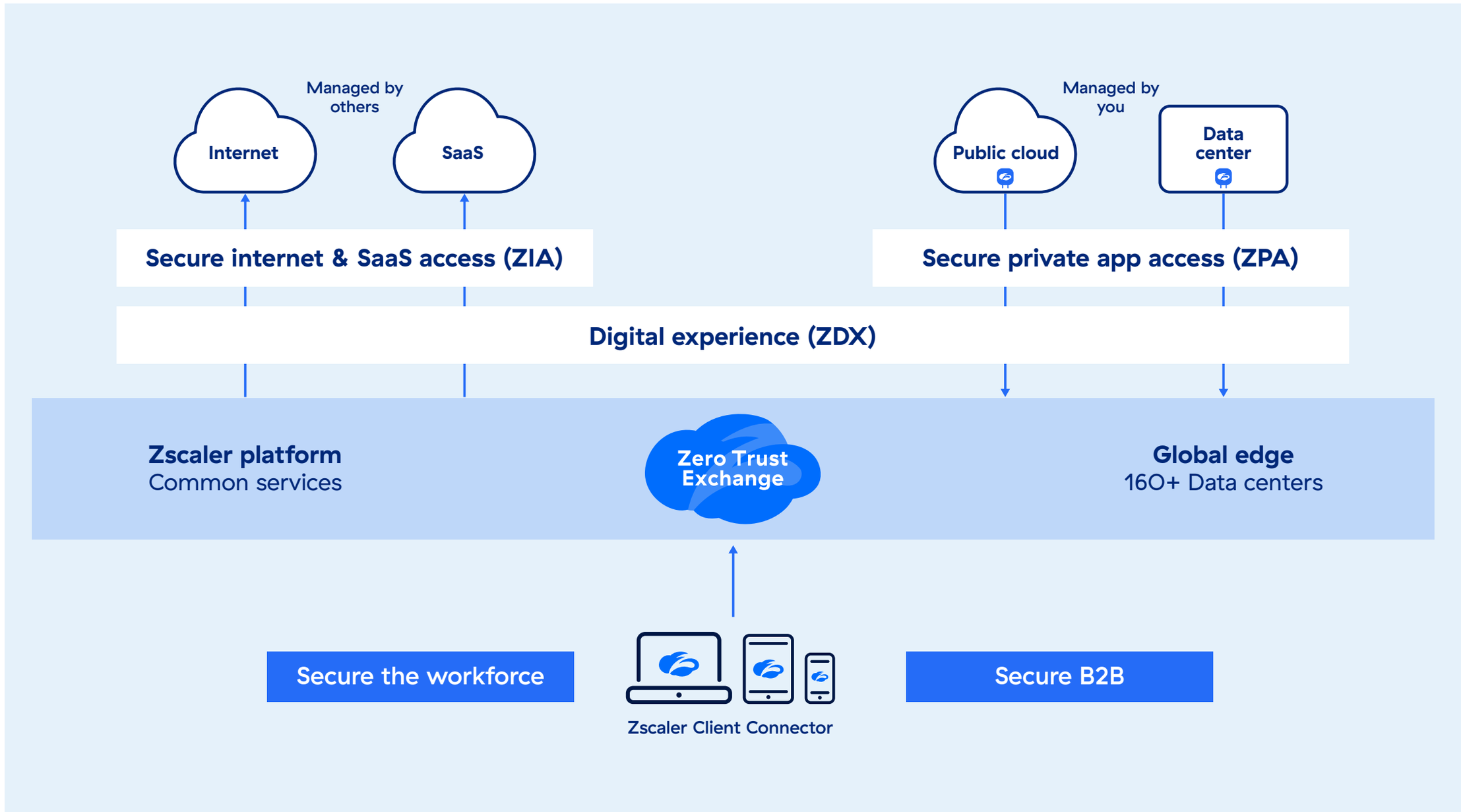
Zscaler Client Connector

Fast, secure, and reliable access to any destination—from any location or device.

