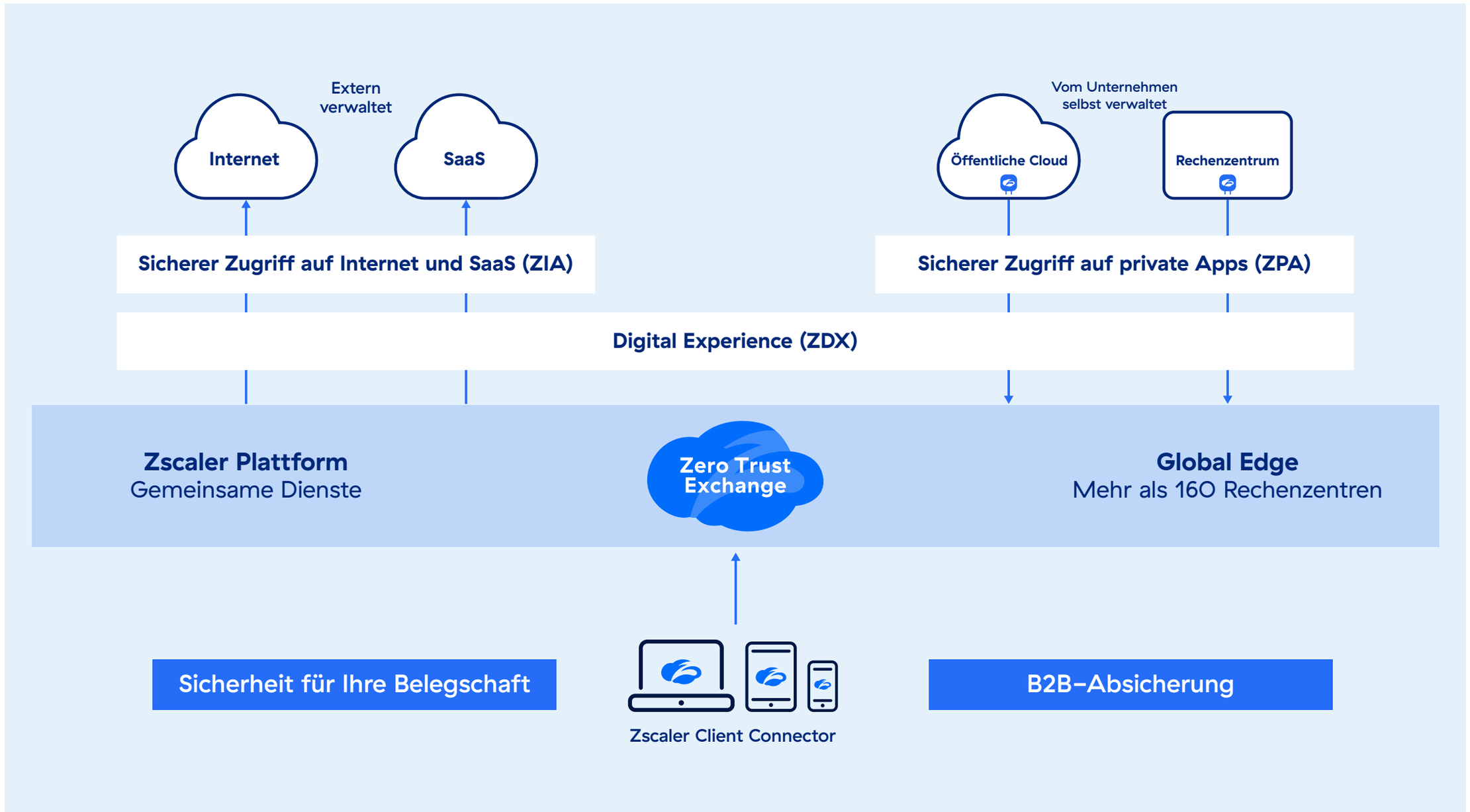
Zscaler Client Connector

Schneller, sicherer und zuverlässiger Zugriff auf jedes Ziel— von jedem Standort und Gerät aus.

