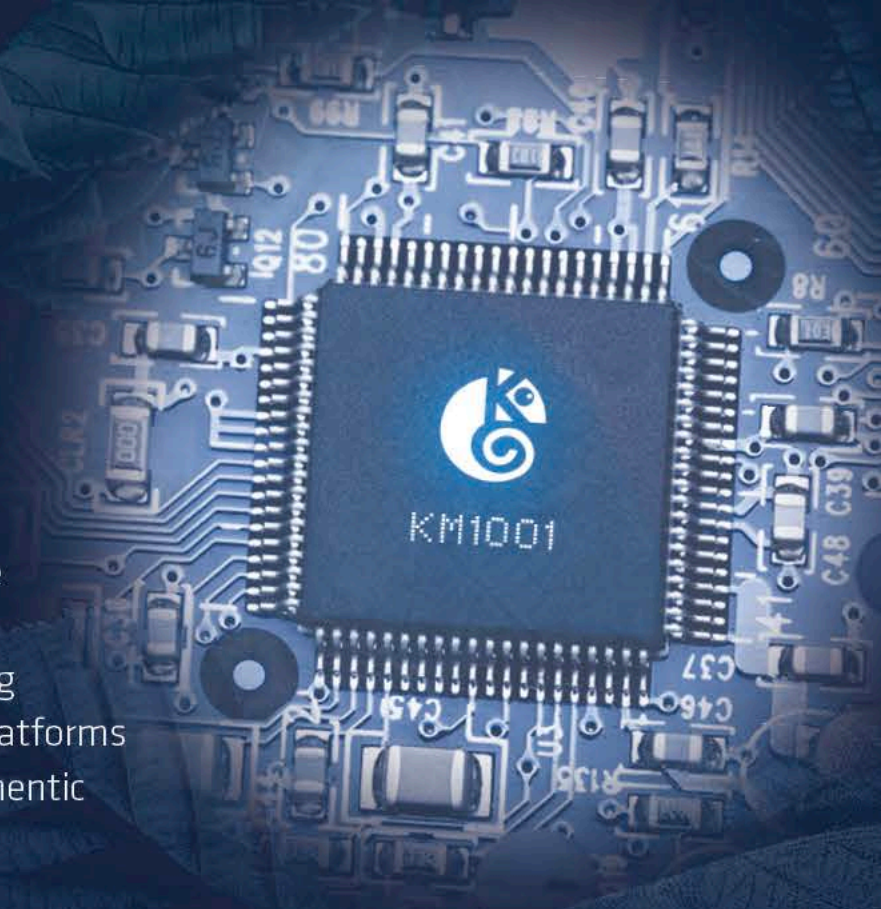
Kameleon

Security from the Hardware up



The Challenge

Today's security challenges are no longer confined to the application and software layers. Organizations are realizing that in order to build a truly secure platform, the underlying hardware needs to get much more security attention. With the threat landscape evolving, supply chain attacks and firmware-based threats are becoming more common and often being discovered in the wild. The need for securing our platforms from the Hardware up is becoming crucial, making sure platforms are running authentic firmware and enforcing the way the hardware manufacture designed them to run.

