JOINT SOLUTION BRIEF

zscaler + Jamf

End-to-end zero trust solution that ensures fast and secure access to internet, SaaS, and private applications—on any network, from any location, and on any device.

INTEGRATION HIGHLIGHTS

✓ **Enhanced device-based security enforcement** with real-time risk assessments.

✓ **Streamlined zero-trust access** for macOS devices to private and cloud-based applications.

✓ **Automated remediation workflows** that enforce security policies dynamically.

The Market Challenge

As enterprises evolve, securing access to critical applications and resources has become more challenging. Organizations need a zero-trust approach that provides continuous security from endpoint to network to application.

Without proper integration, security tools operate in silos, leading to:
- Limited visibility across endpoints and network traffic
- Inconsistent enforcement of security policies
- Increased dwell times for security incidents

A modern security approach requires context-aware, zero-trust access that dynamically adapts to evolving threats.

The Solution

Zscaler and Jamf provide a seamless, device-aware security integration that combines Jamf's Apple device security intelligence with Zscaler's zero-trust access controls.

How It Works:
1. Jamf Device Identity evaluates the macOS device's security posture using Jamf Security Cloud.
2. Jamf Trust (installed on the device) shares the device risk score and management state with Zscaler's policy engine via ZCC.
3. ZCC enforces conditional access policies based on real-time risk insights from Jamf.
4. If a device falls out of compliance (e.g., outdated OS, disabled security controls, detected threats), Zscaler blocks access until security posture is restored.

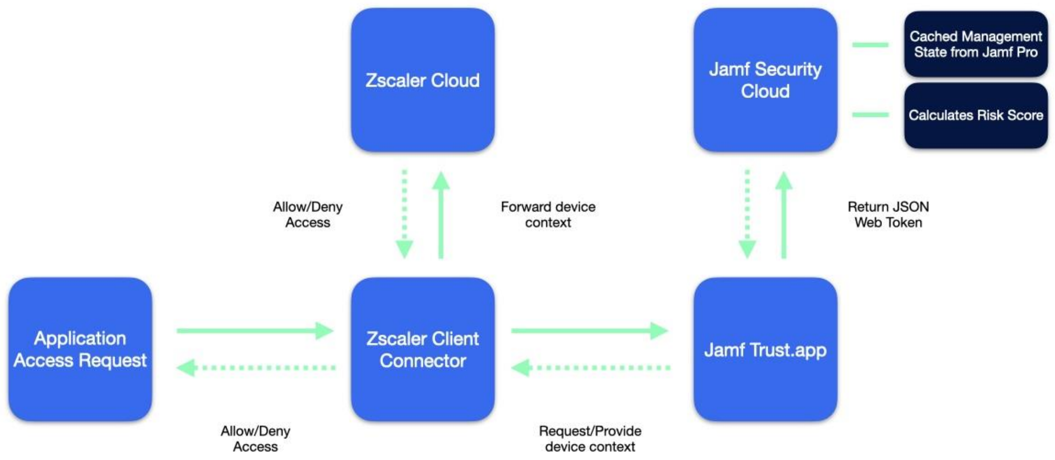
This integration allows organizations to:
- Apply risk-based conditional access for private (ZPA) and public (ZIA) applications.
- Continuously monitor device security posture and adjust access dynamically.
- Reduce reliance on passwords by leveraging device trust for authentication.
- Prevent lateral movement of threats by enforcing zero-trust principles.

Together, Jamf and Zscaler integrate to provide security teams with a holistic view of their macOS security posture.

Solution Components Deep Dive

Jamf and Zscaler integrate to provide security teams with a holistic view of their macOS security posture.

- Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) offer secure zero-trust access.
- Jamf Security Cloud continuously ingests Zscaler logs for deeper security insights and accelerated threat detection.
- AI-driven analytics help security analysts quickly investigate and respond to threats.



Real-Time Risk Signaling

- Jamf Security Cloud evaluates device compliance based on OS version, endpoint security settings, and network activity.
- Zscaler uses Jamf risk scores to enforce access policies dynamically, ensuring only secure devices can connect.
- If a device is compromised, Zscaler can automatically revoke access and trigger remediation workflows.

Enhanced Threat Detection & Prevention

- Blocks phishing sites, malware, and suspicious network activity.
- Enforces security policies across endpoints and networks.
- Strengthens compliance by validating device security posture pre- and post-authentication.

Comprehensive Visibility

Zscaler and Jamf unify endpoint and network security by sharing real-time device context, enabling security teams to enforce dynamic, risk-based access policies. By integrating Jamf's macOS security insights with Zscaler's policy engine, organizations gain comprehensive visibility into device posture and network activity, allowing for seamless threat detection, faster investigations, and automated remediation—all without switching between tools.

> In response to the rise of Apple-specific security threats, Jamf and Zscaler effectively advance the overall security posture of any organization using Apple.
>
> Matt Arsenault
>
> VP, Partnerships & Security Strategy

Zscaler + Jamf Benefits

ACTION	DESCRIPTION
Increase security with passwordless authentication	Eliminate passwords, the most exploited threat vector, by ensuring passwordless access for Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA).
Validate device security controls for all connected devices	Ensure devices meet your organization's security requirements before authentication. If a device is out of compliance, access is denied via policy directives.
Continuous device security evaluation	Verify that critical security settings (e.g., disk encryption, Endpoint Detection & Response) remain active throughout the session.
Automated access revocation for high-risk devices	If a device's risk posture falls out of compliance, Beyond Identity signals Zscaler to log out the user, requiring re-authentication only once compliance is restored.
Simplified management with cloud-based enforcement	Dynamically manage role-based access and simplify IT operations with cloud-native security enforcement.

Conclusion

Zscaler and Jamf provide an end-to-end zero trust solution that enhances macOS security while enabling seamless user access. By integrating real-time device context with policy-driven access controls, organizations can minimize risk, prevent threats, and improve user productivity.

This partnership ensures that security teams can enforce access policies dynamically, block threats in real time, and achieve frictionless zero-trust security without relying on traditional VPNs or perimeter-based defenses.

Learn more at www.zscaler.com/partners/technology

Experience your world, secured.

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