Zimperium Helps Leading mPOS Providers Reduce Compliance Risk and Operational Costs

MAPS™

ZIMPERIUM®

The growing demand for mobile POS systems across retail, hospitality, and healthcare is accelerating the adoption of custom Android-based terminals. Small and medium-sized businesses (SMBs) are opting for Android POS solutions due to their lower costs, ease of integration, and scalability. Meanwhile, emerging technologies such as AI, cloud computing, and 5G are expected to transform the Android POS ecosystem further, making security and compliance more critical than ever.

The Challenge

With accelerated adoption, POS vendors are under increasing pressure to ensure security, meet compliance mandates, and support an ever-evolving ecosystem of third-party applications. This presents challenges, regardless of whether vendors build and manage their hardware and AOSP stacks in-house or rely on third-party OEMs, as both approaches introduce risks and complexities.

There are two key challenges vendors face:

1 PCI DSS Compliance Burden

Vendors must maintain compliance by:

- Patching critical vulnerabilities (CVSS 9+) within 30 days
- Keeping Android OS versions within 2–3 releases of the latest

Resulting Risks

- **Custom AOSP builds** require that every OS or app update be built, tested, and deployed uniquely for each vendor, making each update a costly and time-intensive project.
- **Frequent OS and app updates on terminals** disrupt merchants during business hours, creating a poor experience.

- As of 2023, **40%** of POS terminals sold globally were Android-based. skyquestt.com+15businesswire.com +15datahorizzonresearch.com+15.
- The global installed base of POS terminals reached ~292 million units in 2023, with 110 million mPOS devices, expected to grow to 152 million by 2028 ihlservices.com+2businesswire.com +2globenewswire.com+2.
- The mobile handheld POS market (largely Android-powered) is projected to grow from $33.15B in 2025 to $89.52B by 2035, at a CAGR of 10.3%

2 Marketplace App Security Gaps

Vendors offer expansive app marketplaces that enable third-party developers to build and submit add-on apps for inventory management, payroll, loyalty programs, and more. While this enhances merchant flexibility, it introduces significant risk if those apps are not thoroughly vetted.

Resulting Risks

- **Malicious or poorly built apps** can compromise the payment environment, steal data, or degrade performance.
- **Insecure data handling** practices may violate PCI DSS or privacy regulations.
- **Marketplace bloat** can make oversight difficult. Non-compliant and vulnerable apps may slip through, impacting merchant trust and vendor reputation.

How Zimperium Helps

Zimperium's Mobile Application Protection Suite (MAPS) platform helps mPOS vendors embed app shielding, white-box cryptography, and runtime protections directly into their apps.

Benefits

1. **Enable a Compensating Control**
   Use on-device AI-driven mobile threat detection to reduce the urgency of OS patching, lowering update frequency without compromising compliance.

2. **Protect Against Tampering**
   Leverage app shielding and runtime protections to detect tampering, emulation, and malware, and prevent app execution in untrusted device environments.

3. **App Vetting for Marketplace Hygiene**
   Automatically vet 3rd-party apps before they're published in your POS app store. Detect risky code, privacy violations, or malicious behavior before it reaches merchants.

Business Impact

1. **Reduce PCI Compliance Costs**
   Reduce the frequency of OS updates and eliminate costly compliance fire drills.

2. **Minimize Merchant Disruption**
   Avoid forced updates during merchant business hours. Deliver a seamless merchant experience.

3. **Protect Revenue and Brand**
   Prevent malware, data theft, and fraudulent third-party apps from entering the marketplace and impacting merchants.

4. **Gain Visibility into Device Risk**
   Monitor runtime behavior, OS posture, and app vulnerabilities across your entire fleet.

Secure Your POS Ecosystem. Reduce Compliance Overhead.

Zimperium helps leading POS providers like you build trust, scale securely, and stay compliant—without disrupting your merchants or burning your ops teams.

Request a demo today: info@zimperium.com
www.zimperium.com

About Zimperium

Zimperium is the world leader in mobile security. Purpose-built for mobile environments, Zimperium provides unparalleled protection for mobile applications and devices, leveraging AI-driven, autonomous security to counter evolving threats including mobile-targeted phishing (mishing), malware, app vulnerabilities and compromise, as well as zero day threats. As cybercriminals adopt a mobile-first attack strategy, Zimperium helps organizations stay ahead with proactive, unmatched protection of the mobile apps that run your business and the mobile devices relied upon by your employees. Headquartered in Dallas, Texas, Zimperium is backed by Liberty Strategic Capital and SoftBank.

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com
Zimperium, Inc
4055 Valley View, Dallas, TX 75244