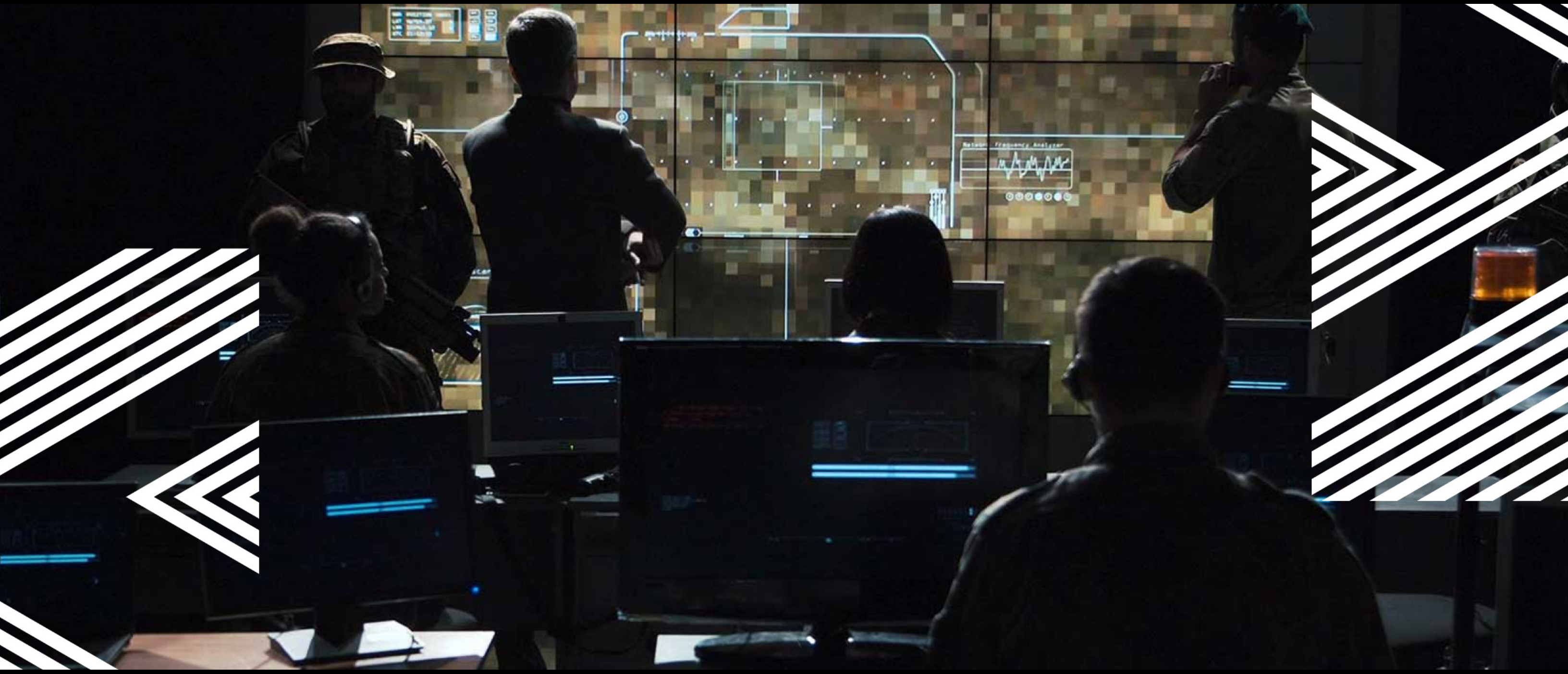
HashiCorp



ManTech | CUSTOMER CASE STUDY

Defending those who defend us

Leading GovCon IT services provider uses HashiCorp to harden defenses and accelerate delivery of critical applications for federal agencies and the military.

About ManTech

In business for more than half a century, ManTech provides advanced mission-focused technology solutions and services for every branch of the federal government: intelligence, federal civilian, and defense agencies. Based in Herndon, VA, the company helps agencies solve their toughest homeland and national security challenges — cost-efficiently, at speed, and where their customers are — land, sea, air, space, cyberspace, and everywhere in-between.

Supporting 9,800 + personnel world wide

Accelerated service delivery from 3 months to 3 weeks

Reduced security risk by decreased human touchpoints

Pursuing level 2 Cybersecurity Maturity Model Certification (CMMC)

240 Development Enclaves across all major CSP's

Eliminated 400 work hours per year

> "Along with policy-driven infrastructure through Terraform, Vault automatically rotates credentials instead of forcing users to store information locally and risk inadvertent exposure. Add in Boundary for standardizing language and protocols for accessing infrastructure and services across our environment, and it creates an end-to-end security posture in line with our zero trust charter."
>
> BENJAMIN LARA
> AUTOMATION ENGINEER, MANTECH

Advancing national and agency security with zero trust

Modern military operations are more advanced and sophisticated than ever. While high-ranking defense officials strategize how best to neutralize threats to national security from abroad, the respective branches under their command must deal with unprecedented challenges in their everyday cyber, data collection and analytics, enterprise IT, and software engineering operations.

