Rundum-Schutz für’s Netzwerk: LANCOM Trusted Access Client für macOS verfügbar

30.04.2025

Der deutsche Netzwerkinfrastruktur- und Security-Lösungsanbieter LANCOM Systems erweitert seine Cloud-verwaltete Remote-Access-Lösung um den LANCOM Trusted Access Client für macOS. Somit können auch Verwender von Apple-Endgeräten die Vorteile der vertrauenswürdigen und sicheren Cloud-managed Secure Network Access-Lösung nutzen.

Pressemitteilung 2025-740

Cloud-managed Remote Network Access für sicheres hybrides Arbeiten

Rundum-Schutz für’s Netzwerk: LANCOM Trusted Access Client für macOS verfügbar

Aachen, 30. April 2025 – Der deutsche Netzwerkinfrastruktur- und Security-Lösungsanbieter LANCOM Systems erweitert seine Cloud-verwaltete Remote-Access-Lösung um den LANCOM Trusted Access Client für macOS. Somit können auch Verwender von Apple-Endgeräten die Vorteile der vertrauenswürdigen und sicheren Cloud-managed Secure Network Access-Lösung nutzen.

Der LANCOM Trusted Access Client ist die vertrauenswürdige Network Access Security-Lösung für Unternehmensnetzwerke. Er ermöglicht einen sicheren und skalierenden Zugriff auf Unternehmensanwendungen für Mitarbeitende im Büro, zu Hause oder unterwegs und schützt damit modernes hybrides Arbeiten von überall und jederzeit. Die LANCOM Trusted Access-Lösung passt sich an steigende Sicherheitsanforderungen in Unternehmen an und ermöglicht sowohl Cloud-managed VPN-Client-Vernetzung für den Zugriff auf ganze Netze als auch den Umstieg auf eine Zero-Trust-Sicherheitsarchitektur für größtmögliche Netzwerksicherheit. Dabei erhalten Benutzer auf Basis granularer Zugriffsrechte ausschließlich Zugangsberechtigung zu Anwendungen, die ihnen zugewiesen wurden (Zero-Trust-Prinzip). Bestehende Systeme zur Verwaltung von Benutzern und Benutzergruppen

(Active Directory) lassen sich vollständig in die LANCOM Management Cloud (LMC) integrieren. Für kleinere Netzwerke bietet die LMC alternativ eine interne Benutzerverwaltung.

LANCOM Trusted Access ist DSGVO-konform und flexibel skalierbar – für kleine Gewerbebetriebe bis hin zu großen Enterprise-Kunden. Je Netzwerk-Teilnehmer werden bis zu drei Endgeräte unterstützt.

Granulare Zugriffskontrolle nach dem Zero-Trust-Prinzip

Mit einer Zugriffsvergabe nach dem Zero-Trust-Prinzip „so viel wie nötig, so wenig wie möglich“ schützt der LANCOM Trusted Access Client Netzwerke vor Bedrohungen und deren Ausbreitung. Das bedeutet: Kein blindes Vertrauen auf Basis eines erfolgreichen Netzwerkzugangs. Der LANCOM Trusted Access Client verifiziert jeden User und gewährt ausschließlich Zugang zu dedizierten, für eine Benutzergruppe freigeschaltete Applikationen. So werden Angriffsmöglichkeiten minimiert und laterale Ausbreitungen von Sicherheitsbedrohungen im Netzwerk verhindert.

Einsatz als Cloud-managed VPN Client

Für einen Vollzugriff auf ein Netzwerk lässt sich der LANCOM Trusted Access Client auch als Cloud-managed VPN Client einsetzen, um die VPN-Verbindungen mobiler Mitarbeitender sicher und zentral zu verwalten.

Cloud Management senkt Betriebskosten

In allen Betriebsarten erfolgen Roll-out von Security-Profilen, Client-Konfiguration und Monitoring über die LANCOM Management Cloud, die als zentrale Instanz alle LANCOM Netzwerkkomponenten verwaltet. Konfigurationsänderungen können einfach und effizient durchgeführt und neue Anwenderinnen und Anwender einfach hinzugefügt oder entfernt werden, ohne dass IT-Administrator und Endgerät physisch vor Ort sein müssen. Diese praktische Verwaltung gepaart mit dem transparenten Benutzer-Monitoring über die LANCOM Management Cloud senkt die Betriebskosten, da sämtliche Clients des Netzwerks zentral und auf einen Blick erreichbar sind.