The Solution

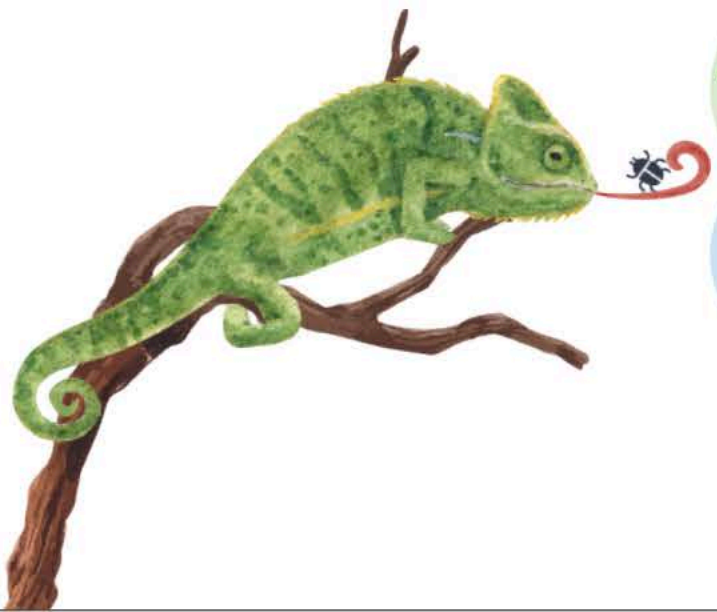
Kameleon's Proactive Security Processing Unit (ProSPU™) is the world's first processor designed to enforce system's security throughout its lifecycle. The ProSPU™ is a Hardware Root of Trust (RoT), controlling the system boot and performing platform and peripheral attestation. Kameleon can extend the RoT role for HW based runtime security by dynamically protecting and securing the computing platform and applications on it. Integrating Kameleon's ProSPU™ enables platform designers to implement Platform Firmware Resiliency and comply with the NIST 800-193 and OCP requirements with minimal effort. In addition, when deployed on Linux-based systems, it makes the platforms resilient to a wide range of software attacks such as malware, ransomware, and rootkits.

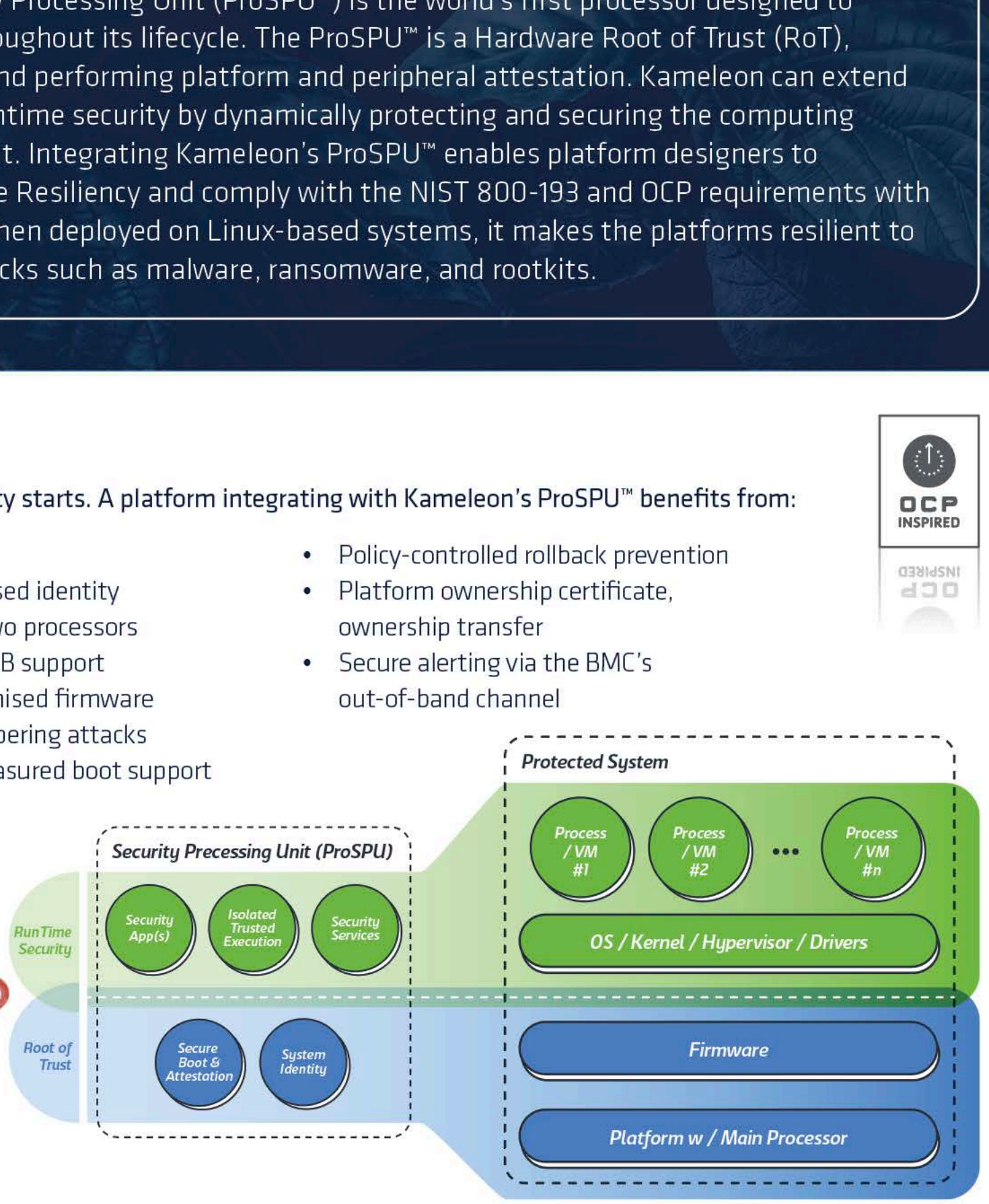
Root Of Trust (RoT)

