carahsoft

FRØNTIERX

Fr0ntierX Capability Statement

Pioneering Secure Computing

Thank you for your interest in exploring this content.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Fr0ntierX, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

Explore More Resources:
carah.io/Fr0ntierXResources

Discover Technology Solutions:
carah.io/Fr0ntierX

Connect With Our Team:
Fr0ntierX@carahsoft.com
866-468-3868

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

FRØNTIERX

Pioneering Secure Computing

Capability Statement

COMPANY DATA

NAICS CODES

541512 / 541511 / 541519 / 518210

CAGE CODE	UEI
02W17	MVS1EACNDSG4

BUSINESS SIZE

Small Business

CORE COMPETENCIES

- Confidential computing and continuous runtime attestation
- Runtime evidence supporting continuous authorization (cATO), RMF, and zero-trust architectures
- Cryptographic policy enforcement and key control conditioned on verified runtime state
- Software and firmware integrity verification for supply-chain assurance
- Sensitive and classified AI/ML and GPU workload protection
- Deployment across cloud, on-prem, sovereign, and edge infrastructure, including air-gapped environments, with no data egress

PAST PERFORMANCE

MITRE — leads the working group on continuous layered attestation of confidential computing systems.

Confidential Computing Consortium — holds a seat on the governing board.

Oracle — product partnership extending the Polaris trust fabric across a commercial product line.

AWS, Microsoft Azure, Google Cloud — active platform partnerships.

Arizona State University — defense research focused on space.

Overview

Fr0ntierX is a secure computing company. Its platform, Polaris, is a trust fabric for live compute: continuous cryptographic proof that sensitive workloads run where they should, under the conditions they should, for as long as they run. Confidential computing proves the environment at launch. Polaris proves it for the life of the workload: anchored in the silicon, it verifies, governs, and enforces the conditions under which each one runs, at every layer above it. If a workload can no longer prove it is trusted, its keys are revoked and it loses access to protected data.

Differentiators

Continuous, not point-in-time

Confidential computing verifies the environment at startup. Polaris keeps verifying that the workload environment stays in its known-good state while the work runs — as often as every few seconds — so a loss of trust triggers enforcement in real time, not at the next audit.

Trust as an operating control

Polaris does not just detect a loss of trust. The customer defines in advance what a violation triggers, turning trust from a one-time check into an enforceable operating control.

One trust model, every environment

No separate trust model for each cloud, processor, GPU, or operator. Polaris brings evidence from any confidential-computing hardware into one evidence, policy, and response model spanning cloud, on-prem, sovereign, edge, and partner-operated infrastructure.

Independently verifiable, nothing to trust

Anchored in the silicon root of trust, the proof stands on its own — the customer can verify it without trusting Fr0ntierX or the cloud provider. Parts of Polaris are open source, and the full codebase is available for review.

Applications

Cloud, On-Prem & Hybrid

Sensitive workloads run under continuous proof they are executing as intended, bringing the assurance once reserved for air-gapped environments to shared and commercial infrastructure.

Edge computing

Forward-deployed and autonomous systems verify their own trusted state locally and enforce policy at the point of operation, with no connection required. If trust cannot be proven, access is restricted, the system reverts to a known-good state, or the workload is isolated.

AI & GPU

Sensitive and classified models run provably protected across the GPU, where the trust chain spans hardware, software, and orchestration. Polaris proves the correct model is in use and unchanged while it runs, applying one trust standard from training through inference.

Agentic workflows

Every agent proves it is running in a genuine, untampered environment before exchanging data, closing off impersonation, interception, and injection.

www.fr0ntierx.com / polaris@fr0ntierx.com / (877) 604-0888

FRØNTIERX