Endpoint Security und Multifaktor-Authentifizierung

Bevor einem Benutzer Zugriff gewährt wird, lässt sich außerdem die Endpoint-Sicherheit bezüglich Betriebssystemversion überprüfen. Jeder User muss zudem seine Identität verifizieren, bevor er Zugriff auf eine Anwendung oder Ressource erhält. Anwendungen und Ressourcen werden nicht netzwerkweit sichtbar gemacht, wodurch das Netzwerk für potenzielle Angreifer unsichtbar bleibt. Zusätzlich kann beim Login eine Zweifaktor- oder Multifaktor-Authentifizierung mit Fingerabdruck, Gesichtserkennung oder einer Authentifizierungs-App auf dem Smartphone verlangt werden.

Einbindung vorhandener Benutzerdatenbanken

Die Netzwerk-Benutzerauthentifizierung erfolgt über eine zentrale Benutzerdatenbank („Identity Provider“, beispielsweise ein Active Directory wie Microsoft Entra ID, ehemals Azure AD). Für kleinere Unternehmen ohne zentrale Benutzerdatenbank steht alternativ ein in die LANCOM Management Cloud integriertes Benutzer-Management zur Verfügung.

Vollständige Integration in die LANCOM Management Cloud

Die LANCOM Management Cloud bietet ein vollständig integriertes Management aller LANCOM Netzwerkkomponenten (Router/Gateways, Firewalls, Switches und WLAN Access Points) inklusive des LANCOM Trusted Access Clients. Auch das Management der zugrundeliegenden Sicherheitsrichtlinien für alle User im Netzwerk erfolgt zentral über die LANCOM Management Cloud. Für umfassende Diagnose und Troubleshooting steht Administratoren ein LANCOM Trusted Access Real-Time Dashboard zur Verfügung.

100% Digitale Souveränität, 100% DSGVO-konform

Der LANCOM Trusted Access Client sowie die LANCOM Management Cloud werden in Deutschland entwickelt. Auch das Hosting sämtlicher Cloud-Daten erfolgt in hiesigen Rechenzentren. Dabei findet ausschließlich der Datenaustausch zur Benutzer-Authentifizierung über die LANCOM Management Cloud statt, alle weiteren Nutzdaten verlaufen direkt zwischen LANCOM Trusted Access Client und LANCOM Trusted Access Gateway – ohne Auskopplung über eine externe Cloud. Somit steht der LANCOM Trusted Access Client für höchste Datensicherheit und höchsten Datenschutz. Er unterliegt und entspricht europäischen Rechtsstandards, ist somit DSGVO-konform und eine IT-Security-Lösung „Engineered in Germany“.

Der LANCOM Trusted Access (LTA) Client ist für macOS Versionen ab macOS 11 (Big Sur) bis zum aktuellen macOS 15 (Sequoia) verfügbar. Zur Nutzung des LTA-Clients wird eine gültige LTA-Lizenz im zugehörigen LMC-Projekt benötigt. Es stehen verschiedene Lizenz-Laufzeiten (1, 3 und 5 Jahre) zur Verfügung sowie Volumenstaffeln für 1 / 10 / 25 / 100 / 250 / 1000 User.

Hinweis:

Der LANCOM Trusted Access Client erfordert auf dem als zentrales Access Gateway genutzten LANCOM Router mindestens die Firmware-Version LCOS 10.80, auf den LANCOM R&S®Unified Firewalls mindestens LCOS FX 10.13.

Weitere Informationen stehen auf der LANCOM Website unter https://www.lancom-systems.de/produkte/router-sd-wan/remote-access/lancom-trusted-access-client zur Verfügung.

Screenshots des LAT-Clients stehen hier zum Download bereit: i13.mnm.is/anhang.aspx