Red River

ACCELERATE MISSION READINESS AND SUCCESS WITH AUTOMATION

Rapid deployment, consistent results and scalability — as much as these are important for modern commercial enterprises, they can mean the difference between mission success or failure for Department of Defense service members.

The DoD has committed itself to modernization across the force. This modernization encompasses IT systems to support warfighter needs. As with any change, there are challenges that military organizations face when seeking to transform their enterprise systems. Automation is able to simultaneously address the need for modernization while providing the ability to scale that modernization across the enterprise at a pace previously unattainable. However, there are still challenges for military organizations seeking to transform, modernize and automate their infrastructure.

The ability to leverage key technology partners and bring expert-level architecture and integrations capabilities makes the automation space one that only a small number of companies are able to successfully tackle, especially when you are working with the DoD. Even fewer truly understand the needs of the DoD compared to a private enterprise.

OVERVIEW OF INFRASTRUCTURE AUTOMATION

Infrastructure automation encompasses a wide breadth of solutions designed to streamline the deployment, patching, maintenance and life-cycle management of mission-critical HW/SW, applications and services. Some of the industry leading technologies in this space include RedHat (Ansible), HashiCorp (Terraform and Vault) and Gitlab Enterprise.

These suites bolster existing DoD technology by automating, streamlining and improving efficiency. Tactical solutions must be fast and flawless. The less friction there is during setup and initial rollout — the easier a system is to operate and maintain — the more successful a mission will be.

To accomplish these goals, the DoD has the opportunity to leverage these and other enterprise tools as well as expert partners and specialists — engineers, architects and consultants who can create best-in-class, responsive, automated systems.

INFRASTRUCTURE AUTOMATION FOR MILITARY AND DOD APPLICATIONS

Developing for the DoD conveys unique challenges:

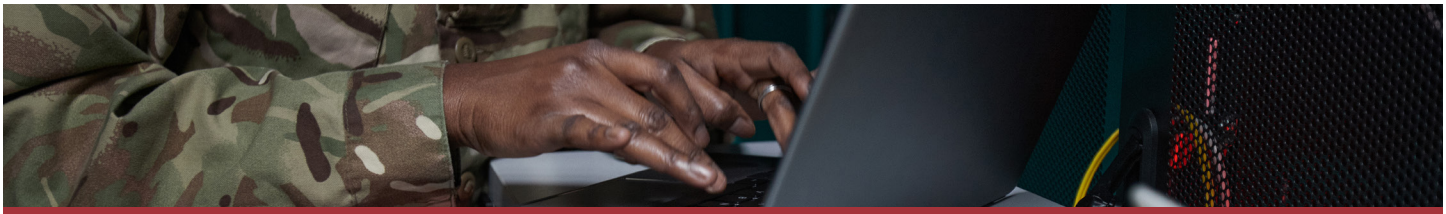
- Systems must be deployable quickly.
- Security baselines need to be consistent and dependable.
- Systems must have scalability and flexibility to meet mission needs.
- Tech must be intuitive and easy to use.

Soldiers are constantly asked to do more with less and do it rapidly, many times in high-stress situations. While they may be experts in a particular field, IT may or may not be their MOS and have not received extensive technology training. They may not be tech experts — they may not have thorough training in technology at all. In response to this, systems must be user-friendly. It must yield thorough, reliable and accurate results, reducing or eliminating the potential for human error.

Platforms that provide automated zero-day security that extend to endpoint devices such as tablets, radios, laptops and others give the ability to reach to the tactical edge.

In manufacturing, automation can improve efficiency by up to 30%. McKinsey estimates that 60% of occupations across the globe consist of 30% automatable activities.

But automation doesn't just reduce workload and increase efficiency: It can save lives. Automation does not get fatigued and does not make mistakes.



