EVERFOX

TECHNOLOGY BRIEF

Accelerate AI. Secure the Mission.

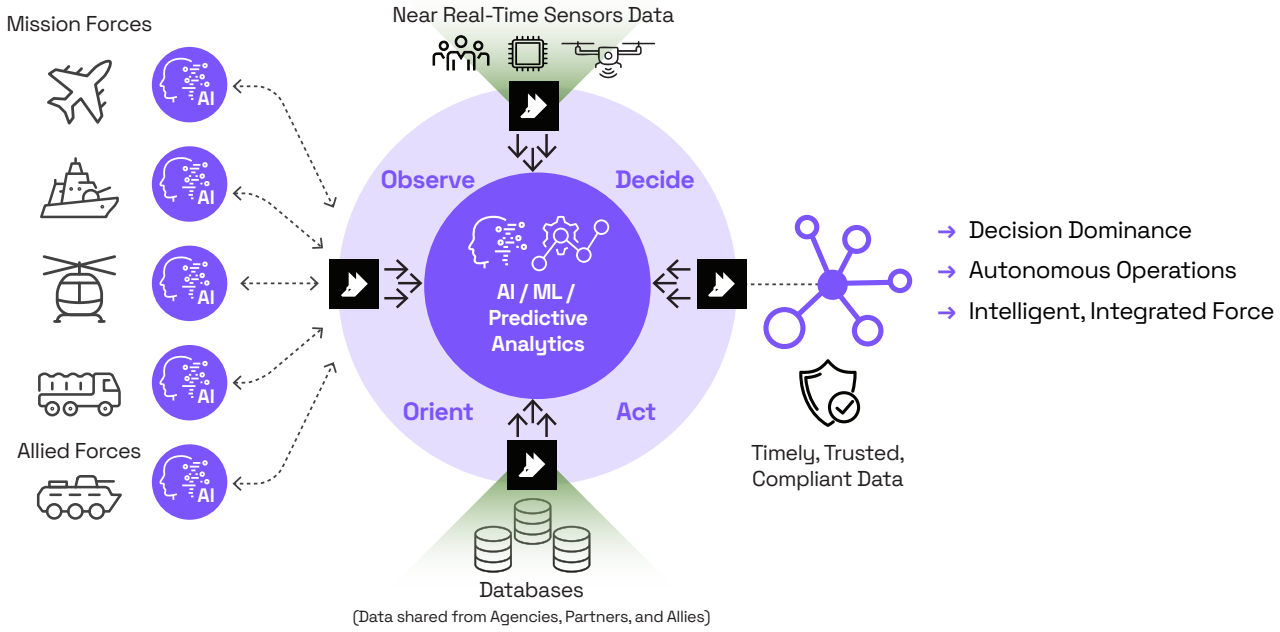
Securing and streamlining the development, management and use of AI systems.

Everfox helps you achieve your artificial intelligence initiatives at mission speed—without sacrificing security and policy control.

