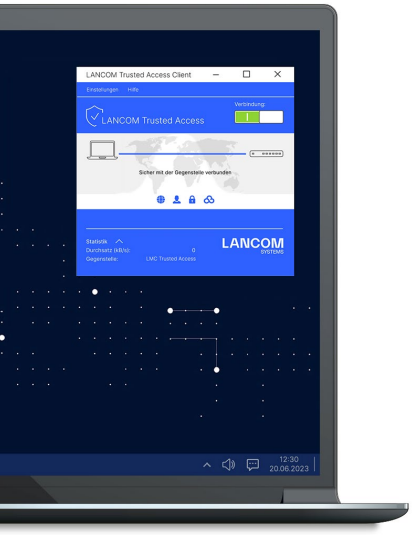
lancom-systems.de

LANCOM Trusted Access Client

Cloud-managed Secure Network Access



LANCOM Trusted Access ist die vertrauenswürdige Network Access Security-Lösung für Unternehmensnetzwerke. Es 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.**

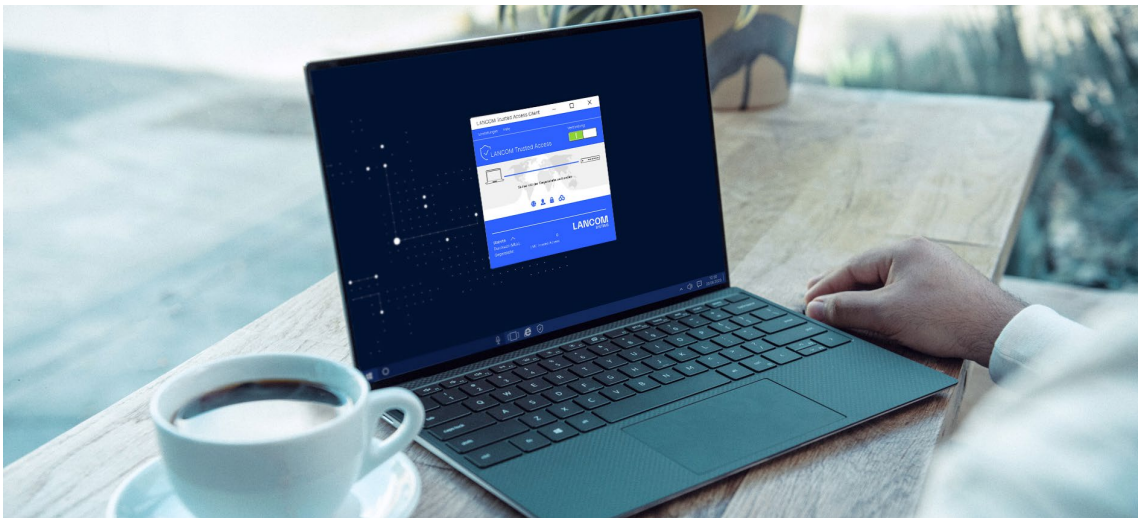
Die LANCOM Trusted Access-Lösung passt sich an steigende Sicherheitsanforderungen in Ihrer Organisation an und ermöglicht sowohl **Cloud-managed VPN-Client-Vernetzung** für den Zugriff auf ganze Netze als auch den Umstieg auf eine **Zero-Trust-Sicherheitsarchitektur** für eine umfassende Netzwerksicherheit. Dabei erhalten Benutzer auf Basis granularer Zugriffsrechte ausschließlich Zugangsberechtigung auf 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 100% DSGVO-konform und skaliert für Kleinunternehmen genauso wie für sehr große Netzwerke mit mehreren tausend Benutzern.

Highlights

- → **Flexibel skalierbare Secure Network Access-Lösung** für Unternehmensnetzwerke, die sich an steigende Sicherheitsanforderungen anpasst
- → **Wahlweise granulare Zugriffskontrolle** auf dedizierte Anwendungen (Zero-Trust-Prinzip) oder ganze Netze (Cloud-managed VPN-Client)
- → **Lateraler Schutz** vor der internen Ausbreitung von Schadsoftware in Verbindung mit Mikrosegmentierung
- → **Migriert nahtlos in bestehende Installationen** durch die Einbindung vorhandener Benutzerdatenbanken im Unternehmen
- → **Endpoint-Security und Multi-Faktor-Authentifizierung** für ein hohes Maß an Sicherheit
- → **Einfacher Zugriff auf externe Cloud-Anwendungen** per Single Sign-On (SSO) ohne Eingabe zusätzlicher Anmeldedaten
- → **Trusted Internet Access mit Full Tunnel-Modus** für mobiles Arbeiten so sicher wie im Büro
- → **Vollständige Integration in die LANCOM Management Cloud (LMC)** für zero-touch Inbetriebnahme und Auto-Konfiguration für ein einfaches und schnelles Ausrollen neuer Remote Access-Verbindungen
- → **100% DSGVO-konform** – Datenverkehr verläuft ohne Auskopplung über eine externe Cloud

