

Logicalis Security Assessment

Cloud Protection Assessment

Volle Transparenz über Cloud- und SaaS-Nutzung, Web-Bedrohungen und Zugriffswege – in 30 Tagen.

Das Risiko: Der Perimeter liegt nicht mehr im Rechenzentrum

Anwender arbeiten hybrid, Anwendungen liegen in der Cloud – der Datenverkehr verlässt Ihr Netzwerk längst direkt ins Internet. Klassische Perimeter-Firewalls, VPN-Backhauling und getrennte Sicherheitssilos sehen davon nur noch einen Bruchteil.

Die Folge: unbekannte SaaS-Dienste im Fachbereich, ungeprüfter verschlüsselter Traffic, überprivilegierte VPN-Zugänge und fehlende Nachweise für NIS2 und Audits. Ein Security Service Edge (SSE) schließt diese Lücke – aber nur, wenn Sie zuerst wissen, was tatsächlich passiert.

Unser Ansatz: 3 Stufen zu voller Transparenz

1

DNS-Security & App-Discovery

Externe DNS-Anfragen werden an Cisco Secure Access weitergeleitet – sofortige Sichtbarkeit über genutzte Cloud-Dienste, Shadow-IT und riskante Domains. Kein Eingriff in den Betrieb.

2

Secure Web Gateway & CASB

Ausgewählter Unternehmens-Traffic wird geroutet – App-Risk-Scoring, Web-Kategorien, Datenvolumen je Dienst sowie Bedrohungserkennung über Cisco Talos.

3

Deep Inspection, DLP & ZTNA

SSL-Entschlüsselung, Data-Loss-Prevention und Analyse der Zugriffswege auf private Anwendungen – inkl. Bewertung des Ablösepotenzials für bestehendes VPN.

Ihr Nutzen: 3 konkrete Reports

- ✓ **Cloud & SaaS Visibility Report** – welche Cloud- und SaaS-Dienste tatsächlich genutzt werden, von welchen Abteilungen, in welchem Datenvolumen und mit welchem Risk-Score – genehmigt vs. Shadow-IT.
- ✓ **Web- & Threat-Risk-Analyse** – blockierte und potenziell schädliche Verbindungen, Command-&-Control-Kommunikation, Phishing- und Malware-Domains sowie riskante Web-Kategorien auf Basis von Cisco Talos.
- ✓ **Zero-Trust- & Access-Readiness-Analyse** – welche privaten Anwendungen über VPN erreichbar sind, wo überprivilegierte Zugriffe bestehen und welche Daten die Organisation über Web- und Cloud-Kanäle verlassen.

Aufwand & Ablauf

Ca. 8 Personentage über 2–3 Wochen • 30-Tage-Testlizenz Cisco Secure Access inklusive • minimaler Aufwand für Ihr Team, kein Eingriff in den produktiven Betrieb.

Cisco Global Gold Partner • 7.500+ Architects of Change in über 30 Ländern • 10.000+ Kunden weltweit

Interesse? Lassen Sie uns sprechen.

Vereinbaren Sie einen unverbindlichen Termin für ein kostenfreies Erstgespräch.

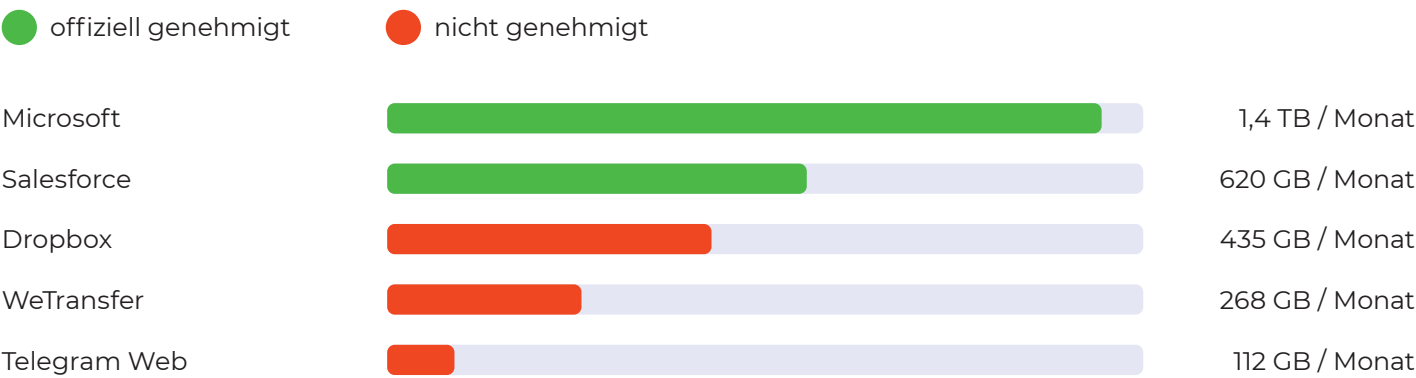
Arun Wadhawan • arun.wadhawan@logicalis.de • +49 1522 2516 526 • www.logicalis.de

So sieht Ihre Auswertung aus

Auszug aus dem Cloud & SaaS Visibility Report – inkl. Shadow-IT-Funden, Bedrohungslage und Zero-Trust-Bewertung

Beispielhafte Darstellung mit fiktiven Werten zur Veranschaulichung. Ihre Auswertung basiert ausschließlich auf den tatsächlich in Ihrem Unternehmen erhobenen Daten.

1 Genutzte Cloud- & SaaS-Dienste (Beispiel)



2 Web- & Threat-Risk-Analyse – Top-Funde (Beispiel)

BEFUND	BETROFFENER BEREICH	EREIGNISSE	RISIKO
Command- & Control-Kommunikation	Client-Netz Standort Nord	17	HOCH
Phishing- & Credential-Harvesting-Domains	Unternehmensweit	284	HOCH
Uploads in nicht genehmigte Filesharing-Dienste	Vertrieb, Projektmanagement	1.106	MITTEL
Neu registrierte Domains (< 30 Tage)	Unternehmensweit	512	MITTEL
Ungeprüfter verschlüsselter Traffic (kein SSL-Insp.)	Remote-Nutzer	38 %	MITTEL

3 Zero-Trust- & DLP-Analyse (Beispiel)

41 private Anwendungen über pauschalen VPN-Zugriff erreichbar

Davon 12 Anwendungen mit Zugriff für Nutzergruppen ohne fachlichen Bedarf. Zusätzlich wurden 23 Datei-Uploads mit potenziell sensiblen Inhalten (Kundendaten, Vertragsdokumente, interner Quellcode) an nicht genehmigte Cloud-Dienste identifiziert. Ablösepotenzial VPN → ZTNA: hoch.

Ihr vollständiger Report schafft eine belastbare Entscheidungsgrundlage.

Am Ende erhalten Sie den vollständigen Report inkl. Handlungsempfehlungen für Governance, DLP, SSE-Architektur und eine schrittweise Migration von VPN zu Zero Trust Network Access.

Arun Wadhawan • arun.wadhawan@logicalis.de • +49 1522 2516 526 • www.logicalis.de