



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

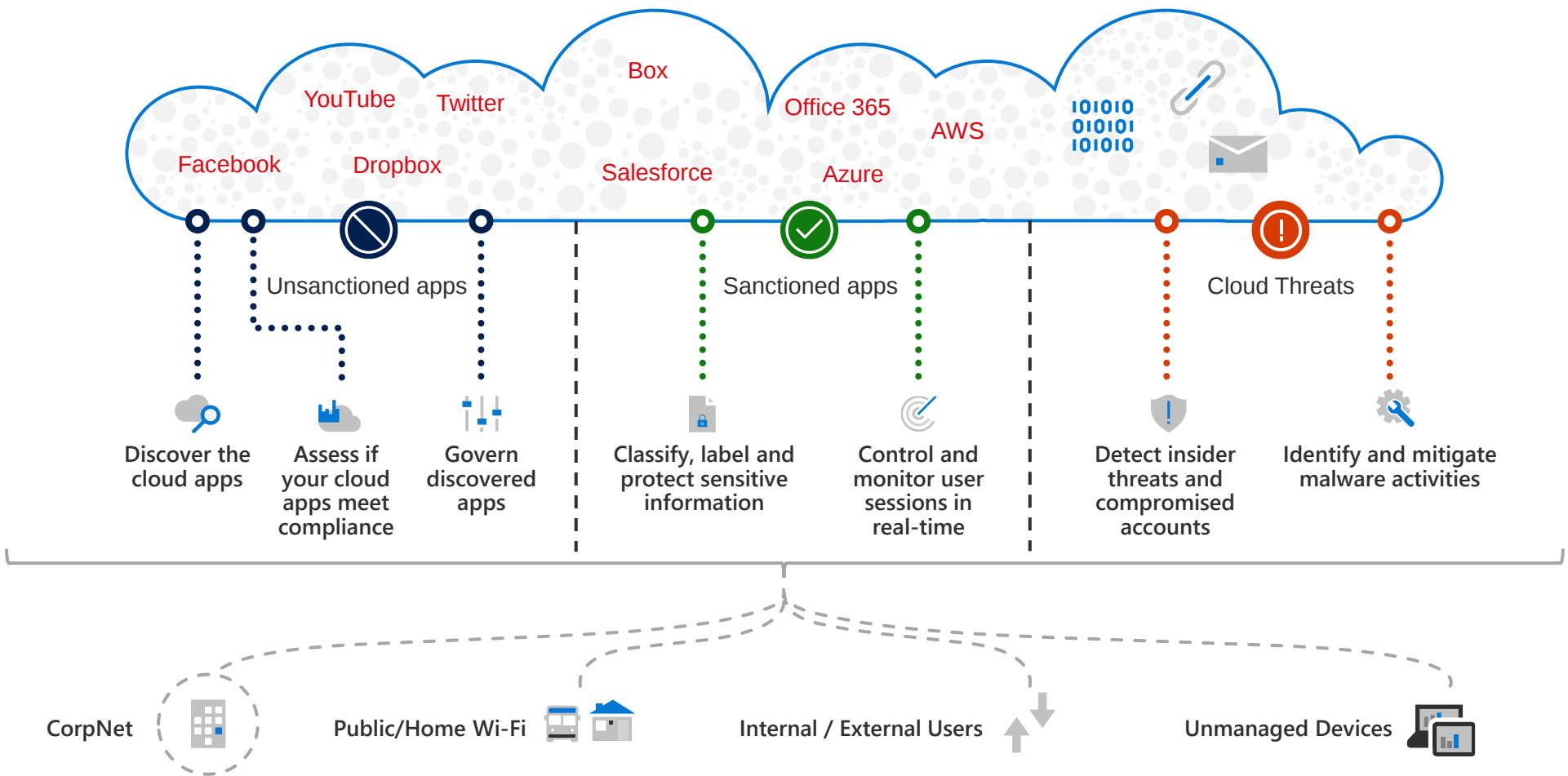
Warum herkömmliche Schutzmechanismen versagen

