

SONICWALL CLOUD APP SECURITY



TRANSPARENZ



E-MAIL-SICHERHEIT DER NÄCHSTEN GENERATION



SCHUTZ VOR BEDROHUNGEN



DATEN-SICHERHEIT



COMPLIANCE



Erkennung von Cloud-Apps



Anti-Phishing



Schutz vor Zero-Day-Malware



Daten-Klassifizierung



Audit



Einblick in die Cloud-Nutzung



Anti-Spoofing



Schutz vor Konto-übernahme



Datenbasierte Zugriffskontrolle



Compliance-Templates



App-Risiko-bewertung



Sandboxing für Anhänge



Durchsetzung von Regeln



Ereignis-überwachung



Erweiterter URL-Schutz

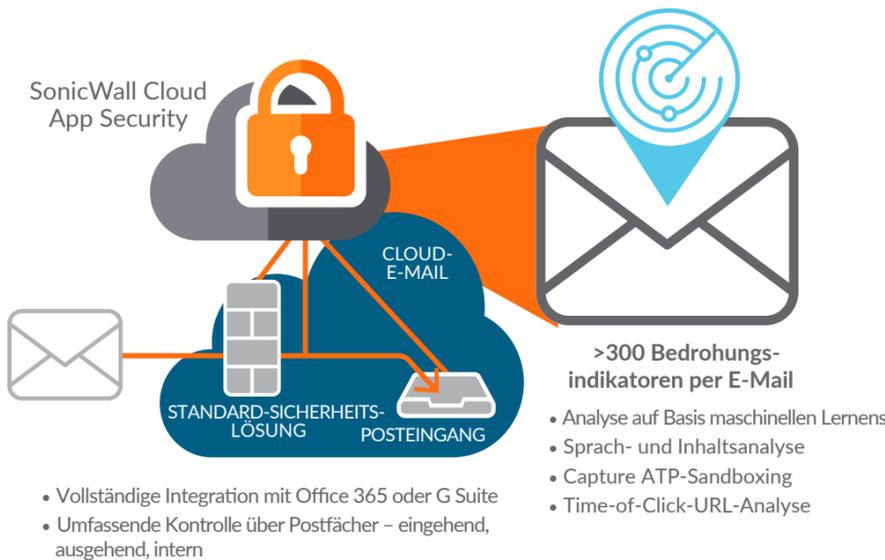
EMAILS SIND DER **BEDROHUNGSVEKTOR NR. 1**, WOBEI **ÜBER 90 %** DER CYBERANGRIFFE MIT EINER PHISHINGMAIL STARTEN - **VERIZON DBIR 2018**



E-MAIL-SICHERHEIT DER NÄCHSTEN GENERATION FÜR OFFICE 365 UND G SUITE



Da E-Mails sich zunehmend zur beliebtesten SaaS-App entwickeln, sind Anti-Phishing-Lösungen und E-Mail-Schutz extrem wichtig für die SaaS-Sicherheit.



SonicWall Cloud App Security bietet einen virtuellen integrierten Schutz, um zu verhindern, dass bösartige E-Mails, die von der Standard-Sicherheitslösung des Cloud-Service-providers nicht entdeckt werden, in Ihren Posteingang gelangen.

Laden Sie unser E-Book herunter: **Phishing im Zeitalter von SaaS**

BIS 2022 WERDEN MINDESTENS **95 % DER CLOUD-SECURITY-PROBLEME** AUF EIN VERSCHULDEN DES KUNDEN ZURÜCKZUFÜHREN SEIN - **GARTNER**



UMFASSENDE SICHERHEIT FÜR SAAS-ANWENDUNGEN (CASB)



Bei der Cloud-Sicherheit teilen sich Kunden und Provider die Verantwortung. Der Kunde ist dabei für die Datensicherheit und die Zugriffskontrolle für Dateien in SaaS-Anwendungen zuständig. Der Cloud-Serviceprovider ist nicht für unerlaubte Zugriffe und die Verbreitung von Malware verantwortlich.



SonicWall Cloud App Security prüft das System auf Zero-Day-Malware und setzt für in SaaS-Apps gespeicherte Daten Richtlinien rund um Compliance und den Schutz vor Datenlecks (Data Loss Prevention, DLP) durch.

Weitere Informationen: [SonicWall.com/CASB](https://www SonicWall.com/CASB)