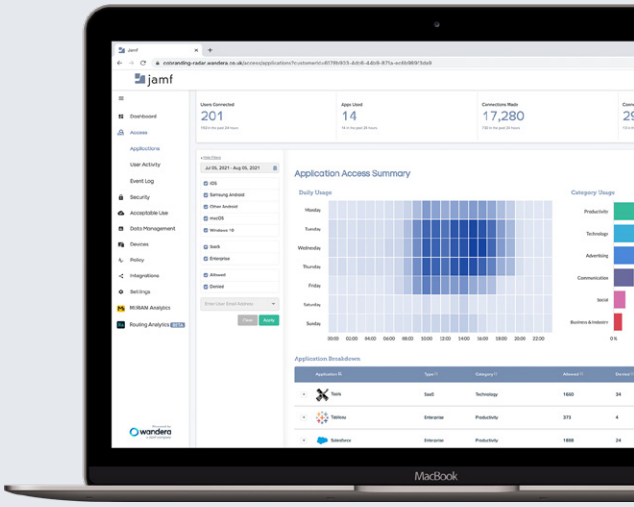
jamf

JAMF PRIVATE ACCESS

A Zero Trust Architecture

Jamf Private Access is a software-defined perimeter that provides end-users with secure connectivity to any corporate resource. Zero Trust policies are enforced by strong authentication and granular authorization technologies.



Strong authentication

Single Packet Authorization ensures only authenticated and authorized users and devices can access corporate applications, to everyone else they are invisible. The identity of users is confirmed via streamlined MFA methods including possession of a specific device or the use of a biometric identifier. Devices must be verified as secure, in the event that Jamf's built-in endpoint risk detection identifies that an operating system or app is compromised, or when content or malware threat is detected, access can be denied.

Granular authorization

Least-privilege access enforced by identity-centric policies, users are granted access to only the resources they need, and those they don't are hidden from them. Specific security requirements must be met to gain access to corporate resources, these can be tailored per-application as needed. When access is granted individual micro-tunnels are established for each application session. The micro-tunnels prevent lateral movement by restricting users to that allocated application. Risk policies can be dynamically applied to separate micro-tunnels.

jamf

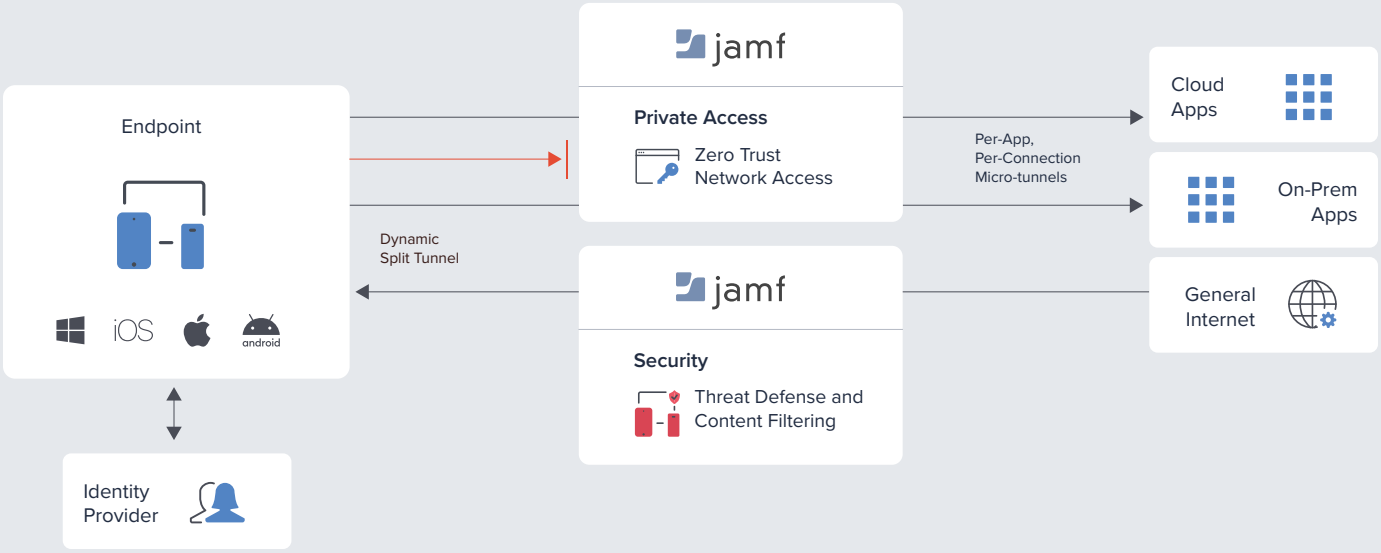
Architecture

Endpoint app

Telemetry from the endpoint such as OS version, system parameters, and device configuration details is collected; this includes checks for the modification of system libraries and privilege escalation. This device-level information, along with user authentication details, is used to assess whether access privileges should be granted. All Jamf capabilities are provided through the all-in-one app.