DATENBLATT

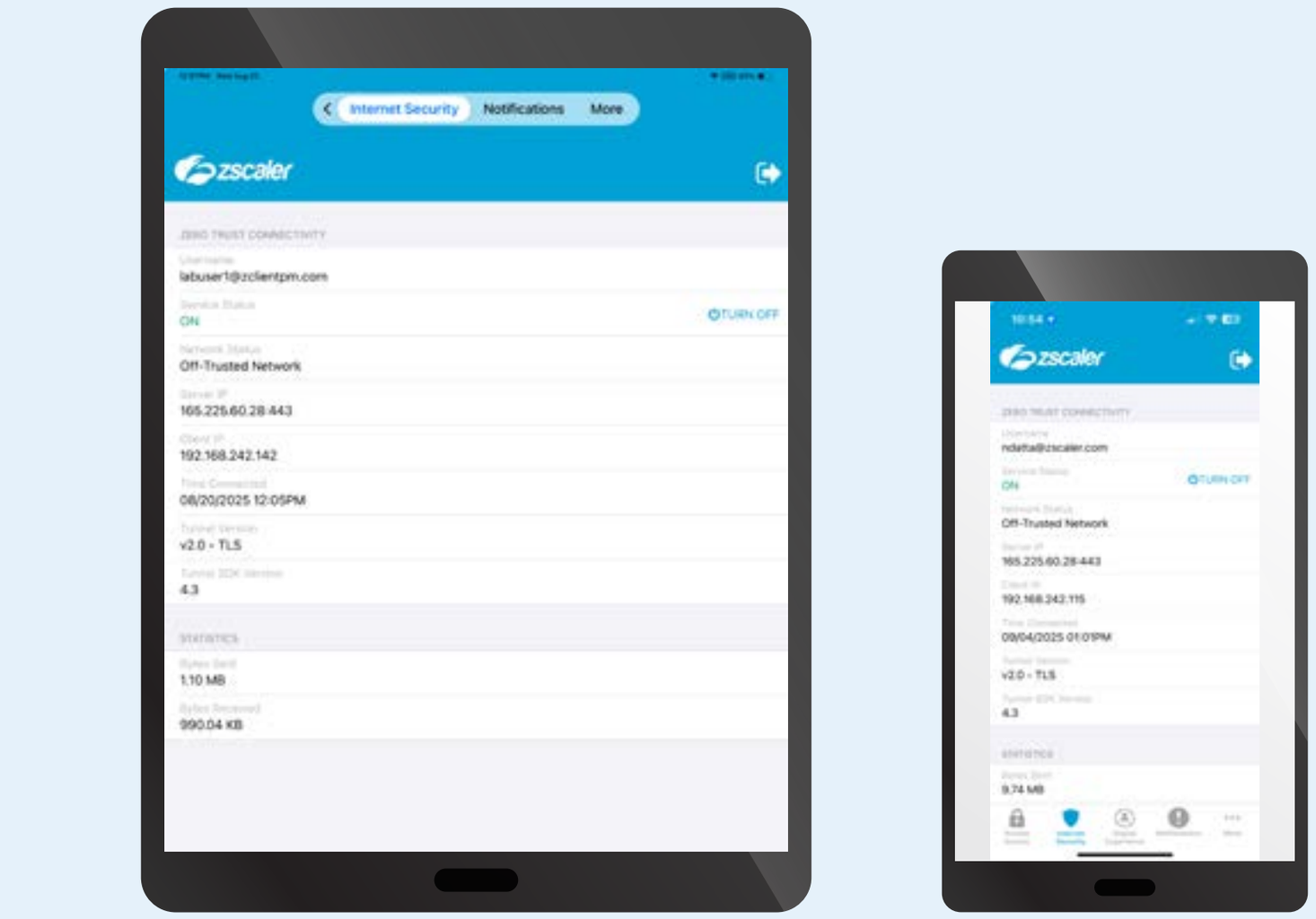


Die Arbeitsabläufe in Unternehmen sind heute grundlegend anders als früher. Mitarbeiter können jetzt eine Vielzahl von Geräten verwenden und von jedem beliebigen Standort aus auf Cloud-Anwendungen und andere Ziele auf der ganzen Welt zugreifen. Diese neuen, hybriden Belegschaften benötigen schnellen und nahtlosen Zugriff auf IT-Ressourcen — doch das darf nicht auf Kosten der Datensicherheit gehen. Unternehmen, die unter heutigen Vorzeichen erfolgreich wirtschaften wollen, müssen global verteilte Endgeräte sichern und ihren Usern gleichzeitig ein produktives Arbeiten ermöglichen. Um dies zu erreichen, setzen zahlreiche IT-Teams auf Zscaler und unseren Client Connector.

Früher, als sich User und Apps noch im Büro befanden, war es sinnvoll, auf netzwerkzentrierte Sicherheits- und Konnektivitätslösungen zu setzen. Heute greifen Mitarbeiter außerhalb des Unternehmens jedoch über Netzwerke auf externe Anwendungen zu, die nicht von den IT-Teams kontrolliert werden. Das Backhauling dieses Traffics zum Rechenzentrum führt zu zusätzlichen Latenzen, die die Produktivität beeinträchtigen. Noch wichtiger ist jedoch, dass Backhauling das Risiko erhöht, da User mit dem Unternehmensnetzwerk verbunden werden und so übermäßige Berechtigungen missbrauchen und sich lateral zwischen netzwerkverbundenen Ressourcen bewegen können. Ganz zu schweigen davon, dass es die Angriffsfläche vergrößert und weitere wichtige Sicherheitslücken mit sich bringt.