LANCOM Trusted Access Client



Granulare Zugriffskontrolle auf Anwendungen nach dem Zero-Trust-Prinzip

Mit seiner 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 ermöglicht die Implementierung von Zugriffskontrollen auf einer sehr granularen Ebene („Software-defined Perimeter“, SDP). Dies bedeutet, dass die Benutzer nur auf die Anwendungen und Ressourcen zugreifen können, die sie benötigen, um ihre Arbeit auszuführen, und dass jeder Zugriff explizit autorisiert werden muss.

Was ist „Zero Trust“?

Gartner definiert Zero Trust als ein Sicherheitskonzept, bei dem die Annahme, dass nichts und niemand innerhalb oder außerhalb des Netzwerks vertrauenswürdig ist, im Vordergrund steht. Im Wesentlichen bedeutet dies, dass jeder Zugriff auf Ressourcen im Netzwerk – egal ob von außerhalb oder innerhalb – stets **autorisiert und authentifiziert** werden muss, bevor er erlaubt wird.

Im Vergleich zu einem klassischen VPN unterscheidet sich das Zero-Trust-Prinzip dadurch, dass Benutzern oder Geräten **kein Zugriff auf gesamte Netze**, sondern ausschließlich auf bestimmte Anwendungen oder Netzwerkressourcen gewährt wird.

Durch eine solche **„Mikro-Segmentierung“** müssen Unternehmensserver nicht mehr in einem Intranet miteinander verbunden sein. Dies verhindert eine ungehinderte Ausbreitung von Ransomware im gesamten Intranet, falls ein Server kompromittiert wird. Somit wird ein Schutz vor dem sogenannten „lateral movement“ geboten.

LANCOM Trusted Access Client

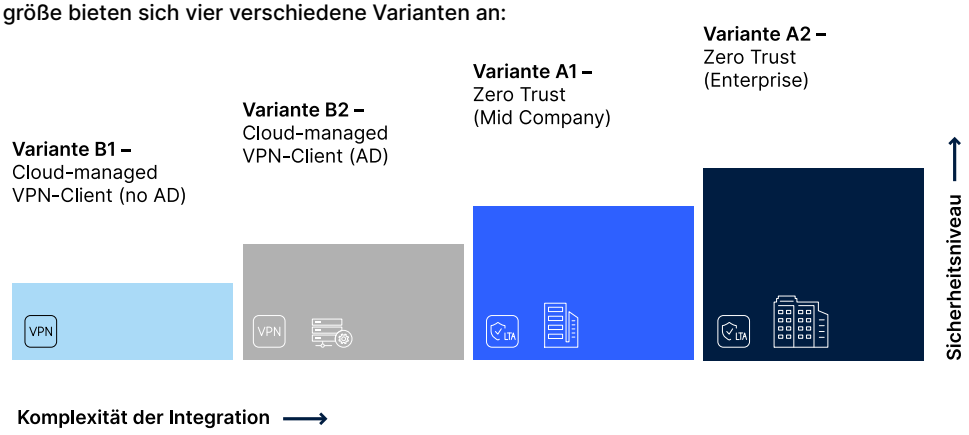
Netzwerksicherheit nach Maß

Der Umstieg von klassischen VPN-Clients hin zu einem Zero-Trust-Modell bedeutet in der Regel einen aufwändigen Komplettumbau der gesamten Sicherheitsarchitektur eines Netzwerks. Nicht so bei LANCOM Trusted Access.

LANCOM Trusted Access erlaubt einen **direkten Umstieg auf eine Zero-Trust-Sicherheitsarchitektur**, denn diese Lösung wächst mit Ihren Sicherheitsanforderungen. Egal, ob Sie Cloud-managed VPN-Client-Vernetzung für weitreichende Netzwerkzugriffe benötigen oder den Schritt zu einer umfassenden Zero-Trust-Sicherheitsarchitektur gehen möchten – LANCOM Trusted Access bietet exakt **passende Ausbaustufen**.

