Schatten-IT neu gedacht: Moderne Abwehr mit Defender

Noah Schulz

claranet | Make modern happen®

PUBLIC
Verantwortlich: Claranet GmbH
Version 1.0 – 03.07.2025

Agenda

- Einführung: Schatten-IT – das unterschätzte Risiko
- Angriffsszenario aus dem Alltag
- Analyse: Wo klassische Schutzmechanismen versagen
- Verteidigung mit Microsoft Defender & Co.
- Best Practices & Empfehlungen

claranet | Make modern happen®

Einführung: Schatten-IT – das unsichtbare Risiko

„Ein Mitarbeiter lädt eine Scanner-App aus dem App Store herunter. Sie verspricht, Dokumente direkt in OneDrive zu speichern. Praktisch – aber was er nicht weiß: Die App liest auch seine Outlook-Kontakte aus und sendet sie an einen Server in Übersee.“

Definition & Relevanz:

- Was ist Schatten-IT?
- Warum ist sie in Cloud-Umgebungen besonders gefährlich?

Bedrohungsszenario: Die harmlose App mit bösen Absichten

- **Drittanbieter-App mit OAuth-Zugriff auf:**
  - OneDrive (Lesen/Schreiben)
  - Outlook (Kalender, Kontakte)

- **Kein klassischer Schadcode → Umgehung von AV & EDR**
- **Datenexfiltration über legitime API-Aufrufe**

- **Risiken:**
  - Keine Alarmierung durch klassische Sicherheitslösungen
  - Compliance-Verstöße (DSGVO, ISO 27001 etc.)
  - Reputationsschäden

Warum herkömmliche Schutzmechanismen versagen

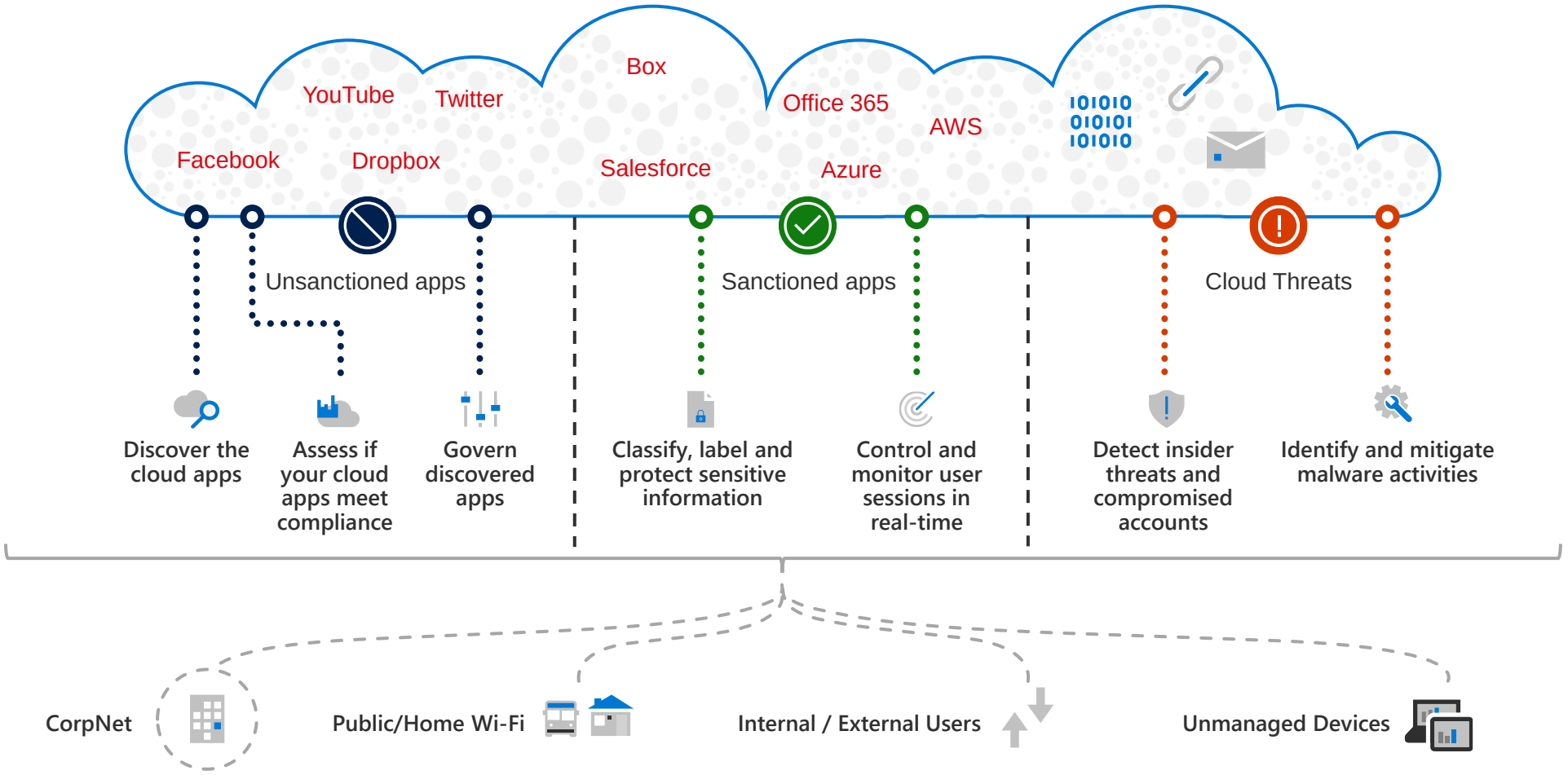
- Kein Malware-Verhalten → kein Antivirus-Alarm
- Kein klassischer Angriff → keine Signatur
- Keine Benutzerbeschwerde → keine Awareness
- App greift nur auf „eigene“ Daten des Users zu → scheinbar legitim

