getting to the end user. No system is 100%, but this one is pretty close."

— Tim Gustafson, System Administrator, PCES Corp.

SAAS SECURITY AND ADVANCED THREAT PROTECTION

Account Takeover & Insider Threats Protection	CAS analyzes every user event across multiple SaaS apps, comparing historical behavior, anomalous activity, and profiles of real-world breaches to identify attacks in real time.
Zero-day Malware Protection	Applies SonicWall Capture ATP multi-engine sandboxing to identify new malware variants within seconds and with fewer false positives. Quarantines all threats before users download them while preventing them from being stored and propagated through apps such as Box, Dropbox, OneDrive and G Drive.
Active Form Analysis	If the resulting page includes a form, CAS identifies look-alike content and malicious code. If a page looks like a Microsoft login but the form posts to an unrelated site, CAS prevents the link from reaching the inbox.
Shadow SaaS Monitoring	Identifies risky cloud applications your employees are using in the office or at home that have been connected to your approved SaaS accounts, without redirecting traffic or using a proxy.

DATA SECURITY

DLP and O365 Email Encryption Integration	Identifies confidential information and applies context-aware policies that confine the data to a particular organization or work group. Ensures PCI, HIPAA, PII, or other protected content does not leak.
Policy-based O365 Email Encryption	Automates the encryption of O365 cloud emails - whether sent internally or externally - without deploying new infrastructure, using the protocols you already know and trust. Enforces regulatory compliance across all your SaaS with cloud-aware, context-sensitive, policy workflows.
Data Classification	Automates the encryption of emails - whether sent internally or externally - without deploying new infrastructure, using the protocols you already know and trust.

COMPLIANCE

Compliance Templates	Reduce administrative overhead by using simple compliance templates to meet sensitive data protection requirements for SOX, PCI, HIPAA and GDPR.
Compliance Audit	Access historical event data for retrospective compliance auditing as well as real time reporting.
Compliance 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 lets us secure a Microsoft Office 365 E3 or F1 plan with SonicWall Advanced Threat Protection. It provides visibility for applications which are used in the company and additional data leakage prevention."

— Daniel Franz, Senior IT Architect at Data-Sec

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 sonicwall.com.

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

SONICWALL®

SolutionBrief-CASforOffice365-COG-5020