Ihr Start mit LANCOM Trusted Access:
Welche Ausbaustufe passt zu welchem Anwendungsfall?

Je nach Benutzerverwaltung, Umsetzung strengerer Sicherheitsrichtlinien und Unternehmensgröße bieten sich vier verschiedene Varianten an:



Wie Sie LANCOM Trusted Access optimal in Ihre Infrastruktur einbinden, erfahren Sie unter www.lancom-systems.de/lta-onboarding. Mit Beantwortung eines interaktiven Fragebogens erhalten Sie in nur wenigen Klicks Ihre passende Ausbaustufe und **Zugang zu Tutorial-Videos**.

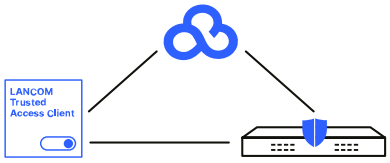
Einsatz als Cloud-managed VPN-Client

Der LANCOM Trusted Access Client lässt sich wahlweise auch als Cloud-managed VPN-Client einsetzen, um somit die VPN-Verbindungen mobiler Mitarbeitender sicher und zentral zu verwalten. Dies bedeutet, dass Konfigurationsupdates einfach und effizient durchgeführt werden oder auch neue Benutzer einfach hinzugefügt oder entfernt werden können, ohne dass ein IT-Administrator oder das Endgerät physisch vor Ort sein muss. Diese praktische Verwaltung gepaart mit dem transparenten Benutzer-Monitoring über die LANCOM Management Cloud senkt Ihre Betriebskosten, da **sämtliche VPN-Clients Ihres Unternehmens zentral und auf einen Blick erreichbar sind**.

LANCOM Trusted Access Client

Systemarchitektur LANCOM Trusted Access

Alles, was Sie für die Umsetzung einer LANCOM Trusted Access-Sicherheitsarchitektur benötigen, sind ein Trusted Access Gateway (Router oder Firewall), die LANCOM Management Cloud (LMC) und den LANCOM Trusted Access Client.



Ausschließlich der Datenaustausch zur Benutzerauthentifizierung findet über die LMC statt (Control Plane). Der anschließende Datenverkehr geschieht ohne Auskopplung über eine externe Cloud (Data Plane).

Weitere Informationen finden Sie im Techpaper LANCOM Trusted Access Systemarchitektur.

Trusted Internet Access: Mobiles Arbeiten so sicher wie im Büro

Mit LANCOM Trusted Access (LTA) verwalten Sie die Zugriffsrechte und Netzwerkverbindungen für mobile Mitarbeitende sicher und zentral über die LANCOM Management Cloud. Dabei wird den mobilen Benutzern der normale Internetverkehr grundsätzlich erlaubt („Split Tunnel“). Um zusätzlich den gesamten Internetverkehr angebundener LTA-Clients abzusichern, aktivieren Sie den „Full Tunnel“-Betrieb. Damit wird der gesamte Datenverkehr durch das zentrale LTA-Gateway (Unified Firewall oder SD-WAN Gateway) geleitet. Der Vorteil: Risiken durch unbefugte Zugriffe, Malware, Phishing und andere Cyberangriffe werden minimiert und können zusätzlich über aktivierte Sicherheitsfunktionen auf dem Gateway wie Anti-Virus oder Content Filter auch bei externen Web- / Cloudbasierten Anwendungen überprüft werden. Wir nennen diesen Betriebsmodus „Trusted Internet Access“.

Endpoint-Security und Multi-Faktor-Authentifizierung für ein hohes Maß an Sicherheit

Bevor einem Benutzer Zugriff gewährt wird, kann die Endpoint-Sicherheit überprüft werden (Betriebssystemversion, Virenschutz, lokale Firewall). Jeder Benutzer muss zudem **seine Identität überprüfen lassen**, bevor er Zugriff auf eine Anwendung oder Ressource erhält. Anwendungen und Ressourcen werden nicht netzwerkweit sichtbar gemacht, wodurch das Netzwerk für 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 Benutzerauthentifizierung erfolgt über eine zentrale Benutzerdatenbank („Identity Provider“, z. B. ein Active Directory wie Microsoft Entra ID (ehemals Azure AD)). Vom Identity Provider übernommene Benutzergruppen können dabei mit individuellen Zugriffsrechten auf die erlaubten Anwendungen versehen werden. Die Gültigkeitsdauer einer Authentifizierung ist einstellbar, Clients können zudem manuell oder automatisch geblockt werden. Für kleine Unternehmen ohne zentrale Benutzerdatenbank steht alternativ ein in die LANCOM Management Cloud integriertes Benutzer-Management zur Verfügung.