THE CRITICAL IMPORTANCE OF INFRASTRUCTURE AUTOMATION

The Department of Defense is in a unique position. It requires technology that is both fast and secure. An extremely powerful tool to help meet its mission-critical goals is through automation. Automation helps reduce risk, increase system reliability, enhance user experience and improve overall security posture. Automation also helps accelerate IT projects — projects which may frequently be time-sensitive.

- **Reduce risk:** Automation reduces the risk of human error, providing long-term stability and consistent results. Even well-trained users may make mistakes, especially in tense or urgent situations.

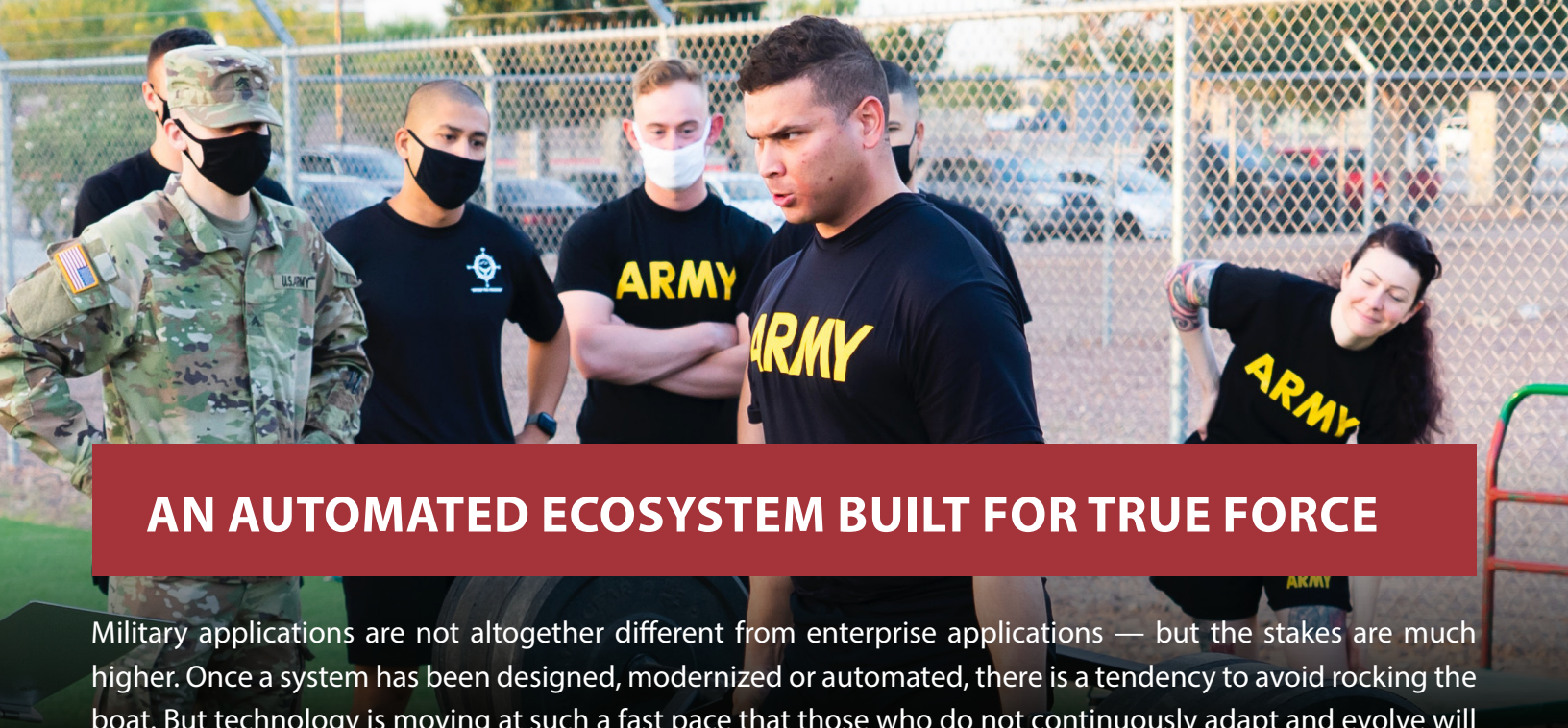
- **Increase reliability:** Automated systems are more reliable than manual ones, as they eliminate potential points of failure. An automated system can quickly check itself (or hundreds or even thousands of devices) with a speed that a human cannot match.

