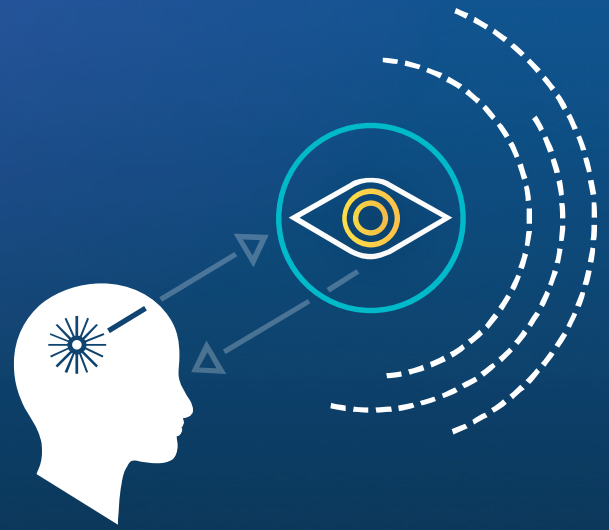
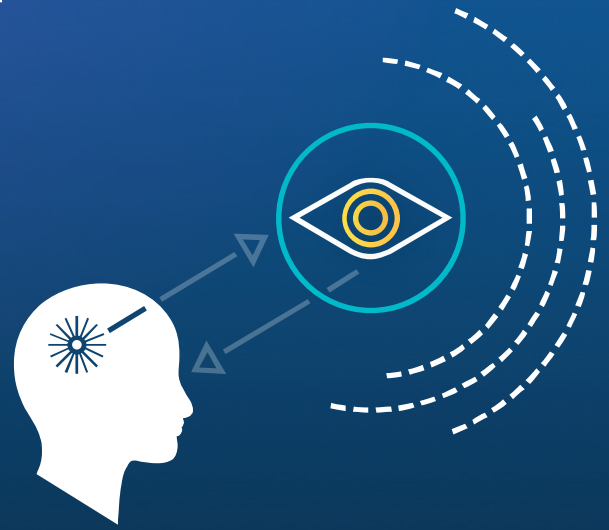
Security and Privacy Vision

QUALCOMM®



A robust and convenient security

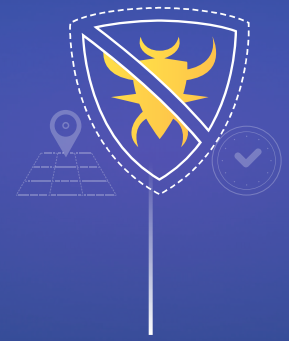
Enabled by hardware-based approach, on-device processing and cognitive technologies



Increasing privacy and security concerns

Malware Attacks

- Proliferation of malware
- Challenging malicious attacks
- Timely detection of new and unknown malware attacks



Authentication Issues

- Passwords are not working
- Current biometric challenges, e.g. spoofing and consistency
- Device credibility/reputation

Privacy Concerns

- User control of personal data
- Lack of transparency
- Stolen personal data

An unprecedented number of intelligent, connected things

A vision for seamless and preemptive security

Enhancing security and privacy, while providing convenient user experience

Preemptive protection

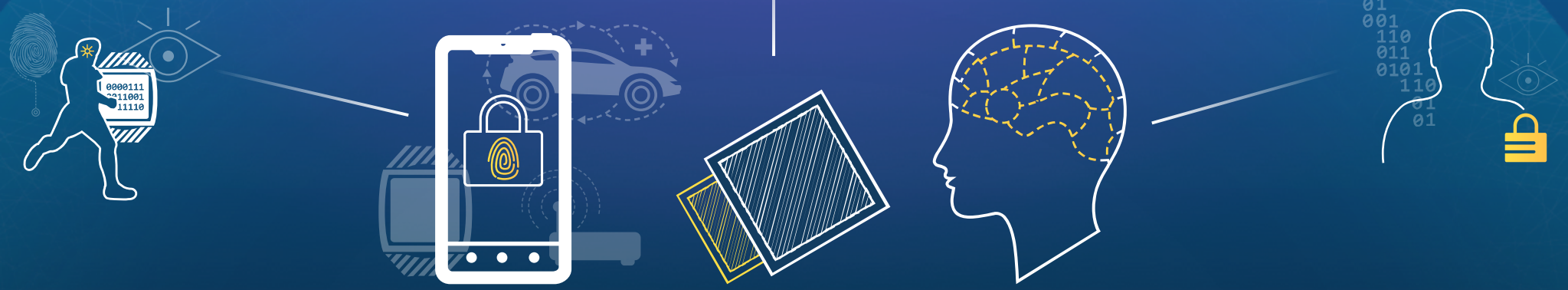
Early detection and isolation of unknown malicious attacks