LANCOM Trusted Access Client

Einfacher Zugriff auf externe Cloud-Anwendungen per Single Sign-On (SSO)

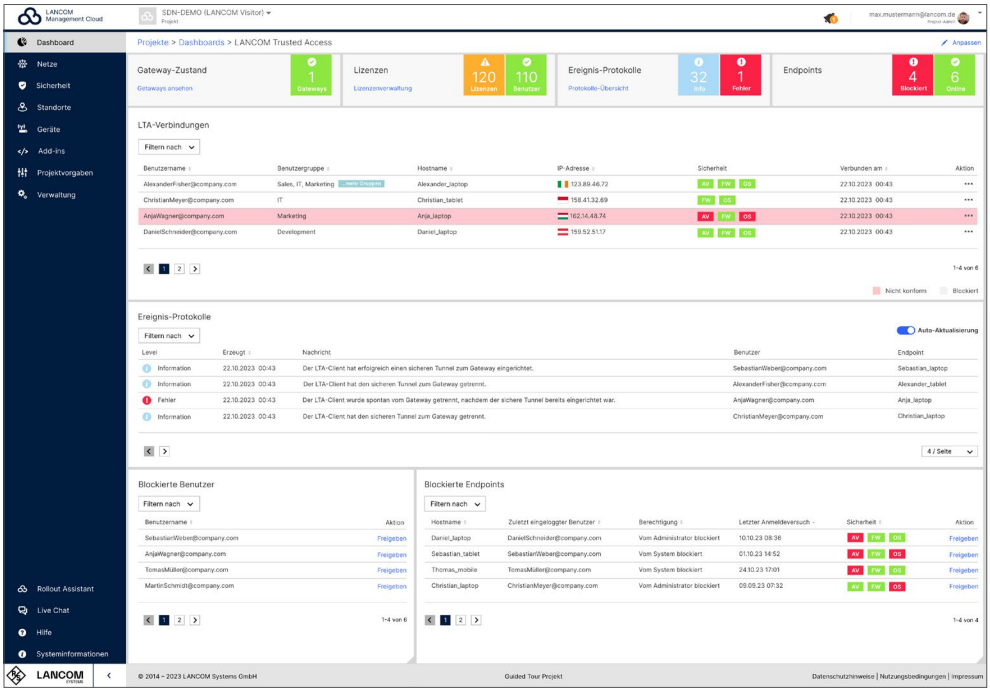
Der LANCOM Trusted Access Client übernimmt die Anmeldeprozesse bei passwortgeschützten Applikationen: Via Single Sign-On (SSO) kann der Benutzer nach einmaliger Anmeldung am Active Directory auf externe Web-Anwendungen bequem und sicher zugreifen – ohne die erneute Eingabe der Zugangsdaten. Das sorgt für besonders **nutzerfreundliche und schnelle Arbeitsprozesse**.

Nahtlose Integration in die LANCOM Management Cloud

Die LANCOM Management Cloud (LMC) bietet ein **vollständig integriertes Management** aller LANCOM Netzwerkkomponenten (Router / Gateways, Firewalls, Switches und Access Points) inklusive des LANCOM Trusted Access Clients. Auch das Management der zugrundeliegenden Sicherheitsrichtlinien für alle Benutzer im Netzwerk erfolgt zentral über die LMC.

Für umfassende Diagnose und Troubleshooting steht Administratoren ein LANCOM Trusted Access **Real-Time Dashboard** bereit. Das Dashboard zeigt aktive Verbindungen mit Benutzername, IP-Adresse, Gerätename und Benutzergruppe an und bietet zusätzliche Informationen wie den Compliance-Status und den letzten Login.

Darüber hinaus können Clients sowohl manuell als auch automatisch blockiert werden, es stehen Informationen zur Anzahl der Benutzer und blockierten Verbindungsanfragen bereit sowie ein zentrales Lizenz-Management und -Monitoring.

