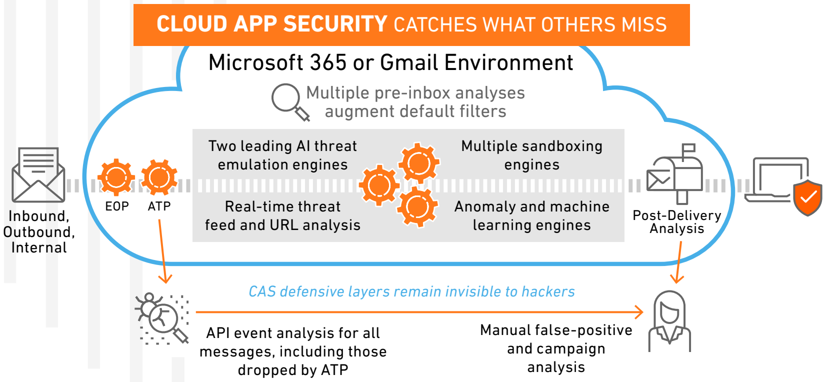
Cloud App Security

Comprehensive email and data protection for Microsoft 365 and Google Workspace

As an integral component of the SonicWall Capture Cloud Platform, the SonicWall Cloud App Security (CAS) extends a complete defense-in-depth security stack for Microsoft 365 and Google Workspace users. The CAS advantage rests primarily on its proven ability to stop low-volume, difficult targeted phishing, credential harvesting and zero-day attacks that bypass Microsoft, Google and conventional Secure Email Gateway (SEG) security filters.

CAS's API-based, multi-layered inline threat prevention system is invisible to hackers, providing highly effective email and data protection for cloud email and SaaS applications. The solution quickly deploys within minutes and employs a combination of machine learning (ML), artificial intelligence (AI) and big-data analyses to provide powerful anti-phishing, attachment sandboxing, click-time URL analysis, impersonation and data leakage protection (DLP).

CLOUD APP SECURITY CATCHES WHAT OTHERS MISS


Microsoft 365 or Gmail Environment
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
EOP
ATP
Inbound, Outbound, Internal
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

HIGHLIGHTS

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

Find the right SonicWall solution for your enterprise:

sonicwall.com/cas

DATASHEET

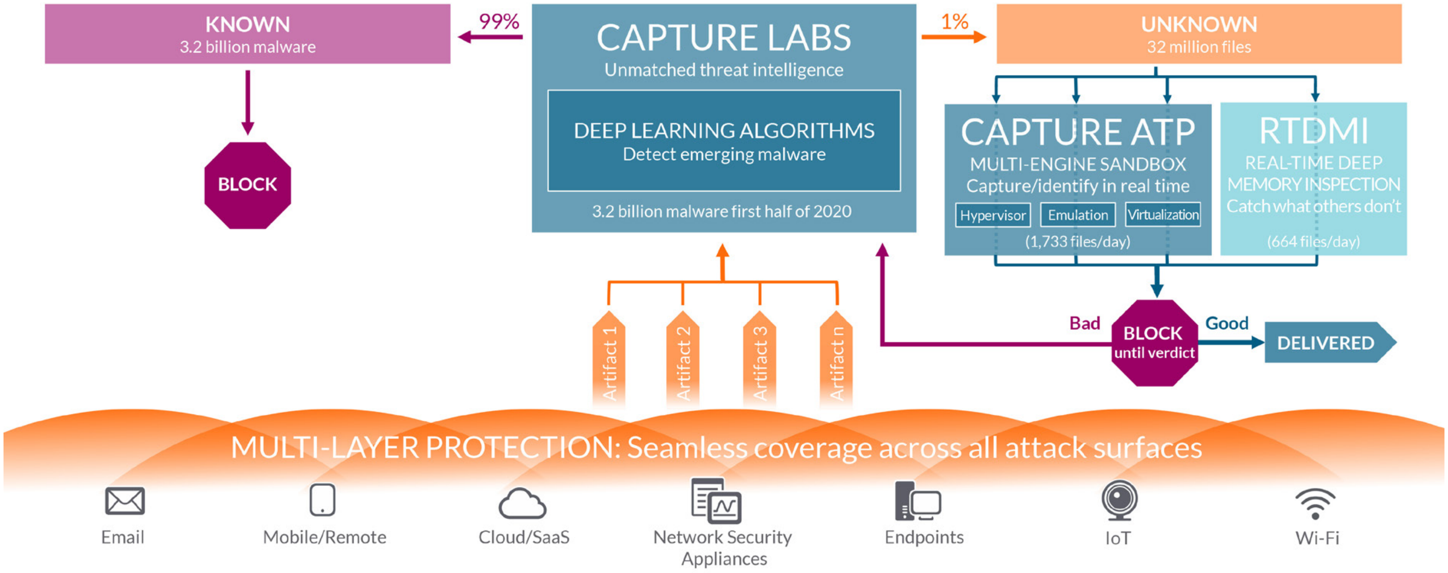
Scan All Email Traffic and Embedded Content

CAS works seamlessly with Microsoft 365 and Google Workspace security filters, such as Exchange Online Protection (EOP). It scans all messages and embedded content, including inbound, outbound and internal emails, detecting advanced phishing, credential harvesting and ransomware attacks bypassing preceding security filters.

When using inline protection, no email, links or attachments can reach the inbox until CAS scrutinizes and decides they are 100% harmless. Using multiple AI models and ML engines that constantly adapt to new phishing schemes, CAS prevents Business Email Compromise (BEC) and blocks targeted phishing, credential harvesting, malware, zero-days, account takeover (ATO) and insider threats with increased efficiency and reduced false positives. 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 or security analysts about potential compromises for post-delivery remediation or recovery measures.

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 immediately benefits all other parts of the defense ecosystem in real-time. The entire process significantly reduces the window of exposure and false positives.



Data Leakage Prevention and Compliance

CAS includes a SmartDLP engine that integrates with Microsoft Office 365 Message Encryption (OME) service to ensure **intellectual property, personal identifiable information (PII), and high-value data do not leave your organization** and out of the wrong hands. SmartDLP lets you establish detailed custom policy templates to control how data is shared and with whom it is shared. It scans over one hundred info-types that span more than 40 countries and supports data classifiers associated with HIPAA, SOX, PCI, GDPR and other international regulatory laws.

CAS Feature Summary

Email Protection

- In-line threat protection
- Policy-based configuration
- Multiple AI-based anomaly engines
- Machine-learning for anti-phishing
- Anti-spoofing
- Microsoft Office 365 EOP Anti-Spam augmentation
- Brand impersonation protection
- User impersonation detection
- Business Email Compromise 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 and insider threats protection
- Zero-day malware protection
- Active-form analysis
- Shadow SaaS Monitoring

Data Security

- Date leak protection
- Policy-based Office 365 message encryption
- Data classification

Compliance

- Compliance templates
- Audit-ready reports
- Compliance enforcement

Licensing and Packaging

SonicWall Cloud App Security	Basic	Advanced
Cloud App Licensed[1]	Office 365 or G Suite	Office 365 or G Suite, Box, Dropbox, Citrix ShareFile
ML-based Anti-Phishing	Yes	Yes
Business Email Compromise	Yes	Yes
Capture ATP* 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, Box, and Citrix ShareFile

[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

SonicWall Cloud App Security provides next-gen security for your users and data in the cloud.

sonicwall.com/cas

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 or follow us on Twitter, LinkedIn, Facebook and Instagram.

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

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. The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON- INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.