Microsoft Defender: Schutzmechanismen im Überblick

Tool	Funktion	Lizenz
Defender for Cloud Apps	App-Discovery, OAuth-Überwachung, Session Control	E5 / E3 + E5 Security
Defender for Office 365	Schutz vor Phishing, App-Zugriffsüberwachung	E5 / E3 + E5 Security
Microsoft Purview (DLP)	Datenklassifizierung, Richtlinien für Datenabfluss	E5 / E3 + E5 Compliance

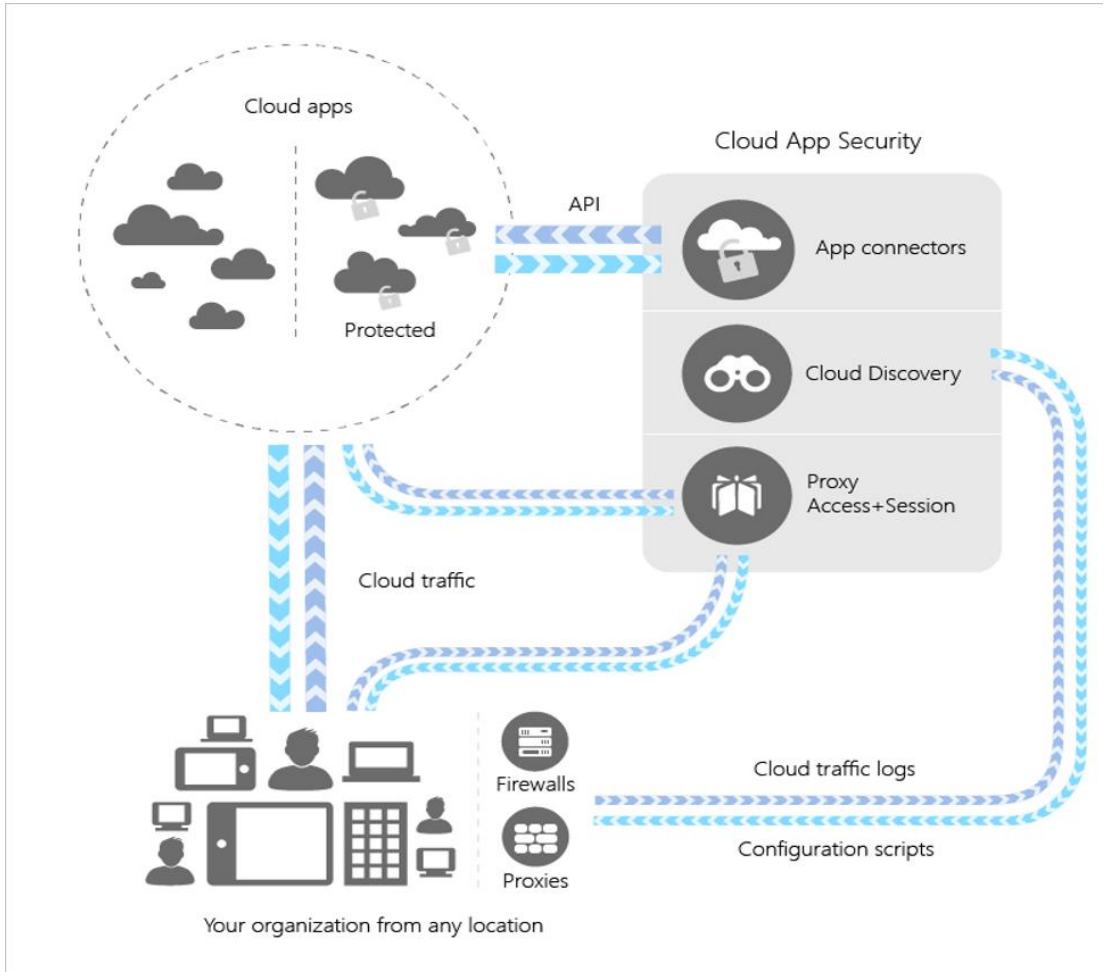
claranet | Make modern happen®

Defender for Cloud Apps



Defender for Cloud Apps

Shadow IT Discovery – Auffinden und Verwalten von Cloud-Anwendungen
Information Protection – Schutz von Informationen während ihrer Übertragung
Threat Protection – Erkennung ungewöhnlichen Verhaltens
Compliance Assessment – Bewertung im Hinblick auf regulatorische Anforderungen