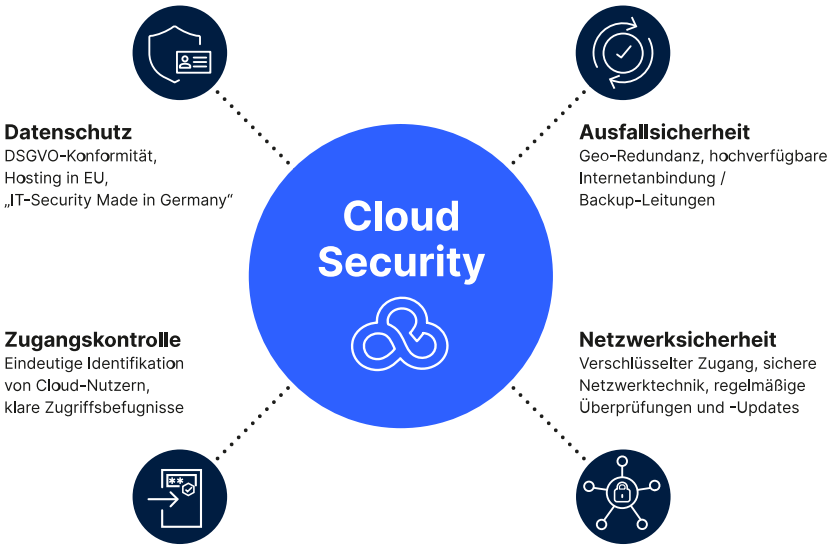


LANCOM Trusted Access Client

100% Digitale Souveränität, 100% DSGVO-konform

Der LANCOM Trusted Access Client sowie die LANCOM Management Cloud (LMC) werden in Deutschland entwickelt, und auch das Hosting sämtlicher Cloud-Daten erfolgt in Rechenzentren in Deutschland.

Ausschließlich der Datenaustausch zur Benutzer-Authentifizierung findet über die LMC 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 überzeugt als **IT-Security-Lösung engineered in Germany**.



Weitere Informationen finden Sie im Infopaper LMC (Public) Datenschutz und Datensicherheit.

LANCOM Trusted Access Client

LANCOM Trusted Access Ausbaustufen

Attribute / Einsatzszenarien	Variante B1 – Cloud-managed VPN-Client (no AD)	Variante B2 – Cloud-managed VPN-Client (AD)	Variante A1 – Zero Trust (Mid Company)	Variante A2 – Zero Trust (Enterprise)
Einsatzempfehlung	Kleine und mittlere Unternehmen	Kleine und mittlere Unternehmen	Mittlere Unternehmen	Große Unternehmen
Voraussetzungen technische Expertise	→ Umgang mit der LMC	→ Umgang mit der LMC → Umgang mit Microsoft Entra ID (ehemals Azure AD) und ggf. Microsoft Entra ID Connect	→ Umgang mit der LMC → Umgang mit Microsoft Entra ID (ehemals Azure AD) und ggf. Microsoft Entra ID Connect	→ Umgang mit der LMC → Umgang mit Microsoft Entra ID (ehemals Azure AD) und ggf. Microsoft Entra ID Connect
Benutzerverwaltung	→ Lokal über die LMC	→ Active Directory	→ Active Directory	→ Active Directory
Zugriffsrechte	→ Vollzugriff Intranet → (Alternativ: Dedizierte Anwendungsfreigabe)	→ Vollzugriff Intranet → (Alternativ: Dedizierte Anwendungsfreigabe)	→ Dedizierte Anwendungsfreigabe	→ Dedizierte Anwendungsfreigabe → Unterteilung in Mikrosegmente (Private VLAN)
Kernfunktionen	→ Cloud-managed VPN-Client → Endpoint-Security-Check (Software-Updates, Antivirus)	→ Cloud-managed VPN-Client → Endpoint-Security-Check (Software-Updates, Antivirus) → Anbindung an Active Directory → Single Sign-On	→ Cloud-managed VPN-Client → Endpoint-Security-Check (Software-Updates, Antivirus) → Anbindung an Active Directory → Single Sign-On → Anwendungsfreigabe für Benutzergruppen	→ Cloud-managed VPN-Client → Endpoint-Security-Check (Software-Updates, Antivirus) → Anbindung an Active Directory → Single Sign-On → Anwendungsfreigabe für Benutzergruppen → Mikrosegmentierung
Komplexität	Gering	Mittel	Hoch	Sehr hoch

