



Führungskräfte möchten die Cloud nutzen und überlassen es Ihnen, **sie zu sichern.**

Zum Glück sind Sie damit nicht allein.

Wir haben 1.200 Entscheidungsträger für Cloud-Sicherheit zu den größten Herausforderungen befragt. Und das sind die Antworten.



13%

vertrauen Anbietern öffentlicher Clouds vollständig die Sicherheit vertraulicher Daten an.



34%

haben das Gefühl, dass die IT-Leiter die Risiken der öffentlichen Cloud vollständig verstehen.

Viele Unternehmen bekamen die Folgen bereits zu spüren.

23%

berichten über Datenverluste oder -kompromittierungen beim Cloud-Dienstanbieter.



20%

berichten über nicht autorisierten Zugriff auf ihre Daten/Services.



Es wird jedoch nicht viel getan, um die Clouds abzusichern.

43%

nutzen keine Verschlüsselung oder Malware-Schutz für die Server der privaten Cloud.



38%

nutzen IaaS ohne Verschlüsselung oder Malware-Schutz.

40%

schützen die in SaaS gespeicherten Dateien nicht mit Verschlüsselung oder Datenkompromittierungsschutz.

k6yBj1y0J
l9PsYoAv

Die meisten Unternehmen haben keinen Überblick über ihre gesamte Cloud-Infrastruktur.



Nur 35%

nutzen eine integrierte Sicherheitslösung.



Lernen Sie eine **effiziente** Möglichkeit zur Integration von **Cloud-Sicherheit** kennen.

Ungeachtet des Unbehagens unter den Sicherheitsexperten gibt es umfassende Sicherheitslösungen für die Hybrid-Cloud. Aufgrund der unausweichlichen Migration von Geschäftsdiensten zu Cloud-Bereitstellungsmodellen müssen sich Sicherheitsarchitekten mit innovativen Sicherheitstechnologien vertraut machen, die Transparenz und Sicherheitsverwaltung für alle Clouds vereinen.



Gesamten Bericht herunterladen.

Erfahren Sie im Bericht *Blauer Himmel oder dunkle Wolken? Der Stand der Dinge bei der Migration zur Cloud* mehr darüber, wie 1.200 IT-Sicherheitsexperten aus aller Welt die Sicherheit ihrer Clouds gestalten wollen.

www.intelsecurity.com/hybridcloudsecurity