Seamless authentication

Continuous, multi-factor authentication

Enhanced privacy

Advanced privacy that lets users control their data



On-device **Hardware-based** **Cognitive**

On-device processing is key for security and privacy

User privacy

Ability to enjoy services without the need to upload sensitive personal data to the cloud

Critical data protection

On-device storage of keys and biometric data

Always-on protection

Ability to deal with zero-day malware and phishing attacks

Personalized security

Adapting to device capabilities and user preferences

On-device

Hardware-based security is the foundation

Security embedded into the silicon and firmware

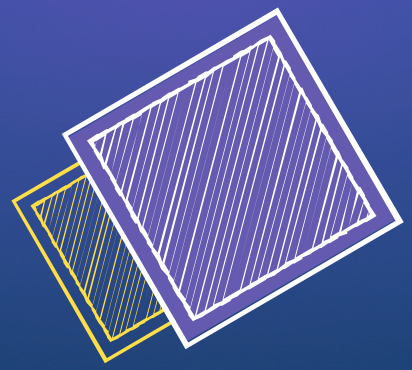
Enhanced security
Ensuring overall system security and device health

Rich user experience
Providing unobtrusive, efficient solutions

Extensible platform
Providing security services through open standards

HW firewall to isolate security functions from HLOS

HW cryptography engines



Secure execution environment

Robust storage of keys

Detection of rootkits* and malware

Hardware-based security

* Malicious code that gains low level access and remains hidden from apps and OS

Cognitive technologies support more intuitive devices

Reasoning

Learn, infer context and anticipate

Perception

Hear, see, monitor and observe

Action

Act intuitively and interact naturally

Cognitive Technologies

- Computer vision
- Always-on sensing
- Cognitive connectivity
- Machine learning
- Intuitive security
- Immersive multimedia

Making security more convenient through cognitive technologies

By applying behavioral analysis

Behavioral classification

Classifies device and user activity based on pre-defined behavior models

Behavioral observation

Monitors device software activities, as well as apps and user behaviors

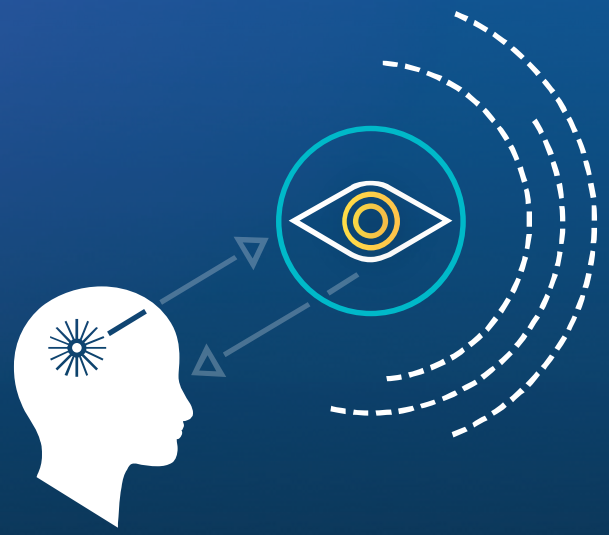
Actuation

Takes intuitive actions to enable robust and convenient security

Learns and adapts

Key focus areas of our security vision

Providing preemptive protection and seamless authentication, while protecting user privacy



