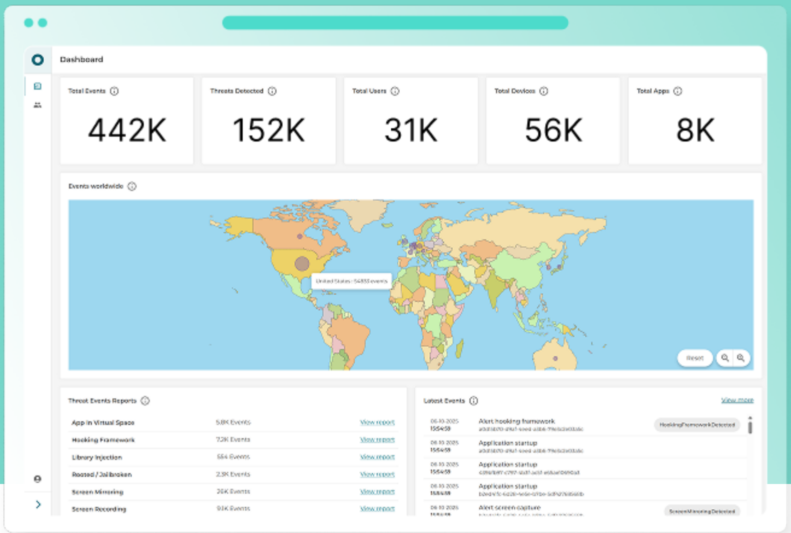
OneSpan

## Stay ahead of threats with

# Threat View


Dashboard

| Total Events | Threats Detected | Total Users | Total Devices | Total Apps |
|---|---|---|---|---|
| 442K | 152K | 31K | 56K | 8K |

Events worldwide

United States : 54833 events

Threat Events Reports

| | | |
|---|---|---|
| App in Virtual Space | 5.8K Events | View report |
| Hooking Framework | 7.2K Events | View report |
| Library Injection | 554 Events | View report |
| Rooted / Jailbroken | 2.3K Events | View report |
| Screen Mirroring | 20K Events | View report |
| Screen Recording | 9.1K Events | View report |

Latest Events

View more

| | | |
|---|---|---|
| 06-10-2025 | Alert hooking framework | HookingFrameworkDetected |
| 06-10-2025 | Application startup | |
| 06-10-2025 | Application startup | |
| 06-10-2025 | Application startup | |
| 06-10-2025 | Alert screen capture | ScreenMirroringDetected |

Datasheet

## From detection to prevention and compliance

**Threat View empowers organizations to surpass compliance mandates and gain comprehensive and actionable insights into mobile threats by leveraging both a lightweight on-prem deployment approach and seamless client-side implementation.**

### Why Threat View?

Mobile threat landscapes are constantly and rapidly evolving, with new attack techniques constantly being invented to target and compromise even the most well-protected apps. Continuous monitoring of the mobile apps you have in production is crucial to stay ahead of threat actors.

By translating threat and device telemetry into easy-to-use dashboards, detailed reports, and audit trails, Threat View empowers you to prevent potential fraud losses, meet regulatory compliance, and protect your brand reputation, while maintaining operational efficiency and scalability.

### Identify, understand, and respond to mobile threats early

Threat View collects comprehensive threat and device data, from malware and injection attacks to device fingerprints and geolocation. Thanks to its intuitive dashboard, maps, real-time event list, and customizable reports, your security team can easily understand the full context of a potential attack:

- **What** happened?
- **How, when, and where** did it happen?
- **Who** did it?

This information allows you to identify attack trends, high-risk devices/users, and unusual patterns, so your team can respond to security incidents early, before damage occurs.

### Remain agile through rapid on-prem deployment

Cut down time-to-market and deploy Threat View in a matter of days with Docker-based containers within your infrastructure, eliminating external cloud dependencies for maximum data security and privacy. Strengthen regulatory data residency compliance without sacrificing scalability.

### Ensure secure collaboration with role-based access

Threat View delivers more than just basic role management by offering three predefined workflow-specific access:

- **Account Owner**
- **User Admin**
- **Insight Viewer**

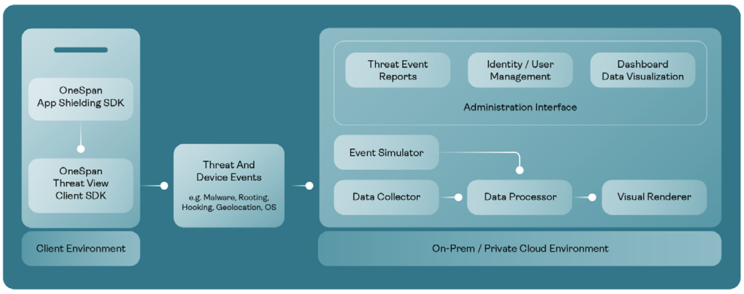
These workflows are purpose-built for SOC, IT, and compliance teams. This approach reduces the risk of accidental or unauthorized changes or data exposure, enforces least-privilege governance, and allows full audiability, maintaining security and regulatory compliance without increasing operational complexity.

