WHITEPAPER

Unleashing Artificial Intelligence (AI)

Secure, Dynamic and Future-Ready Solutions

EVERFOX

Making AI Work for Federal Missions

Artificial Intelligence is no longer a future concept—it's here, and it's rapidly transforming how federal agencies operate, analyze and respond. Across missions, AI is accelerating insight, automating routine tasks, and uncovering patterns in data too vast for human analysis. But this transformation depends on something more than models or algorithms. It depends on secure, trusted, and timely access to the right data.

A New Model for Data-Driven Decision-Making

For AI to deliver on its promise, agencies must integrate it into systems, built with fundamentally different expectations- about speed, interoperability, and security. That means more than deploying new tools. It requires a shift in how agencies approach risk, operations, and digital modernization.

This integration signifies more than mere automation, it represents a revolutionary shift in governmental foresight and action. By leveraging AI, federal entities are not only enhancing existing processes but transforming their approach to anticipating and preemptively addressing challenges.

Yet with the opportunity comes complexity. Government systems must balance confidentiality with access, secure against emerging cyber threats, and ensure the integrity of the information fueling AI engines. Traditional solutions weren't built with these demands in mind. New capabilities—spanning secure infrastructure, policy-enforcing data flow, content sanitization, and AI-powered threat detection—are essential to make AI work at mission speed.

This whitepaper offers a strategic view of how federal agencies can build secure, dynamic, and future-ready environments for AI. It explores technologies, operational frameworks, and secure principles needed to scale AI with confidence- while protecting what matters most.

Preventative Cybersecurity and User Activity Monitoring

Unfortunately, the power of AI is not limited to benign use cases. The UK's National Cyber Security Centre (NCSC) predicted in 2024 that AI "will almost certainly increase and heighten the impact of cyber attacks over the next two years," and noted that "all types of cyber threat actor – state and non-state, skilled and less skilled – are already using AI." Generative AI in particular has been a boon to attackers, leading to a 1,265% growth in phishing attacks since the fourth quarter of 2022 – phishing attacks with a success rate as good or better than human-generated phishing emails.

Because phishing emails and other web-based attacks can use relatively common zero-day technical vulnerabilities in everyday applications like web browsers, detection-based security such as endpoint detection and response (EDR) may not prove sufficient in preventing attacks. Instead, technologies like Hardsec Remote Browser Isolation (RBI) can isolate code processing on remote systems, providing the user with an interactive video feed of web browsing to practically eliminate the risk of web code-based attacks. Advanced CDR, described above, can be applied as an in-line email solution to rebuild files without malicious code or links.

For the risks that cannot be prevented, AI's integration into everyday operations necessitates a fresh approach to risk management. AI-driven User Activity Monitoring systems can proactively identify and mitigate insider threats through advanced linguistic analysis and machine learning. These systems detect misuse of AI, helping to safeguard human-AI interactions, ultimately safeguarding the organization against internal risks. By identifying threats early, these systems protect government integrity and operational security.

