Leidos + HP: Delivering Trusted AI to Government

When it comes to solving the U.S. government's most challenging missions using Artificial Intelligence, it's critical to design and deliver Trusted AI solutions that provide comprehensive security and resilience. That's why Leidos partners with another giant in the tech space, HP, to deliver Trusted AI solutions to our government customers through HP's secured hardware supply chain. Today's cyber adversaries are capable of attacking every aspect of a system, from social engineering (password and phishing attempts aimed at users) to adversarial AI to supply chain attacks aimed at hardware components. Our partnership with HP means you not only benefit from the rigorous security protocols that impact everything we do at Leidos—including our sophisticated defenses against adversarial AI, but also the trusted supply chain that HP has so thoroughly tested and implemented into their hardware delivery.

While security is our priority and always will be, innovation and progress always drive how we help government meet and exceed its mission. HP shares this philosophy and is recognized in the space as a leader that always seems to find itself a step ahead of the competition. Our relationship with HP means Leidos engineers and HP experts are in close contact and collaboration and pass on this shared expertise to our government customers.

The power of Leidos Trusted AI and the sophisticated secure supply chain at HP, we help you identify both subtle and complex patterns in data, extract valuable information, and deliver critical insights while protecting systems and data from being compromised.

OUR APPROACH

The Leidos approach to delivering Trusted AI to government stakeholders is greatly elevated by our close relationship with HP. As a household name both in government and commercial IT circles, HP enjoys a sterling reputation as an innovator and industry leader. But the strength of our relationship goes beyond the respect and trust HP has earned over the years. There are identifiable and traceable processes and technologies that make HP an ideal partner for Leidos in delivering Trusted AI solutions. Perhaps most importantly is the sophisticated supply chain HP employs that places trusted components into trusted systems. We're proud to work beside HP who has truly done the work to build a fully trusted supply chain. As an HP reseller, when we sell an HP-built workstation to the U.S. government combined with Leidos system integrations, every component in the workstation is fully traceable to trusted sources.

Of course trusted hardware is only part of the story. Through our Trusted AI approach and our Leidos SecDevOps process, we are develop and deliver secure AI solutions that are integrated into secure software that operates over secure data. This end-to-end approach—with security paramount at every level of hardware and software—allows us to set a new standard for cybersecurity for our U.S. government customers.

OUR CAPABILITIES

By leveraging HP's secure supply chain combined with Leidos Trusted AI software, we're able to ensure full-spectrum security. From the bare metal hardware where the technology is housed to the software stack on the machine, and everything in between—HP workstations and Leidos systems integrations provide a seamless, end-to-end security solution for the U.S. Government.

As malevolent cyber actors evolve and increase in sophistication, it's important for AI/ML integrators to understand that these attacks target every part of the system including the supply chain, including the hardware, the software and of course the user him/herself. In fact, one of the most recent catastrophic cyberattacks on the U.S., SolarWinds, was not a lucky phishing effort. But an attack on a government IT supply chain. This new reality is why we believe it is critical to work with a hardware provider who approaches its security philosophy with the same seriousness and sense of responsibility that we do.

leidos

Leidos Trusted AI Features	Benefits
Integrated adversarial AI defense	Detects when adversaries are attacking Leidos Trusted AI using spoofing or data poisoning attacks, continuing to operate effectively while notifying system owners.
Resilient AI	Automatically detects AI algorithms are operating outside normal bounds, allowing humans to intervene or continuing to operate in safe modes.
Adaptive AI	Reduces the time and cost to update models as the world changes.
Explainable AI	Provides human-understandable interfaces that increase trust and allow humans to treat AI as a partner.
Contextual control	Allows humans to adjust the level of automation or assistance provided by AI as the situation changes.
Delivers in-depth analysis of unstructured data and identify security risks earlier.	Increases tech stack security as security flaws are identified and fixed before they become an issue.
Combines previously isolated and unused data to identify areas for improvement.	Improves innovation levels for organizations, providing opportunities to enhance processes, products, services, and more.
Provides full visibility into automated algorithms.	Fosters trust between humans and computers, as AI/ML solutions depend on both to work effectively.

A NEW INTEGRATION

In April of 2021, HP announced a new integration with Anaconda, one of the world's most popular data science platforms. A true foundation for machine learning, Anaconda pioneered the use Python—a high-level, open-source programming language—and is a champion in Python's vibrant community. Because of our close collaboration with HP in delivering AI/ML capability, we're able to pass along this new integration to our customers and offer pre-bundled software packages and configurations available in a secure and managed environment, making data scientists' jobs much easier.

These preloaded software stacks inside HP workstations along with Leidos system integrations means the guesswork and time spent configuring your environment are things of the past.

WHY PARTNER WITH LEIDOS?

In combining our expertise in delivering data-rich solutions and experience designing and building AI/ML systems with HP's first-in-class hardware, we're able to offer a trusted solution from every angle—360°.

Our commitment to innovation and philosophy of progress is shared at HP and we make the case for this claim nearly every day. As AI/ML solutions become more commonly understood and implemented in both the private sector, it's important to keep in mind that security cannot be taken for granted. Even the most sensitive government data can potentially be at risk if a vendor has not taken every precaution. We believe our disciplined, science-based approach to AI/ML and HP's shared commitment to full-scope security makes your organization competitive today and secure into the future.

NEXT STEP

At Leidos, we pride ourselves on creating solutions to technically challenging problems of global importance. When deployed correctly, AI/ML has the power to do incredible things. For reliable, resilient, and secure AI/ML solutions, contact us today.

FOR MORE INFORMATION

leidos.com/ai | ai@leidos.com

leidos