carahsoft

FRØNTIERX

Polaris Technical Brief

The continuous trust model for live compute.

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

The continuous trust model for live compute.

Polaris continuously determines whether live compute remains trusted and makes that state enforceable. Across confidential and conventional computing environments, it appraises the strongest available evidence, including hardware-rooted attestation where supported, against customer-defined policy and issues a current trust verdict. Access to keys, protected data, models, services, and sessions remains conditional on that verdict.

MODEL OVERVIEW

- **Evidence collection.** Layered evidence across platform, accelerator, image, OS, kernel, runtime, configuration, identity, and location where supported.
- **Policy appraisal.** Evidence is appraised against approved baselines and customer-defined policy.
- **Trust verdict.** A current verdict indicating whether the workload and supporting environment remain in policy.
- **Enforcement.** Trust state governs access and response when required conditions change.

CONTINUOUS TRUST LOOP

1. **Establish trusted context.** Identify the workload and environment using the strongest evidence available.
2. **Collect layered evidence.** Gather applicable platform, accelerator, image, OS, kernel, runtime, configuration, identity, and location evidence.
3. **Appraise against policy.** Compare evidence against approved baselines and customer-defined policy and issue a current trust verdict.
4. **Bind verdict to access.** Govern keys, data, models, tools, services, identity, gateways, and sessions.
5. **Re-appraise continuously.** Reevaluate trust throughout execution and change access or response when required conditions change.

In short — Access remains conditional on the current trust state of the compute using it.

LAYERED EVIDENCE MODEL

L1 Platform
Platform identity, configuration, firmware, and infrastructure state; hardware-rooted TEE evidence where supported.

L1-GPU Accelerator
GPU identity, confidential-computing state, attestation, firmware, driver, and runtime measurements.

L2 Image integrity
OS, boot components, workload image, executable artifacts, and approved software baseline.

L3 Runtime state
Evidence from the executing workload and environment, continuously appraised against policy.

L3.1 Kernel integrity
Kernel-integrity signals used to determine whether the environment remains approved.

LOCATION & PLACEMENT

Where supported, Polaris can cryptographically establish where a workload is running and make placement part of trust policy, including approved infrastructure, provider, region, jurisdiction, sovereignty, or residency.

CHANNEL & SESSION BINDING / RA-TLS

Where required, Remote Attested TLS (RA-TLS) can bind runtime evidence to a live client connection, allowing the relying party to verify the compute environment associated with that connection.

DEPLOYMENT SURFACE

Confidential CPU
AMD SEV / SEV-SNP, Intel TDX, and other supported environments.

Confidential GPU
NVIDIA H100, H200, Blackwell, and other supported environments.

Conventional compute
Platform, image, OS, kernel, runtime, identity, configuration, and location evidence.

Portability
Cloud, on-premises, sovereign, hybrid, edge, disconnected, and partner-operated.

Customer control
Customer-defined policy and enforcement; no bulk-data inspection required.

Post-quantum
ML-KEM-768 and ML-DSA where supported.

WHERE POLARIS APPLIES

Sensitive compute increasingly spans infrastructure no single organization fully controls. Polaris provides one trust model across it.

Federal, defense & intelligence / AI & GPU / sovereign & hybrid cloud / critical infrastructure / edge & disconnected / supply chain & partner infrastructure