# Kontrolle und Sicherheit für SaaS-Anwendungen

SaaS-Anwendungen – von Dropbox Business über Office 365 bis Salesforce.com – werden immer populärer, bergen aber neue Sicherheits- und Compliance-Risiken. Der «Cloud Access Security Broker» Aperture von Palo Alto Networks schafft Abhilfe.

Es ist bequem, cloudbasierte SaaS-Dienste zu nutzen, statt Software auf unternehmenseigenen Servern zu installieren und aufwendig zu warten. Entsprechend populär sind sie. Von der Datenablage mit den Business-Editionen von Dropbox, Google Drive und Co. über die Source-Code-Verwaltung mit Github bis hin zu Geschäftsanwendungen wie Salesforce.com: SaaS-Anwendungen sind nicht mehr wegzudenken.

So nützlich diese Services auch sind – sie bergen beträchtliche Risiken: SaaS-Anwendungen werden oft unkontrolliert an der IT-Abteilung vorbei direkt von den Fachabteilungen in Betrieb genommen. Sensible Daten liegen nicht mehr im Unternehmen, sondern weit verteilt bei verschiedenen Cloud-Anbietern. Oft fehlt gar den einzelnen Nutzern selbst der Überblick, welche Daten wo abgelegt sind. Für die bestehende IT-Sicherheitsarchitektur sind SaaS-Dienste und die damit verarbeiteten Daten nicht sichtbar. Zudem werden die in der firmeneigenen IT geltenden Regeln bei der SaaS-Nutzung umgangen. Und es besteht die Gefahr, dass durch unbedachten Datenaustausch Schadsoftware ins Unternehmensnetzwerk gelangt.


***Mit Aperture von Palo Alto Networks lassen sich SaaS-Applikationen und Dokumente in der Cloud umfassend schützen.***

### Aperture schärft den Blick auf SaaS-Anwendungen

Damit auch SaaS-Anwendungen sicher und regelkonform in die IT-Landschaft eingebettet sind, braucht es ein passendes Werkzeug. Die Marktforscher von Gartner bezeichnen entsprechende Tools als «Cloud Access Security Broker» – also als Vermittler für den sicheren Zugang zu cloudbasierten Diensten. Aperture von Palo Alto Networks erfüllt die dabei gestellten Anforderungen optimal.

Die Lösung gewährleistet die volle Visibilität über alle Aktivitäten rund um die Nutzer von SaaS-Diensten und die betroffenen Dateien und Verzeichnisse – während des gesamten Lebenszyklus eines SaaS-Benutzerkontos. Daraus ergibt sich ein kompletter Audit Trail für jeden User: Bis ins Detail wird klar, wer was wann und wie lange mit wem geteilt hat. Und es sind retrospektive Analysen möglich – egal ob die untersuchten Aktivitäten vor einer Stunde oder vor Jahren stattgefunden haben.

Aperture betrachtet überdies nicht nur die Zugriffe, sondern scannt und analysiert die Inhalte, die mit den SaaS-Diensten verarbeitet werden. Zudem klassifiziert Aperture die Dokumente automatisch. So lässt sich etwa erkennen, ob ein Dokument juristisch relevante Angaben oder Geschäftsgeheimnisse enthält und entsprechend behandelt werden muss. Die Vertraulichkeit der Daten bleibt dabei gewährleistet. Der Aperture-Administrator kann zwar aktiv nach Sicherheitsverletzungen suchen sowie automatische Alarmmeldungen definieren, hat jedoch keinen Zugriff auf die eigentlichen Dokumente. Wichtig: Der Scanvorgang lässt sich auf die europäischen Datenschutzgesetze abstimmen.

Bei der Beurteilung eines möglichen Sicherheitsproblems verschafft Aperture klare Erkenntnisse. Spekulieren gehört der Vergangenheit an. Das Unternehmen weiss genau, was zu jedem Zeitpunkt mit seinen Daten passiert ist, und erkennt rasch, wenn Compliance- und Datenschutzregeln verletzt werden. Aperture bietet zudem integrierten Malware-Schutz auf Basis der WildFire-Cloud von Palo Alto Networks.

### Universell einsetzbarer Cloud-Service

Als reiner Cloud-Dienst setzt Aperture keinerlei Änderungen am Unternehmensnetzwerk voraus, benötigt keine Softwareinstallation und ist für die Nutzer völlig transparent. Der Dienst kommuniziert direkt mit den SaaS-Lösungen und nutzt dabei die nativen APIs der einzelnen Anwendungen.

Aperture ergänzt die umfassende Sicherheitsplattform von Palo Alto Networks um die neue Dimension eines Cloud Access Security Brokers, lässt sich aber eigenständig auch in Umgebungen nutzen, wo keine weiteren Palo-Alto-Networks-Produkte im Einsatz stehen.

### Aperture: die Highlights

- Erlaubt es, SaaS-Anwendungen sicher und kontrolliert zu nutzen
- Komplette Visibilität über alle Aktivitäten rund um SaaS-Nutzer, Dateien und Verzeichnisse
- Retroaktive Analyse über den gesamten Lebenszyklus von SaaS-Benutzerkonten
- Liefert zeitnahe Erkenntnisse über Datenschutz- und Compliance-Verletzungen
- Granulare, kontextsensitive Überwachung und Durchsetzung von Unternehmensregeln
- Integrierter Schutz vor bekannter und unbekannter Malware

BOLL
IT Security Distribution

**BOLL Engineering AG**

Jurastrasse 58
5430 Wettingen

Tel. 056 437 60 60
info@boll.ch
www.boll.ch