Software-Defined Perimeter

Only packets from authenticated users is allowed to travel over the Jamf network. Consisting of over 30 data centers worldwide Private Access is low latency and highly resilient service. Sessions can be terminated or routes altered, in real-time, according to Zero Trust policies such as when a device risk state changes.



Dynamic Split-Tunnel

Individual packets are routed based on application layer properties to reduce the transmission time and minimize the latency for each app. Web browsing data can be tunneled to Jamf's secure cloud or routed directly to the internet.

Micro-tunnels

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.

Software-Defined Perimeter

Only packets from authenticated users is allowed to travel over the Jamf network. Consisting of over 30 data centers worldwide Private Access is low latency and highly resilient service. Sessions can be terminated or routes altered, in real-time, according to Zero Trust policies such as when a device risk state changes.

jamf

Workflows

End-user enrolment

The Jamf app can be pushed to any endpoint enrolled into a device manager, personal and unmanaged devices can find the app in the device's respective app stores. Jamf's app is activated via SSO or with the user's business credentials, the end-user does not configure any settings.

Deploying applications

Connectivity to new applications via Jamf is configured entirely through the unified console, no connectors need to be deployed at any stage. Set up is done using the application's hostname not IP address and no internal routing information is required.

Policy assignment

Synchronization with the identity provider allows all lifecycle management tasks to be automated. Security and access policies are assigned and managed in real-time by this integration. Permissions can be assigned to user groups and individuals, and different security requirements can be set for each application.

Monitoring and reporting

Jamf's dashboard allows events to be reviewed in real-time with real-world names, not just device IDs. Custom reports can be exported on-demand from the console or the granular data can be viewed through any 3rd party tool integrated with Jamf's log streaming services.

Availability and resilience

The Jamf platform is built entirely in public cloud data centers using industry-standard operating systems and applications. Jamf's edge infrastructure is built across 30+ data centers worldwide to provide 99.99% availability for users in any location. To ensure capacity Lazy Loading is used to intelligently allocate resources when required. Should one of the edge data centers be unavailable Jamf's Dynamic Split-Tunnel will automatically reroute traffic to an available data center without dropping any sessions.

Privacy and compliance

Data at rest or in transit is encrypted end-to-end across Jamf's platform. All end-user usage information is deleted automatically after 6 months and personal details are wiped when a user is unenrolled. Jamf is a member of the EU-US Privacy Shield and is ISO27001, GDPR, CCPA and HIPAA compliant.

Compatibility

Endpoint app

The app works with all modern operating systems including iOS, Android, Windows 10 and macOS.

Device manager

The Jamf app can be pushed with all common device management services. Conditional Access/Launch policies can be enforced and enhanced with this integration.

Identity provider

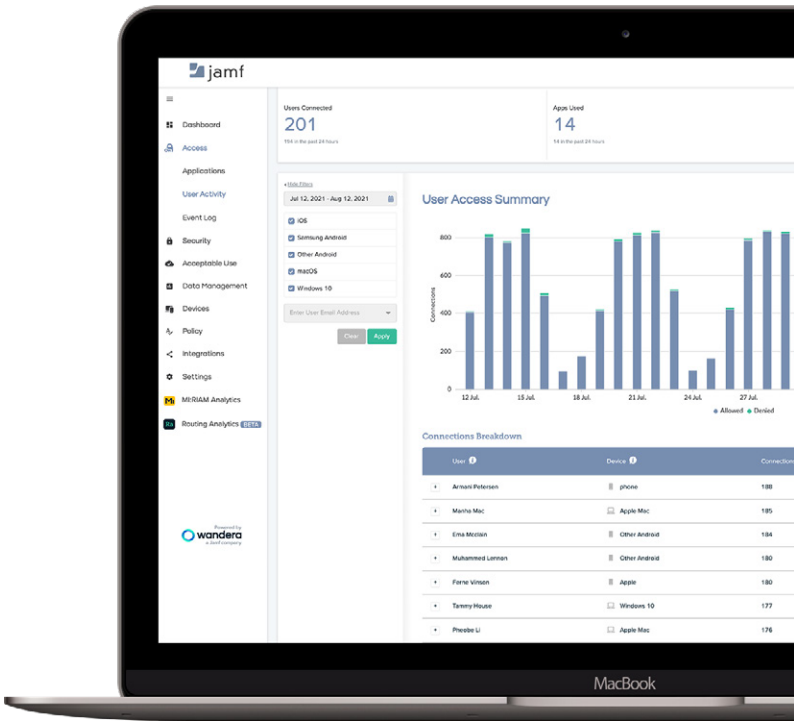
Jamf has native integration with Microsoft Azure Active-Directory, any provider can be used if federated with Azure Active-Directory.

Application type

Private Access supports any application using any protocol, and any hosting location may be used: on-premises, private/public cloud, and even SaaS.

Log streaming

Jamf supports most popular SIEM and SOAR services out-of-the-box. Customizable open APIs and datastreams allow Jamf's logs to be securely shared via TLS connections with any tool.



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, contact your Jamf Authorized Reseller.