Archon Client

Pre-configured laptop with integrated hardware.

For more information about Archon Client and the Archon suite of secure network computing solutions, visit: **caci.com/archon**

Remote and geographically dispersed personnel who handle sensitive information can't afford to risk compromised data or identities. They need a mobile device built to support their work securely and seamlessly, shielding them from cyberattacks, system vulnerabilities, and other unknown, evolving threats.

This critical security need is central to the National Security Agency (NSA) Commercial Solution for Classified (CSfC) Mobile Access Capability Package (MACP). Yet, most of today's CSfC-compliant mobile devices are costly, complicated, and difficult to deploy and manage at scale.

Archon Client fulfills the promise of the CSfC MACP by creating a CSfC-compliant laptop that is secure, easy to manage, and one that users want to use.

DELL Technologies
TITANIUM PARTNER

CACI

The Archon Client difference

Tailored to the mission

We meet with customers to understand mission requirements – including allowed tasks, edge network connectivity, and offline operation – and security policies for specific users and teams.

User-friendly

Users need little or no training because security doesn't change the laptop user experience. Archon Client delivers a high-quality user experience without compromise for both thick and thin client use cases.

Continual updates

Only your team can configure updates through Archon Manager, which drops updates over the air, including certificate renewals. Archon Client liberates personnel to securely operate anywhere and meet their missions with CSfC compliance and unparalleled security.

Deployed instantaneously

Users can work from their preconfigured laptops minutes after they download a security certificate.

FEATURES

High assurance, NIAP-accredited Archon operating system

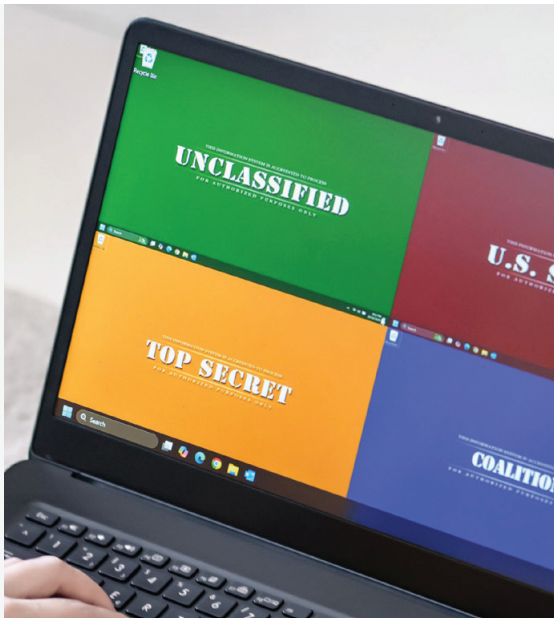
Our highly secure operating system serves as the platform for separate, immutable virtual machines hosting captive portal, inner and outer VPN connections. Our operating system provides secure boot, encrypts data at rest, and authorizes firmware and hardware during manufacturing.

Internal retransmission device

Archon Clients include Archon Sidearm, an integrated internal retransmission device, which meets the NSA MACP 2.6.

Embedded security control framework

We embed hardware with agency-specific cryptographic services and security policies during the U.S.-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 whitelist authorized tasks rather than blacklisting prohibited tasks for a higher level of assurance.



About the Archon Suite

Empower your end users to securely work from anywhere at any scale. From next-generation devices to hardware and data services, the Archon® Suite of CSfC capabilities make securing your edge simple, fast and efficient.

caci.com/archon

CACI