Abhilfe schafft eine Zero-Trust-Architektur. Zscaler stellt diese als Service über die Zero Trust Exchange bereit, die weltweit größte Cloud-Sicherheitsplattform, die als intelligente Schaltzentrale fungiert und Zero-Trust-Verbindungen anhand unternehmensspezifischer Richtlinien herstellt, ohne User im Netzwerk zu platzieren. Die Zero Trust Exchange gewährt kontextbasierten Direktzugriff auf IT-Ressourcen nach dem Prinzip der minimalen Rechtevergabe von über 160 Präsenzpunkten weltweit. Mit anderen Worten: IT-Teams können Bedrohungen und Datenverluste stoppen und hervorragende Anwendererfahrungen für alle User unabhängig vom Standort und Gerät gewährleisten.

Als ressourcenschonender, vielseitig einsetzbarer Endgeräre-Agent spielt der Zscaler Client Connector eine zentrale Rolle bei der Bereitstellung von Zero-Trust-Verbindungen. Unabhängig vom User-Standort ermöglicht er direkten Zugriff auf das Internet und IT-Ressourcen nach dem Prinzip der minimalen Rechtevergabe. Darüber hinaus bietet er eine Vielzahl weiterer Funktionen, die die Sicherheit und Konnektivität weiter verbessern und gleichzeitig Punktprodukte und ihre dedizierten Agents überflüssig machen.



Vorteile des Zscaler Client Connector

Die Vorteile des Client Connector lassen sich in die unten aufgeführten sieben Kategorien einteilen. Weitere Einzelheiten finden Sie in der Tabelle am Ende dieses Datenblatts.

Zero-Trust-Kommunikation zu jedem Ziel: Unternehmen benötigen keine separaten Lösungen mit separaten Agents mehr, um den Zugriff auf verschiedene Verbindungsziele zu sichern. Client Connector ermöglicht Zero-Trust-Zugriff nach dem Prinzip der minimalen Rechtevergabe auf jedes Ziel, einschließlich Web, SaaS und private Unternehmensanwendungen. Dies entspricht den Empfehlungen von Gartner für SSE und SASE und stellt sicher, dass die Geräteleistung nicht durch unnötige Agents beeinträchtigt wird.

