Accelerating Simplicity

At ID Technologies we have a clear mission - to make it simpler for our customers to buy and use IT that’s fit for their purpose. We don’t say that IT projects are ever easy - IT is hard to do well, the stakes are often high and technology is evolving rapidly. But there is much we can do to ease our customers’ experience and minimize time-to-value. We call our process “Accelerating Simplicity”.

Our Guiding Principles

Differentiation
We work with proven capabilities we know will outperform the market and at lower cost.

Time-to-Value
We make the value of IT spend more quickly accessible to the customer.

Customer Relevance
We work only with partners whose products and approach align with the unique contexts and goals of our customers.

Simplifying the path to CSfC compliance—from the endpoint to the cloud

All missions have a common requirement—fast, secure, reliable communications. Success requires attention to where data is created, how it moves across the network, and where it lands.

At the edge. Personnel at the edge need an ultra-secure mobile device with an operating system hardened against cyberattacks. Cryptographic services and security policy configured in hardware rather than software. Connection to untrusted wired or wireless networks only via a wired connection to a retransmission device, as stipulated in the NSA Commercial Solutions for Classified (CSfC) Mobile Access Capability Package (MA CP). And a way to prevent adversaries aware of government internet points of presence from tracking connections to discover field assets’ identity or location.

Across the WAN. To convert data from local sensors to actionable intelligence, tactical teams need fast access to analytics servers that may be thousands of miles away. In areas with high WAN latency, teams can’t perform time-sensitive analytics such as facial recognition. Headquarters personnel also need fast WAN performance—in their case, to support growing use of cloud services. Throwing more bandwidth at the problem is prohibitively costly and doesn’t guarantee reliable performance.

To the cloud. IDC projects that the world will produce 300% more data from 2020 to 2025 than it did in the previous five years. Agency IT teams need the scale and operational ease of public cloud storage—but with the security and control of an on-premises deployment.

Achieve CSfC-compliant communications from the edge to the cloud with the Archon Solution Suite. A federal government vendor since 1988, our mission at ID Technologies is to make it simpler for you to buy and use IT that supports your mission. We designed Archon products to realize the vision of the CSfC Program: “to securely communicate based on commercial standards in a solution that can be fielded in months, not years.” Read on for more.

At the edge

Enable tactical assets with a secure end-user device

Zero-vulnerability laptop: Archon ZV
Tactical users need a mobile device that protects against operating system vulnerabilities, configuration errors, errant or malicious code, traffic sniffing, location tracking, and other threats. The Archon Zero Vulnerability (ZV) platform creates a zero-trust operating environment with customized security. Starting with a Dell laptop, we add: a real-time operating system, an internal retransmission device, and factory configuration for mission requirements.
Built-in retransmission device: Archon SideArm RD
The CSfC MA CP requires that personnel connecting end-user devices to non-government-owned Wi-Fi, cellular, or wired networks use a retransmission device (RD). The end-user device must connect to the RD via a wired, not wireless connection. The Archon SideArm internal transmission device (IRD) is a self-contained router (wired, wireless, and LTE) integrated into the Archon ZV laptop. Archon SideArm has its own processor, memory, Wi-Fi and LTE chips; and separate firewalls for Wi-Fi, cellular, and Ethernet, relying on the laptop only for power.

Obfuscation and misattribution: Archon CAMO
Most identity-protection solutions create a cover identity for investigators or analysts. But adversaries can also identify assets by tracing their connections to government internet points of presence (PoPs). The problem is that the PoP is a fixed target. Archon CAMO is designed to prevent adversaries from associating mobile users with CSfC enclaves and other government servers. With Archon CAMO, the government server is no longer a fixed target because it appears to move constantly.

The world is listening: GoSilent
The GoSilent Security solutions were designed to protect from both the outside-in and the inside-out. Secure any user or device simply by connecting to a GoSilent cube. Compatible with any IP-enabled device (no matter how old) and effective over any connection (no matter how public) with near zero configuration required. Security so simple, “it just works.”

Over the WAN
Connect the edge to the cloud as if it were next door
Rapid analytics at the tactical edge: Archon Proxima
Archon Proxima is an enterprise-class networking solution that makes the WAN perform like a global LAN. One compact device is deployed at the edge, another in the data center. Working together, the edge and data center devices create a globally distributed, scale-out file system rivaling the experience with local resources.

Global managed SD-WAN solution: Archon Cloud Fabric
Archon Cloud Fabric is a managed SD-WAN solution designed to deliver an excellent, predictable WAN experience over less-expensive, smaller links. We used an SD-WAN overlay to unite your existing WAN infrastructure—any vendor’s wired, wireless, and satellite equipment and links—with our private internet circuits. Our circuits connect to more than 500 Performance Hubs around the world. Performance Hubs give you access to thousands of last-mile network providers and are located near major cloud providers, reducing latency.

To the cloud
Keep content secure in a scalable, on-premises storage cloud
Agency storage requirements are growing ever larger, fed by video, Internet of Things data, and artificial intelligence and machine learning applications.

Archon Cloud Storage combines the best of cloud and on-premises storage to deliver high performance, control, and security compliance. As a fully managed service, Archon Cloud Storage includes high-performance hardware dedicated exclusively to you, plus complete lifecycle services—all for a low monthly fee. We can deploy and manage your hardware anywhere—in your data center or in a top-tier data center. Users experience fast performance thanks to a globally distributed, purpose-built object storage architecture, and leading disk drive technology.

Next G?
Archon leverages NSA CSfC Capability Packages to ensure your data is protected over any method of transport, including 5G. Building CSfC into your private 5G rollout provides not only secure access to your data over a wireless link but a clear path to ATO. Having CSfC implemented in your infrastructure and on your end user device provides a clear, documented and repeatable path forward that the NSA will certify.

Learn more at idtec.com.
We welcome the opportunity to discuss the art of the possible for your mission.