A vision for seamless and preemptive security

Enhancing security and privacy, while providing convenient user experience

Preemptive protection

Early detection and isolation of unknown malicious attacks

Seamless authentication

Continuous, multi-factor authentication

Enhanced privacy

Advanced privacy that lets users control their data

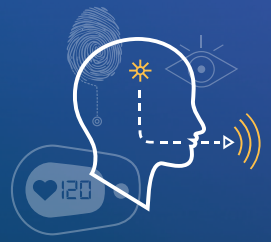
On-device **Hardware-based** **Cognitive**

Supporting seamless authentication

Applying on-device intelligence to multi-factor authentication

Continuous multi-factor authentication engine

- Reliable and accurate user identification
- Selects appropriate factors based on context and availability



Biometric

things only the user IS

Behavioral

things only the user DOES

Other devices

things only the user HAS

Biometric

Fingerprint identification while typing and holding the phone

Voice identification during your normal conversation through the microphone

Iris and face identification while looking at the front-facing camera

Heartbeat authentication while wearing a watch

Behavioral

Other Devices

Biometric

Behavioral

Your typical activities at certain places and times help authenticate you

Hand grip authentication by simply holding your phone

Authentication by simply walking and moving in your own unique way

Other Devices

Biometric

Behavioral

Other Devices

Your smartwatch confirms it's you to your smartphone

Continuously being authenticated

Based on who you are, what you do, and other devices you have

Vision for fingerprint authentication

On-device, hardware-based approach allows data to stays on the device

Secure

- Robustness
- Accuracy and consistency
- Anti-spoofing

Convenient

- Simply touch or hold the device
- Multi-finger
- A quick response

A vision for seamless and preemptive security

Enhancing security and privacy, while providing convenient user experience

Preemptive protection

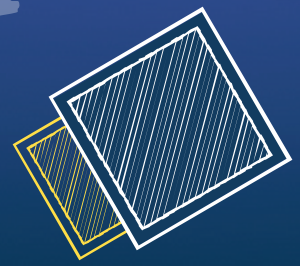
Early detection and isolation of unknown malicious attacks