LANCOM Trusted Access Client

Features	
Zero-touch Auto-Konfiguration	→ Einfaches und schnelles Ausrollen neuer Remote Access-Verbindungen per Zero-touch Auto-Konfiguration. Hinweise: → Dies bedeutet, dass der Anwender einen installierten Client (frei und kostenlos herunterladbar oder alternativ über eine Software-Verteilung wie z. B. Baramundi durch die zentrale IT installiert) einfach durch Eingabe der Zugangsdaten mit den Zielanwendungen verbinden kann. → Es werden Administratorenrechte benötigt, um den Client auf einem Rechner zu installieren. → Der Benutzername muss die Domäne beinhalten (z. B. über die E-Mail-Adresse), damit die LANCOM Management Cloud (LMC) das passende Projekt mit der Domäne findet
Anbindung bestehender AD-Benutzer oder LMC-interner Benutzer	→ Nahtlose Einbindung vorhandener Benutzerdatenbanken (via Microsoft Entra ID (ehemals Azure AD)) → Alternatives Benutzermanagement innerhalb der LANCOM Management Cloud (ohne AD) Hinweise: → Bei AD-Anbindung ist sicherzustellen, dass im AD eine geeignete Gruppenstruktur bzw. Zugehörigkeit hinterlegt ist, anhand derer dann die LMC die Anwendungsfreigaben für die Benutzergruppen aktiviert. → Bei Nutzung der LMC-internen LANCOM Trusted Access (LTA-) Benutzerverwaltung (d. h. ohne AD) stehen folgende Funktionen nicht zur Verfügung, da diese auf Microsoft Entra ID-Funktionen basieren: Single Sign-On und Multi-Faktor-Authentifizierung
Software-defined Perimeter	Zentrale & dynamische Steuerung von Zugriffsrechten und Profil-Deployments. Der Client-Zugriff erfolgt auf Applikations- bzw. Dienstebene. Das zugehörige Enforcement findet dabei durch die LTA-Gateways statt, die entsprechende Anwendungs- und Dienstefreigaben durch Verbindungsziele anhand von URLs, IP-Adressen, Ports und Protokollen realisieren. Weitere Funktionen: → LMC-interne PKI (vollautomatisch) → Mikrosegmentierung (Private VLAN) durch manuelle Port-Isolation der sich im LAN befindlichen Switches → SSO Agent (via Microsoft Entra ID)
Zentrales Benutzer-Monitoring	→ LTA-Dashboard in der LANCOM Management Cloud → Anzeige der zugreifenden Remote-Endpoints → Anzeige der aktiven Verbindungen mit Benutzername, IP-Adresse, Gerätename, Benutzergruppe und weiteren Informationen (Compliance-Status, letzter Login) → Anzeige des Lizenzstatus → Das LTA-Dashboard ist nur für IT-Administratoren einsehbar
Endpoint Security	→ Compliance Enforcement (Einwahl von LTA-Clients mit fehlenden Betriebssystem-Updates unterbinden) → Conditional Access durch Überprüfung von Sicherheitsparametern wie aktivierte System-Firewall, Anti-Virus-Status oder Betriebssystem-Updates → Sperrung von LANCOM Trusted Access-Benutzern (direkt aus der LMC heraus, unabhängig vom AD-Status des Benutzers)
Schutzmechanismen	→ Multi-Faktor-Authentifizierung (via Microsoft Entra ID)
Höchste Verschlüsselungsstandards	→ Integriertes Zertifikatsmanagement (PKI) → State-of-the-art Kryptographie gemäß BSI TR 02-102 (Empfehlung des Bundesamts für Sicherheit in der Informationstechnik)

