jamf

Security gaps are expanding. Here's how to close them.

Hybrid work, mobile devices and advanced threats have broken perimeter security. A layered approach is the way forward.

WHY LEGACY FAILS

The perimeter is gone. The risk is not.

More devices	more attack surface
More mobility	less control
More complexity	slower response

Cloud services, remote work, BYOD and untrusted networks have eroded the boundaries that legacy tools were designed to protect.

THREAT LANDSCAPE

Today's threats are sophisticated, converged and relentless.

100M+
Customer records compromised in recent breaches

2.1B
Downloads with known vulnerabilities in 2023

$25M
Lost to deepfake campaign targeting CFO

90%+
Of attacks now exfiltrate data instead of encrypting

KEY THREAT CATEGORIES

Social Engineering & Phishing
Email, spear, whaling, smishing, vishing and QR code phishing, plus novel techniques like Fake Airplane Mode and Fake Lockdown Mode

Nation-State / APT Attacks
90% of alerts originate outside critical infrastructure. Top targets: education, government and think tanks. Avg cost: $1.6M per incident

Supply Chain Attacks
Tripled in 2023, compromising partners and suppliers as indirect entry points

Mobile Threats
43% of compromised devices fully exploited (187% YoY). 80% of phishing sites target mobile. Unique mobile malware up 51%

AI-Enhanced Threats
5 APT groups observed weaponizing AI to enhance attack capabilities

NATION-STATE THREATS

Targeted attacks by the numbers.

Top targeted sectors

- Education 100%
- Government 75%
- Think Tanks / NGOs 69%
- IT 69%

9 in 10
organizations believe they've been targeted by state-affiliated actors

$1.6M
average cost per nation-state incident

WHY ONE SIZE DOESN'T FIT ALL

The device landscape has changed.

Legacy solutions designed for static, office-based desktops can't secure today's dynamic, multi-device environments.

25%
macOS market share in the U.S.

96%
Of CIOs expect Mac fleet growth in 12–24 months

3.6
Average devices per user globally (2023)

96%
Of mobile devices on enterprise networks are personal

MOBILE: UNCHECKED RISK

Mobile is the front door no one's guarding.

The average user has 3.6 devices. That's 4× the attack vectors per person, often with no specialized endpoint protection.

43%
Of compromised devices fully exploited (187% YoY increase)

80%
Of phishing sites target mobile devices

51%
Increase in unique mobile malware (920,000+ samples)

96%
Of mobile devices on enterprise networks are personally owned

STRATEGIC FRAMEWORK

The Four C's of closing security gaps.

1. **Consistency**
Treat every endpoint the same regardless of device type, form factor, OS or ownership model.

2. **Compliance**
Establish baselines, monitor deviations and maintain auditable proof through telemetry data.

3. **Consolidation**
Unite IT and Security into one cohesive team to break silos, share intelligence and unify workflows.

4. **Cost Savings**
Drive ROI through native tooling, automation, streamlined processes and BYOD programs.

LAYERED SECURITY MODEL

Defense-in-depth = layers that catch what others miss.

If a threat bypasses one control, the next layer is there to stop it. Integration of these three foundations creates stop-gap measures across your entire infrastructure.

Device Management
Deploy configurations, enforce policies and maintain control at scale

Identity & Access
Verify users and devices before granting access to protected resources

Endpoint Security
Detect and respond to threats across every device in real time

Management + Identity + Security → Defense-in-Depth

KEY TECHNOLOGIES

How the layers work in practice.

Zero-Touch Deployment
Devices secured from first power-on. Configs, apps and policies deployed automatically during setup for corporate and BYO devices.

Threat Hunting
Proactive detection of unknown threats through baselines, telemetry and automated remediation workflows.

ZTNA
Never trust, always verify. Encrypted microtunnels, least privilege access and continuous health checks replacing legacy VPN.

Advanced Threat Response
IoC/IoA analysis, timeline construction and APT elimination. Investigation times reduced from weeks to minutes.

OUTCOMES

Why it matters.

- **Stronger protection across devices**
- **Faster threat detection and response**
- **Reduced operational overhead**
- **Consistent security across environments**

Explore the full framework for building integrated, layered security across your organization.

jamf

Download the White Paper

www.jamf.com
© 2026 Jamf, LLC. All rights reserved.