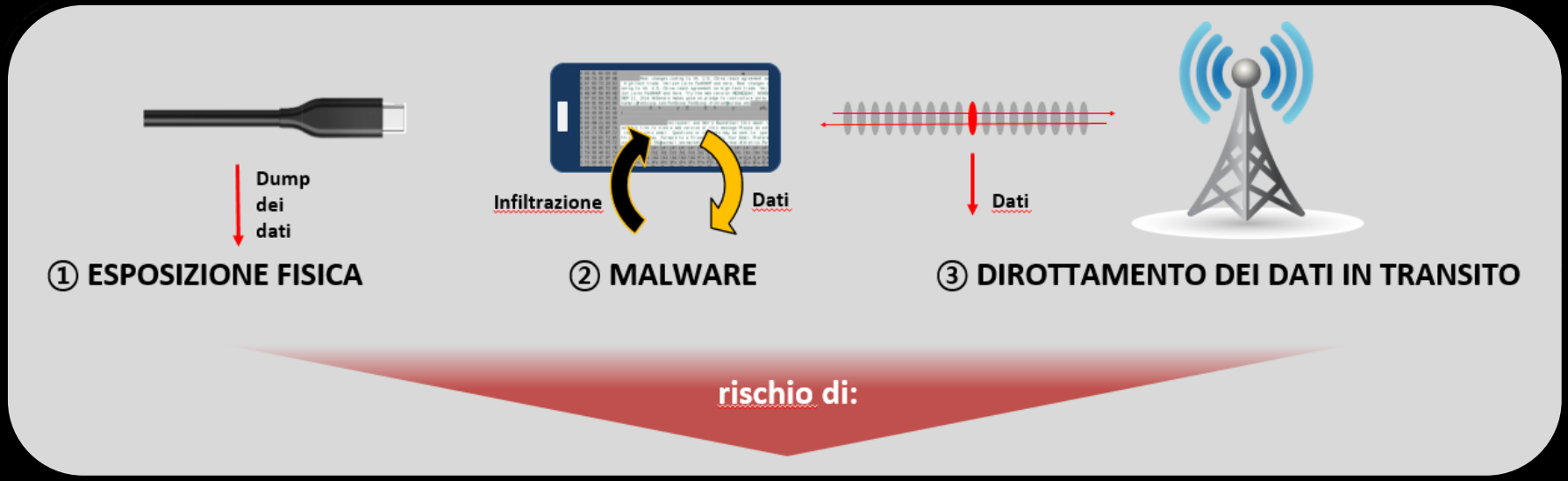
SAMSUNG
Samsung Knox
Aprile 2020
Samsung Electronics

SAMSUNG

Dispositivi mobile, differenti tipi di minacce

Le tipologie di minacce sono differenti in base al tipo di endpoint, alle tecnologie coinvolte e alla tipologia i dati accessibili. Ecco le minacce tipiche dello scenario di networking mobile che coinvolgono gli endpoint.