LANCOM Trusted Access Client

Software- und Security Updates	Alle allgemeinen Software- und Security Updates des LANCOM Trusted Access Clients, der LMC sowie der LANCOM Trusted Access Gateways sind über die lizenzierte Client-Laufzeit inklusive
MSI-Installer	Der MSI-Installer kann über Kommandozeilenoption weitere Informationen während der Installation mitgeben (für Softwareverwaltungssysteme): → LANCOM_PRODUCT_TYPE=AVC → LANCOM_PRODUCT_TYPE=LTA → MGMCLOUD_URL=cloud.lancom.de → MGMCLOUD_DOMAIN=mycompany.com
Betriebsmodus	→ Split Tunneling: Der Internet-Traffic wird direkt am LTA-Client ausgekoppelt. → Full Tunneling: Der gesamte Traffic wird immer über das LTA-Gateway geroutet. In Kombination mit auf dem LTA-Gateway (LCOS oder LCOS FX) aktivierten Sicherheitsfunktionen wie Anti-Virus oder Content Filter wird der Betriebsmodus „Trusted Internet Access“ genannt.
Unterstützte Gateways	VPN-Router / -Gateways bzw. Unified Firewalls (Hardware oder vRouter / vFirewall) mit folgenden Betriebssystemversionen: → LCOS ab 10.80 → LCOS FX ab 10.13
Unterstützte Identity Provider (IdP)	→ Microsoft Entra ID (ehemals Azure AD) → Die Anbindung an lokale AD-Server erfolgt durch Microsoft Entra ID Connect (ehemals Azure AD Connect). → Alternativ steht eine integrierte lokale Benutzertabelle in der LMC für kleine Installationen bereit.
Unterstützte Betriebssysteme	→ Microsoft Windows 10 / 11 (auf Intel x86-64 Prozessorarchitektur) → macOS Sequoia 15 → macOS Sonoma 14 → macOS Ventura 13 → macOS Monterey 12 → macOS Big Sur 11

Lizenzen
Pro Benutzer können jeweils bis zu drei Endgeräte parallel genutzt werden.
Für LANCOM Partner mit Service Provider License Agreement steht ein separates pay-per-use-Lizenzmodell zur Verfügung.

		Art.-Nr.
LANCOM LTA-CL-1Y 1 License	Lizenz für 1 LANCOM Trusted Access-Benutzer in der LANCOM Management Cloud, sicherer Remote Access (Zero-Trust-Prinzip oder Cloud-managed VPN), Angabe der LMC-Projekt-ID und einer E-Mail-Adresse für den Lizenzversand notwendig, Laufzeit 1 Jahr	50400
LANCOM LTA-CL-1Y 10 Licenses	Lizenz für 10 LANCOM Trusted Access-Benutzer in der LANCOM Management Cloud, sicherer Remote Access (Zero-Trust-Prinzip oder Cloud-managed VPN), Angabe der LMC-Projekt-ID und einer E-Mail-Adresse für den Lizenzversand notwendig, Laufzeit 1 Jahr	50401
LANCOM LTA-CL-1Y 25 Licenses	Lizenz für 25 LANCOM Trusted Access-Benutzer in der LANCOM Management Cloud, sicherer Remote Access (Zero-Trust-Prinzip oder Cloud-managed VPN), Angabe der LMC-Projekt-ID und einer E-Mail-Adresse für den Lizenzversand notwendig, Laufzeit 1 Jahr	50402
LANCOM LTA-CL-1Y 100 Licenses	Lizenz für 100 LANCOM Trusted Access-Benutzer in der LANCOM Management Cloud, sicherer Remote Access (Zero-Trust-Prinzip oder Cloud-managed VPN), Angabe der LMC-Projekt-ID und einer E-Mail-Adresse für den Lizenzversand notwendig, Laufzeit 1 Jahr	50403
LANCOM LTA-CL-1Y 250 Licenses	Lizenz für 250 LANCOM Trusted Access-Benutzer in der LANCOM Management Cloud, sicherer Remote Access (Zero-Trust-Prinzip oder Cloud-managed VPN), Angabe der LMC-Projekt-ID und einer E-Mail-Adresse für den Lizenzversand notwendig, Laufzeit 1 Jahr	50404
LANCOM LTA-CL-1Y 1000 Licenses	Lizenz für 1000 LANCOM Trusted Access-Benutzer in der LANCOM Management Cloud, sicherer Remote Access (Zero-Trust-Prinzip oder Cloud-managed VPN), Angabe der LMC-Projekt-ID und einer E-Mail-Adresse für den Lizenzversand notwendig, Laufzeit 1 Jahr	50405