### Comply with data protection regulations

You can seamlessly maintain data security and accountability within the Threat View system while confidently proving data protection regulations adherence (i.e., GDPR) using Threat View's built-in granular data controls, data portability, and cryptographically secured audit trails for every system event.

### Highlights

- **Rapid deployment**
  Install on-prem or on private cloud with Docker in days, not months
- **Data security & compliance**
  GDPR-ready controls and tamper-proof audit logging
- **Role-based access**
  Empower secure and compliant collaboration across your whole team
- **Modular microservices**
  Threat intelligence, reporting, auditing, and user management microservices that scale as you grow
- **8 widgets, 7 chart types**
  Instantly transform complex threat data into digestible actionable insights



## How does Threat View work?

Threat View client SDK continuously monitors device telemetry and mobile threat events collected by the Mobile App Shielding SDK within your app. It will then send these insights to the Threat View server component in your on-prem or private cloud, where granular data is analyzed, visualized, and transformed into actionable security intelligence and audit trails.

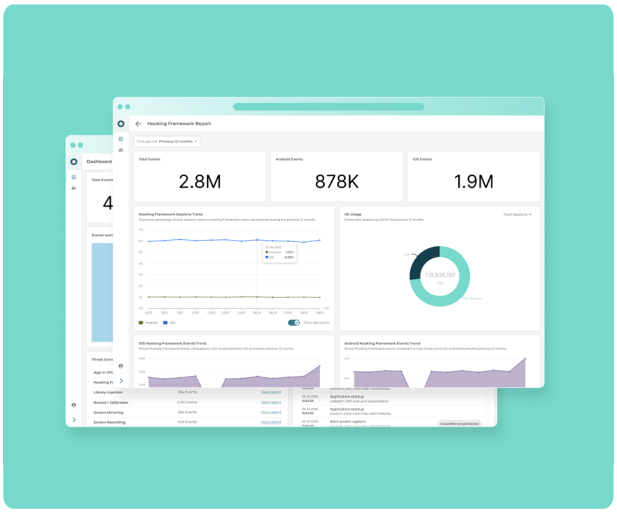


*Figure 1. Threat View dashboard*

## Monitored data

You can conveniently visualize and analyze the following device data and threat events on the web-based Threat View Dashboard, accessible via the Threat View Administration Interface

| | Android | iOS |
|---|---|---|
| **Device data**<br>(i.e., OS, OS version, device language, device fingerprint, time of the event) | ✓ | ✓ |
| **Geolocation data** | ✓ | ✓ |
| **App data**<br>(i.e., App version and release date, app installation date, app journey information, app activity lifecycle) | ✓ | ✓ |
| **App runs rooted/jailbroken mobile device**<br>On Android, this threat event type also indicates the probability that the app is rooted/jailbroken and displays it as a number between 0 and 100. | ✓ | ✓ |
| **Hooking framework is present in the app** | ✓ | ✓ |
| **Screenshot is being taken** | | ✓ |
| **Library injection into the app detected** | | ✓ |
| **Untrusted keyboard present** | | |
| **Untrusted screenreader present** | ✓ | |
| **Screen is being mirrored** | ✓ | |
| **Screen is being recorded** | ✓ | |
| **App is launched via a virtual space app** | ✓ | ✓ |

## System requirements and supported platforms

### Server-side Component

Installation system requirements:

- 3.2 GB for the Docker images
- 4 GB RAM is recommended as minimum
  - 8GB is recommended for running the Event Simulator, as this produces data in the events database
- An internet connection for the PostgreSQL and MariaDB database images, or a local Docker repository with those images

OneSpan Threat View server-side component and Admin interface can be run from all common internet browsers.

### Client-side SDK

**Android**

- Minimum Android 7 (API level 24), target Android 15 (API level 35)
- Kotlin: 1.9.0 or later
- Gradle: 8.0 or later
- AGP: 8.10.0 or later
- Target SDK: 36
- ProGuard: Consumer rules are automatically applied from the SDK artifact - no additional configuration required.
- App Shielding: 7.4.2 or later. The final APK must be shielded using the Shielding Tool.

**iOS**

- iOS 15 or higher
- Swift 5 or higher
- Xcode 16 or higher

## About OneSpan

OneSpan is a global leader in digital security, trusted by thousands of enterprises across 100+ countries—including more than 60% of the world's 100 largest banks—to safeguard digital accounts, secure financial transactions, and prevent fraud. Our award-winning solutions provide passwordless authentication, digital transaction security, and advanced mobile application protection, helping organizations meet the highest security standards and global compliance requirements. As cyber threats grow more sophisticated, OneSpan delivers cutting-edge technology to safeguard customers, mitigate risks, and ensure trust in every digital interaction.

Learn more at
**OneSpan.com**

Contact us at
**OneSpan.com/contact-us**