DATA SHEET

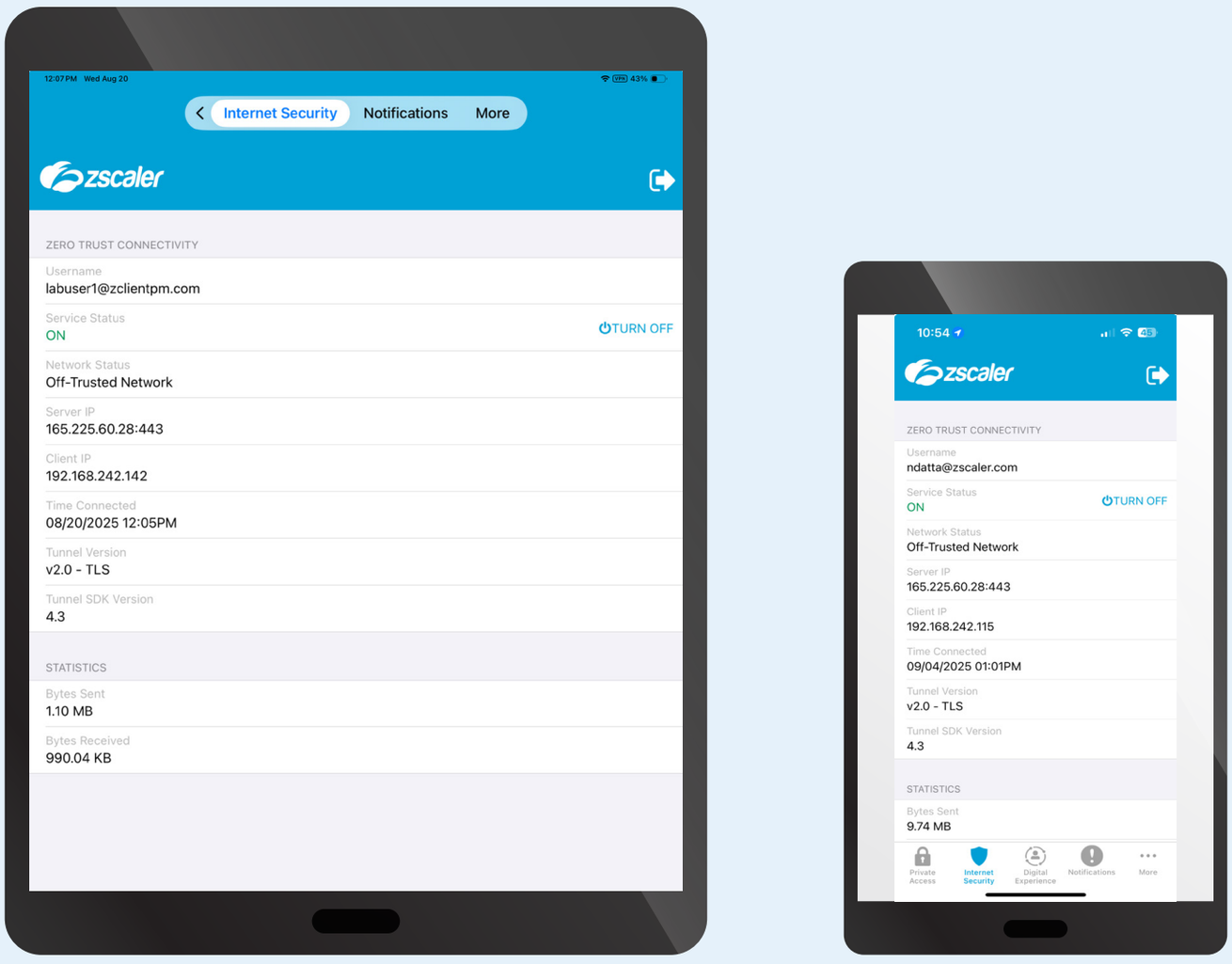


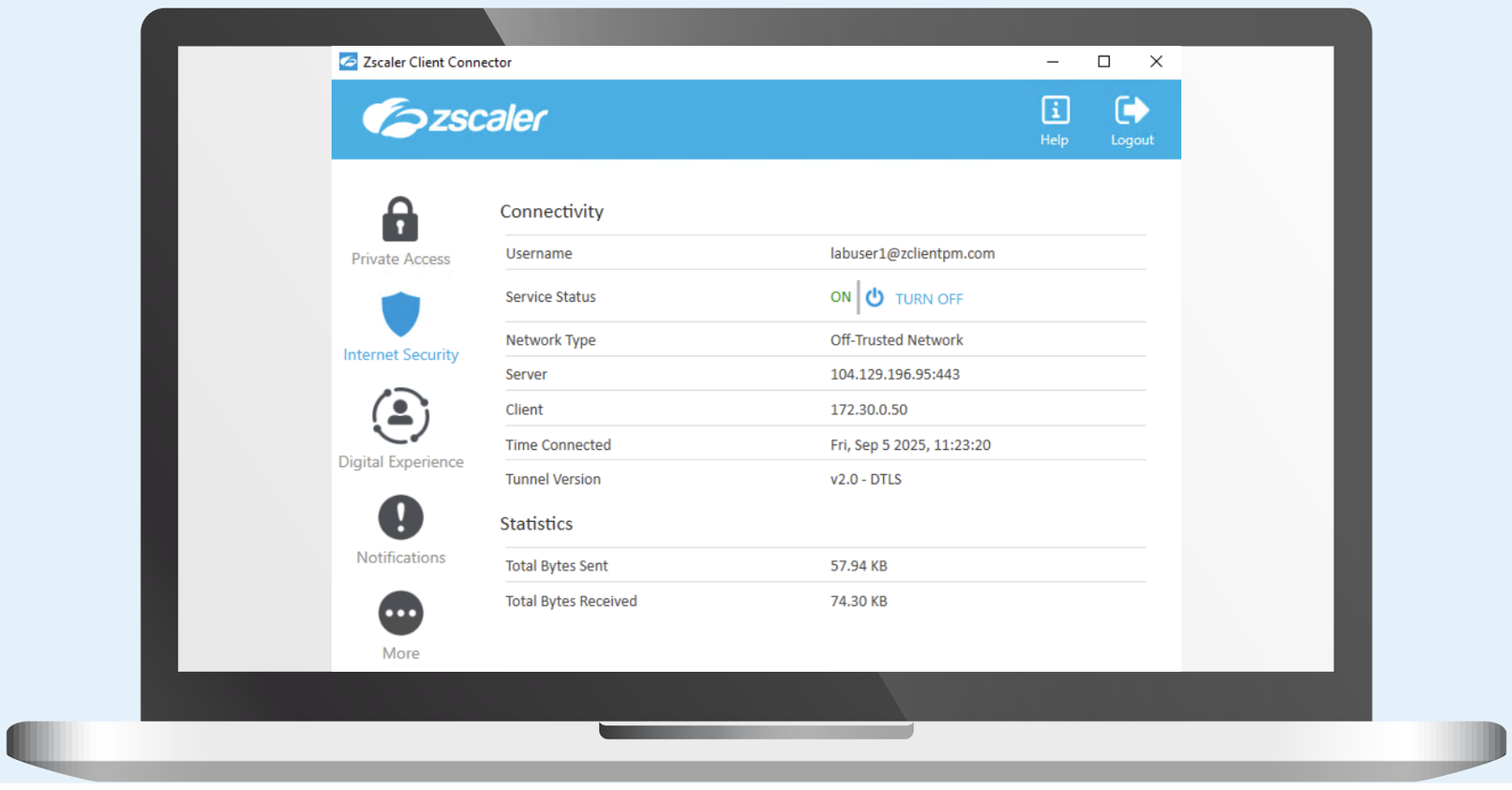
Employees today work drastically differently than they used to. They can now use a wide variety of devices, while working from anywhere, to access cloud apps and other destinations around the world. This new, hybrid workforce demands fast and seamless access to IT resources—but that can't come at the cost of exposing data to risk. So, for any organizations that want to succeed today, they must secure globally distributed endpoints while also ensuring productive user experiences. To accomplish this, countless IT teams turn to Zscaler and its endpoint agent, Client Connector.

In the past, when users and apps were located at the office, it made sense to rely on network-centric security and connectivity solutions. But today, off-premises employees are accessing off-premises apps via networks that IT teams don't control. Backhauling this traffic to the data center to secure it adds latency that disrupts productivity. More importantly, backhauling increases risk by connecting users to the corporate network, allowing them to abuse excessive permissions and move laterally across network-connected resources—not to mention, it expands the attack surface and entails other key security weaknesses.