Zero-Trust-Kommunikation für jedes Gerät. Unternehmen müssen nicht nur den Zugriff auf jedes Ziel sichern, sondern auch den Zugriff auf jedes Gerät. Denn Mitarbeiter nutzen heute eine Vielzahl von Desktops, Laptops, Tablets und Smartphones mit unterschiedlichen Betriebssystemen. Client Connector kann jedes Gerät sichern und so die Sicherheit und Produktivität Ihrer Mitarbeiter gewährleisten.

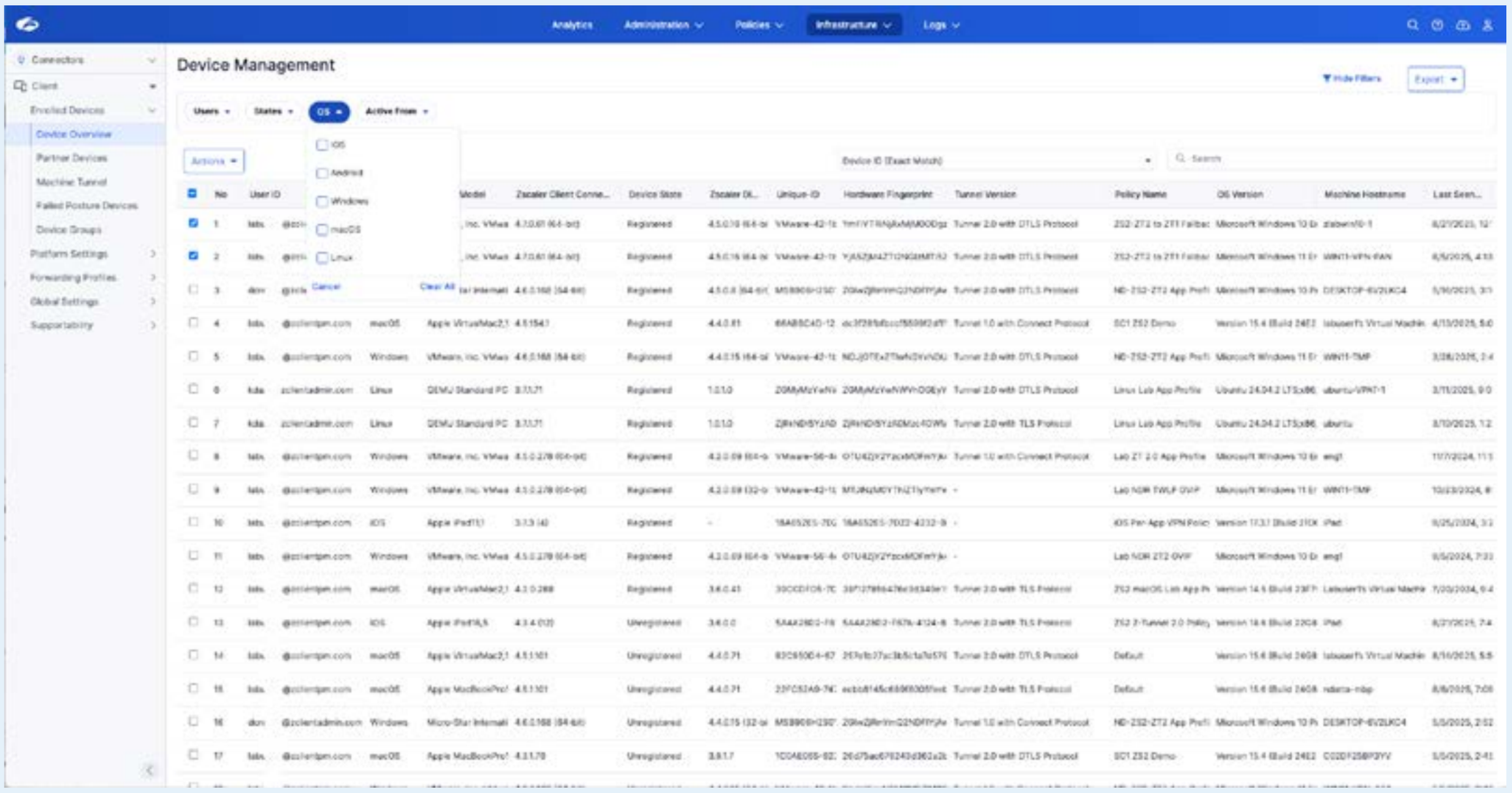
Kontextbewusste, intelligente Sicherheit Identität allein reicht nicht aus, um den Zugriff auf IT-Ressourcen zu regeln (Identitäten können gestohlen werden, und selbst legitime User können ihren Arbeitgebern versehentlich schaden). Stattdessen müssen Unternehmen den Zugriff kontext- und risikobasiert regeln. Client Connector ermöglicht dies durch Bereitstellen von Einblicken in den Gerätesicherheitsstatus, die eine intelligente, adaptive Zugriffskontrolle ermöglichen.

