Technologies

ARCHON
SECURE ACCESS ANYWHERE

Archon Zero Vulnerability Platform
Work securely at the edge with the world's first un-hackable laptop

Mobile personnel working with sensitive and classified information can't risk information leakage or identity disclosure. They need a mobile device that enables them to work efficiently while protecting against operating system vulnerabilities, configuration errors, errant or malicious code, traffic sniffing, location tracing, and other threats. The NSA had this requirement in mind when it created the Commercial Solution for Classified (CSfC) Mobile Access Capability Package (MA CP). But most of today's CSfC-compliant mobile devices are expensive, complicated to use in the field, and difficult to roll out and manage at scale.

Solution: pre-configured laptop with integrated hardware

The Archon Zero Vulnerability (ZV) platform realizes the promise of the CSfC MA CP, building on a Dell Latitude laptop to create a zero-trust operating environment with customized security:

- **Real-time operating system.** The military-grade RTOS provides Secure Boot, encrypts data at rest, and authorizes firmware and hardware during manufacturing. A separation kernel prevents incorrect or malicious code from causing harm by blocking processes from writing outside of their assigned memory regions.

- **Internal retransmission device.** When laptops connect over untrusted networks, the CSfC MA CP requires use of a retransmission device with a wired (not wireless) connection to the laptop. The Archon SideArm routing device is embedded in the Archon ZV laptop, enforcing compliance.

- **Factory configuration for mission requirements.** Agency specific cryptographic services and security policies are embedded in the hardware during the US based factory process. Settings such as allowed tasks, edge network connectivity, and offline operation can only be changed over the air—not by users. We white-list allowed tasks rather than black-listing prohibited tasks for a higher level of assurance.

- **Obfuscation of the user device and the destination server.** Optional Archon CAMO software routes transmissions from the device through a multi-hop path—a unique path for each session—adding another layer of encryption at each hop. Adversaries monitoring traffic leaving the laptop can't see the destination server; adversaries monitoring government servers can't see the device at the other end of the connection.

How it works: shipped pre-configured, ready to use in minutes

- We meet with you to understand your mission requirements, including allowed tasks, edge network connectivity, and offline operation.

- Laptops are configured with your security policy at the factory—tailored for individual teams or users if needed—and then shipped to you.

- Users can begin using the preconfigured laptop in minutes, as soon as they download a certificate.

- Personnel need little or no training because security does not alter the user experience. The Archon ZV laptop supports any mission applications running on Windows, Linux, Android, or POSIX.

- Configuration can only be modified over the air, by your team or us. Use Archon Manager to make updates over the air, including certificate renewals. Users can't change the configuration, providing

---

The Archon ZV difference

- **CSfC MA CP compliance.** The Archon SideArm retransmission device is integrated into the laptop chassis, ensuring compliance and saving personnel from having to carry a separate device.

- **Works with or without a network connection.** We can configure the Archon ZV to operate as a thin client, thick client, or both.

- **Rapid rollout at scale.** The Archon ZV laptop is shipped pre-configured. It's ready to use out of the box, in minutes.

- **Secure, over-the-air operating system and firmware updates.** Update Archon ZV laptops anywhere in the world as soon as new code is available, from a secure management server. Not waiting for personnel to bring their device to a central location reduces the window of vulnerability.

Learn more

Contact ID Technologies at sales@idtec.com.

IDtec.com