SECURING THE ENTERPRISE WORKFORCE

From chip to cloud

The modern workforce can be productive from anywhere, exposing remote workers to more risks than when working within a traditional office space. That's because home and public Wi-Fi networks, such as in cafés, are not always built with enterprise-grade security.

Protect your corporate fleet with laptops powered by the Snapdragon® 8cx Gen 3 Compute Platform, engineered with advanced endpoint security features, zero trust sensor framework, and persistent connectivity to cloud intelligence.

A FORTRESS OF ADVANCED SECURITY FEATURES

The Snapdragon 8cx Gen 3 is equipped with the latest in endpoint security to help prevent hardware attacks and further support maximum security by eliminating the need for external controllers.

Layered Platform Secure Boot
Protection and security from the moment the device powers on, with firmware validation to verify signed boot images. This decreases the threat attack surface by removing the need for an external controller.

Qualcomm® Secure Processing Unit
An added layer of hardware security, with multilevel protection against threats that brings the most advanced security features to a Windows PC in a protected execution environment.

Qualcomm® Trusted Execution Environment (TEE)
Designed to allow trusted execution of code and to protect against viruses, Trojans, and root kits.

Microsoft Hyper-V Enabled
Creates secure, virtual environments to enable multiple OSes or OS instances to run on the same physical system.

Microsoft Secured-Core PC
Enables the latest PC security for the most secure Windows devices out-of-the-box (requires OEM enablement).

Hardware Accelerated Encryption
Delivers high-speed encryption to secure business-critical data through a hardware key manager.

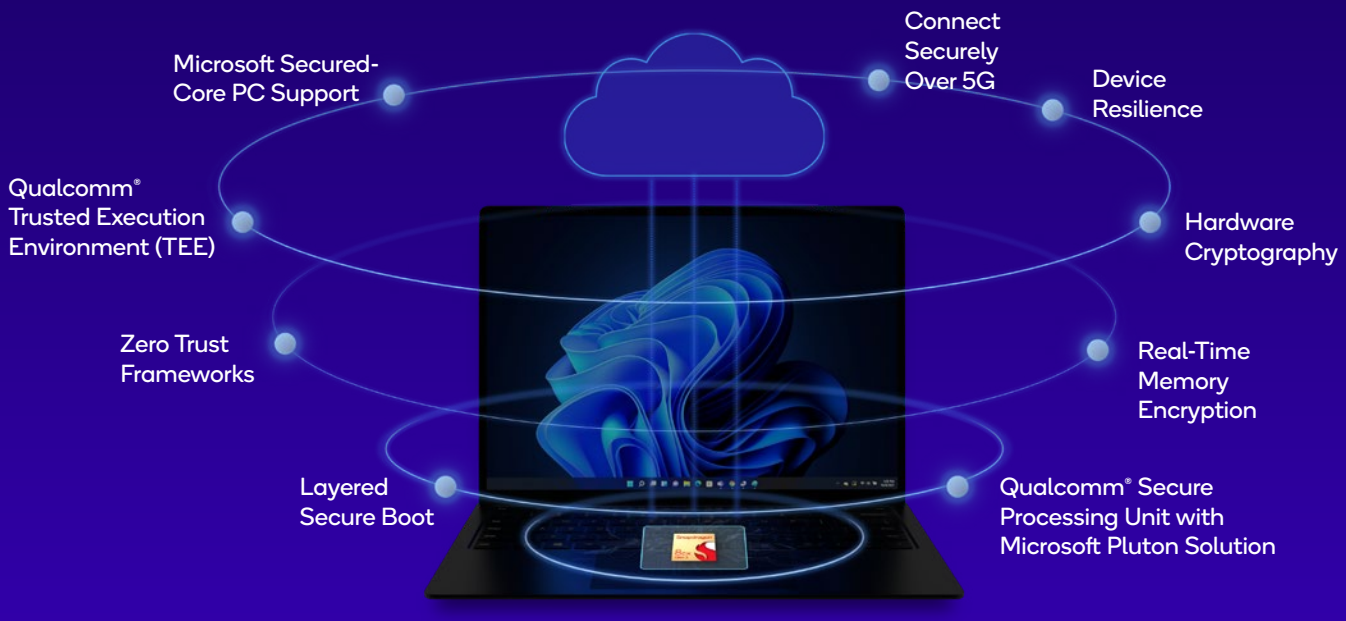
Runtime Memory Encryption
Hardware-accelerated encryption of data stored in memory to protect against threats, such as cold boot attacks.

Peripheral Management
Dynamically and remotely manage user interfaces, such as USB and camera.

All comparisons made are in reference to previous generation, Snapdragon 8cx Gen 2 Compute Platform. Results will vary depending on OEM implementation and other factors. Battery life varies significantly based on device, setting, usage, and other factors. Snapdragon and Qualcomm are branded products of Qualcomm Technologies, Inc. and/or its subsidiaries.

Snapdragon

Chip-to-Cloud Security



ZERO TRUST PROTECTION

To help keep data secured and untampered, the Snapdragon 8cx Gen 3 Compute Platform offers encrypted security layers outside the OS.

Trusted Location

GPS sensor information accessible outside the operating system layer to bring about and maintain highly secure geofencing policies for location-based zero trust decisions.

Device Health Monitoring

Verifies device boot status, device configuration, and OS health by assigning a unique serial key for IT to send specific encrypted data to the device.

Connection Health Monitoring

Connection health monitoring can uncover a spoofed network, blocking Man in the Middle attacks that lead to data breaches.

Identity Management

Biometric sensors for identity access management, including Windows Hello Face Recognition. Plus, continuous authentication through low-power sensors, leveraging AI (Computer Vision) to maintain identity access throughout device session.

ALWAYS-CONNECTED SECURITY

With the Snapdragon 8cx Gen 3, you get increased device visibility and management features, with persistent connectivity to the corporate network to ensure compliance across the corporate fleet of devices.

Always-On, Always-Connected

Increases visibility for threat detection and response through persistent connectivity (5G/4G/Wi-Fi), even out of Wi-Fi range or in low-power idle states (network activation required).

Cloud Intelligence

Persistent link to cloud AI for deep analysis of corporate fleet of endpoints to monitor for and protect from malicious activity.

Edge AI

A dedicated Qualcomm® AI Engine runs security applications quickly and efficiently, without draining CPU resources. Used in combination with cloud connectivity (so security providers can keep applications up-to-date), AI can detect threats up to 7x faster than on x86 PCs.

Real-Time Telemetry

Increased device telemetry can enable cloud intelligence to help detect threats and remediate vulnerabilities.

All comparisons made are in reference to previous generation, Snapdragon 8cx Gen 2 Compute Platform. Results will vary depending on OEM implementation and other factors. Battery life varies significantly based on device, setting, usage, and other factors. Snapdragon and Qualcomm are branded products of Qualcomm Technologies, Inc. and/or its subsidiaries.

Snapdragon