Seamless authentication

Continuous, multi-factor authentication

Enhanced privacy

Advanced privacy that lets users control their data



On-device **Hardware-based** **Cognitive**

Providing preemptive protection from zero-day malware

Protecting users before they see an issue

Detection

- System-wide behavioral analysis
- Detection of rootkits

Blocking

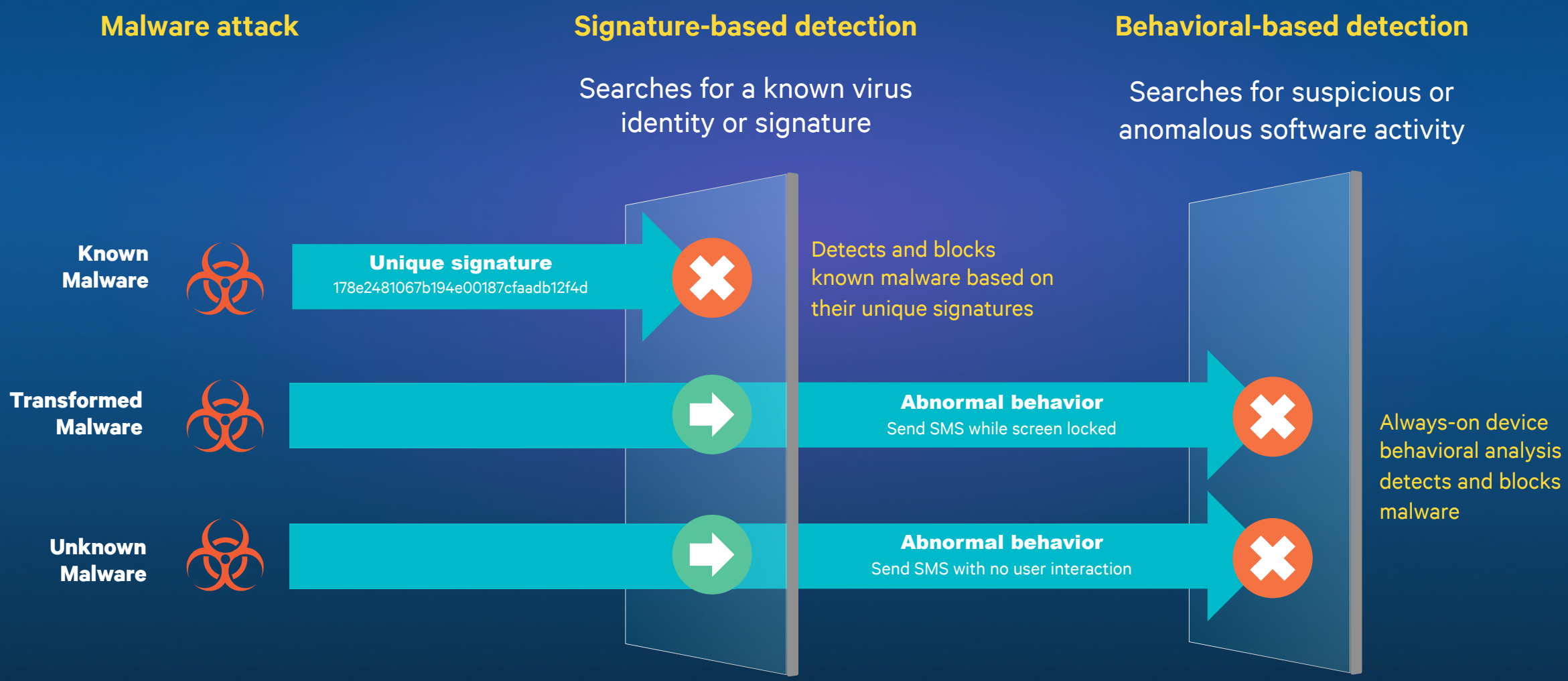
- Block malicious activities

Removal

- Uninstall malware

Zero-day protection

Behavioral analysis complements signature-based detection



A vision for seamless and preemptive security

Enhancing security and privacy, while providing convenient user experience

Preemptive protection

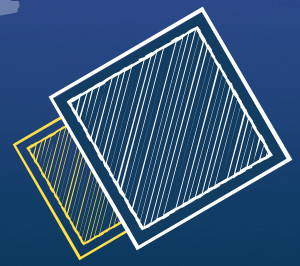
Early detection and isolation of unknown malicious attacks

Seamless authentication

Continuous, multi-factor authentication

Enhanced privacy

Advanced privacy that lets users control their data



On-device **Hardware-based** **Cognitive**

Enhanced privacy - users control their data

A user's conflicting wants

Personalized services and experiences

Control and ownership of their data

Giving control back to users

On-device processing

- Makes it possible for personal data to stay on the device
- Supports personalized services without compromising user privacy
- Protects biometric data and keys from harvesting and replay attacks

Enhanced privacy - users control their data

Personalized services and experiences

Control and ownership of their data

Giving control back to users

On-device processing

Data protection

- Hardware encryption of stored enterprise and personal data
- Cryptographic hardware keys that stay on the device
- Robust remote wipe of data

Enhanced privacy - users control their data

Personalized services and experiences

Control and ownership of their data

Giving control back to users

On-device processing

Data protection

Behavioral analysis

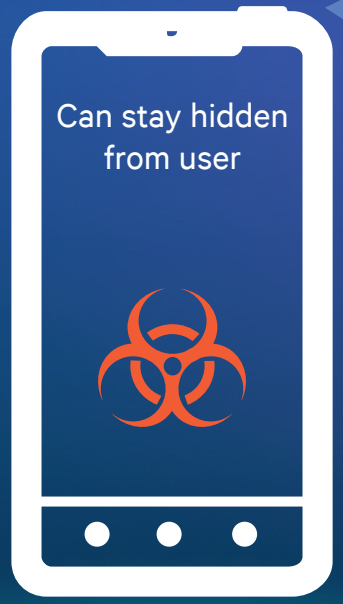
- Monitors software for suspicious activities
- Classifies activities to detect privacy violations
- Remove, stop, or make user aware of privacy violation