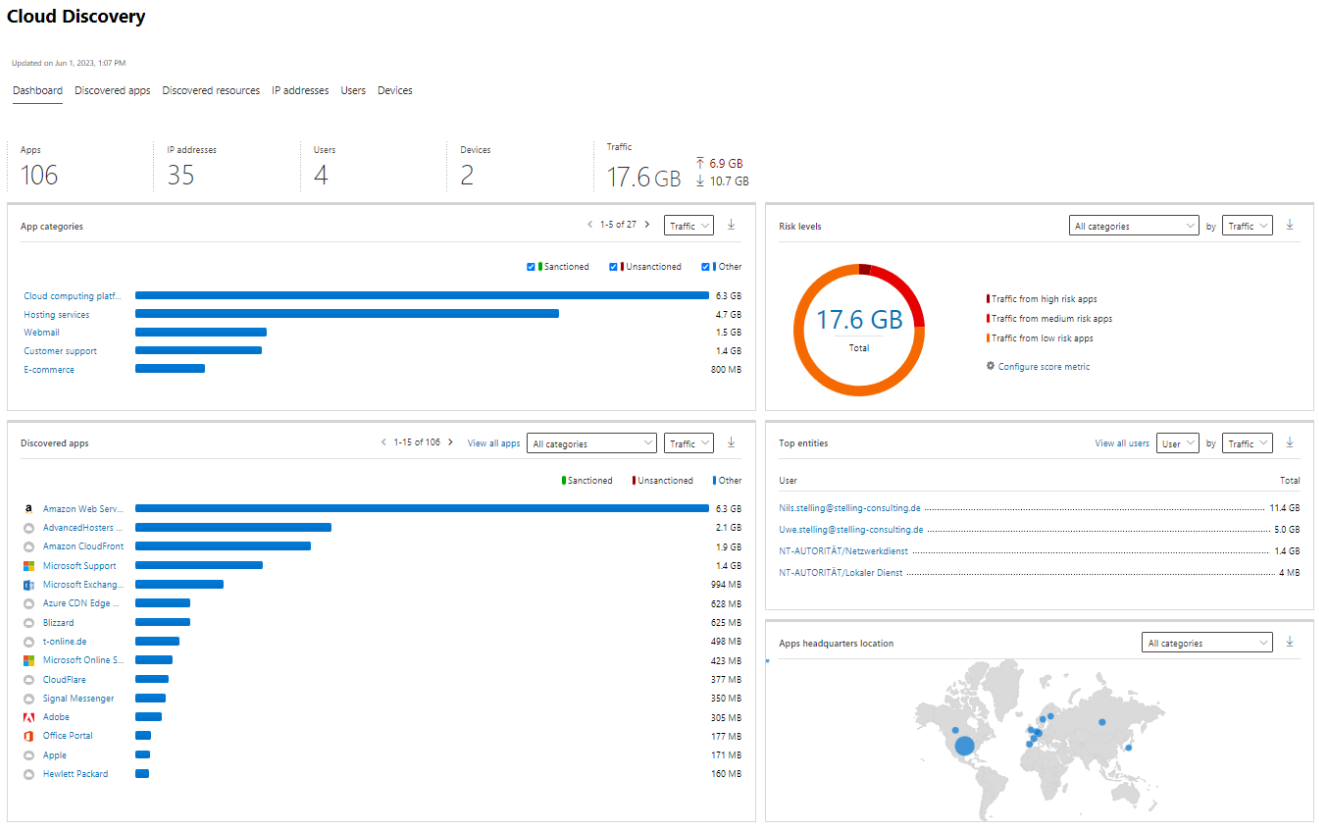


claranet | Make modern happen®

Cloud Discovery

Datenquellen für Cloud Discovery

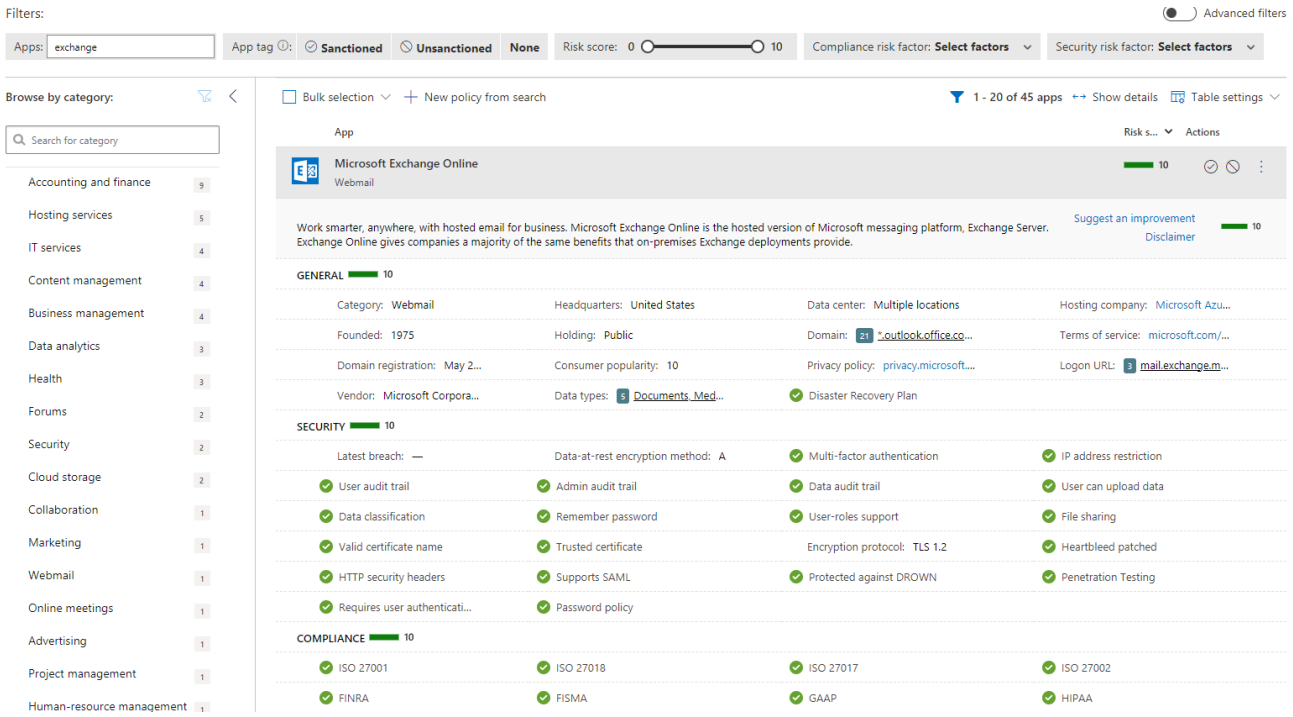
- Cloud Discovery verwendet Ihre Datenverkehrsprotokolle
- Ermittelt und analysiert Cloud-Apps in Ihrer Organisation
- Protokolldateien aus Firewalls sammeln
- Protokolldateien aus Vertretungen sammeln
- Integration mit Microsoft Defender für Endpunkt



