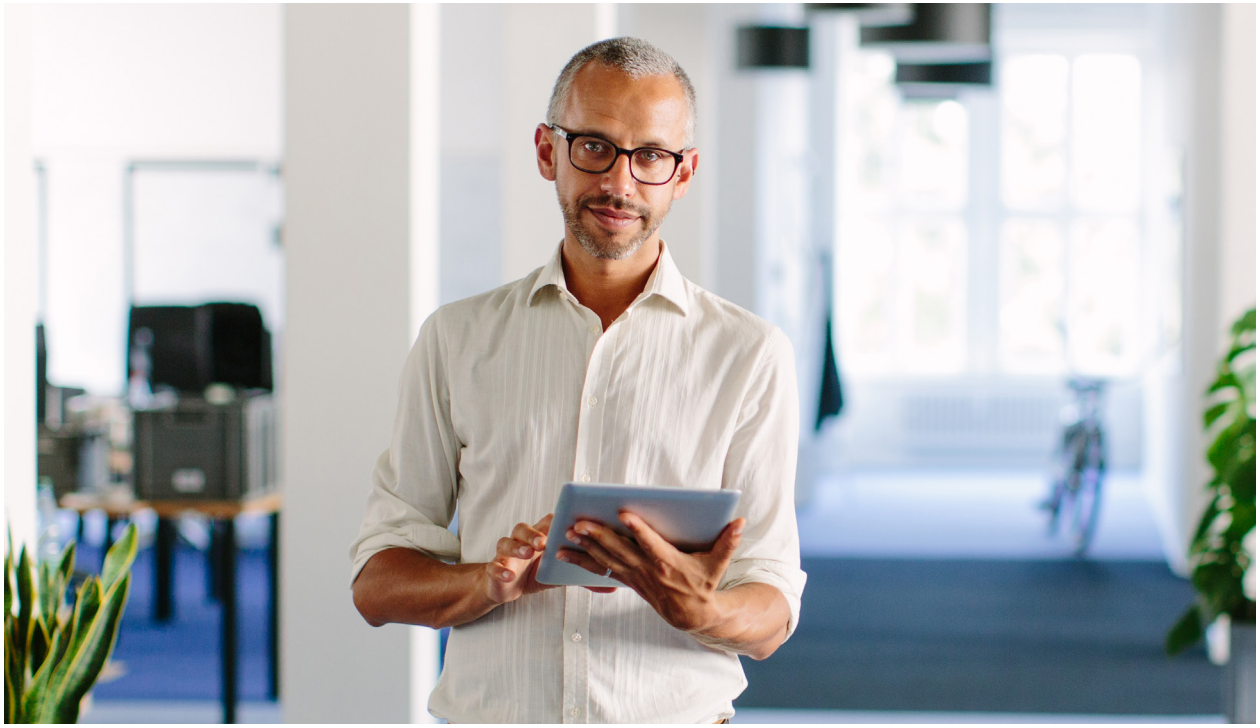
Protect your devices, users and applications from cyber threats

Jamf Threat Defense provides cloud-based security that operates on the device and in the network



Powerful endpoint security

Jamf Threat Defense detects and tackles the broadest range of endpoint threats, including device vulnerabilities and malicious or risky apps. Comprehensive risk assessments are continuously performed to identify threats so security policies can be enforced in real-time.

Network defences protect users and data

Stop attacks before they hit with in-network defences. Block malicious sites, including zero-day phishing, which are designed to capture business credentials. Prevent command-and-control and data exfiltration by blocking connectivity to risky sites. For additional safety, connections are secured automatically when man-in-the-middle attacks are detected.

Adaptive access to your applications

Elevate your security by allowing only secure and trusted devices to access business applications. Use Conditional Access to prevent app access when an endpoint is compromised or at high risk. Adaptive access policies can be enforced through Jamf Private Access or Jamf's flagship device managment solution, Jamf Pro.

Comprehensive threat detection and prevention

Advanced app insights

Jamf Threat Defense provides advanced app intelligence that can be used both for app-vetting workflows and security investigations. A risk score is given for each app, along with a detailed report listing the permissions and embedded URLs that put both user and organisational data at risk.