On-device behavioral analysis to detect privacy violations

Making users aware of data leakage

Non behavioral-based detection

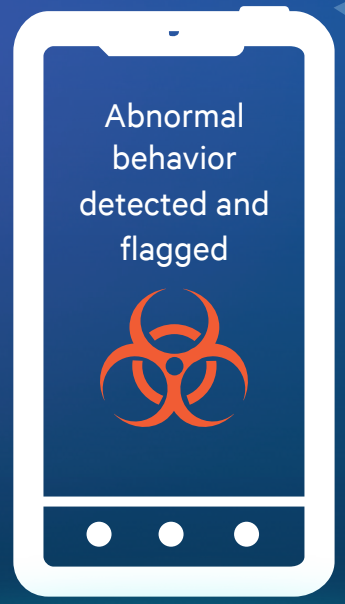
New spyware is installed on device by clicking on a bad app or link



Tracks user or uploads personal info (contact list, location history, pictures, etc.)

Behavioral-based detection

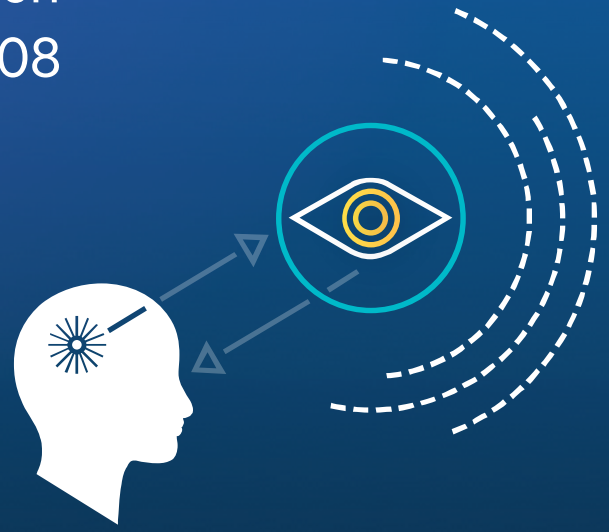
New spyware is installed on device by clicking on a bad app or link



User notified, leakage can be blocked, and spyware can be removed

Qualcomm Technologies security leadership

By building on its hardware-based foundation, Qualcomm has been offering proven security solutions for billions of devices since 2008

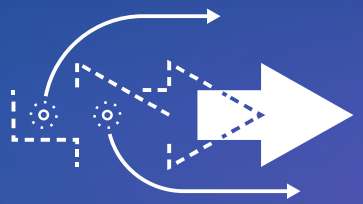


Qualcomm Technologies security leadership

Uniquely positioned to address security issues

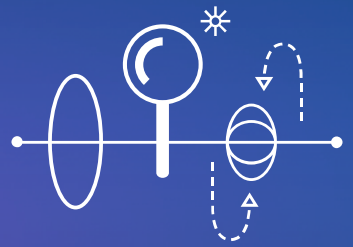
Industry traction

- Qualcomm security powers billions of devices



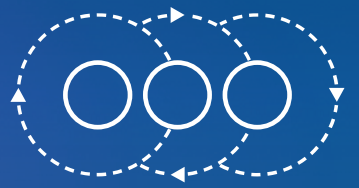
History of success

- Qualcomm® Snapdragon SecureMSM™ technology first introduced 2008
- 1st to receive Common Criteria's Mobile Device Fundamentals Protection Profile (MDFPP) certification



Holistic system approach

- End-to-end solutions
- Hardware-based security foundation
- Custom hardware engines and integrated software