- **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

Defender for Cloud Apps



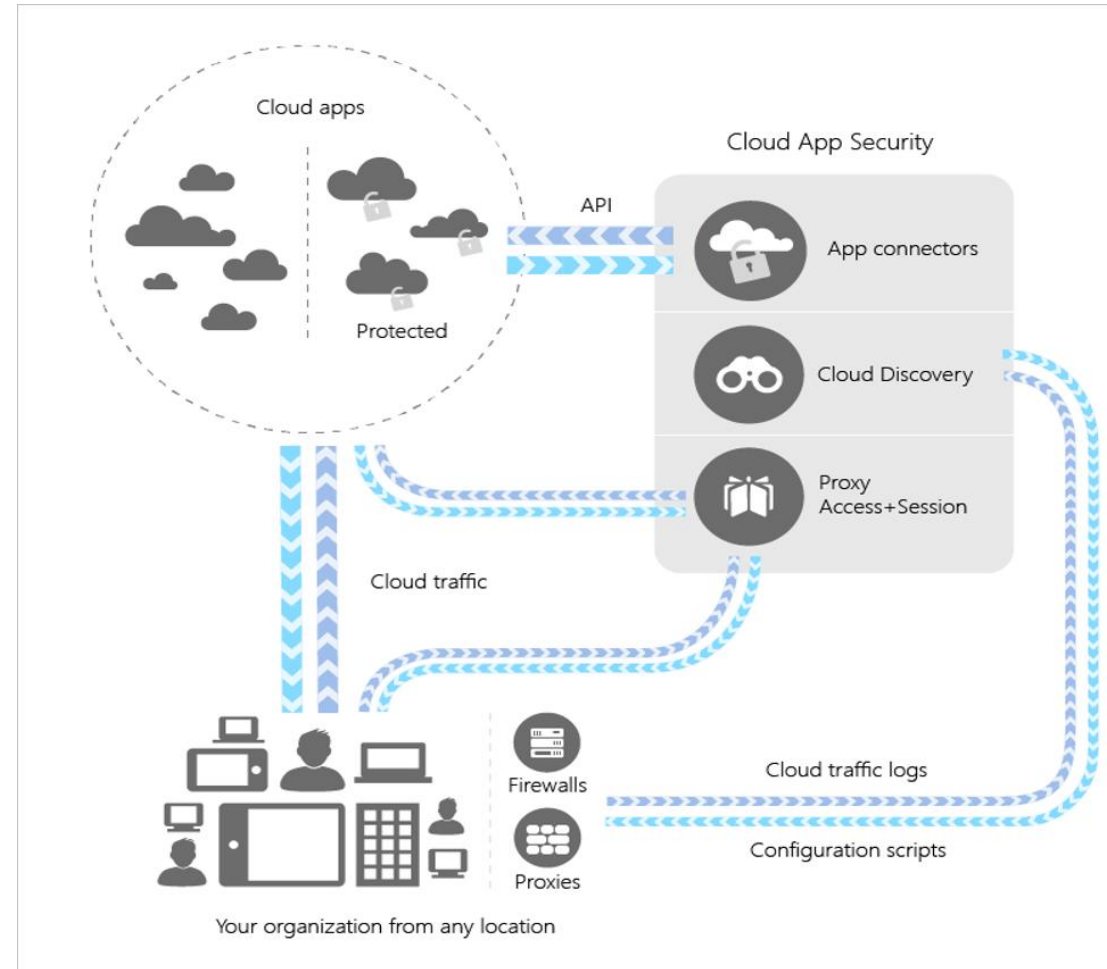
Defender for Cloud Apps

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



Cloud Discovery

Datenquellen für Cloud Discovery

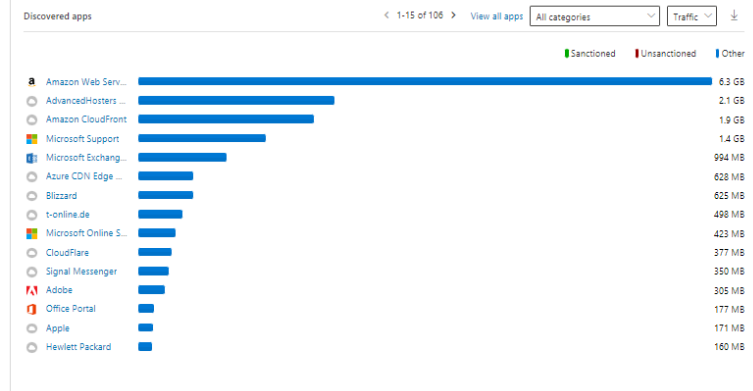
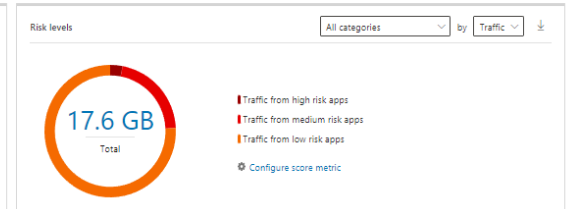
- Cloud Discovery verwendet Ihre Datenverkehrsprotokolle
- Ermittelt und analysiert Cloud-Apps in Ihrer Organisation
- Protokolldateien aus Firewalls sammeln
- Protokolldateien aus Vertretungen sammeln
- Integration mit Microsoft Defender für Endpunkt

Cloud Discovery

Updated on Jun 1, 2023, 1:07 PM

Dashboard Discovered apps Discovered resources IP addresses Users Devices

Apps 106 IP addresses 35 Users 4 Devices 2 Traffic 17.6 GB $\mp$ 6.9 GB $\pm$ 10.7 GB



Top entities View all users User by Traffic

User	Total
Nils.stelling@steling-consulting.de	11.4 GB
Uwe.stelling@steling-consulting.de	5.0 GB
NT-AUTORITÄT/Netzwerkdienst	1.4 GB
NT-AUTORITÄT/Lokaler Dienst	4 MB



Cloud App Catalog

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

Filters: App tag: ☒ Sanctioned ☒ Unsanctioned ☐ None Risk score: 10 Compliance risk factor: **Select factors** Security risk factor: **Select factors** ☐ Advanced filters

Browse by category:

- Accounting and finance 9
- Hosting services 5
- IT services 4
- Content management 4
- Business management 4
- Data analytics 3
- Health 3
- Forums 2
- Security 2
- Cloud storage 2
- Collaboration 1
- Marketing 1
- Webmail 1
- Online meetings 1
- Advertising 1
- Project management 1
- Human-resource management 1