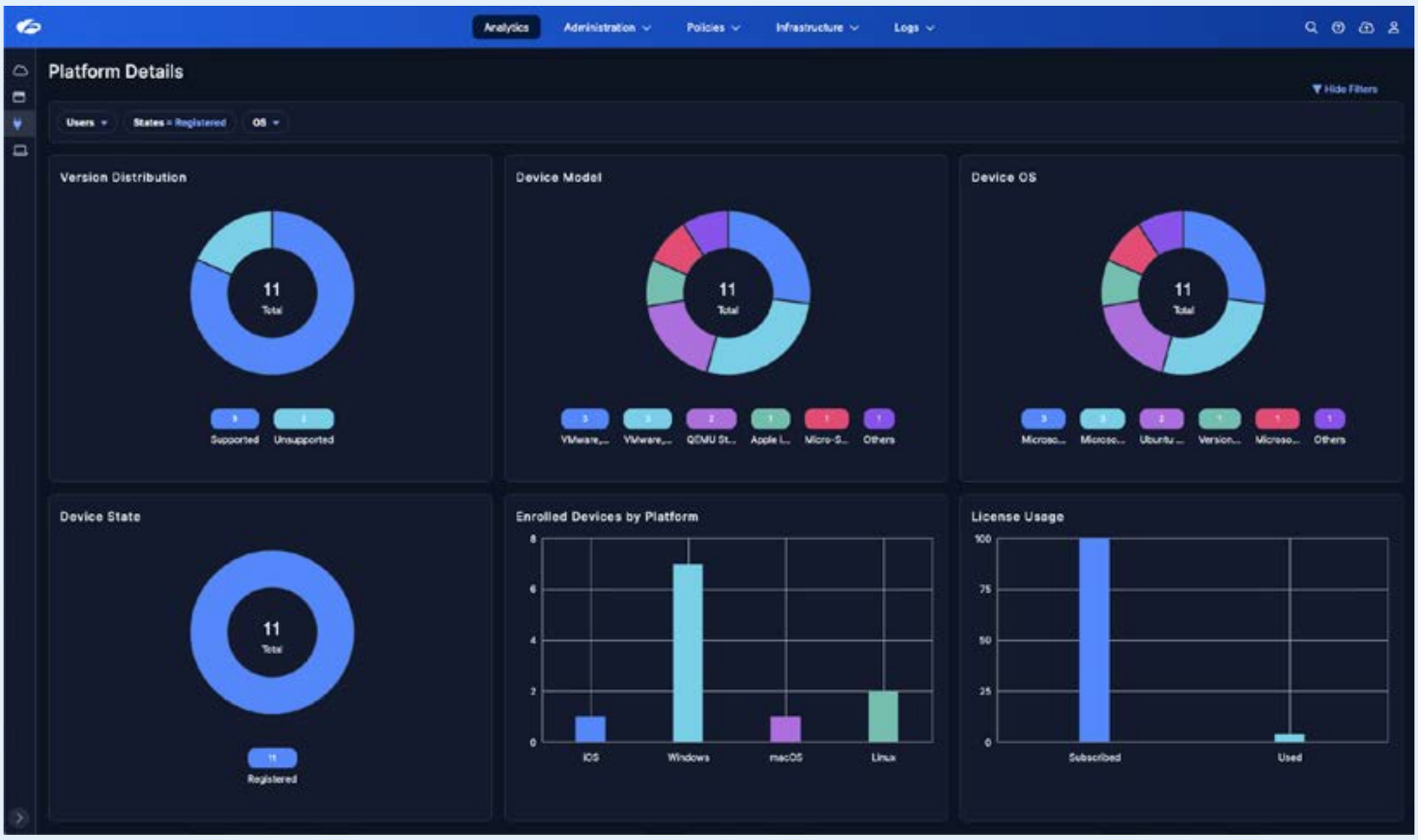
Datenschutz auf Endusergeräten: Im Rahmen des umfassenden Datensicherheitsangebots von Zscaler bietet Client Connector Endpoint DLP. Damit können Unternehmen Wechseldatenträger, Netzwerkfreigaben, die Synchronisierung persönlicher Cloud-Speicher und das Drucken auf Endgeräten sichern, ohne ein weiteres Einzelprodukt zu benötigen, das separat verwaltet werden muss.