Enabling Multi-Domain AI Intelligence

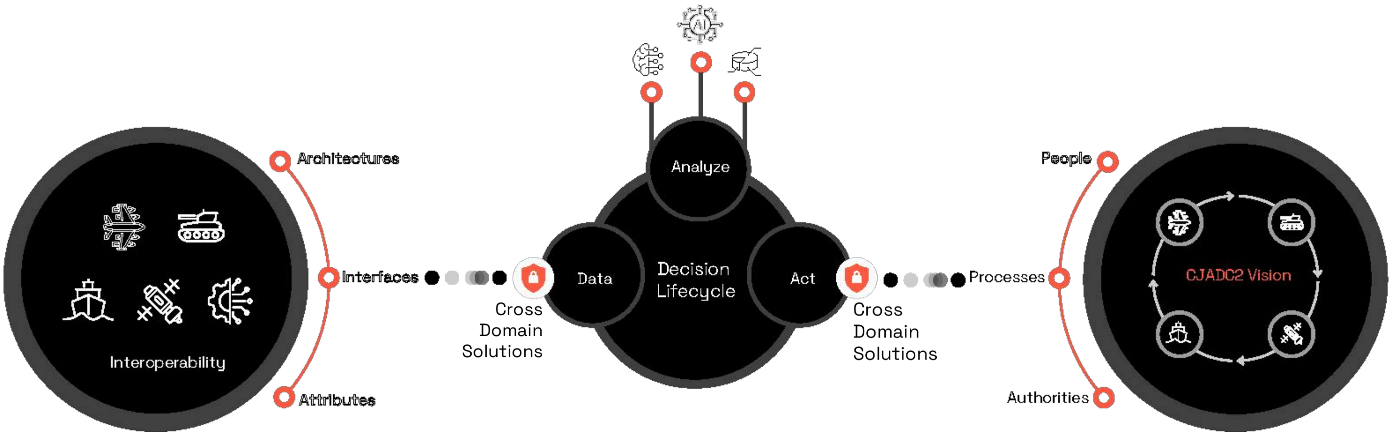
In today's rapidly evolving government AI environments, cross domain security solutions are critical for enabling fast, reliable, and secure data transfer between disparate networks. These solutions are essential for safeguarding sensitive information while facilitating seamless collaboration and analysis across different classification levels.

For instance, AI systems require access to vast amounts of data, including open-source information and data from other classification levels, to make informed decisions. Cross Domain Solutions (CDS) play a vital role in bridging legacy systems with modern AI technologies, helping to facilitate a smooth integration and uninterrupted information flow.

As government agencies increasingly adopt AI to enhance decision-making, the speed and reliability of cross domain access and transfer solutions become paramount. These solutions must not only help provide data integrity and security but also support the rapid consolidation and processing of both classified and unclassified intelligence for AI-driven insights.

Furthermore, they must allow users to run AI queries and models at multiple classification levels, such as Secret, Top Secret, and Unclassified, and compare the results for action. Additionally, non-attributed AI queries of unclassified data can be performed from high-classification levels, providing an extra layer of security.

Figure 1: Cross Domain Solutions Bridge Legacy Systems in Modern AI Environments



Hardening AI Solutions

In an AI-driven environment, security is paramount. Hardware Security ("Hardsec") solutions are designed to fortify AI systems against adversarial threats, hardening data protection and resilience.