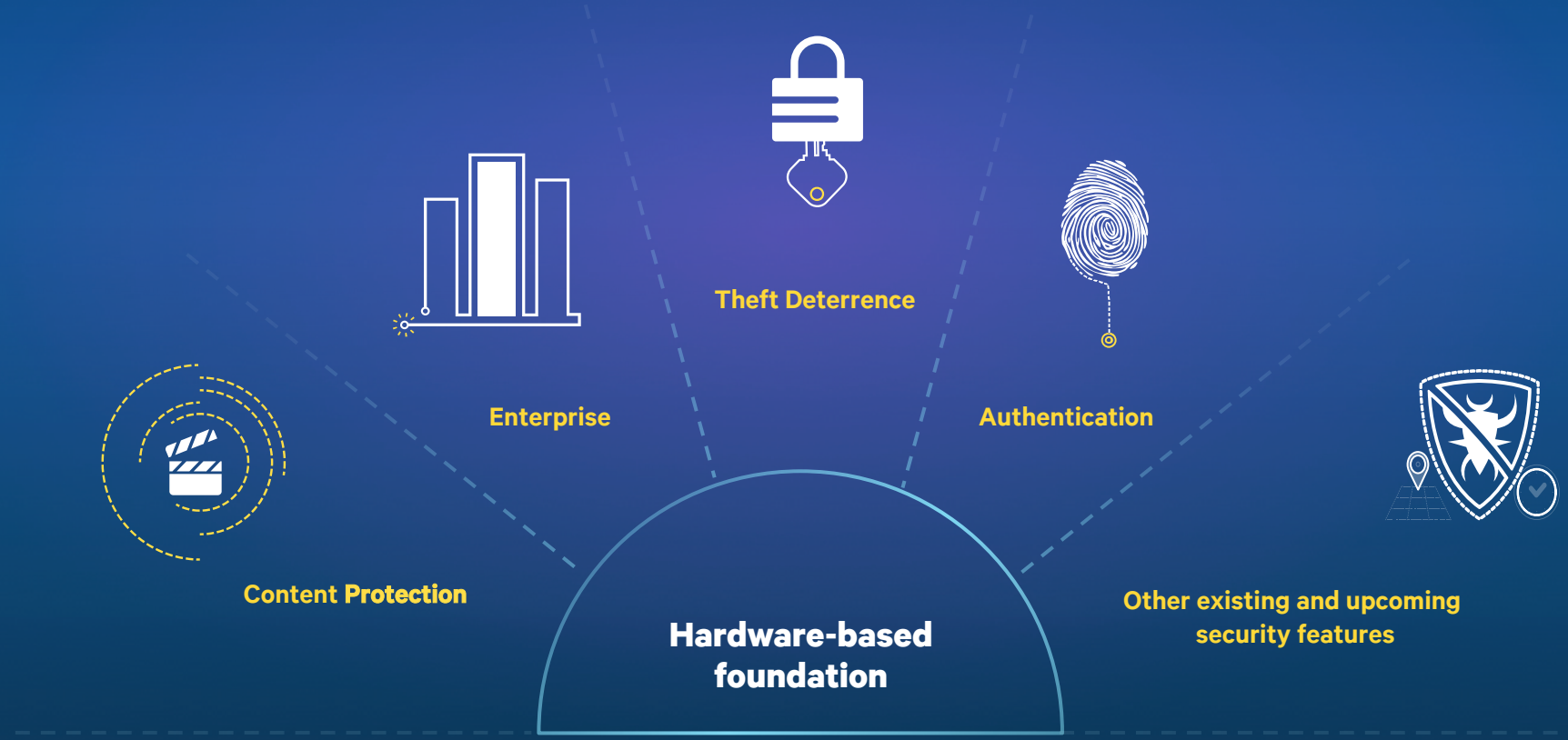


Ecosystem support

- Active participants in many open standards
- Working with leading security application providers