Erkennung versteckter Bedrohungen in Ihrer Umgebung. Bedrohungsakteure nisten sich häufig in Unternehmensumgebungen ein, um sie im Vorfeld eines Angriffs auszuspionieren. Client Connector nutzt eine Deception-Technologie mit realistischen Decoys wie App-Lesezeichen, Cookies, Sitzungen und Passwörter, um diese Angreifer anzulocken. Sobald auf die Decoys zugegriffen wird, generiert der Client zuverlässige Warnmeldungen.

Hervorragende User Experience und höhere Produktivität Im Gegensatz zu herkömmlichen Tools, die den Traffic übers Rechenzentrum umleiten, leitet Client Connector ihn auf dem kürzesten Weg zum Ziel. Darüber hinaus bietet er Zscaler Digital Experience (ZDX) Einblick in Geräteereignisse und -zustand. Administratoren erhalten dadurch einen vollständigen Überblick über die Userverbindung, können Probleme mit der User Experience schneller lösen und die Produktivität von Usern und Administratoren steigern.

Optimiertes Cloud-basiertes Management: Die Verwaltung des Client Connector mit der einheitlichen Benutzeroberfläche Experience Center von Zscaler ermöglicht operative Exzellenz. Er unterstützt kontinuierliches Richtlinien- und Lebenszyklusmanagement zur Verwaltung von Weiterleitungen und Sicherheit sowie Upgrades und Rollbacks — mit integrierten Dashboards und Reporting. Administratoren können Aufgaben außerdem über OneAPI automatisieren, eine zentrale API für die gesamte Zscaler-Plattform.





MODULE DES ZSCALER CLIENT CONNECTOR	
Zscaler Internet Access	ZIA basiert auf einer jahrzehntelangen Führungsrolle im Magic Quadrant für Secure Web Gateway (SWG) und ist die Zscaler-Lösung, die den Internetzugang sichert und gleichzeitig eine Vielzahl granularer Funktionen zum Schutz vor Bedrohungen durchsetzt.
Zscaler Private Access	Zscaler Private Access bietet nahtlose Zero-Trust-Kommunikation für alle User, die auf private Anwendungen zugreifen, mit KI-gestützter User-zu-App-Segmentierung und kontextabhängigen Richtlinien, die zur Risikominderung beitragen.
Zscaler Digital Experience	Zscaler Digital Experience bietet durchgängige Transparenz in Bezug auf User Experience und ermöglicht die schnelle Erkennung, Fehlerbehebung und Lösung von Performance-Problemen, wodurch die Produktivität sowohl für Administratoren als auch für Enduser gesteigert wird.
Zscaler Endpoint DLP	Zscaler Endpoint Data Loss Prevention (DLP) ist Teil der umfassenden Zscaler Data Security. Sie bietet die erforderliche Transparenz und Kontrolle über Gerätedaten und reduziert gleichzeitig die Kosten und Komplexität der Datensicherheit.
Zscaler Deception	Zscaler Deception setzt in Ihrer gesamten IT-Umgebung realistische Decoy-Assets als Köder ein, um versteckte Gegner aus der Reserve zu locken und hochpräzise Warnmeldungen zu generieren, mit denen Unternehmen Bedrohungen schneller erkennen und stoppen können.