The RoT is where the platform security starts. A platform integrating with Kameleon's ProSPU™ benefits from:

- NIST 800-193 PFR compliance
- A unique and unclonable PUF-based identity
- Platform Secure Boot for up to two processors
- Secure firmware updates, incl. A/B support
- Recovery of corrupt and compromised firmware
- Protection against firmware tampering attacks
- TPM integration for platform measured boot support
- Peripheral attestation
- Configurable security policies
- Policy-controlled rollback prevention
- Platform ownership certificate, ownership transfer
- Secure alerting via the BMC's out-of-band channel

OCP INSPIRED





Supply Chain Protection

Attacks aiming to compromising devices along the supply chain has gained momentum in recent years because it's extremely difficult to keep track of the entire supply chain and validate every component to the full security extent.

- Supply chain security starts at manufacturing and is maintained throughout the entire lifecycle
- Unique self-generated ID Enrolment to the secured data base and guarantees only trusted device will be assembled
- The device is factory locked at assembly house so only customer's code can be programed

Run Time Protection

The ProSPU™ protects the operating system and applications on the server during run-time, ensuring not only that the platform starts secure, but that it stays secure throughout the lifecycle.

- Integrity monitoring of kernel and user apps
- Kameleon's patented "Moving Target Defense" protection, to prevent 0-days exploitation
- Support for multiple flavors of Linux
- A platform for 3rd party security add-ons, enabling easy extensibility with custom run-time protections
- Cryptographic services (SHA, HMAC, ECC, RSA)