Dynamic data encryption

Jamf Threat Defense prevents compromised Wi-Fi infrastructure from exposing sensitive data by using real-time encryption. The service operates quietly in the background, with no user interaction required.

Cloud-based security features and capabilities

Always-on endpoint defence

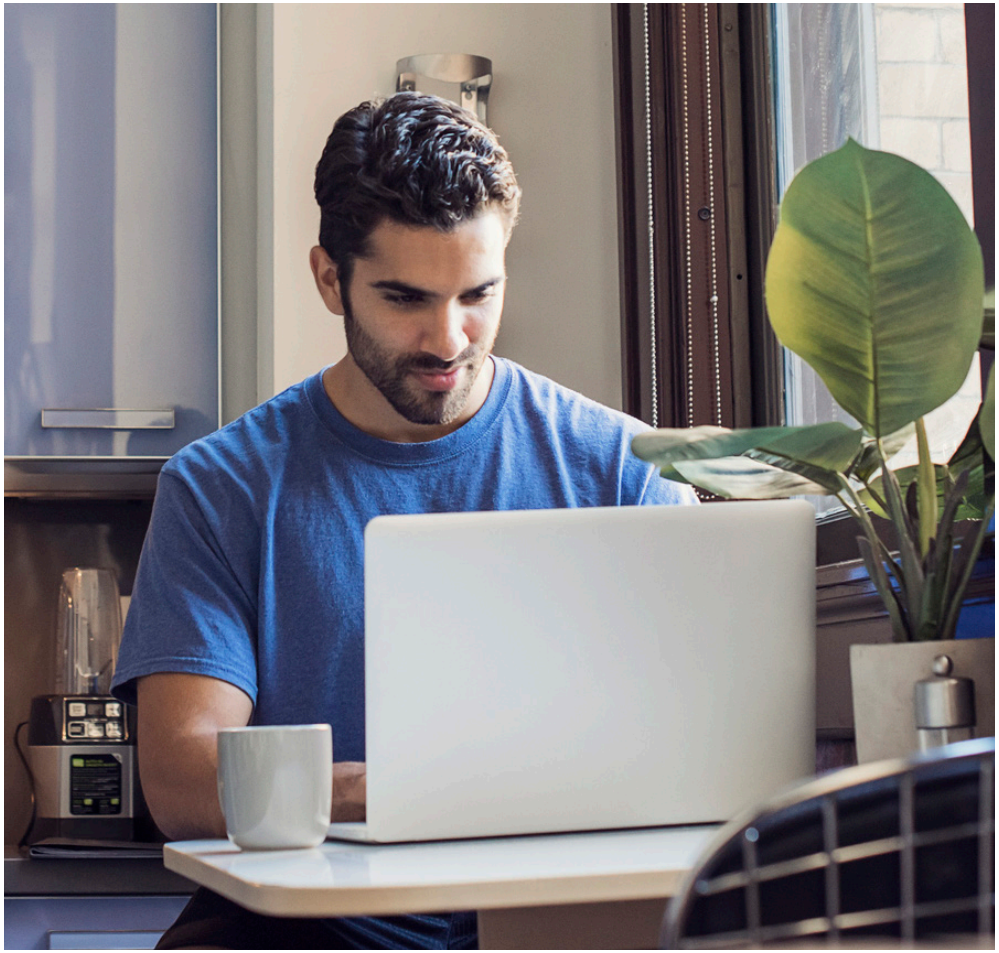
Jamf Threat Defense protects mobile employees and devices by using an endpoint app to identify malicious software, vulnerable configurations and risky connections before a breach can occur.

Real-time reporting and policy controls

The unified policy engine enables admin to quickly configure a security policy. Enforcement happens immediately, so policies can be tuned and tailored on the fly. Detailed reports can be viewed inside the Jamf Threat Defense portal or easily exported to third-party tools.

Unified operations and management

Jamf Threat Defense integrates directly with management infrastructure, so the service can be deployed quickly to managed devices. The integration also simplifies event monitoring and threat hunting for ThreatOps by adding human readable names to reporting.



Jamf Threat Defense works seamlessly with existing IT services and technologies to pre-empt and equip your technology remotely to deal with any dangers.

Seamless integration with Microsoft, Google, Cisco and other business technology brands helps extend the value of your existing technology infrastructure.