



# Vertraulichkeit und Datenschutz in Microsoft OneDrive

OneDrive ist eine Cloud-basierte Speicherplattform, die von Microsoft angeboten wird. Betrachten Sie es als eine Festplatte in der Cloud, auf der Sie Ihre Daten speichern können. Im Gegensatz zu einem lokalen Speicher können Sie bequem von praktisch jedem Gerät - Desktop, Smartphone, Tablet - und von überall über das Internet auf Ihre Daten zugreifen. Daten, die in der Cloud gespeichert werden, sind größeren Risiken ausgesetzt und müssen daher besonders geschützt werden. Die clientseitige Verschlüsselung ist ein praktikabler Schutz, der gewährleisten kann, dass die Daten sicher sind, selbst wenn sie in gehosteten Umgebungen wie OneDrive in der Microsoft Cloud gespeichert sind.

## Wie können Sie Daten mit conpal LAN Crypt schützen?

conpal LAN Crypt ist eine client-seitige Verschlüsselungslösung, die Verschlüsselung auf Dateiebene bietet. Die leistungsstarke Schlüssel- und Richtlinienverwaltung unterstützt die Verschlüsselung von Daten mit unterschiedlichen Schlüsseln für geschäftliche, persönliche und gemeinsame Daten. Die Ver- und Entschlüsselung findet auf dem lokalen Gerät statt. Somit sind die Daten auf dem lokalen Rechner, beim Verlassen des Clients und bei der Übertragung geschützt. Weder Microsoft noch andere Personen haben Zugriff auf die Klartextdaten oder den zur Verschlüsselung verwendeten Schlüssel. conpal LAN Crypt hilft Unternehmen, ihre Daten auch in Cloud-Umgebungen sicher und vertraulich zu halten.

### Schutz aktivieren

**1** **DEFINIEREN SIE, WELCHE TEAMS ODER CHANNELS SIE SCHÜTZEN**  
Definieren Sie in der Admin-Konsole von conpal LAN Crypt eine Verschlüsselungsregel für OneDrive. Eine einzige Regel mit dem <OneDrive>-Platzhalter reicht aus, um zu gewährleisten, dass sämtliche in OneDrive hochgeladenen Daten verschlüsselt sind. Definieren Sie zusätzliche Regeln, wenn eine feingliedrigere Kontrolle erforderlich ist. Sollten Sie mit dem Resultat nicht zufrieden sein, können Sie jederzeit die geschützten Bereiche nachjustieren, um sie so weiter Ihren Bedürfnissen anzupassen.



**2** **AKTIVIERUNG DER POLICY**  
Vergewissern Sie sich auf Ihrem Client, dass der conpal-LAN-Crypt-Client installiert ist. Sie können dies ganz einfach tun, indem Sie die App auf Ihrem Handy, das App-Symbol im Benachrichtigungsfeld (Windows) oder in der Menüleiste (MacOS) suchen. Aktualisieren Sie nun die Policy. Sämtliche Daten, welche Sie in Ihrem lokalen Sync-Ordner erstellen, werden nun automatisch verschlüsselt.



### Upload auf OneDrive

**3** **VERBINDUNG MIT ONEDRIVE**  
Vergewissern Sie sich auf Ihrem Client, dass der Microsoft-OneDrive-Client installiert ist. Dies ist schnell möglich, indem Sie nach dem App-Symbol in Benachrichtigungsfeld (Windows) oder der Menüleiste (MacOS) suchen. Melden Sie sich bei Ihrem OneDrive-Konto an und starten Sie den Upload. Fertig – Sie können loslegen.



### Access Anywhere

**4** **WINDOWS ODER MACOS**  
Verwenden Sie Ihren lokalen Sync-Ordner, um auf Ihre in OneDrive gespeicherten Daten zuzugreifen. Ver- und Entschlüsselung erfolgen on-the-fly im Hintergrund. Die Daten werden verschlüsselt, bevor sie in der Cloud gespeichert werden. Dokumente können auch dann geteilt werden, wenn sie verschlüsselt sind. Beachten Sie jedoch, dass derjenige, mit dem Sie das jeweilige Dokument teilen möchten, ebenfalls Zugriff auf den entsprechenden Verschlüsselungs-Key benötigt.



**5** **SMARTPHONE ODER TABLET**  
Die App von conpal LAN Crypt erlaubt Ihnen das Öffnen von verschlüsselten Dateien, welche via OneDrive gespeichert wurden. Starten Sie die App und navigieren Sie durch Ihre Ordner. Dateien können mit der conpal-LAN-Crypt-App oder direkt aus der Teams-App heraus geöffnet werden. Verschlüsselte Dateien werden entschlüsselt, bevor sie angezeigt werden. Die Verschlüsselung erfolgt lokal innerhalb der App, um die Vertraulichkeit Ihrer Daten zu gewährleisten.

