jamf

JAMF PRIVATE ACCESS

Enable fast, simple and secure Zero Trust Network Access to any corporate resource.

Provide teams the flexibility to work at any time and from anywhere by connecting them securely to the applications they need.

Private Access uses identity and app centric policies to enable productivity while eliminating the broad discoverability and reachability of data and apps that users should not be able to access.

Strong Security

Private Access is architected using a cloud-based software-defined perimeter (SDP) that creates secure, isolated connections for each application. Through least-privilege enforcement and real-time device posture checks, access is granted to each application only for specific, authorized users.

Enhanced Manageability

Private Access uses an entirely cloud-based architecture which requires no on-premises equipment to manage or complex sizing requirements. Private Access is more efficient, avoiding the need to full tunnel all traffic which is unnecessarily expensive, but without losing visibility and control of what is being accessed (i.e. policy without routing).

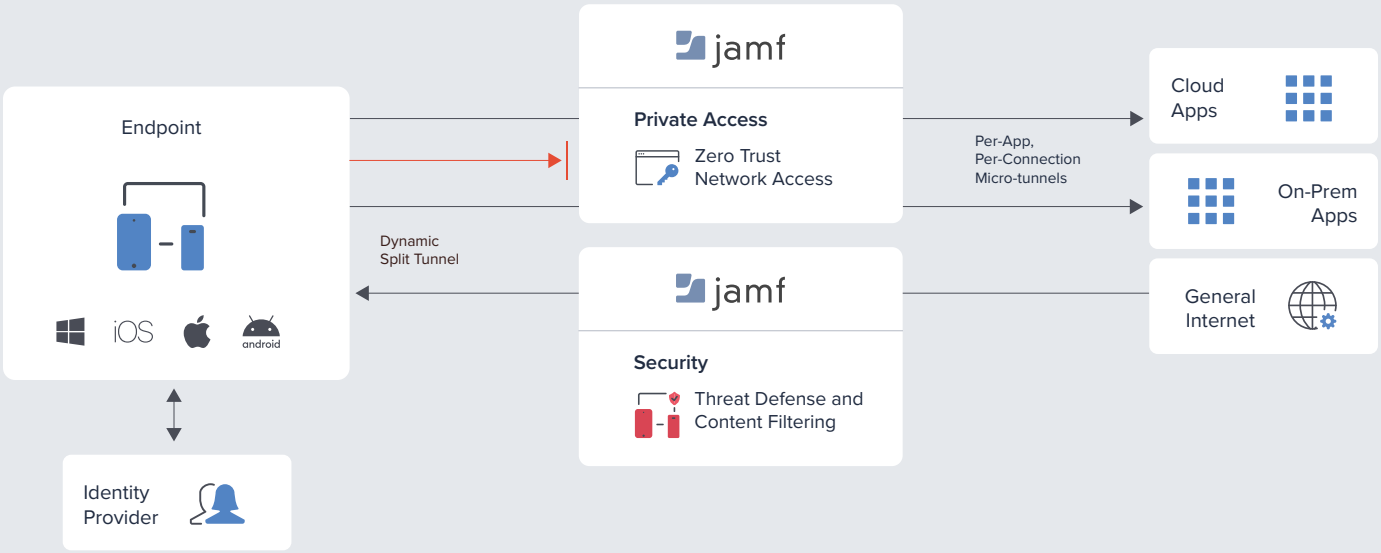
Intuitive User Experience

Private Access utilizes a protocol that was designed for fast and secure remote working. When coupled with our cloud scale and the ability to avoid unnecessary traffic backhauling, users enjoy a seamless access experience where latency issues are eliminated. The service is efficient and gracefully accommodates network transitions, allowing the user to go from cellular to Wi-Fi and back again without disruption.

jamf

Architecture

Built in the cloud Jamf's state of the art architecture can scale to provide access to any application hosted in the public or private cloud, as well as on-premise. The Jamf Solution Guide can be found online and contains details of Jamf's architecture.



Required

- Any app (supports on-premises, cloud, SaaS)
- Any device (supports all modern operating systems)
- Any identify provider (with Azure AD federation)

Not Required

- No hardware to deploy
- No device certificates to manage
- No manual traffic routing to configure

Optional

- Endpoint management to streamline deployment
- Centralized security logging for enhanced visibility and response
- Dedicated egress IP address and server locations

Features

Cloud SDP

Private Access is architected using a cloud-based software-defined perimeter that creates secure, isolated connections for each application. Through least- privilege enforcement and real-time device posture checks, access is granted to each application only for specific, authorized users.

App Microtunnels

Private Access is a Zero Trust Network Access solution, the device and any apps running on it are blind to network infrastructure. Private Access uses app-level microtunnels, enabling fine-grained control both at connection establishment and throughout active sessions.

Session Reporting

Detailed session reporting enables monitoring of active users and the application they are using. Real-time statistics provide insight into unusual activity, session duration or bandwidth requirements. Comprehensive visibility allows administrators to monitor inappropriate content, detect malware and identify data leaks.

Next-Generation Protocols

The majority of endpoints utilize Wi-Fi or cellular connections, but users and applications require the performance expected from a wired connection. Private Access makes connecting security fast, versatile and lightweight, by providing a silent and seamless service even if the user is working while on the move.

Identity Based Solution

Private Access uses identity-based policies to assign user and application permissions. Integration with existing directory services allows for rapid deployment and management of policies. The only way for a tunnel to be established is for the user to have the appropriate permissions to the specified application.

Dynamic Split-Tunnel

Private Access uses an intelligent tunneling protocol that routes only the traffic from an application on the authorized user's device to the associated application on the other side of the Cloud SDP. This ensures that the app microtunnel policy is properly enforced, while also delivering an optimal experience to the end user.

Single Packet Authorization

Eliminate the discoverability of applications by unauthenticated parties. Single Packet Authorization requires the identity of the user and device to be verified before brokering access.

Adaptive access

Private Access provides real-time user and device risk assessments that can influence routes and be used as signals via third-party integrations. If a device risk state should change, Private Access can terminate a session or alter routes, according to policy, in real-time.

Jamf Private Access works seamlessly with your existing IT services and technologies.

Deep integrations with Microsoft, Google, Cisco and more help you extend the value of your existing tech stack.

jamf

www.jamf.com

To learn more about how Private Access can safely connect workers to devices app and corporate data, please visit **jamf.com**