irdeto
Building a Secure Future.™

Datasheet

CLOAKWARE® TRUSTED TELEMETRY

Extend device management to untrusted embedded devices, including medical instruments and consumer wearables

As connected devices proliferate throughout Health Care Providers like hospitals, clinics, diagnostic services, etc. medical IT departments are challenged to manage, monitor and constrain the devices to ensure prescribed operation and provide the necessary patient safety. This is especially difficult for medical devices that are based on embedded processors and operating systems where they may not support standard SIEM agents or data collection protocols.

Even AI-augmented 'behavioural' SIEM systems are challenged by the scale of IoMT deployment.

Medical Device Manufacturers (MDM) are encouraged by the FDA to address cybersecurity risks in their medical products, post sales, after deployment.

Manage the proliferation of connected devices in HDOs

Irdeto's Cloakware Trusted Telemetry features a small, portable agent well suited to extend security coverage even to tiny microprocessor and RTOS based systems. Critical security events are passed by default in the protected telemetry packets and agent APIs make it easy to add additional system or application level data as required. Having robust, reliable security telemetry data can help SIEM systems scale to accommodate the massive increase in connected devices that we are experiencing today. Qualified, integrity verified telemetry data can also unburden cognitive/AI based systems since no deductions or complicated forensics are required. Trusted Telemetry provides near real-time detection of device exploits for timely containment.

Better FDA compliance

FDA has important Quality System regulation (21 CFR part 806) recommendations outlined in the 2016 document "Postmarket Management of Cybersecurity in Medical Devices." This document "emphasizes that manufacturers should monitor, identify, and address cybersecurity vulnerabilities and exploits as part of their postmarket management of medical devices." Trusted Telemetry provides indications of device integrity, revision level, suspicious libraries & activities as well as other cybersecurity events of interest like device attachments and output devices available that can support FDA's guidance and compliance reporting.

KEY BENEFITS

Near real-time detection of exploits

- Extends trust to untrusted devices (devices deployed in a hostile environment, like consumer wearable instruments, portable/mobile devices with medical apps, etc.)
- Produces trusted logs for critical security events
- Near real-time detection of exploits
- Supports a broad range of robust, integrity verified telemetry
- Supports a multi-layer security-in-depth philosophy which reduces dependence on fallible perimeter security
- Leverages the renowned Cloakware® anti-hacking technologies in a simple, easy-to-deploy fashion

Trusted / robust security telemetry

- Provides both system and application level telemetry data (see over)
- Produces reliable critical security events, like:
  - Integrity Verification (detect tampering)
  - Hooking detection
  - Jailbreak / rooting detection
  - Privilege escalation
- Easy API to extend protections to device apps and for apps to produce proprietary telemetry

Server plays well with others

- Telemetry server provided to process messages, store and forward events
- Containerized server for easy deployment
- Available as part of Cloakware Software Services or separately
- Seamless integration with popular SIEM systems like IBM's QRadar

Agent provides broad device coverage

- Portable C code for broadest possible device coverage
- Small size (footprint)
- Simplified OS abstraction layer for easy porting
- Pre-integrations for several popular embedded OS (Inquire about rollout)
  - iOS, Linux, FreeRTOS
  - Android, Wear OS, VxWorks, uCOS, ThreadX, in future (inquire)

KEY TECHNOLOGIES & FEATURES

Cloakware® Defense-in-Depth

Trusted Telemetry leverages Cloakware Software Protection (CSP) to build a multi-layered security shield for the agent. Multiple overlapping protections ensure that even if the device's security is breached on one front there will be effective protections remaining to foil an attack.

Anti-reverse engineering. The agent utilizes the sophisticated Cloakware transcoder that transforms code and data, entangling both together, in such a way that semantic information is destroyed, and the software becomes almost impossible to reverse engineer. Additional protections like anti-debug provide security-in-depth.

Integrity Verification. A robust integrity verification is essential to establishing a software root-of-trust on constrained devices like embedded IoMT instruments. This puts the 'trust' in the telemetry.

Protected Communications. Trusted Telemetry packets are secured end-to-end using advanced whitebox cryptography on the agent side to hide keys and cryptographic operations in plain sight.

(CSP is also available as a separate product. It can be licensed by OEMs to provide protection of proprietary code and data in their applications which is often key IP in medical IoT products today).

Critical Security Events and System-level Telemetry

Cloakware anti-hacking technologies provide built-in critical security events that are relayed by Trusted Telemetry in such a way they cannot be tampered with:

- Jailbreak / root kits
- Hooking libraries
- Debugger attachment
- Tampering of agent software
- Falsified telemetry messages

The agent, under direction of the application, can also be used to produce valuable system-level information that could help with ongoing FDA compliance and device maintenance:

- OS versions
- Hardware model
- Suspicious reboot patterns
- Privilege escalation
- Unrecognized processes
- USB devices attached
- Output devices available / enabled

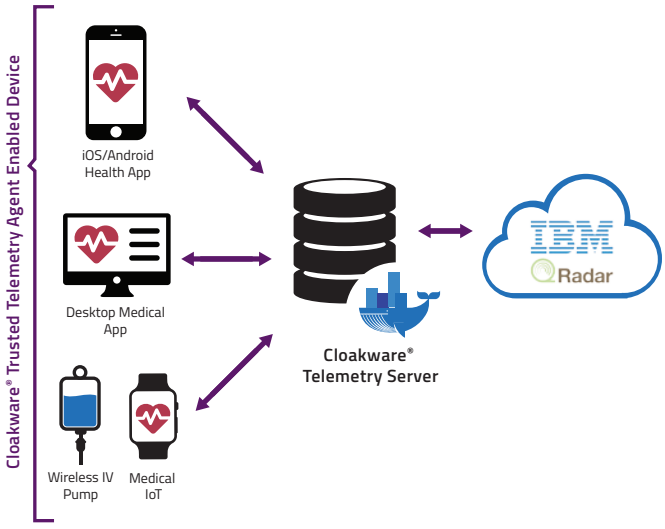

Figure 1 Trusted Telemetry integration with SIEM system

Application Level Telemetry

An easy API facilitates extending general telemetry data into the application layer. You can produce your own events and alerts to broaden the scope of security coverage relevant to your particular application.

Cloakware Software Services

Trusted Telemetry is part of the family of Cloakware Software Services. These include:

- Automated Software Protection (AI-driven automatic software protection available as a cloud-based service, 2H2019)
- Software Forensics (watermarking and piracy tracking, introduced 2H2018)
- Trusted Telemetry (agent, server component and dashboard / filtering, introduced 1H2019)

CONTACT US

For more information on Cloakware Software Protection, please visit:

https://irdeto.com/cloakware-software-protection/
https://irdeto.com/contact-us/