Zero trust architecture is the solution to these problems. Zscaler delivers it as a service from the Zero Trust Exchange, the world's largest cloud security platform, which acts as an intelligent switchboard to provide any-to-any zero trust communications by using business policies—not networks. The Zero Trust Exchange delivers least-privileged access directly to IT resources based on context rather than a user's IP address, and it does so at the edge from over 160 points of presence worldwide. In other words, IT teams can stop threats and data loss while giving users exceptional digital experiences on any device, anywhere.

Zscaler Client Connector plays a central role in delivering any-to-any zero trust communications. It is Zscaler's lightweight yet multifaceted endpoint agent, which facilitates performant, least-privileged access directly to the internet and IT resources for users everywhere. Additionally, it provides a wealth of other functionality that further improves security and connectivity while eliminating point products and their dedicated agents.





Zscaler Client Connector Benefits

Client Connector's benefits can more or less be grouped into the seven categories shown below. For even more detail, see the table at the end of this data sheet.

Zero trust communications to any destination
Organizations no longer need separate solutions with separate agents to secure access to different destinations. Client Connector provides least-privileged, zero trust access to any destination, including the web, SaaS, and private apps. This is inline with Gartner's vision of SSE and SASE, and ensures that devices aren't slowed down by agent bloat.

Zero trust communications for any device
Beyond securing access to any destination, organizations must secure access on any device. That's because employees now use a diverse assortment of desktops, laptops, tablets, and smartphones with a variety of operating systems. Fortunately, Client Connector can secure any device, keeping your employees both safe and productive.

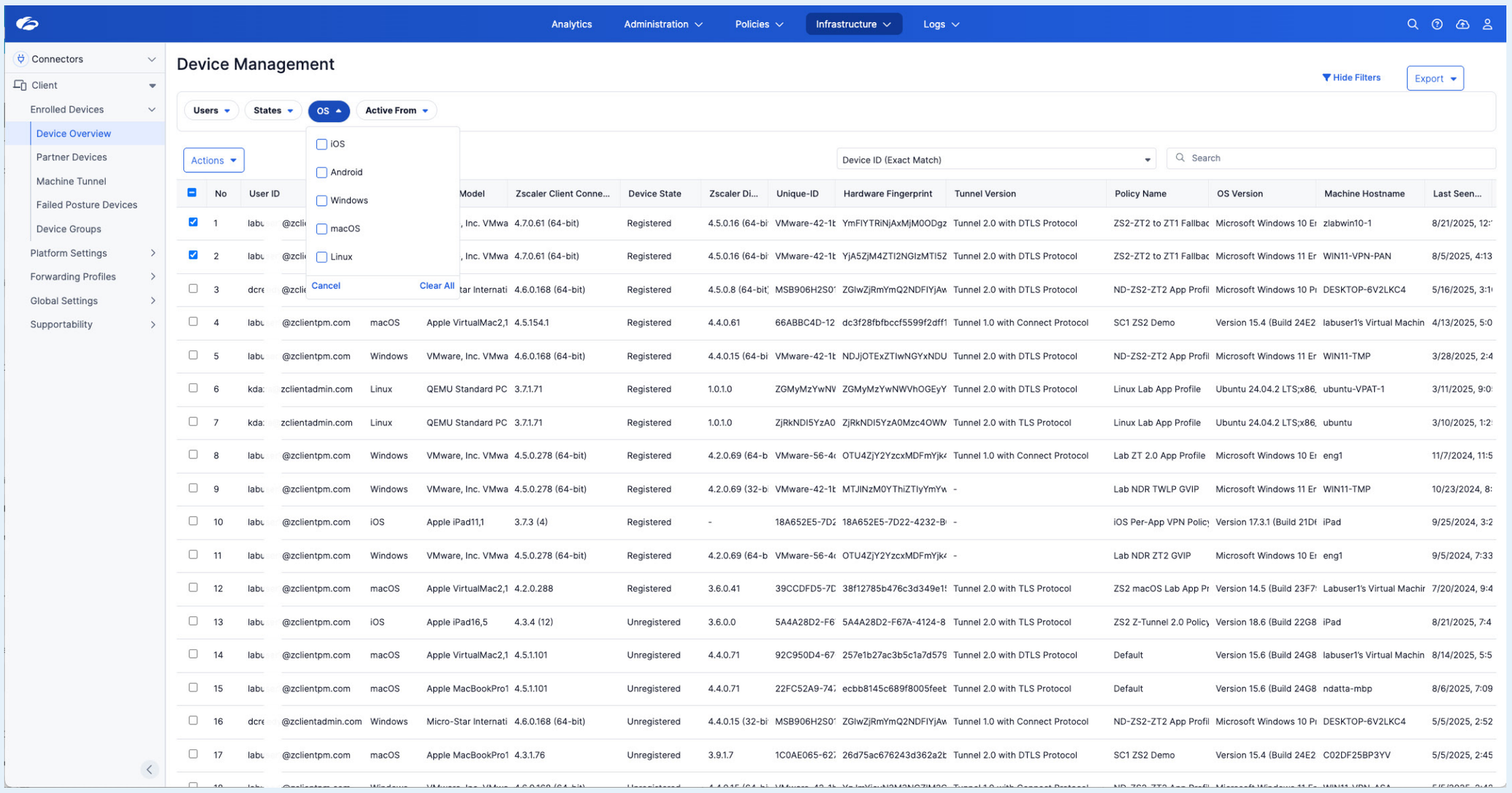
Context-aware, intelligent security
Identity alone is not enough to govern access to IT resources (identities can be stolen, and even legitimate users can carelessly harm their employers). Organizations must govern access based on context and risk. Client Connector enables this by providing device security posture insights that enable intelligent, adaptive access control.