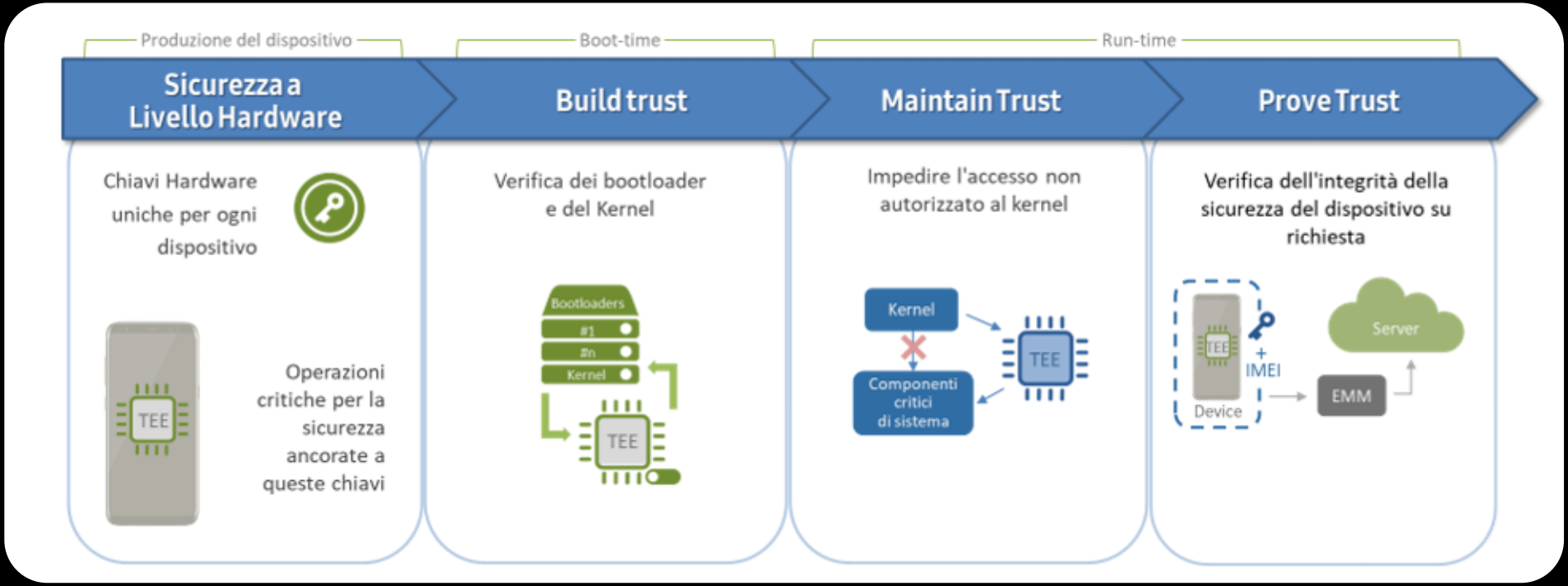


- Accesso a qualsiasi dato presente sul dispositivo
- Furto dei profili e credenziali del proprietario del dispositivo

SAMSUNG

Misurazione della conformità

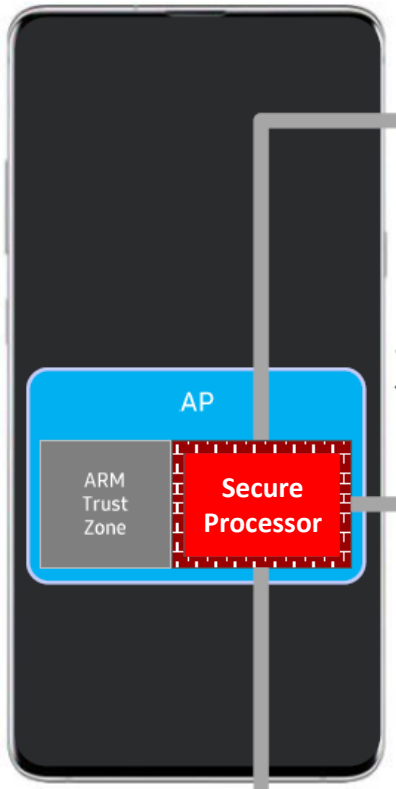
Un'efficace "root of trust" è in grado di apportare un cambio di paradigma, spostando l'enfasi dalla configurazione della conformità alla misurazione della conformità.



- KeyStore basato su HW – protezione dello storage a dispositivo spento
- Ispezione all'accensione
- Misurazioni di conformità durante le fasi di funzionamento per proteggere il sistema e garantire l'integrità dei processi core

Misure di sicurezza aggiuntive

Protezione contro attacchi Hardware e Side Channel



"Tamper-resistant Processor"

- *Independent Processor, RAM, ROM*
- *Secure against Hardware attacks and Side-Channel attacks*

Qualcomm : SPU (Secure Processing Unit)
S.LSI : STRONG

PP0084 EAL-4+ Cert
※ Exynos AP: EAL-5+

[BSI PP0084 Cert]

Security IC Platform Protection Profile with Augmentation Packages / BSI (Germany)

* Evaluation Assurance Level

Lv.	Description	Remark
EAL7	Formally Verified Design and Tested	
EAL6	Semi-formally Verified Design and Tested	
EAL5	Secure against whitebox attacks	Hubble(LSI)
EAL4	Secure against known hardware attack	Hubble(QC)
EAL3 이하	Insecure against hardware attacks	

[US Certification]

FIPS 140-2 Cryptographic Module Validation
NIAP(MDFPP CC) and DoD STIG (TBD)

Privacy Protection

Weaver app: Lock Screen (PIN/Pattern/Password)