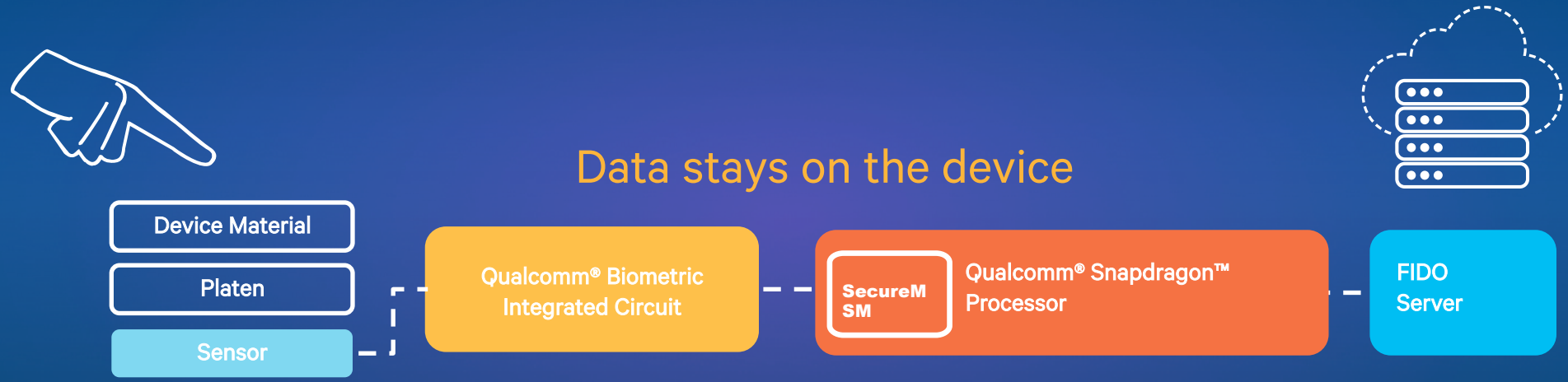
Offering multi-dimensional security solutions

Built on the foundation of SecureMSM Technology



Qualcomm® Snapdragon Sense™ ID 3D fingerprint technology

The mobile industry's first end-to-end ultrasonic-based biometrics solution



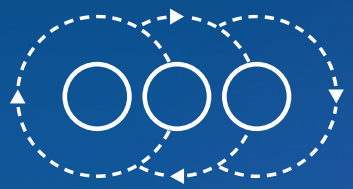
Captures three-dimensional acoustic detail within the outer layers of skin

Superior imaging detail for accurate detection of unique fingerprint characteristics

Less likely to be spoofed than capacitive-based sensors

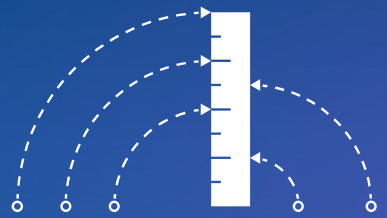
Offering broad ecosystem support

Driving end-to-end security solutions through collaboration and support



Industry organizations

- FIDO
- SCSA
- GlobalPlatform
- Trusted Computing Group
- W3C

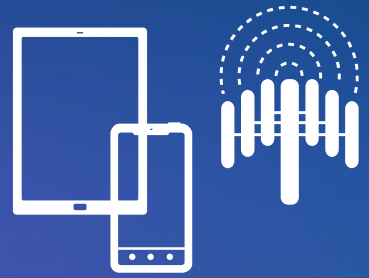


Public policies

- Certification (e.g. Common Criteria, FIPS 140-2)
- Data protection and privacy regulations (e.g. HIPPA)
- Phone theft, fraud (e.g. Kill Switch)
- Cybersecurity

Software and services

- Open standards
- Provisioning and signing services
- Software development kits
- Trusted execution environment porting kits



OEM and operator support

- Manage unique keys per device
- Key provisioning and services
- Sensor porting kits

Ecosystem partners

- Studios
- Financial institutions
- Enterprise services
- Public sector (e.g. healthcare)
- Distributors

A vision for seamless and preemptive security

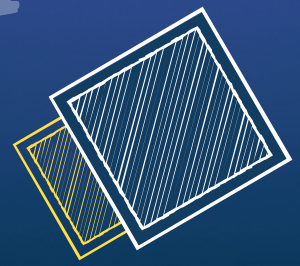
Enhancing security and privacy, while providing convenient user experience

Preemptive protection

Early detection and isolation of unknown malicious attacks

Seamless authentication

Continuous, multi-factor authentication



Enhanced privacy

Advanced privacy that lets users control their data

On-device **Hardware-based** **Cognitive**

Thank you

Follow us on:

For more information on Qualcomm, visit us at:
www.qualcomm.com & www.qualcomm.com/blog