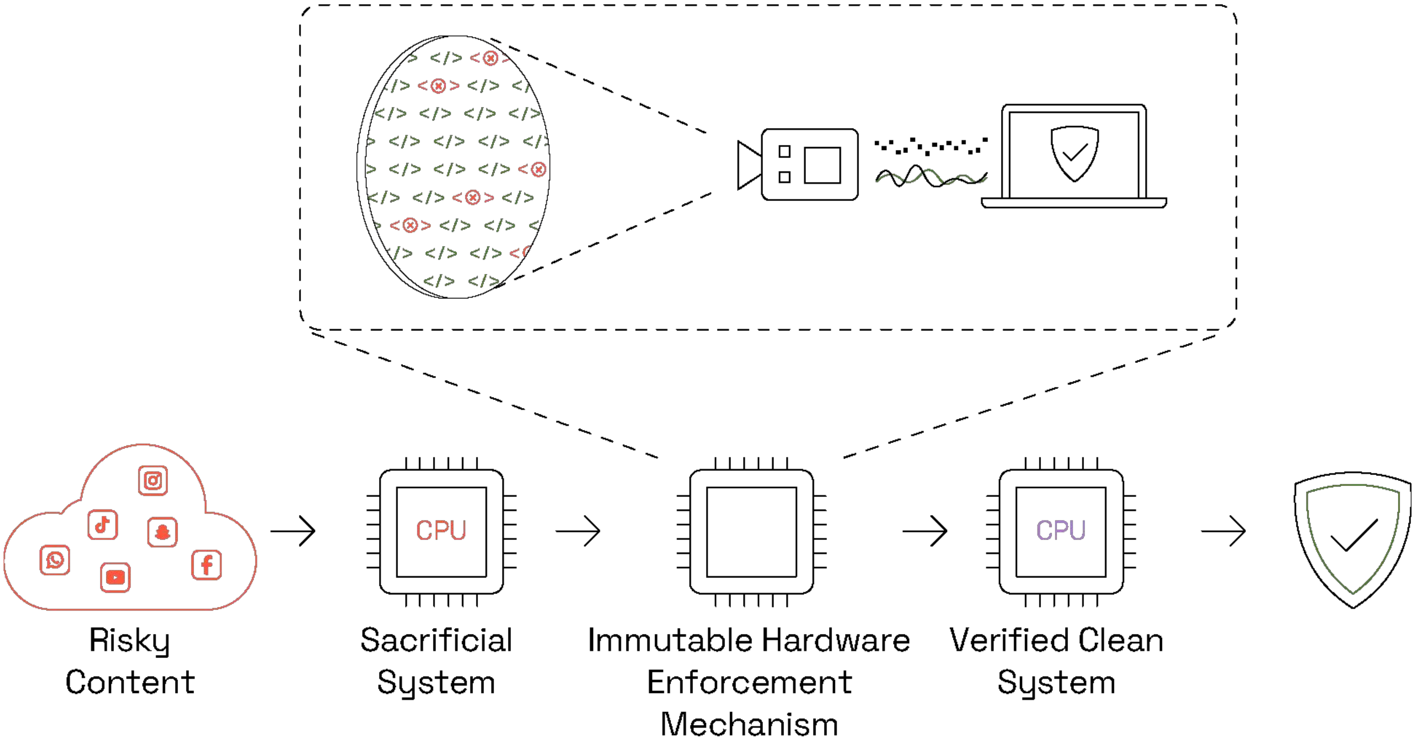
These enhanced security measures protect against data breaches and help facilitate AI deployments to operate safely within government infrastructures, building immunity against potential cyber vulnerabilities. This security foundation is crucial in maintaining the integrity and operational continuity of sensitive data.

To further enhance security, a layered approach that incorporates multiple security measures to create a robust security perimeter is critical. This includes leveraging non-Turing machine logic for security enforcing functions, which allows data to flow through the transfer appliance to be fully validated by the Hardware Security Enforcement Fabric.

Think of it like a movie projector: the source system projects data onto a secure screen, but no unverified data crosses the boundary— just verified safe content like pixels and waveforms. Non-Turing enforcement hardware validates that only the approved formats and signals pass through: no code, no malware, just policy-approved content.

By doing so, AI systems are better protected against evolving cyber threats and can maintain higher levels of security and reliability.

Figure 2: Fortifying AI Systems: Hardsec Measures Against Adversarial Threats



Empowering Clean Data: Content Disarm and Reconstruction

The accuracy and reliability of AI systems are contingent upon the quality of their data. Content Disarm and Reconstruction (CDR) technologies help facilitate data purity by systematically cleansing incoming data streams. This process isolates and neutralizes threats, thereby providing for better data integrity and elevating the quality of AI analytics, which is critical for informed decision-making. Reliable and clean data is essential for maximizing AI's potential to deliver accurate insights across federal operations.

In AI environments where data is shared between classified and unclassified environments, it's critical to assess data for potential threats before sending it up to classified environments, to prevent contamination. Advanced CDR technology can be integrated with Cross Domain Solutions to rebuild data streams and remove threats while preserving essential information. This cleansing helps to provide accurate and reliable data that your AI systems need to make informed decisions.

To facilitate data purity and mitigate novel attacks leveraging AI, implementing CDR technology in conjunction with other security measures, such as hardware-enforced security solutions, will improve security posture. By doing so, you can create a comprehensive security framework that protects your AI systems from cyber threat while protecting the integrity of your data.

