



Zimperium: The First Mobile Threat Provider to Achieve FedRAMP “Authority to Operate”

Providing federal agencies complete, end-to-end mobile threat protection



THE FIRST FEDRAMP AUTHORIZED MTD

Dallas, TX-based Zimperium is the first mobile threat defense (MTD) provider to be granted an Authority to Operate (ATO) by the U.S. Department of Homeland Security and U.S. Immigration and Customs Enforcement under the Federal Risk and Authorization Management Program (FedRAMP).

A cloud-based application deployed on the AWS GovCloud infrastructure, [Zimperium Federal Cloud \(ZFC\)](#), is the United States government version of Zimperium zConsole, the management and reporting component of Zimperium [zIPS](#), the leading enterprise MTD solution.

The Zimperium FedRAMP-authorized solution provides security teams with visibility to the threats and vulnerabilities across all mobile devices in the organization to enable assessment of risk, identification of security gaps and rapid enactment of remediation.

Zimperium

Package ID

- FR1731347234
- Package Access Request Form

FedRAMP Authorization Details

- Authorization Type: Agency
- Independent Assessor: Kratos SecureInfo

Agencies using this service

- Department of Homeland Security
- Immigration and Customs Enforcement

ON-DEVICE PROTECTION

Like their government counterparts throughout the world, many United States agencies are protecting mobile devices against both known and zero-day threats with Zimperium's on-device, machine learning-based MTD solution, [zIPS](#). zIPS leverages our award-winning machine learning engine, z9, to protect mobile data, apps and sessions against device compromises, network attacks, phishing attempts and malicious apps. To date, zIPS has detected 100 percent of zero-day mobile exploits without requiring an update.

FEDRAMP ATO CLOUD-BASED MANAGEMENT

zConsole is Zimperium's management and reporting console, including threat forensics, policy administration and industry-leading integrations with EMM



and SIEM solutions. It is the only MTD solution that can handle multiple EMMs in a single tenant, and also the only one that can operate in any cloud environment or even on-premise.

Many U.S. federal agencies that seek to protect devices with an MTD solution desire, or are required to use, a solution that is FedRAMP authorized. With the ATO from FedRAMP, Zimperium is the choice to meet that need.



UNIQUE BENEFITS ENABLE SOLE SOURCE ACQUISITION

Government agencies consistently “sole source” Zimperium solutions since they include capabilities that are completely unique. In particular, Zimperium’s differentiating capabilities include:

- Zimperium is the first and only machine learning-based solution for detection of both known and unknown device, network, phishing and app attacks on mobile devices;
- Zimperium is the only MTD solution that provides on-device threat detection that operates even when the device is not connected to a network... or when it is owned by an attacker;
- Zimperium is the most enterprise-ready and friendly solution, with advantages in EMM integrations, group based policies, forensics and deployment options... now including FedRAMP ATO with [Zimperium Federal Cloud \(ZFC\)](#); and
- Zimperium provides the best SDK for embedding protection into mobile apps.



Zimperium, the global leader in mobile device and app security, offers real-time, on-device protection against Android and iOS threats. The Zimperium platform leverages our award-winning machine learning-based engine - z9 - to protect mobile data, apps and sessions against device compromises, network attacks, phishing attempts and malicious apps. Headquartered in Dallas, TX, Zimperium is backed by Sierra Ventures, Samsung, Telstra, Warburg Pincus and SoftBank. Learn more at www.zimperium.com or our official blog at <https://blog.zimperium.com>.

© Copyright 2020 Zimperium | All rights reserved.