Microsoft Exchange Online Webmail 10 ☐ ☐ ☐

Work smarter, anywhere, with hosted email for business. Microsoft Exchange Online is the hosted version of Microsoft messaging platform, Exchange Server. Exchange Online gives companies a majority of the same benefits that on-premises Exchange deployments provide. [Suggest an improvement](#) [Disclaimer](#) 10

GENERAL 10

Category: Webmail	Headquarters: United States	Data center: Multiple locations	Hosting company: Microsoft Azu...
Founded: 1975	Holding: Public	Domain: outlook.office.co...	Terms of service: microsoft.com/...
Domain registration: May 2...	Consumer popularity: 10	Privacy policy: privacy.microsoft...	Login URL: mailexchange.m...
Vendor: Microsoft Corpora...	Data types: Documents, Med...	Disaster Recovery Plan	

SECURITY 10

Latest breach: —	Data-at-rest encryption method: A	Multi-factor authentication	IP address restriction
User audit trail	Admin audit trail	Data audit trail	User can upload data
Data classification	Remember password	User-roles support	File sharing
Valid certificate name	Trusted certificate	Encryption protocol: TLS 1.2	Heartbleed patched
HTTP security headers	Supports SAML	Protected against DROWN	Penetration Testing
Requires user authenticati...	Password policy		

COMPLIANCE 10

ISO 27001	ISO 27018	ISO 27017	ISO 27002
FINRA	FISMA	GAAP	HIPAA

Arbeiten mit sensiblen Daten

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

Files

Queries: **Select a query**  Save as

×

Sensitivity label

▼

Microsoft Information Protection

▼

equals

▼

Confidential-All Employees, Confidential-Anyone (not...