Protecting against AI-Accelerated Threats

Unfortunately, the power of AI is not limited to benign uses. The UK's National Cyber Security Centre (NCSC) predicted in 2024 that AI "will almost certainly increase and heighten the impact of cyber attacks over the next two years," and noted that "all types of cyber threat actor – state and non-state, skilled and less skilled – are already using AI." Generative AI in particular has been a boon to attackers, leading to a 1,265% growth in phishing attacks since the fourth quarter of 2022 – phishing attacks with a success rate as good or better than human-generated emails.

In addition, adversaries are using Gen AI to deliver more frequent, timely, and believable phishing attacks. Preemptive threat extraction from both email attachments and the websites linked to in emails is no longer optional— it's foundational. Using preventative technologies like Advanced CDR and Hardsec Remote Browser Isolation supports a Zero Trust approach to web and email by stopping threats before they reach the user.

Because phishing emails and other web-based attacks can use relatively common zero-day technical vulnerabilities in everyday applications like web browsers, detection-based security such as endpoint detection and response (EDR) may not prove sufficient in preventing attacks. Instead, technologies like Hardsec Remote Browser Isolation (RBI) can isolate code processing on remote systems, providing the user with an interactive video feed of web browsing to practically eliminate the risk of web code-based attacks. Advanced CDR, described above, can be applied as an in-line email solution to rebuild files without malicious code or links.

In a 2025 Cyber 360 Report, 71% of IT security directors in government defense and regulated industries recognize the fact that threat detection technology comes too late, as the damage is already done.

Partnering with Everfox as You Embrace AI

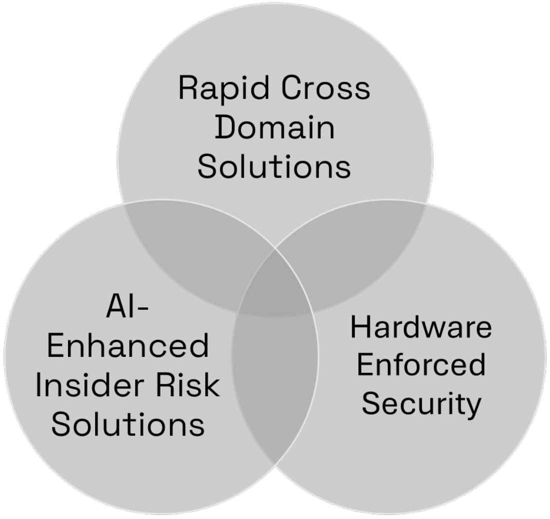
Everfox has defended the world's critical data and networks against complex cyber threats for over 20 years. As a commercial provider of Priority Cybersecurity solutions, Everfox's vast experience allows us to help customers confidently navigate many unique challenges of secure AI adoption.

At Everfox, we do more than provide point solutions — we empower federal agencies to evolve, innovate, and excel in today's dynamic environment. Whether securing multi-domain data flows or enabling AI across diverse mission sets, Everfox technologies are designed to increase security while also driving meaningful gains in efficiency, capability and operational productivity.

We aim to be a leading partner in the federal AI revolution, fueling innovation by facilitating trusted access of the right data to the right person at the right time.

Today, we help our customers through:

Figure 3: Everfox AI Solutions


Rapid Cross Domain Solutions
AI-Enhanced Insider Risk Solutions
Hardware Enforced Security

AI-Enhanced Insider Risk Solutions

In a world where new threats are frequently powered by AI, robust insider risk programs will act as a crucial line of defense, proactively identifying and mitigating internal vulnerabilities before they evolve into significant security breaches.

The Everfox Evershield solution is a comprehensive insider risk management platform designed to detect and mitigate potential threats from within an organization by monitoring user activity, identifying suspicious behaviors, and providing tools to investigate and respond to potential insider threats.

Our solution gives analysts and investigators the right tools needed to collect, explore, and gain insight into risky behavior. These capabilities are part of a broader framework: Everfox solutions are designed to improve your organization's security posture and readiness models with anomaly detection, risk adaptive protection, investigation workflow management, program improvement tracking and reporting.

