AirWatch Integration with Zimperium

Zimperium Mobile Threat Protection integrated with AirWatch EMM to detect, analyze and remediate mobile threats

Contents

Overview

AirWatch and Zimperium have partnered to provide a complete enterprise mobile security system that delivers sophisticated threat protection for mobile devices. The integrated solution secures devices against known and unknown threats to ensure corporate data and networks are not compromised by an advanced mobile attack.

Together, AirWatch and Zimperium enable enterprises to manage and secure iOS and Android devices against host- and network-based attacks. Zimperium continuously detects and analyzes threats and provides AirWatch with the visibility to enact risk-based policies to remediate against these attacks.

The integrated solution provides IT Security Administrators with a way to safely enable BYOD and strike the balance between empowering mobile employees to be more productive with the device of their choice, while at the same time securing mobile devices against advanced threats.

Benefits of the Integration

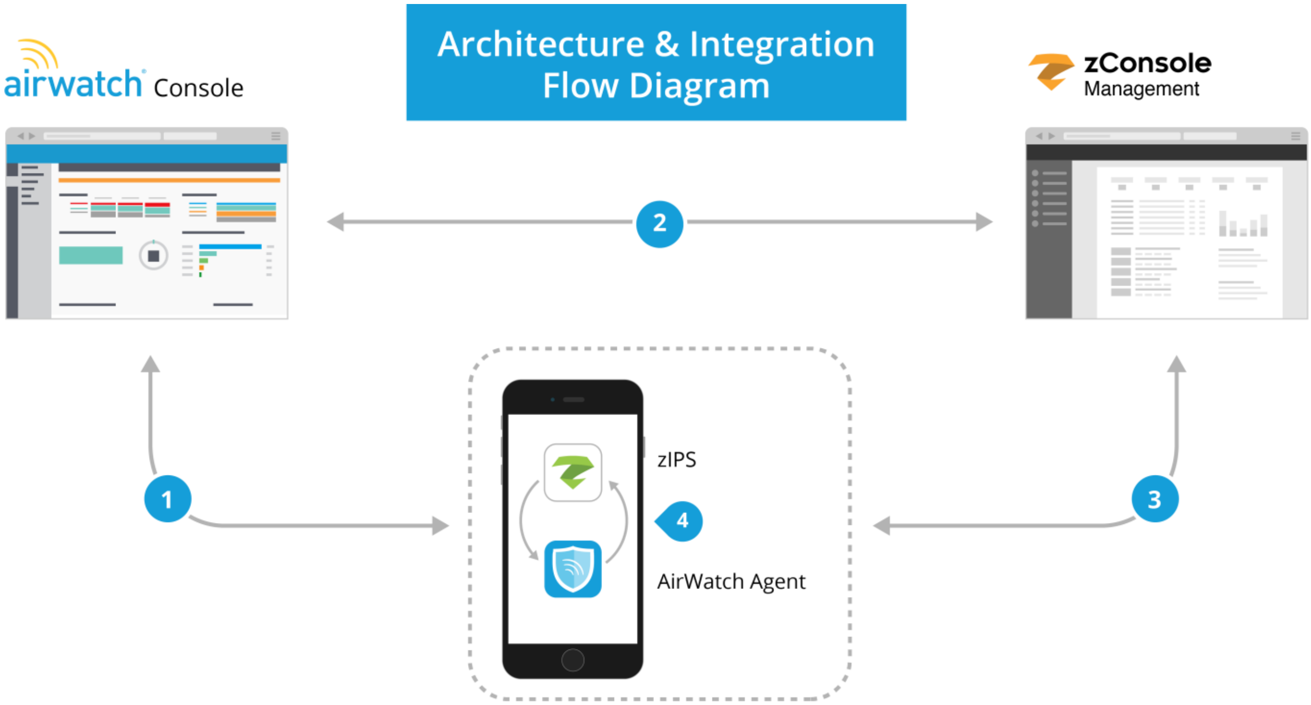
- Provides for ease of deployment of the Zimperium zIPS – Mobile Threat Protection app to a large number of devices and ensures cyberattack protection is always enabled by enforcing the use of the app
- Removes devices from compromised wireless networks when a Man-in-the-middle attack is detected
- Enforces risk-based compliance policies to remediate depending on the severity of a threat such as a malware attack, e.g., disable connections to corporate services (email or other apps, Wi-Fi, and VPN), remove enterprise applications from the device
- Provides configurable end-user notifications and administrator alerts by attack type along with comprehensive forensics

	AirWatch	Zimperium
Host- and network- based mobile threat detection	✗	✓
Application Distribution	✓	✗
Attack Classification and Forensics	✗	✓
Remediation Policy Enforcement	✓	✗
Comprehensive Monitoring and Reporting	✓	✓
Multi-Platform Support	✓	✓

Platform Support

The AirWatch and Zimperium integrated solution for the AirWatch Console and Zimperium zConsole integration works for Apple devices with iOS 7 and above and Android devices with OS4 and above. The AirWatch and Zimperium integrated solution for the AirWatch Agent and Zimperium zIPS integration works only for Android devices with OS4 and above.

Architecture & Integration Points



1. AirWatch provides an easy-to-use policy management solution to deploy and upgrade the Zimperium zIPS – Mobile Protection solution to a large number of devices through its enterprise app delivery capability. The deployment is administered in the AirWatch console using Smart Groups through REST APIs. Smart Groups are selected and the zIPS app is pushed and synchronized to the users/devices in those groups.
2. The AirWatch Administrator can set up different workflows to handle various situations and threats which the zConsole can choose through its policy page. The zConsole instructs the AirWatch console to move the device to a SmartGroup in the Threat Response Matrix (TRM) to determine actions that AirWatch takes on the device to remediate threats, e.g., disconnect from a compromised network, disable connections to corporate services or remove an app from a device.
3. The Zimperium Mobile Threat Protection solution is comprised of the zIPS app and the zConsole which communicate with each other. This is not a point of integration with AirWatch. Host- and network-based threats are detected on the device and communicated to the zConsole where mobile threat response policies are set and administrators can view and analyze their mobile threat environment.
4. The AirWatch app and the zIPS app now have the ability to communicate directly, as well, to provide immediate security on the device. That is, if the device or an app is under attack, zIPS can make a callback to

the AirWatch agent, alerting that the device/app has been compromised. The AirWatch agent will display the Zimperium alert and launch the Zimperium app so that the threat information can be seen and defined policy actions can be triggered.

Requirements

If you would like to take advantage of the enhanced mobile threat management provided by the AirWatch-Zimperium integrated solution, ensure you have the following resources available:

- AirWatch version 8.0+
- For the AirWatch and Zimperium zConsole integration, which is available for both iOS and Android, the requirements are Zimperium zIPS version 1.6 or higher for Android and zConsole version 2.2 or higher with AirWatch API Integration activated. For the zIPS app integration with the AirWatch agent, it is only available for Android and the requirements are Zimperium zIPS version 1.7 or higher and zConsole version 2.3.0.0 or higher with AirWatch API Integration activated.

To ensure your environment is compatible and to get started with the AirWatch and Zimperium integration, contact your Zimperium representative as well as AirWatch Support.

Implementation Process

To find detailed instructions on how to Implement this integrated solution, please refer to the Zimperium AirWatch Implementation Guide on the Zimperium Support Portal.