Appknox

Telecom security at scale

How a global operator secured 14 markets (MENA) with Appknox

Overview

Challenge

With operations across 14 countries, the telecom provider relied on mobile apps as primary channels for engagement, transactions, and support. Rapid digitization introduced risks the existing security model couldn't keep up with: counterfeit apps on third-party stores threatened brand trust, inconsistent regional practices created uneven defenses, and long, manual VAPT cycles slowed releases.

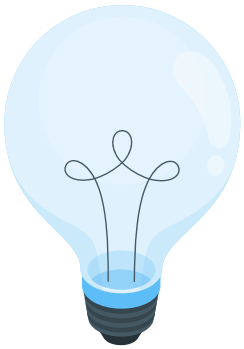
Without centralized visibility, vulnerabilities went undetected, and periodic testing left critical gaps. The provider needed faster, continuous testing to match DevSecOps pipelines and broader monitoring to protect against third-party abuse.

Solution

Appknox addressed both speed and scale. Storeknox provided proactive monitoring of third-party stores, identifying counterfeit apps for swift takedowns. Automated assessments, paired with manual VAPT, accelerated testing without losing depth. CI/CD integration brought continuous security checks into DevSecOps workflows, while a centralized dashboard unified visibility across 14 markets. Together, these capabilities standardized security and enabled faster, more reliable releases.

Results

The provider reduced vulnerability detection and remediation times by 50–70%, fixing critical issues within 24 hours. Counterfeit app risks were contained through proactive monitoring, while embedded testing in CI/CD pipelines sped up secure releases by nearly 50%. A single-pane dashboard gave complete visibility across regions, improving risk prioritization. Automation cut security operations costs by more than 50%, and systematic detection reduced incidents by 75%.



What Appknox helped achieve

- Proactive third-party monitoring safeguarded the brand by reducing abuse and counterfeit app risks across multiple stores.
- Automated VAPT with CI/CD integration and continuous testing enabled 50–70% faster detection and remediation, cutting delays and aligning seamlessly with DevSecOps velocity.
- Centralized dashboards simplified risk management across 14 countries, while streamlined processes delivered >50% savings on security infrastructure and personnel costs.

INDUSTRY

Telecom

SERVICE LOCATION

Africa & Middle East (14 countries)

HEADQUARTERS

Dubai, UAE

REVENUE

$20 Billion

EMPLOYEES

15000+

SECURITY TEAM SIZE

20-25

About the company

One of the world's leading telecom service providers, headquartered in Dubai, UAE, the company operates across the globe, serving hundreds of millions of subscribers with mobile voice, data, and digital services. With a strong footprint in emerging markets, it plays a pivotal role in enabling connectivity and driving digital inclusion, supported by its extensive network infrastructure and commitment to innovation.

The challenges

Operating across 14 countries in Africa and the Middle East, a leading telecom provider serves millions of customers who rely on its mobile services daily. With rapid digitization, its mobile applications and digital assets became primary channels for customer engagement, transactions, and support.

This expansion introduced new risks, ranging from brand abuse on third-party stores to maintaining protection of apps within fast-moving DevSecOps pipelines. The operator needed a solution that could provide both broad monitoring and deep security testing. Here are some of the top challenges faced by the telecom provider:

1. Exposure to malicious clones and counterfeit apps

Apps distributed through multiple third-party stores were frequently targeted by fraudulent clones and repackaged versions, putting customers and brand reputation at risk.

2. Inconsistent security practices across regions

Managing security operations across 14 countries introduced inefficiencies, with variations in compliance requirements, testing environments, and enforcement standards leading to gaps in consistency.

3. Time-intensive and resource-heavy VAPT cycles

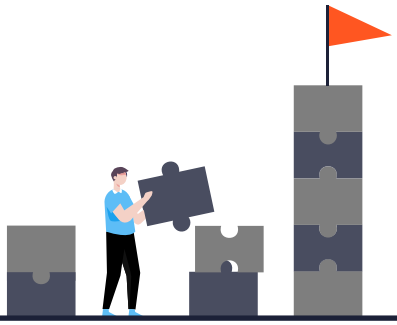
Traditional penetration testing slowed down secure releases. Long, manual testing cycles created bottlenecks in keeping pace with fast-moving DevSecOps pipelines.

4. Limited visibility across a growing app portfolio

With multiple teams and regions managing applications, the provider lacked a single-pane view of vulnerabilities, making it difficult to detect, prioritize, and remediate risks effectively.

5. Manual and periodic testing left gaps

The growing volume of apps required continuous security assessments, but manual, periodic testing failed to match release velocity, leaving critical exposures unaddressed.



The solution

Managing application security across geographies and app stores required a unified, continuous approach. Appknox addressed these needs with a combination of proactive monitoring, automated testing, and centralized visibility:

1. Third-party store monitoring with Storeknox

Continuous scanning of third-party app stores detected counterfeit or malicious versions early, enabling swift takedowns to protect users and brand reputation.

2. Standardized security across 14 countries

Consolidating vulnerability assessments into a single platform allowed the provider to maintain consistent security practices across regions, simplifying compliance and governance.

3. Automated and manual VAPT for accelerated testing

Automated vulnerability detection paired with deep manual penetration testing reduced the time and effort required, eliminating release bottlenecks.

4. Centralized dashboards for complete visibility

A single-pane view of vulnerabilities across all applications gave leadership clear insights, streamlined remediation, and improved decision-making at scale.

5. Continuous testing integrated with CI/CD pipelines

Appknox's integration into DevSecOps workflows ensured ongoing vulnerability detection, aligning security with development speed without slowing down releases.

The impact

After integrating Appknox's Storeknox and continuous VAPT capabilities in early 2025, Airtel achieved clear, measurable improvements across key performance parameters.

Parameter	Before Appknox	After Appknox	Impact
Vulnerability coverage	With manual or ad-hoc scans, many issues are missed	Automated detection with broader coverage	~ 45–50% more vulnerabilities detected early
Incident rate	High risk of breaches and security incidents	Systematic detection and remediation	~ 75% fewer security incidents
Time to remediation	Longer cycles, delayed fixes	Rapid identification and remediation workflows	Critical vulnerabilities fixed within 24 hours
Release cycles	Security testing slowed releases	Embedded testing in CI/CD processes	~ 50% faster, secure release cadence
Cost and resource usage	Heavy reliance on manual testing and internal teams	Streamlined automation and reduced manual overhead	> 50% reduction in security operations costs

Key numbers

51
Applications Analyzed

341
Vulnerabilities in 1st Scan

15
Critical scans

> Appknox is an enterprise-grade security platform that helps developers, security researchers, and enterprises build a safe and secure mobile ecosystem faster with automated security checks.

- Senior Manager, Cybersecurity

The Appknox advantage

Appknox is an enterprise-grade security platform that helps developers, security researchers, and enterprises build a safe and secure mobile ecosystem faster with automated security checks.

THE APPKNOX IMPACT

<90 mins
comprehensive automated VA

<1%
false negatives

8+
compliances

Trusted by Gartner, loved by enterprises

- Recognized in Gartner Peer Insights Voice of Customer
- Gartner Hype Cycle for Application Security
- Gartner Notable Vendor

Unleash the power of superior scalable security with Appknox today.

Scan now to speak to a cybersecurity expert