SECURING THE MODERN WORKFORCE

In today's hybrid work world, employees and their laptops are everywhere—and threats are, too. Protect your corporate fleet with Copilot+ PCs powered by the Snapdragon® X Series Processors, engineered for modern deployment and workflow management at the edge. With multilevel threat protection and intelligent security features baked into the silicon, company data can be protected both on device and from chip to cloud.

With a persistent connection, IT departments are able to support employees from a distance by monitoring device performance in real-time, proactively addressing issues as they arise, and ultimately keeping work in motion.

THE MOST SECURE WINDOWS DEVICES OUT-OF-THE-BOX

Snapdragon X Series processors have Microsoft Secured-Core certifications, protecting your corporate fleet from attacks with advanced endpoint security features, a zero trust sensor framework, and the ability to save confidential data on device.

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 and support for Microsoft Pluton security architecture to store sensitive data on device.

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.

Snapdragon

Chip-to-Cloud Security

ZERO TRUST PROTECTION

Give your IT departments better manageability with encrypted security layers and auto-healing device resilience that detects and recovers corrupt firmware and BIOS.

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 automatic facial authentication and lock features to protect from others seeing confidential data on-screen.

ALWAYS-CONNECTED SECURITY

Increase device visibility and management features through a persistent connection to the corporate network.

Always-On, Always-Connected
Built-in 5G/4G/LTE connection enables compliance across an entire corporate fleet of devices—even in sleep mode (network activation required).

First Always-Sensing ISP in a PC
An upgraded Qualcomm® Sensing Hub heightens security with the first Always-Sensing ISP in a PC, enabling new privacy features like presence detection for a better login experience, as well as wake on approach, lock on leave, and adaptive dimming.

On-device AI
Improves company security and end user privacy by reducing risks linked with transferring, storing, and using AI in the cloud. Your fleet is also protected against cyberthreats with security that extends far beyond corporate firewalls—helping to keep confidential data secure, wherever laptops roam.

Real-Time Telemetry
Increased device telemetry can enable on-device and cloud intelligence to help detect threats and remediate vulnerabilities.

Snapdragon