SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Solution Innovation Case Study:

Mitigating the Risk of Surveillance via Compromised Smartphone Cameras and Microphones

The Security Executive Council (SEC) Solution Innovation Partner (SIP) program evolved as a means for practitioners to choose a trustworthy risk mitigation provider with confidence when there is a myriad of options in the marketplace. Proven Solution Innovation Practice Case Studies help to evaluate performance claims and differentiate security solution providers for business outcomes including risk mitigation, return on investment, and security assurance.

This Solution Innovation Case Study offers a proven process approach for mitigating risk(s) online that could result in injury or impairment of people, assets, critical processes, products and/or brand reputation. This proof point examines representative risk issues, mitigations and result outcomes as validated by the Security Executive Council and the end-user.

The following operational case study was demonstrated by a United States Federal Government Agency using the Privoro SafeCase™ solution which provides independent, hardware-based protections for off-the-shelf smartphones. Security Today magazine selected the Privoro SafeCase™ as a "Govies Government Security Award Winner" for 2019 – Cyber Defense Solution.

Risk Issues and Mitigation Opportunities:

1. Smartphones are vulnerable to hacking, with a heightened risk of exploitation when traveling through choke points, highly trafficked and/or targeted areas such as international airports, financial districts and tourist destinations.
2. Corporate espionage is a multi-billion-dollar global issue perpetrated by malicious actors hijacking the smartphone cameras and microphones of targeted victims.
3. Most smartphones lack the proper security capabilities to protect a user or device. Spyware can infect all layers of a smartphone (app, OS, firmware and chip) and cost as little as a hundred dollars and range upwards of over a million for more sophisticated capabilities.
4. Malicious actors can remotely hijack the microphones of a target's smartphone to listen in on conversations happening in the vicinity of the device.

Solution Requirements:

- Protection of sensitive conversations 24x7 – inside and outside of secure facilities – against unwanted surveillance.
- A high-security smartphone case that neutralizes potentially compromised microphones through intelligent audio masking.
- Worry-free ability to still use a smartphone to go about day-to-day business, utilizing the email, messaging, and cloud storage capabilities already on their devices.

Solution Innovation Case Study:
Mitigating the Risk of Surveillance via Compromised Smartphone Cameras and Microphones

Delivered:

- Improved the end user`s smartphone integrity confidence while travelling internationally from a 1 out of 10 to a 9 out of 10.
- Enabled five additional international critical meetings/calls that may not have occurred prior to the adoption of the Privoro SafeCase™.
- Two international business trips were approved based on the existence of the Privoro SafeCase™.
- Proactive reporting to end user continuously improving to report non-compliant users that have been given the SafeCase™ solution

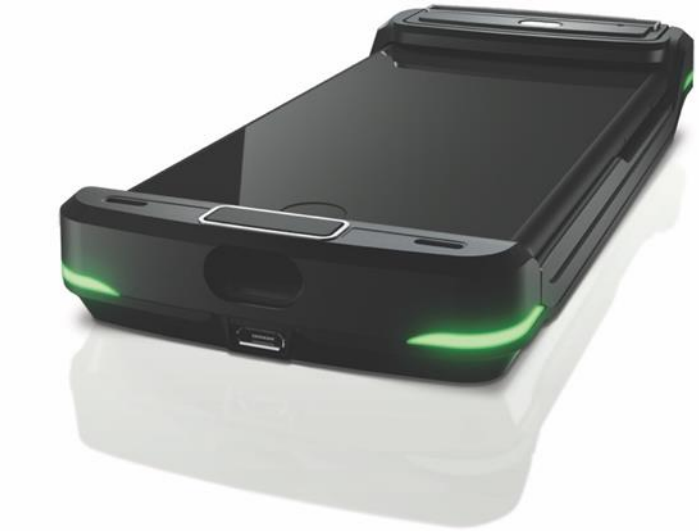

Figure 1: Image of Privoro SafeCase™

Outcome and Benefits of Service Including ROI:

- SafeCase™ has its own components – processor, memory, wireless communications and more – that are completely isolated from the paired smartphone.
- SafeCase's processor is used exclusively for running authenticated firmware.
- SafeCase™ relies on its own Hardware Root of Trust (HRoT) to serve as a secure foundation for the mobile protections enabled by the case.
- Key personnel are no longer constrained for international travel due solely to smartphone risks.
- End user is able inform Privoro and other cleared entity service/technology roadmaps for communications security considerations up to and including potential allowance of smart devices in Sensitive Compartmented Information Facility (SCIF) environments.
- End user is now confidently able to influence strategic partners to adopt technology to close the gap on smartphone vulnerabilities

SIP Case Study Authentication Process

This process was overseen by a Security Executive Council subject matter expert with 20+ years of experience in developing and leading people and asset protection programs as a trusted security advisor for global, multinational organizations. End-user authenticated May 2019.

Note: *The Security Executive Council's Solution Innovation case study represents a snapshot in time to demonstrate a solution to a specific-organization's issue. End-user diligence, trial and measurement are strongly recommended for any contemplated risk mitigation activity.*

A General Comparison of Competition

Client Service/Resource Attributes or Capabilities	**Privoro YES/NO**	Company A YES/NO	Company B YES/NO
Mitigates risk of mobile espionage	**Yes**	No	No
Resistant to advanced chip-based attacks	**Yes**	No	No
Cloud-integrated for logging and reporting	**Yes**	No	No
Independent Hardware Root of Trust (HRoT)	**Yes**	No	No
Supports COTS iPhones	**Yes**	No	No
Testing by US Intel Agencies	**Yes**	No	No
Adopted by US Intel, DoD and Policy Makers	**Yes**	No	No
Manufactured in US ITAR compliant facility	**Yes**	No	No