Keys and Sensitive Data Protection

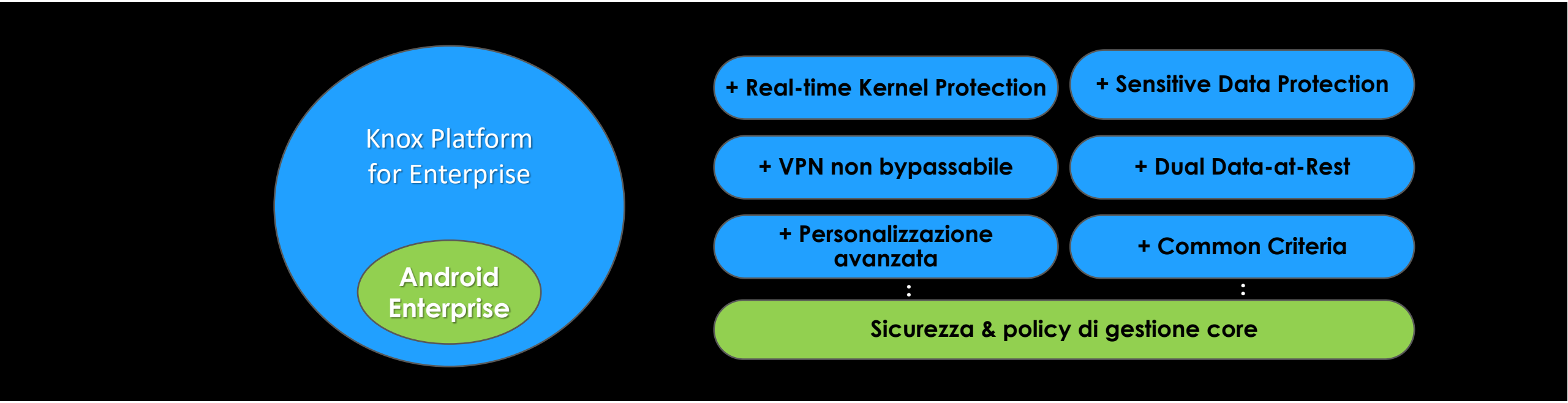
Strongbox keymaster app

Blockchain Private Key Protection

SAMSUNG

Piattaforma Knox per le Imprese: Scelto dai clienti

Fornisce funzionalità estese su Android Enterprise, rispondendo a severi requisiti di sicurezza



Certificazioni governative globali:

Common Criteria

SAMSUNG

Processi industriali sicuri

Uno dei principali criteri per valutare la forza della sicurezza dei prodotti per un'organizzazione è determinare se ha processi di sicurezza resilienti.

Durante il ciclo di sviluppo, è importante implementare un ciclo di vita di sviluppo sicuro.

All'interno dell'ambiente di produzione, la protezione della catena di approvvigionamento è una delle principali preoccupazioni degli acquirenti e dei regolatori.

Una volta che il prodotto è sul mercato, una pronta risposta per mitigare qualsiasi vulnerabilità appena rilevata è cruciale e deve essere prevista una gestione del ciclo di vita dei processi di segnalazione, mitigazione e aggiornamento delle vulnerabilità.

Questi processi di sicurezza devono essere implementati secondo i principi di governance della sicurezza accettati a livello internazionale. È quindi importante sviluppare e attuare una solida politica di sicurezza delle informazioni basata su standard internazionali.

Samsung ha adottato una politica di sicurezza delle informazioni sviluppata internamente, basata su ISO / IEC 27002.

SAMSUNG

Proposizione Samsung B2B

Connesso, Protetto, Produttivo

Samsung Knox

Suite completa di soluzioni di mobilità aziendale Samsung per sicurezza, gestibilità e produttività

Distribuzione

- Knox Configure
- Knox Mobile Enrollment

Gestione

- Knox Manage
- Knox E-FOTA

Sicurezza

- Knox Platform for Enterprise

Samsung Business Services

Servizi premium progettati per le aziende che utilizzano dispositivi mobili Samsung e soluzioni Knox

- Servizi di Personalizzazione software
- Servizi di supporto tecnico
- Servizi di garanzia

SAMSUNG

Servizi di personalizzazione software

Progettato per trasformare dispositivi consumer in macchine pronte per specifiche esigenze del cliente

Ottimizzazione delle prestazioni per scopi specifici

- Prevenzione usura eccessiva della batteria
- Maggiore durata della batteria
- Scansione del codice a barre più rapida / accurata
- Supporto di reti private

⋮

Supporto per periferiche dedicate

- Antenna radio tattica
- Ricetrasmittenti
- Batterie esterne di grandi dimensioni
- Dispositivi Bluetooth speciali

⋮

Personalizzazione del dispositivo a livello di sistema

- Remap dei tasti (es: Push-To-Talk)
- Accensione / spegnimento automatici del dispositivo in base all'alimentazione
- Uso simultaneo di altoparlanti e cuffie

⋮

Rilascio on-demand delle patch di sicurezza

- Security patch più frequenti

Precaricamento di app private / rimozione app

- Rimozione app "consumer" preinstallate