- **Enhance user experience:** Automating mundane processes makes life easier for users and allows them to focus on their mission-critical tasks. No one in a dangerous environment wants to determine whether their radio has been compromised by a zero-day exploit, even if they really have to.

- **Improve security posture:** Automation can strengthen security by automating patching, vulnerability scans and other security checks. Automation can also reinforce security standards by locking down devices and permissions.

- **Increase agility:** Finally, automation allows the DoD to leverage its existing IT investments and better manage system complexity during rapid technological change. Automation helps ensure that technology is running optimally and efficiently — allowing military forces to stay ahead of the curve both now and into the future.

Infrastructure automation is critical for DoD operations. To meet its objectives, the DoD should consider working with professional solutions providers that understand not only what works but why it works — and how they can tailor their solutions to optimize the performance of their systems. There are many effective platforms and businesses in the nation that together provide a wide variety of tools. But more essential than knowing these tools is knowing how to choose the right ones.



AN AUTOMATED ECOSYSTEM BUILT FOR TRUE FORCE

Military applications are not altogether different from enterprise applications — but the stakes are much higher. Once a system has been designed, modernized or automated, there is a tendency to avoid rocking the boat. But technology is moving at such a fast pace that those who do not continuously adapt and evolve will be left behind.

We talked to one US army customer who had automation under control — they were using Ansible. We said to them, "That's great. But have you thought about these three other areas where you could expand your modernization strategy?"

After extensive collaboration with the end-user customer, we had a complete proof-of-concept and a plan going forward that would apply automation across their Enterprise Architecture. By engaging in these collaborative sessions, we were able to identify valuable aspects of automation that had previously not been considered. This obviously created a superior plan for the customer, which better addressed their mission requirements.

Automation technology has moved at such an incredible pace that the opportunities to advance the efficiency of the entire enterprise are almost constantly increasing. Consultants who specialize in state-of-the-art technologies and are knowledgeable regarding the needs (and constraints) of the DoD are necessary to reveal and implement ideal infrastructure solutions.

Because it's not just about the technologies involved. It's about being able to integrate them into a truly plug-and-play system — about creating a system that is built, from the ground up, in the service of the organization.

> *"We cannot afford a leveling of technology advantage. It is imperative for the department to nurture early research in emerging technologies to prevent technological surprise. We must leverage critical state-of-the-art commercial technology where rapid advancements are trying to accelerate our military capabilities."*
>
> *- Under Secretary of Defense for Research and Engineering of the United States*

OEM AUTOMATION TECHNOLOGIES

Enterprise automation technologies provide a wide range of services for the military. These services can include HW/infrastructure, software deployment and security hardening, patch management and lifecycle management. By automating these processes, the DoD can reduce risk and improve system reliability while still providing an intuitive user experience.

RED HAT: ANSIBLE AND STIGIAN

Ansible is an automation platform that supports the entire system lifecycle, from development to deployment. It can automate everything from the initial setup of new machines to ongoing maintenance tasks such as application updates — tasks that a soldier may not have the time (or expertise) to complete.

Another tool used to deploy software and systems quickly is Stigian. Stigian is a secure configuration management tool that simplifies the system setup process. It allows administrators to deploy security hardening based on different standards in a matter of minutes, ensuring that every machine complies with the exact baseline security requirements. When in the field, Stigian makes it easier for large volumes of technology to be deployed quickly.

Together, RedHat Ansible and Stigian ensure that standards of security, safety and reliability are met, even in the harshest environments.

