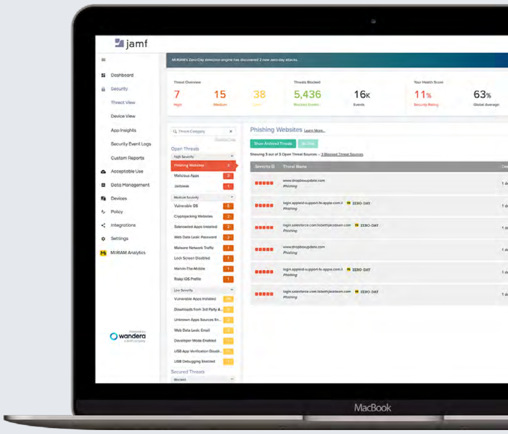
jamf

JAMF THREAT DEFENSE

Protect your devices, users and applications from cyber threats



MIRIAM's Zero-Day detection engine has discovered 2 new zero-day attacks.

Showing 3 out of 3 Open Threat Sources – 3 Blocked Threat Sources

Severity	Threat Name
●●●●●	www.dropboxupdate.com *Phishing*
●●●●●	login.appleid-support-fe-apple.com.il ZERO-DAY *Phishing*
●●●●●	login.salesforce.com.lisbethjacobsen.com ZERO-DAY *Phishing*
●●●●●	www.dropboxupdate.com *Phishing*
●●●●●	login.appleid-support-fe-apple.com.il ZERO-DAY *Phishing*
●●●●●	login.salesforce.com.lisbethjacobsen.com ZERO-DAY *Phishing*

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

Powerful endpoint security

Threat Defense detects and remediates the broadest range of endpoint threats including device vulnerabilities, malware and risky apps. Comprehensive risk assessments are continuously performed to identify threats, enabling security policies to be enforced in real-time.

Network defenses protect users and data

Stop attacks before they begin with in-network defenses. Content protection blocks malicious sites, including never-before-seen zero-day phishing sites designed to capture business credentials. Additionally, Threat Defense prevents command-and-control and data exfiltration by blocking connectivity with risky sites. Connections are secured automatically when person-in-the-middle attacks are detected.

Adaptive access to your applications

Elevate your security posture by allowing only secure and trusted devices to access business applications. Threat Defense continously monitors a broad set of telemetry and contextual inputs that can be used to prevent application access when an endpoint is compromised or at high risk. Adaptive access policies can be enforced natively through the Zero Trust Network Access solution or Jamf's management solution, Jamf Pro.

Comprehensive threat detection and prevention

Zero-day network protection

Threat Defense identifies and blocks even the most sophisticated attacks on the network, including zero-day phishing attempts, command and control communication, and cryptojacking. The service works with any app, including web browsers, email, social media and SMS.

Real-time risk assessments

Threat Defense continuously evaluates endpoint risk–from vulnerable OS to malicious profiles–enabling organizations to quickly identify devices that are out of compliance, and to enforce true zero trust access policies.

Detailed app insights

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

Dynamic data encryption

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

Leading security features and capabilities

Always-on endpoint defense

Threat Defense protects mobile workers 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 allows administrators to quickly configure a security policy; enforcement occurs immediately allowing policies to be tuned and tailored on the fly. Detailed reports can be viewed inside the Threat Defense portal or exported to third-party tools via easy-to-use integrations.

Conditional Access policies

Prevent business applications from being accessed when risk thresholds exceed predefined values. Conditional Access policies can be enforced natively within the Threat Defense network or via integration with Jamf or an Identity Provider.

Unified operations and management

Threat Defense integrates directly with management infrastructure enabling the service to 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 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 Threat Defense can protect users, mobile devices and organizational data, please visit jamf.com

Feature Matrix

Jamf Threat Defense, Jamf Data Policy
and Jamf Private Access

	Jamf Threat Defense	**Jamf Data Policy**	**Jamf Private Access**
Core Components	Jamf Threat Defense	Jamf Data Policy	Jamf Private Access
Jamf Security Cloud	✓	✓	✓
Endpoint App	✓	✓	✓
Admin Console	✓	✓	✓
Essential Integrations	Jamf Threat Defense	Jamf Data Policy	Jamf Private Access
MDM/UEM integrations for streamlined deployments	✓	✓	✓
Identity Provider integrations for end user activations	✓	✓	✓
SIEM/SOAR/EDR integrations for InfoSec workflows	✓	✓	✓
Public APIs and Data Export	✓	✓	✓
Common Settings	Jamf Threat Defense	Jamf Data Policy	Jamf Private Access
Privacy & Anonymity Controls	✓	✓	✓
Customizable notifications for users and admins	✓	✓	✓
Context-aware policy (by user, group, device, network, etc.)	✓	✓	✓
Endpoint Security	Jamf Threat Defense	Jamf Data Policy	Jamf Private Access
Device risk and vulnerability assessments	✓		
App intelligence	✓		
Mobile malware protection	✓		
Network Security	Jamf Threat Defense	Jamf Data Policy	Jamf Private Access
Zero-day phishing protection	✓		
Malicious traffic blocks (spam, cryptojacking, etc.)	✓		
Risky hotspot protection	✓		
Data & Usage Policy	Jamf Threat Defense	Jamf Data Policy	Jamf Private Access
Data caps & Usage limits by MB/GB		✓	
Content filtering for websites & native apps		✓	
Shadow IT discovery		✓	
Modern Remote Access and VPN Alternative	Jamf Threat Defense	Jamf Data Policy	Jamf Private Access
Fast, encrypted microtunnels			✓
Protected access to on-premises applications			✓
Protected access to cloud-hosted applications			✓
Conditional Access	Jamf Threat Defense	Jamf Data Policy	Jamf Private Access
via MDM	✓		
via MAM-WE (BYOD)	✓		
via IDP	✓		
via native Private Access	✓		✓