claranet | Make modern happen®

Cloud App Catalog

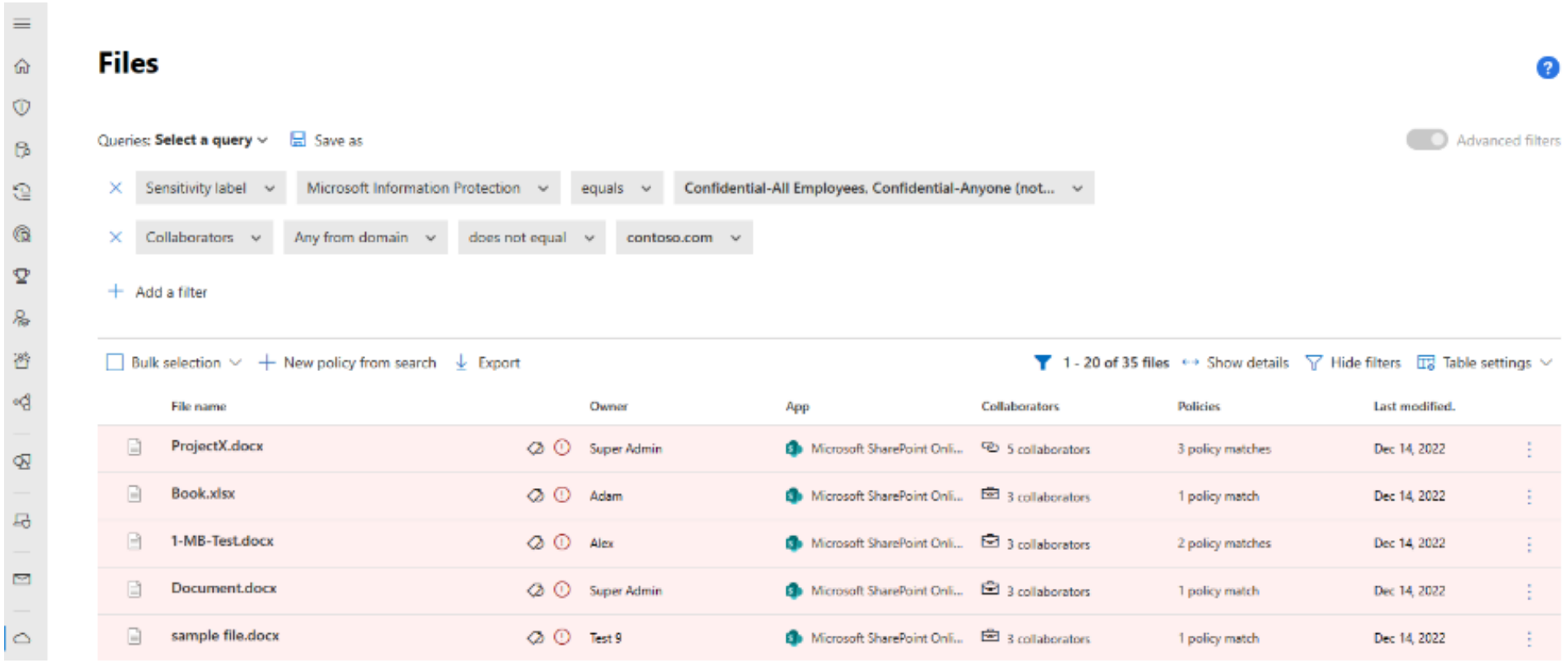
- Mehr als 31.000 Web Applikationen bewertet
- Berücksichtig werden mehr als 90 Kriterien
- Einstufung von 0 bis 10



claranet | Make modern happen®

Arbeiten mit sensiblen Daten

Integration in Purview ermöglich Erkennung, wer mit sensiblen Daten arbeitet.