HASHICORP: TERRAFORM, VAULT AND CONSOLE

Terraform is an open-source infrastructure-as-code solution from HashiCorp that allows developers to define, deploy and manage cloud infrastructure. It can be used to define a system's extent of operations — including security protocols, networking requirements, resource allocation and more.

Terraform eliminates the need for manual configuration in the field and can help reduce the time it takes to set up a system from months to days or even hours. This is an especially crucial advantage for the DoD, where time-to-deployment may mean the difference between mission success and failure.

HashiCorp also provides HashiCorp Vault, a tool that provides authentication and password management services — at volume, without a significant amount of human interaction. Another service offering is HashiCorp Console, which provides application automation services. Together, these systems make it easier for DoD solutions to be managed on the fly.

GITLAB ENTERPRISE

Enterprises can't work without Git. Neither can the Department of Defense. GitLab Enterprise provides critical code management tooling to ensure that the systems that are operable by the DoD stay that way.

GitLab provides a platform that allows code to be managed, monitored and shared easily. It is designed for teams to use, so it's easy to collaborate on projects in the field — even when access to other systems may be limited. This makes it easier for developers and administrators to share information quickly and safely with one another. And if an issue occurs, all the changes can simply be rolled back.

ENTERPRISE SOLUTIONS VS. THE DEPARTMENT OF DEFENSE

A company can work with the exact enterprise solutions that the Department of Defense works with — but still not truly understand how these automation solutions must be applied to the DoD infrastructure. There are a few major differences between deploying for enterprise and deploying for the DoD.

- **Regulations:** First and foremost, the DoD must deploy following stringent regulations based on government security requirements, such as NIST. These standards ensure the safety of any solution deployed by the Department of Defense.

- **Requirements:** There is a need for speed when deploying to this environment — DoD solutions frequently have vastly different requirements than enterprise solutions. If a network goes down within an organization, emails may not be sent. If a network goes down within hostile territory, connectivity with soldiers could be lost.

- **Reliability:** Any DoD solution must remain accurate and reliable long-term, as well as be able to scale up or down following changing mission needs. This requires a robust automation platform that is also extremely flexible.

Thus, while the same solutions may be used in a private or public enterprise, how they are applied is frequently quite different.

GAIN AGILITY WHILE GAINING GROUND WITH RED RIVER

"I have never seen OEMs work so cohesively together toward the benefit of our goal as you've done with RedHat and HashiCorp in our environment."

Any company can work with one of these suites. And that company may become an expert in that suite's offerings — they may know that suite inside and out. But what happens if that solution isn't the best?

At Red River, we have a deep understanding of the DoD's needs — and a deep understanding of the technologies available. Many organizations focus on a single utility; they are a RedHat, Ansible or GitLab shop. We understand that different tasks may require different tools. Our thorough knowledge of all these suites lets us always determine the best solutions for any organization, public or private.

There will always be unique concerns in military and DoD contracting. Frequently, failure simply isn't an option. So, while the solutions being used are solutions frequently used in enterprises, they have to be curated and integrated differently. They have to be bomb-proof.

We can bring the right tools to the right place. At Red River, integrate OEMs to create a complete, well-automated system that meets the needs of the military and the DoD — providing the speed, ease of use and reliability that such an organization needs. Rather than supporting a single system or collection of systems, we expertly connect the best possible tools. And we do it all while keeping the mission in mind.

Find out more about what makes Red River the best in DoD IT. Ask us about traditional infrastructure automation, tactical deployments and the work we've done with the US Army.

ABOUT RED RIVER

Red River brings together the ideal combination of talent, partners and products to disrupt the status quo in technology and drive success for business and government in ways previously unattainable. Red River serves organizations well beyond traditional technology integration, bringing 25 years of experience and mission-critical expertise in security, networking, analytics, collaboration, mobility and cloud solutions. To learn more, visit redriver.com.