As the threat landscape continues to evolve, our AI-enhanced technology empowers agencies to proactively manage insider threats with precision, enabling secure and productive environments. We leverage machine learning linguistic analysis to detect potential risks before they materialize, safeguarding organizational integrity.

Rapid Cross Domain Solutions

Everfox Raise-the-Bar compliant cross domain solutions are specifically designed to meet the unique challenges of government AI environments, providing secure and efficient data transfer between disparate networks. Our innovative access solutions allow operators to leverage AI capabilities across multiple classification levels from a single device with multiple monitors— eliminating the need for physically separated workstations and KVMs. With Everfox CDS technology, users can securely access different classification levels through isolated, policy-enforced sessions- simplifying workflows and enhancing decision-making without compromising security.

Key features of Everfox Cross Domain Solutions include:

- **Secure Information Flow**: Our technology facilitates controlled and sanitized data transfers, maintaining the integrity and confidentiality of information.

- **Compliance with Regulations**: Adherence to stringent standards such as those set by National Institute of Standards and Technology (NIST) to meet the highest levels of security and reliability.

- **Efficient and Fast Data Exchange**: Everfox solutions optimize data transfer processes, allowing seamless collaboration between enterprise and battlefield environments while meeting tactical requirements. Our solutions also facilitate non-attributed AI queries on unclassified data from high classification levels, enabling secure and efficient information sharing.

Our cross domain solutions can be augmented with Everfox hardware-based security measures, including diodes, to facilitate secure connectivity and data sanitization when transferring information from high-risk networks like the internet into classified environments.

By supporting the rapid consolidation and processing of intelligence, enabling bidirectional transfer of AI data and models, and facilitating high-speed decision-making, Everfox solutions are essential as government agencies adopt AI technologies. Our systems empower intelligent policies, more effective resource allocation, and improved operational efficiency, ultimately driving mission success in complex and asymmetric data environments.

Hardware Enforced Security

AI solutions require unwavering protection. As the cyber threat landscape continues to evolve, global governments, critical infrastructure organizations and regulated industries must reinforce their approach to cybersecurity. The NIST and other major cybersecurity entities recognize the benefits of a hardsec approach to security. Everfox Garrison Hardsec solutions leverage non-Turing machine logic for security enforcing functions by ensuring all data flowing through the transfer appliance is validated by the Hardware Security Enforcement Fabric. Everfox data diodes allow you to meet stringent regulatory requirements for hardware-based data separation and one-way data flow while maintaining strict control over data integrity and flow.

By implementing a Hardsec approach to security, you can create an additional barrier against cyber threats, helping to maintain security of sensitive data against evolving adversarial tactics. This fortified layer of security acts as a first line of defense, protecting AI systems from data breaches and other cyber vulnerabilities.

Specifically, our hardware-based solutions provide the following benefits:

- **Enhanced security**: Our hardsec solutions provide an additional layer of protection against cyber threats, helping to maintain security of sensitive data.

- **Regulatory compliance**: Our data diodes help users meet stringent regulatory requirements for hardware-based data separation and one-way data flow.

- **Data Integrity**: Our solutions help to provide control over data integrity and flow, to prevent data breaches and other cyber vulnerabilities.

- **Risk-mitigated access**: Our hardsec remote browser isolation, available in on premises and cloud delivery models, allows users to access the public internet without fear of AI-accelerated attacks on the browser and other web-centric applications.

