The World’s First Unhackable Laptop

We’ve Redefined “Secure”

UNHACKABLE – the world’s only EAL 6+ certified separation kernel means you know what is executing on your platform and where. Factory installed, use case specific security policy means zero vulnerabilities from improper configuration. It literally cannot be configured improperly. No hardware configuration management. Repeat. No hardware configuration management. Security Application operations center – do you really trust your client operating environment? Put security applications where they belong – away from your user environment.

The ID Technologies Zero Vulnerability (ZV) Mobile Client Built on Dell® 7000 Series

- Intel® UHD Graphic 620 with Displayport over USB Type-C with Core i7 vPro
- 16GB, 2x8GB, 2400MHz DDR4 Memory
- M.2 256GB SATA Class 20 Solid State Drive
- 14.0” FHD (1920x1080) Anti-Glare, HD CAM/Mic, WWAN/WLAN, Mag Alloy back, Non Touch
- Intel® Dual-Band Wireless-AC 8265 Wi-Fi + BT 4.2 Wireless Card (2x2)
- 60 Whr Express Charge Capable (4-cell)

ID Technologies Zero Vulnerability (ZV) Mobile Client

Powered by the ITEGRITY EAL 6+ Certified Operating System
Customized security policy factory configured
Mission ready upon receipt
Appliance model means configuration management not required
Solution Security Architecture is fully Commercial Solution for Classified (CSfC) Compliant
The Archon Protects Your Data.

Platform Features

- Embedded security appliance on COTS Dell Laptop
- Developed using secure development and coding practices (e.g. NIST 800-160, Orange Book)
- Automated security configuration and provisioning
- Key Management integrated into platform
- Leverages Intel VPro Security and performance features
- Secured with INTEGRITY™ fingerprint verified at boot
- High Assurance Process Separation
  - Hardware enhanced Micro-Virtualization
- Secure Boot
  - Highly trusted software to perform Boot integrity validation and verification
  - Hardware integrity checks
  - Removal of extraneous code in BIOS and firmware
  - Run-time software restrictions
- Hardware Components
  - Authenticity verification
  - Integrity verification
  - Cryptographic Digital Fingerprint
- Software Components
  - Embedded software authenticity verification
  - Firmware dedicated to components actively utilized
- I/O controls
  - Communication to hardware controlled by High Assurance RTOS
  - Malicious communications not permitted
- CSFC Compliant stack per container
  - Network Communication
  - Data Storage