FUNKTIONEN UND DETAILS DES CLIENT CONNECTORS	
Umfassende Betriebssystemunterstützung	**Desktop- und Thin-Clients:** • Microsoft Windows 11 und Windows 10 auf x64 und ARM64 • Apple macOS Tahoe (26), Sequoia (15) und Sonoma (14) auf Intel und Apple Silicon • Linux-Desktops (RHEL, CentOS, Fedora, Ubuntu, Debian, openSUSE, Arch Linux, Maya OS) • Google Android auf ChromeOS • eLux und IGEL OS **Mobilgeräte:** • Apple iOS 17, 18 und 26 • Google Android 10, 11, 12, 13, 14, 15 und 16
VDI-Support für Einzel- und Multi-User	• Windows 365 Cloud-PC, Azure Virtual Desktop • AWS Workspaces • Citrix Virtual Apps und Desktops • Omnissa Horizon und Horizon Cloud Multisession-VDI-Umgebungen werden mit Client Connector für VDI unterstützt

Breite Unterstützung für verschiedene Traffic-Typen	• Alle Ports und Protokolle (Z-Tunnel 2.0) • Nur Webtraffic (Z-Tunnel 1.0) • Client-zu-Client-Traffic • Server-zu-Client-Traffic
Tunneltransport	DTLS 1.2, TLS 1.2 und HTTP CONNECT
Verschlüsselung	• Gegenseitige TLS-Authentifizierung • SSL-Pinning für Control Channel Connectivity • FIPS140-Konformität
Optimale RZ-Auswahl	Automatische Auswahl, richtlinienbasiert: Geolokalisierung, bevorzugte RZs, Latenz und Verkehrsziel
Layer-3-Protokollunterstützung	IPv4 und IPv6
Flexible Konnektivitätsmethoden	• Vom User initiiert • Auf Anfrage • Pre-Login-Unterstützung mit Machine Tunnels • Jederzeit aktiv • Unterstützung für Enterprise-VPN-Profil oder Per-App-VPN-Profil unter iOS • Dual-Tunnel-Unterstützung (Enterprise VPN und Per-App VPN-Profil) auf iOS • Arbeitsprofil-Unterstützung für Android
Bereitstellungs- und Lebenszyklusoptionen	• Bereitstellung mit MDMs und UEMs wie Intune, Workspace ONE, JAMF Pro, MobileIron, MaaS360, SCCM und anderen Lösungen • Bereitstellung mit Microsoft GPO in Active Directory (AD) • Manuelle Bereitstellungen mit direkten Downloads von Zscaler • Cloudverwaltete Release-Updates und Rollback-Support • Nahtlose Verteilung vertrauenswürdiger Stamm-CA-Zertifikate zur SSL-Prüfung • API-basierte Richtlinien- und Geräteverwaltung
Userbereitstellung gemäß Branchenstandard	• System for Cross-Domain Identity Management (SCIM) • Just-in-time-Bereitstellung auf SAML 2.0-Basis • Just-in-Time-Bereitstellung von Zugriffsrechten für User im Notfall • Maschinenschlüssel-basierte automatische Geräte-Bereitstellung • Token-basierte automatische User-/Geräte-Bereitstellung • SCEP-basierte Zertifikatsbereitstellung* • Microsoft AD- oder LDAP-Verzeichnisserver-Synchronisierung • Manuelles Hinzufügen oder Massenupload von Usern zur gehosteten Userdatenbank