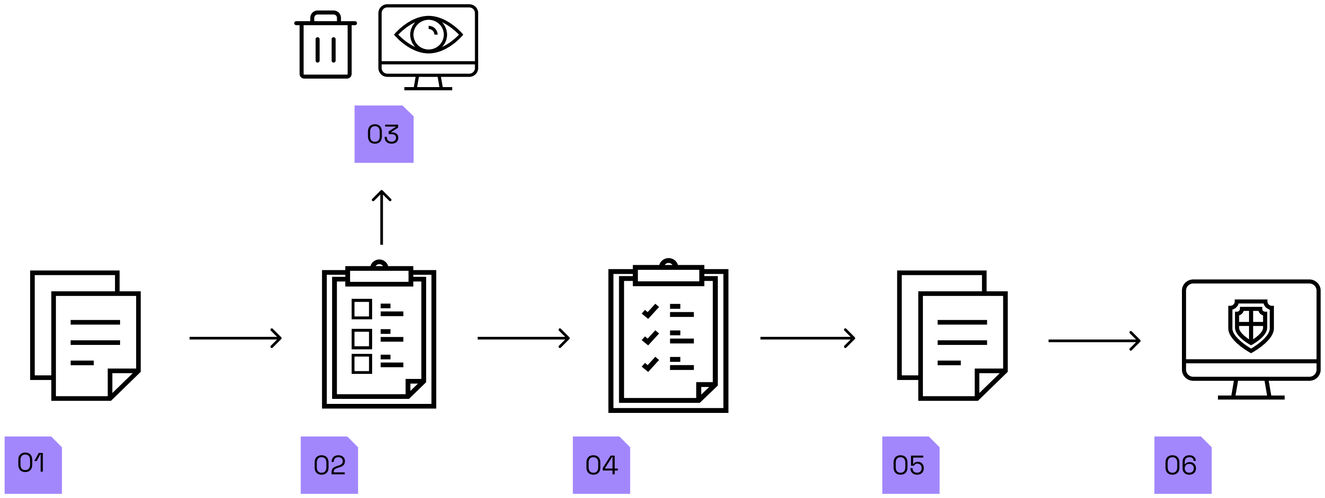
By combining these benefits, you can create a security solution designed to protect your AI systems from cyber threats while preserving the integrity of your data.

Everfox CDR

In AI environments, it is crucial to verify data before transmitting it to classified environments, as malicious content could compromise the integrity of both the data and the mission. Everfox CDR technology is designed to cleanse incoming data streams, rebuilding essential content into a verified safe file and leaving embedded threats behind, helping AI models operate on clean data.

By removing threats, rather than relying solely on detection-based approaches, Everfox CDR increases the efficiency of security operations centers (SOCs). Fewer alerts mean less analyst fatigue, faster triage, and improvements in prevention efficacy, especially against sophisticated, AI-accelerated threats. CDR can also be deployed as an in-line email filter to defend against phishing attacks that leverage generative AI techniques. To further assure the security of CDR-cleansed content, Everfox's hardsec technology can be used to verify the transformation.

Figure 4: Everfox CDR



01

File Received
A document, image, email or other supported file type is received.

02

Analysis & Recipe Creation
Everfox CDR examines the file's legitimate content and creates a set of instructions (a recipe) for creating a new file with the same content but without including any of the original data.

03

Original File Discarded
The original file is either discarded or stored securely, complete with any malware, in your forensic suite for later analysis.

04

Recipe Verification
The generated recipe is verified to confirm it is complete, consistent and not carrying anything extra.

05

File Reconstruction
The recipe is followed to create a new, clean file, equivalent to the original legitimate content, but not necessarily the same bytes.

06

Secure Delivery
The newly built functional file is delivered to the user in near real-time.

Pioneering AI Integration in Government

At Everfox, we do more than provide solutions—we empower federal agencies to evolve, innovate, and excel in today's dynamic environment. Everfox solutions allow our government customers to not only increase security, but to realize efficiencies in the areas of cost, capabilities, and productivity – by doing more with less.

Connect with our team today to explore how our technologies can guide your organization through the complexities of AI integration, helping to secure the dynamic, future-ready transformations that AI promises to deliver.

Learn more at everfox.com

About Everfox

Everfox, formerly Forcepoint Federal, has been a trailblazer in defense-grade cybersecurity for more than two decades. Leading the way in delivering innovative, high-assurance solutions. But we're just getting started.

Learn More

www.everfox.com