Konnektoren

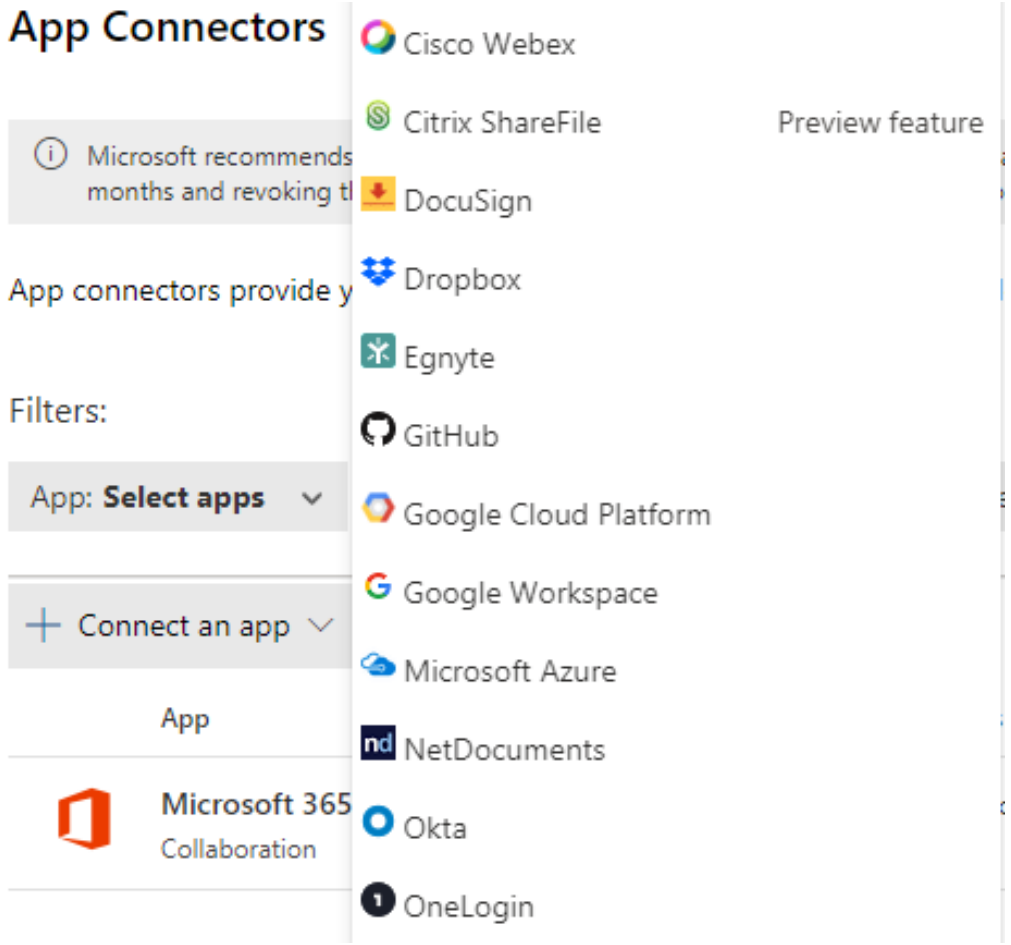
- Verbindung zur API, die vom App-Ersteller bereitgestellt wird.
- Die angebotenen Dienste variieren je nach App.

Gängige Einschränkungen von Connector-APIs:

- Drosselung (Throttling)
- API-Grenzwerte
- Dynamische Zeitverschiebung
- API-Zeitfenster

Ermöglicht eine bessere Transparenz in Bezug auf die Apps.

- **Alle Kommunikation erfolgt über sicheres HTTPS.**



claranet | Make modern happen®

Best Practices & Empfehlungen

- **App-Governance etablieren:** Nur geprüfte Apps zulassen
- **OAuth-Überwachung aktivieren:** Defender for Cloud Apps nutzen
- **DLP-Richtlinien definieren:** Besonders für OneDrive, SharePoint, Exchange
- **Awareness schaffen:** Mitarbeitende sensibilisieren
- **Zero Trust Prinzipien anwenden**

Fazit & Q&A

Kernaussagen:

- Schatten-IT ist kein hypothetisches Risiko – sie ist Realität.
- Microsoft Defender bietet starke Werkzeuge, um diese Risiken zu erkennen und zu minimieren.
- Sicherheit beginnt mit Transparenz – und endet mit klaren Richtlinien.

claranet | Make modern happen®

PUBLIC
Verantwortlich: Claranet GmbH
Version 1.0 – 03.07.2025