Platform Integration & Interfaces

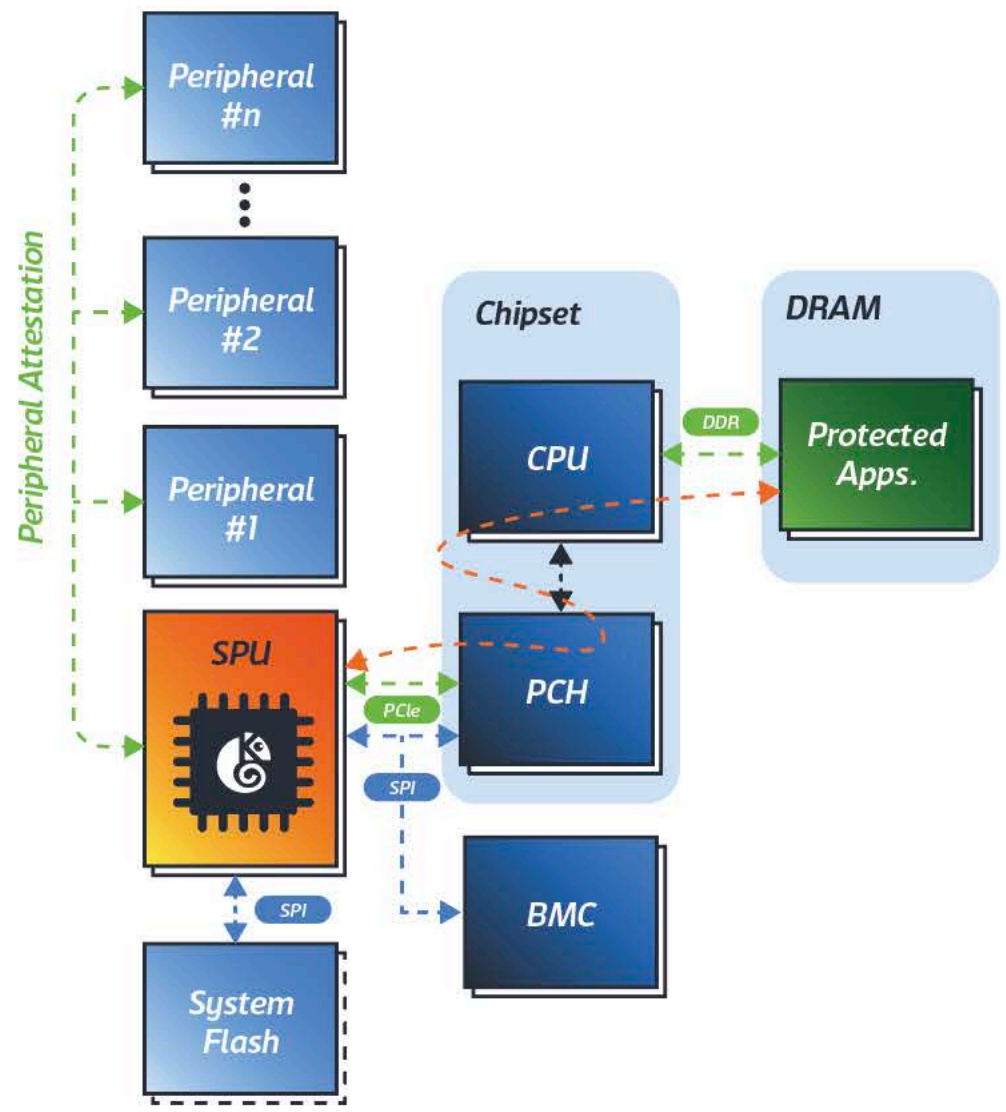
- SPI interposers (to intercept BIOS and BMC)
- SPI for external ProSPU™ Flash
- I2C interfaces (for BMC/PCH connections)
- PCIe (for run-time protection)
- SMBus (for peripheral attestation)
- PWR and RST controls
- GPIOs (for platform customization)
- OTP Fuse Array

Form Factors

- Chip on board based on ZU3CG 21cm X 21cm form factor, 784 pins.
- As a DC-SCM card, compliant with Open Compute DC-SCM spec.

Target Applications & Use-Cases

- Public and private cloud Data Centers servers
- Cloud Edge Servers
- Network, Storage and Security appliances
- Industrial IoT platforms



About

Kameleon, founded in 2019, is a fab-less semiconductors vendor that develops an advanced HW cyber security platform for computing systems. While the technology is generic and could fit almost any intelligent device, Kameleon's first product is focused on data centers and managed computers, with an extensive roadmap to expand into the edge, including IoT, automotive and mobile.

We'd love to hear from you!

info@kameleonsec.com

Kameleon Inc.
1365 Marilyn Drive, Mountain View, CA94040, USA
19 Tarshish Industrial Park St., Caesaria, Israel