Unterstützte Authentifizierungoptionen	• SAML 2.0 • Kerberos • Zertifikate und Chipkarten • Multifaktorauthentifizierung (MFA) • FIDO2-konforme Hardware-Token-Unterstützung • Maschinenschlüssel-basierte Geräteauthentifizierung zur Unterstützung vor der Anmeldung • Token-basierte User-/Geräte-Authentifizierung • Passwörter • Unterstützung für Step-up-Authentifizierung • Browserbasierte Authentifizierung
Single Sign-On	• Nahtloses SSO für Windows • Kerberos SSO • Microsoft Enterprise SSO-Plug-In für macOS und iOS • Unterstützung für Apple Enterprise SSO Framework • Unterstützung der OKTA SSO-Erweiterung
Richtlinienbasierte Userbeschränkungen	• Manipulationsschutz • OTP- und Kennwortbeschränkungen zur Steuerung der User-Abmeldung, des Client-Exits und der Dienststoppbeschränkungen
Unterstützte Sprachen	Englisch, Französisch
Enduser-Benachrichtigungen	**Desktop- und Betriebssystem-Benachrichtigungsunterstützung für:** • Benachrichtigungen zu akzeptablen Nutzungsrichtlinien • Servicestatus • Software-Updates • Authentifizierung und regelmäßige erneute Authentifizierungen • Inline-Datensicherheitsereignisse • DLP-Benachrichtigungen und Workflow für Endgeräte • Ereignisbenachrichtigungen zu Richtlinien für den Zugriff auf Internet und private Unternehmensanwendungen • Advanced Threat Protection • Zscaler Zero Trust Firewall, IPS- und DNS-Sicherheitsbenachrichtigungen • Unterstützung für Co-Pilot-Benachrichtigungen innerhalb von Zscaler Digital Experience
Integrierte Tools zur Fehlerbehebung	• Automatisierter verschlüsselter Protokollabruf • Manuelle Protokollexporte • Unterstützung für automatisierte und manuelle Paketerfassung • Automatisierungsunterstützung für Serviceüberwachung und -verwaltung

Umfangreiche Status-Unterstützung	• Dateipfad • Registrierungsschlüssel und -wert • Zertifikatvertrauen • Client-Zertifikat mit CRL • Servervalidiertes Client-Zertifikat • Firewall-Status • Vollständige Festplattenverschlüsselung • Statusmeldungen für AD Domain Join • Statusmeldungen für Entra Domain Join • Prozessprüfungen • Echtzeit-Erkennung von Carbon Black • Client-Ausgangs-IP • Echtzeit-Erkennung von Microsoft Defender • Echtzeit-Erkennung von CrowdStrike • CrowdStrike ZTA Device OS Score • CrowdStrike ZTA Sensor Score • Virenschutz-Erkennung • Überprüfung der Betriebssystemversion • JAMF-Agent-Erkennung • JAMF-Risikostufe • Unbefugte Änderungen • Eigentumsvariable • Version des Zscaler Client Connector
Weitere Funktionen	• Disaster Recovery und Business Continuity-Support • Eingebettete Captive-Portal-Verwaltung mit optionaler Netzwerksperre • Client Connector-Endgerät-Firewallverwaltung mit lokaler LAN-Blockierung • Gerätequarantäne-Unterstützung • Automatisierte Erkennung und Umschaltung vertrauenswürdiger Netzwerke • Unterstützung für Umgebungen ohne Standardroute (NDR)

Über Zscaler

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Die Zscaler Zero Trust Exchange™ schützt tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlusten. Als weltweit größte Inline-Cloud-Sicherheitsplattform wird die SASE-basierte Zero Trust Exchange™ in über 150 Rechenzentren auf der ganzen Welt bereitgestellt. Weitere Informationen erhalten Sie auf **www.zscaler.com/de**. Gerne können Sie uns auch auf X folgen **@zscaler**.

+1 408 533 0288 **Zscaler, Inc. (Hauptsitz) • 120 Holger Way • San Jose, CA 95134, USA** **zscaler.com/de**

zscaler™

Zero Trust Everywhere