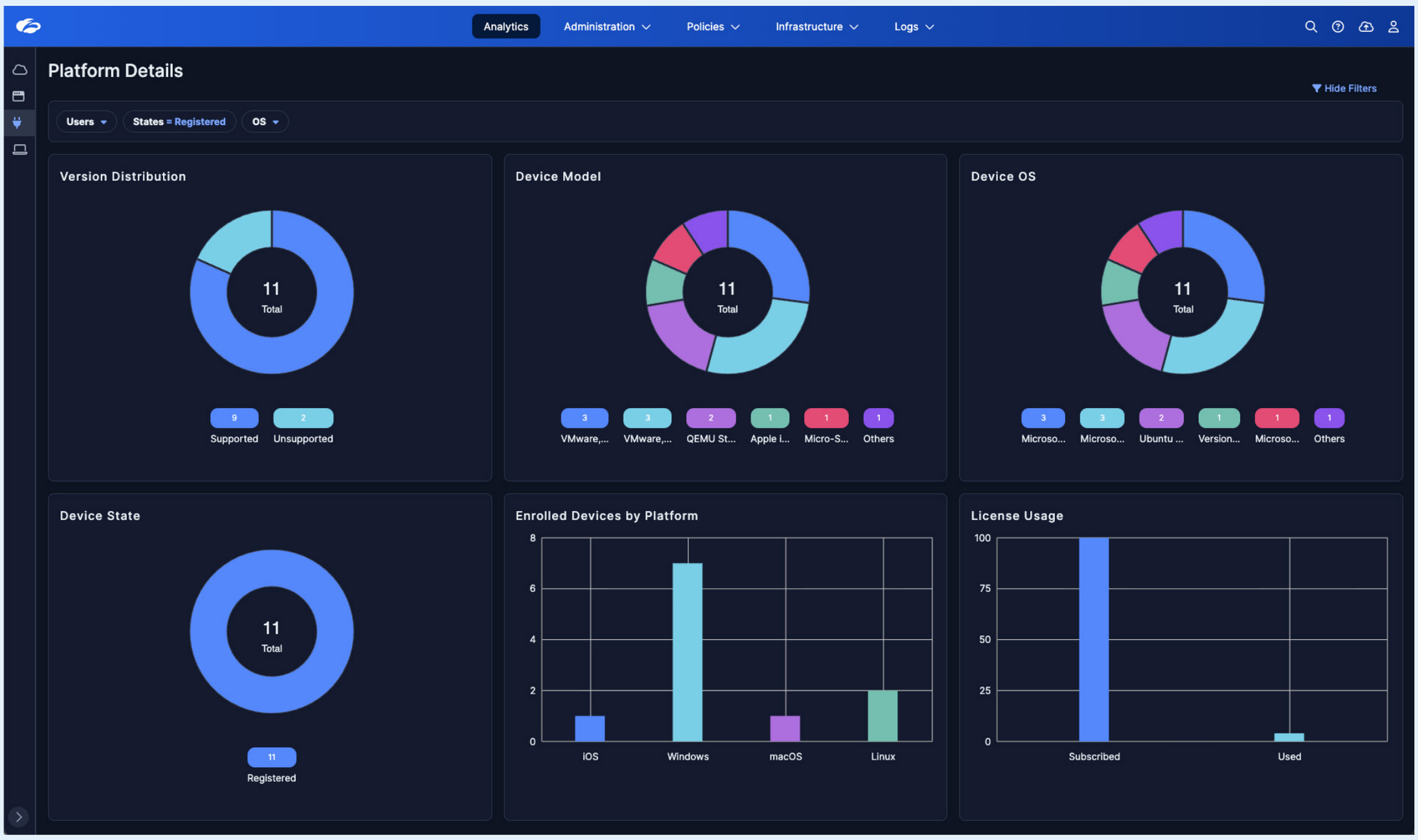
Data protection on end user devices
As part of Zscaler's complete data security offering that secures any leakage channel, Client Connector offers endpoint DLP. With it, organizations can secure removable storage, network shares, personal cloud storage sync, and printing on endpoints without needing another point product that has to be managed separately.