LANCOM Trusted Access Client

LANCOM LTA-CL-3Y 1 License	Lizenz für 1 LANCOM Trusted Access-Benutzer in der LANCOM Management Cloud, sicherer Remote Access (Zero-Trust-Prinzip oder Cloud-managed VPN), Angabe der LMC-Projekt-ID und einer E-Mail-Adresse für den Lizenzversand notwendig, Laufzeit 3 Jahre	50410
LANCOM LTA-CL-3Y 10 Licenses	Lizenz für 10 LANCOM Trusted Access-Benutzer in der LANCOM Management Cloud, sicherer Remote Access (Zero-Trust-Prinzip oder Cloud-managed VPN), Angabe der LMC-Projekt-ID und einer E-Mail-Adresse für den Lizenzversand notwendig, Laufzeit 3 Jahre	50411
LANCOM LTA-CL-3Y 25 Licenses	Lizenz für 25 LANCOM Trusted Access-Benutzer in der LANCOM Management Cloud, sicherer Remote Access (Zero-Trust-Prinzip oder Cloud-managed VPN), Angabe der LMC-Projekt-ID und einer E-Mail-Adresse für den Lizenzversand notwendig, Laufzeit 3 Jahre	50412
LANCOM LTA-CL-3Y 100 Licenses	Lizenz für 100 LANCOM Trusted Access-Benutzer in der LANCOM Management Cloud, sicherer Remote Access (Zero-Trust-Prinzip oder Cloud-managed VPN), Angabe der LMC-Projekt-ID und einer E-Mail-Adresse für den Lizenzversand notwendig, Laufzeit 3 Jahre	50413
LANCOM LTA-CL-3Y 250 Licenses	Lizenz für 250 LANCOM Trusted Access-Benutzer in der LANCOM Management Cloud, sicherer Remote Access (Zero-Trust-Prinzip oder Cloud-managed VPN), Angabe der LMC-Projekt-ID und einer E-Mail-Adresse für den Lizenzversand notwendig, Laufzeit 3 Jahre	50414
LANCOM LTA-CL-3Y 1000 Licenses	Lizenz für 1000 LANCOM Trusted Access-Benutzer in der LANCOM Management Cloud, sicherer Remote Access (Zero-Trust-Prinzip oder Cloud-managed VPN), Angabe der LMC-Projekt-ID und einer E-Mail-Adresse für den Lizenzversand notwendig, Laufzeit 3 Jahre	50415
LANCOM LTA-CL-5Y 1 License	Lizenz für 1 LANCOM Trusted Access-Benutzer in der LANCOM Management Cloud, sicherer Remote Access (Zero-Trust-Prinzip oder Cloud-managed VPN), Angabe der LMC-Projekt-ID und einer E-Mail-Adresse für den Lizenzversand notwendig, Laufzeit 5 Jahre	50420
LANCOM LTA-CL-5Y 10 Licenses	Lizenz für 10 LANCOM Trusted Access-Benutzer in der LANCOM Management Cloud, sicherer Remote Access (Zero-Trust-Prinzip oder Cloud-managed VPN), Angabe der LMC-Projekt-ID und einer E-Mail-Adresse für den Lizenzversand notwendig, Laufzeit 5 Jahre	50421
LANCOM LTA-CL-5Y 25 Licenses	Lizenz für 25 LANCOM Trusted Access-Benutzer in der LANCOM Management Cloud, sicherer Remote Access (Zero-Trust-Prinzip oder Cloud-managed VPN), Angabe der LMC-Projekt-ID und einer E-Mail-Adresse für den Lizenzversand notwendig, Laufzeit 5 Jahre	50422
LANCOM LTA-CL-5Y 100 Licenses	Lizenz für 100 LANCOM Trusted Access-Benutzer in der LANCOM Management Cloud, sicherer Remote Access (Zero-Trust-Prinzip oder Cloud-managed VPN), Angabe der LMC-Projekt-ID und einer E-Mail-Adresse für den Lizenzversand notwendig, Laufzeit 5 Jahre	50423
LANCOM LTA-CL-5Y 250 Licenses	Lizenz für 250 LANCOM Trusted Access-Benutzer in der LANCOM Management Cloud, sicherer Remote Access (Zero-Trust-Prinzip oder Cloud-managed VPN), Angabe der LMC-Projekt-ID und einer E-Mail-Adresse für den Lizenzversand notwendig, Laufzeit 5 Jahre	50424
LANCOM LTA-CL-5Y 1000 Licenses	Lizenz für 1000 LANCOM Trusted Access-Benutzer in der LANCOM Management Cloud, sicherer Remote Access (Zero-Trust-Prinzip oder Cloud-managed VPN), Angabe der LMC-Projekt-ID und einer E-Mail-Adresse für den Lizenzversand notwendig, Laufzeit 5 Jahre	50425

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info@lancom.de | lancom-systems.de