▼

×

Collaborators

▼

Any from domain

▼

does not equal

▼

contoso.com

▼

+ Add a filter

☐ Bulk selection

+

New policy from search

↓

Export

1 - 20 of 35 files

↔ Show details

⌵ Hide filters

⌚ Table settings

▼

File name	Owner	App	Collaborators	Policies	Last modified
 ProjectX.docx	  Super Admin	 Microsoft SharePoint Onli...	 5 collaborators	3 policy matches	Dec 14, 2022 
 Book.xlsx	  Adam	 Microsoft SharePoint Onli...	 3 collaborators	1 policy match	Dec 14, 2022 
 1-MB-Test.docx	  Alex	 Microsoft SharePoint Onli...	 3 collaborators	2 policy matches	Dec 14, 2022 
 Document.docx	  Super Admin	 Microsoft SharePoint Onli...	 3 collaborators	1 policy match	Dec 14, 2022 
 sample file.docx	  Test 9	 Microsoft SharePoint Onli...	 3 collaborators	1 policy match	Dec 14, 2022 

Konnektoren

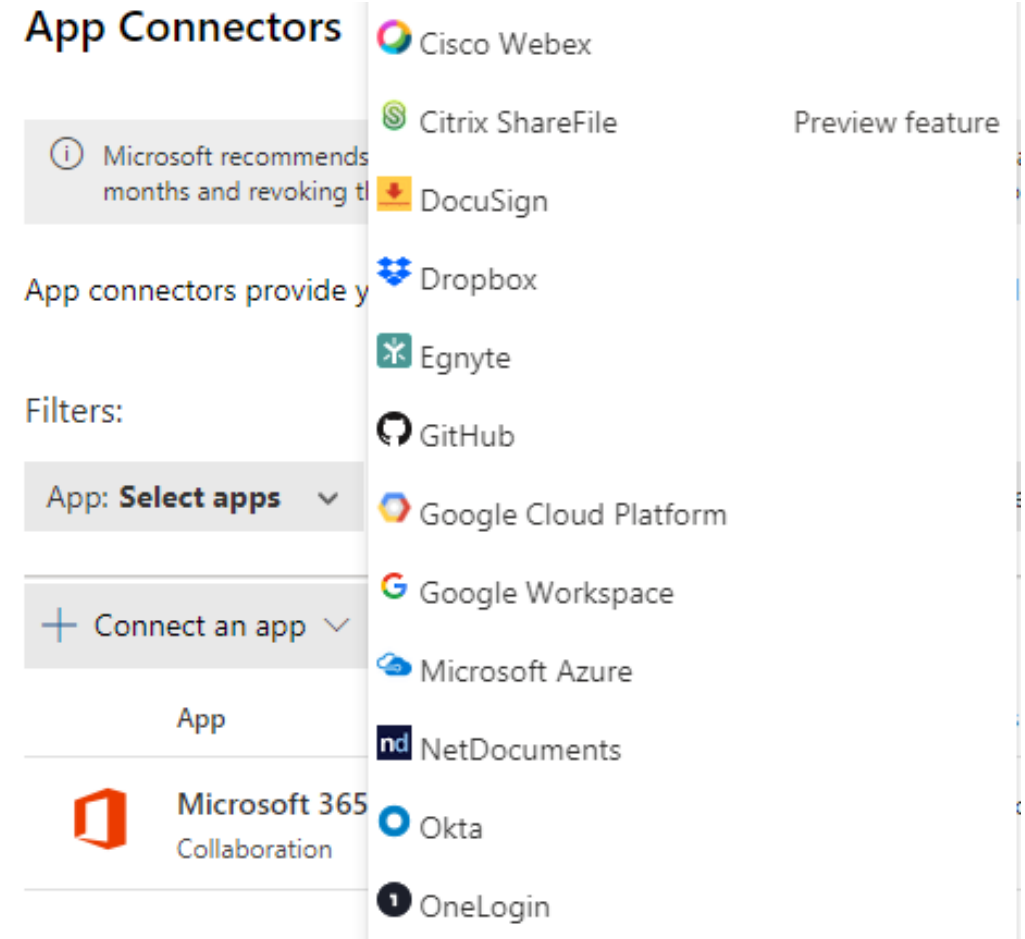
- Verbindung zur API, die vom App-Ersteller bereitgestellt wird.
- Die angebotenen Dienste variieren je nach App.

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.**



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.