Detection of hidden threats in your environment
Stealthy adversaries often hide in organizations' environments to perform reconnaissance for malicious schemes. Client Connector employs deception technology that uses realistic decoys of app bookmarks, cookies, sessions, and passwords to lure these attackers. Once the decoys are accessed, it generates high-fidelity alerts.

Superior user experiences and productivity
Unlike legacy tools that backhaul traffic, Client Connector steers traffic via the shortest path to its destination. It also gives Zscaler Digital Experience (ZDX) visibility into device events and health, giving admins a full view across the user connection, accelerating resolution of user experience issues, and enhancing productivity for users and admins.

Streamlined cloud-based management
Managing Client Connector with Zscaler's unified UI, Experience Center, unlocks operational excellence. It enables ongoing policy and lifecycle management to administer forwarding and security, and upgrades and rollbacks—with integrated dashboards and reporting. Admins can also automate tasks via OneAPI, a single API for the entire Zscaler platform.





ZSCALER CLIENT CONNECTOR MODULES	
Zscaler Internet Access	Built on a decade of leadership in the Magic Quadrant for Secure Web Gateway (SWG), ZIA is the Zscaler solution that secures access to the internet while enforcing a variety of granular threat protection functionality.
Zscaler Private Access	Zscaler Private Access offers seamless zero trust communications for all users accessing any private applications, with AI-powered user-to-app segmentation and context-aware policies that help reduce risk.
Zscaler Digital Experience	Zscaler Digital Experience provides end-to-end visibility into user experiences and enables rapid detection, troubleshooting, and resolution of performance issues, enhancing productivity both for admins and end users.
Zscaler Endpoint DLP	Zscaler Endpoint Data Loss Prevention (DLP) is part of the complete Zscaler Data Security solution. It provides the visibility and control you need over data on devices while reducing the cost and complexity of data security.
Zscaler Deception	Zscaler Deception deploys realistic decoy assets throughout your IT environment to lure hidden adversaries and generate high-fidelity alerts that allow organizations to detect and stop threats more quickly.