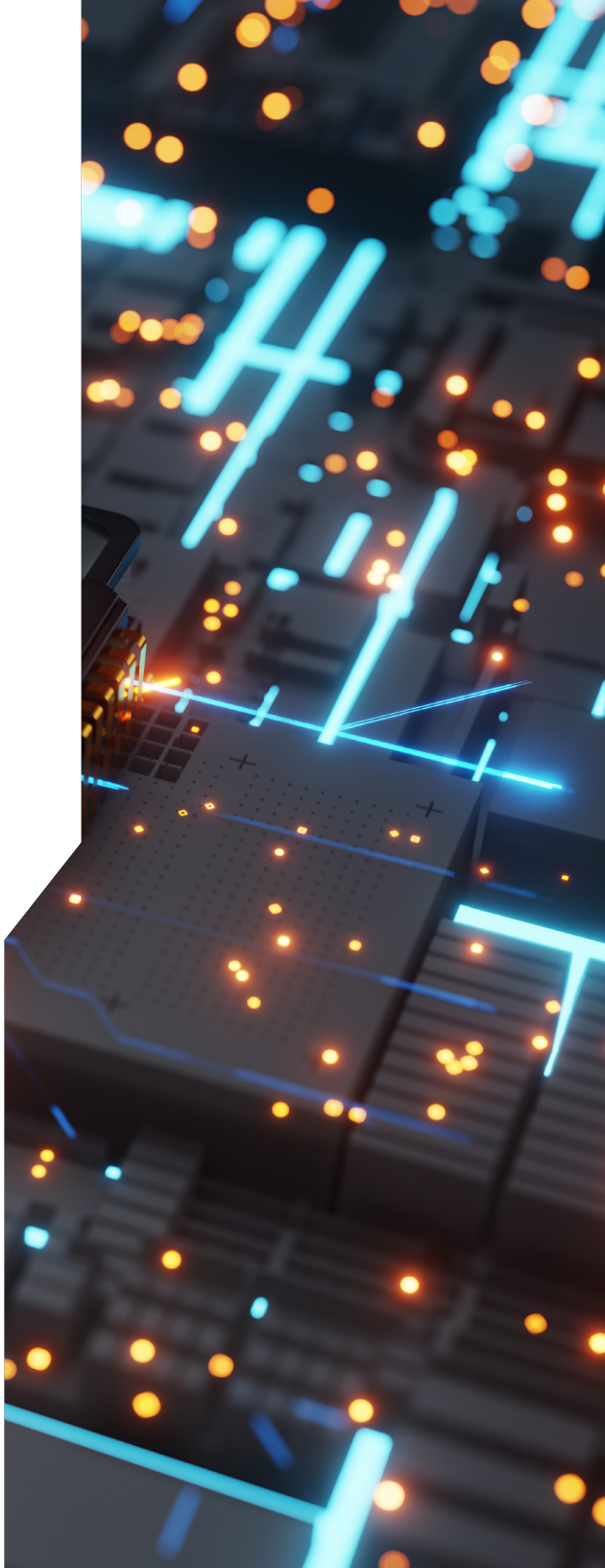
Whether you're training AI models, deploying multi-domain systems requiring near-real-time data feeds, or accelerating analysts' ability to extract insights from multi-source information, Everfox provides the secure data movement and controlled access required to maintain the advantage over our adversaries.

Everfox delivers the following:

- Secure cross domain data transfer for AI pipelines
- Centralize, automated threat removal and some elements of the transformation process
- Protect AI systems from compromised developer and end user machines
- Secure multi-partner sharing across classifications
- Insider risk monitoring to protect AI model integrity



- Decision Dominance
- Autonomous Operations
- Intelligent, Integrated Force



Achieve AI-Powered Interoperability While Preserving Zero Trust Security Posture.

Policy-enforced Data Transfer and Transformation

Everfox can enforce classification and security policies as data is traversing between two disparate networks, each with its own zero trust and data centric security frameworks.

- Removes threats such as scripts, macros, and hidden metadata
- Redacts unauthorized fields and sensitive content based on policy
- Enforces labeling and formatting rules, including file type, size, and metadata constraints
- Standardizes and verifies format and structure before transferring to destination
- Automates policy-driven flows for batch and streaming ingestion
- Maintains audit logs for security, compliance and model provenance

Isolate AI Systems and End Users from Threats

Isolate AI training and deployment environments from developer workstations, preventing the introduction of malware or corrupted data.

- Enforce one-way data flows into AI environments
- Prevent exfiltration, backdoors, or covert tampering
- Maintain integrity of sensitive model architectures and weights

Give personnel on high side networks secure access to AI systems residing on lower classification networks.

- Seamless “browse-down” access with hardware enforced isolation
- Policy-controlled and fully auditable sessions

Provide secure access to AI environments for allied users and coalition partners while preserving data sovereignty and mission confidentiality.

- Remote virtual sessions with keyboard-video-mouse (KVM) isolation
- Role-based access control and session policy enforcement
- Supports Five Eyes, NATO, and other federated access frameworks

Insider Risk Management

Detect insider misuse—whether it’s privileged manipulation by a developer or subtle poisoning attempts by an end user.

- Monitor behavior across all user tiers and AI lifecycle stages
- Detect anomalous access patterns, data corruption attempts, or model degradation
- Linguistic analysis and advanced behavioral analytics help get ahead of threats
- No-code model tuning; easily adapt to new behaviors.
- Scales to 400k+ endpoints
- Full video session playback with annotated timelines.