CLIENT CONNECTOR FEATURES AND DETAILS	
Comprehensive operating system support	**Desktop and thin clients:** • Microsoft Windows 11 and Windows 10 on x64 and ARM64 • Apple macOS Tahoe (26), Sequoia (15), and Sonoma (14) on Intel and Apple Silicon • Linux desktops (RHEL, CentOS, Fedora, Ubuntu, Debian, openSUSE, Arch Linux, Maya OS) • Google Android on ChromeOS • eLux and IGEL OS **Mobile:** • Apple iOS 17, 18, and 26 • Google Android 10, 11, 12, 13, 14, 15, and 16
Single user and multi-user VDI support	• Windows 365 Cloud PC, Azure Virtual Desktop • AWS Workspaces • Citrix Virtual Apps and Desktops • Omnissa Horizon and Horizon Cloud Multi-session VDI environments supported with Client Connector for VDI

Broad support for traffic types	• All ports and protocols (Z-Tunnel 2.0) • Web traffic only (Z-Tunnel 1.0) • Client-to-client traffic • Server-to-client traffic
Tunnel transport	DTLS 1.2, TLS 1.2, and HTTP CONNECT
Encryption	• Mutual TLS authentication • SSL Pinning for control channel connectivity • FIPS140 compliance
Optimal DC selection	Automatic selection Policy-based: Geolocation, Preferred DCs, Latency and traffic destination
Layer 3 protocol support	IPv4 and IPv6
Flexible connectivity methods	• User initiated • On-demand • Pre-login support with Machine Tunnels • Always On • Enterprise VPN Profile or Per-App VPN profile support on iOS • Dual-tunnel support (Enterprise VPN and Per-App VPN Profile) support on iOS • Work Profile support for Android
Deployment and lifecycle options	• Deploy using MDMs and UEMs like Intune, Workspace ONE, JAMF Pro, MobileIron, MaaS360, SCCM, and other solutions • Deploy using Microsoft GPO in Active Directory (AD) • Manual deployments using direct downloads from Zscaler • Cloud managed release updates and rollback support • Seamless distribution of trusted root CA certificates for SSL inspection • API-based policy and device management
Industry standard user provisioning	• System for Cross-Domain Identity Management (SCIM) • Just-in-time SAML 2.0 based provisioning • Just-in-time provisioning for Emergency User Access • Machine-key-based device auto-provisioning • Device-token-based user/device auto-provisioning • SCEP based certificate provisioning* • Microsoft AD or LDAP Directory Server synchronization • Manual addition or bulk upload of users to Hosted User DB

Supported authentication options	• SAML 2.0 • Kerberos • Certificates and smart cards • Multi-factor authentication (MFA) • FIDO2-compliant hardware token support • Machine-key-based device authentication for pre-login support • Token-based user/device authentication • Passwords • Step-up authentication support • Browser-based authentication
Single sign-on	• Seamless SSO for Windows • Kerberos SSO • Microsoft Enterprise SSO plug-in for macOS and iOS • Apple Enterprise SSO Framework support • OKTA SSO Extension support
Policy-based user restrictions	• Anti-tampering support • OTP and password restrictions to control User Logout, Client Exit, and service stop restrictions
Supported Languages	English, French
End-user notifications	**Desktop and OS notification support for:** • Acceptable Usage Policy notifications • Service status • Software updates • Authentication and periodic re-authentications • Inline data security events • Endpoint DLP notifications and workflow • Internet and Private App access policy event notifications • Advanced Threat Protection • Zscaler Zero Trust Firewall, IPS and DNS security notifications • Zscaler Digital Experience Co-pilot notification support
Built-in troubleshooting tools	• Automated encrypted log fetch • Manual log exports • Automated and manual packet capture support • Automation support for service monitoring and management

Extensive posture support	• File Path • Registry Key and Value • Certificate Trust • Client certificate with CRL • Server-validated Client certificate • Firewall status • Full Disk encryption • AD Domain Join status • Entra Domain Join status • Process checks • Real-time Carbon Black detection • Client Egress IP • Real-time Microsoft Defender detection • Real-time CrowdStrike detection • CrowdStrike ZTA Device OS Score • CrowdStrike ZTA Sensor Score • Detect Antivirus • OS version checks • JAMF agent detection • JAMF Risk level • Unauthorized modification • Ownership variable • Zscaler Client Connector Release Version
Other capabilities	• Disaster Recovery and Business Continuity support • Embedded Captive Portal Handling with optional Network Lockdown • Client Connector endpoint firewall management with local LAN blocking • Device Quarantine support • Automated Trusted Network detection and switching • No Default Route (NDR) environment support

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

zscaler™

Zero Trust Everywhere