For more than 50 years, ManTech has provided advanced mission-focused technology solutions — from cybersecurity and secure mission IT to advanced analytics and missions operations — and services for federal intelligence, federal civilian, and defense agencies. But protecting the systems and information the military needs to protect the nation demands advanced tools and protocols.

"We played a key role in the DoD's Zero Trust Reference Architecture and helping federal agencies implement the President's Cybersecurity Executive Order," says Robert Lara, Technical Director of Cybersecurity Programs for ManTech. "Secrets management is a huge part of an effective zero trust environment and doing it manually just isn't effective for doing it at scale."

Modernized security posture to protect high-value targets

Things change quickly in the defense space, meaning they have to move quickly in tech, too. ManTech saw a lot of core infrastructure changes in the market — the systems in use and how users' access impacted security postures — due to natural evolution and from outside influences like the war in Ukraine as well as a sharp rise in nation-state cyber warfare.

"Given our focus on DoD and Intelligence agencies, the types of information we deal with are among the most sensitive and high-value around, but our previous processes for securing access were built around manually managing certificates and copying and pasting keys from one system to another," Lara says. "With just a small central DevOps team manually managing secrets and these processes, we felt like we would be unnecessarily inviting risk continuing this way as our team and business expanded."

Lara and his colleagues, including Automation Engineer Benjamin Lara, wanted to both improve the company's — and by extension, its clients' — security posture while also modernizing its core operations to align with rapidly changing market demands.

That was especially important as ManTech began building out its microservices app, which had to integrate with many systems that each had to authenticate via a unique ID that was manually managed in Kubernetes and required an operator to continuously update tokens. And, as a DevOps-first organization, ManTech needed a DevOps-friendly approach for identity-driven privileged access to machines that could both create credentials while avoiding exposing secrets.

After a thorough search for a secrets management solution, ManTech adopted HashiCorp Vault, alongside HashiCorp Boundary, because of the cloud-agnostic solutions' unique and expansive automation capabilities. Unlike other solutions that require extensive manual copy/paste inputs and depend on security information and event management (SIEM) tools for log visibility, HashiCorp solutions tackle each operation without manual intervention.

With Vault, developers follow a dedicated path for securely deploying both infrastructure and content. Using security as code accelerates end users gaining access to the resources they need all within the confines of a security audit apparatus.

Automated database credential rotation significantly mitigates the cyber threat from stolen keys by automatically creating, rotating, and revoking database credentials through an automated workflow and API. At the same time, Boundary's automated access management uses granular, logical roles and services to enable access to applications and critical systems without the need to manage credentials or expose the network.

"Ultimately, we wanted security baked right into all of our processes from the very beginning for simplicity and enhanced protection," Benjamin Lara says. "Along with policy-driven infrastructure through Terraform, Vault automatically rotates credentials instead of forcing users to store information locally and risk inadvertent exposure. Add in Boundary for standardizing language and protocols for accessing infrastructure and services across our environment, and it creates an end-to-end security posture in line with our zero trust charter."

Challenges

Replacing manual processes for credential cycling, key management, and coordinating access to various cloud-based services and destinations

Enabling zero trust architecture across the organization for greater security

Automating key security and operational processes to improve efficiency and cost management

> “Now, we orchestrate identification and authentication in Vault and operate under a global policy, which has helped us slash our production cycles from several months to just two or three weeks.”
>
> BENJAMIN LARA
> AUTOMATION ENGINEER, MANTECH

Seamless multi-cloud security orchestration drives competitiveness and control

Both Laras say that the combination of HashiCorp Terraform and Vault has been a powerful catalyst for ManTech’s continued growth and for reimagining its security posture. With Vault, ManTech can minimize friction among backend processes and tools to make the entire development lifecycle simpler, smoother, and safer.

In particular, ManTech’s infrastructure and automation group replaced separate manual processes for creating databases, VPN tunnels, and provisioning infrastructure with seamless and secure automated workflows. It also meant they no longer had to rely on one person for key management and could automate dynamic, on-demand credential rotation in the Active Directory, or that users no longer had to copy and paste data from one place to another, significantly reducing potential disruptions, risk to the company’s reputation, and the likelihood of security incidents occurring.

Meanwhile, swapping time-consuming (and occasionally error-prone) processes with airtight automatic ones freed teams to work faster and without violating zero trust principles — all while also replacing the equivalent of approximately 20 full-time employee hours per team, per password rotation period (every 90 days) across the Enterprise Infrastructure Support group. Equating to a staggering 400 hours saved over the course of a year.

“As engineers, we have to operate seamlessly within our multi-cloud, hybrid IT environment. Before Vault and Terraform, we had to coordinate with a number of teams to coordinate access to maintain our security standards, which could take months and delay product releases or updates,” Benjamin Lara explains. “Now, we orchestrate identification and authentication in Vault and operate under a global policy, which has helped us slash our production cycles from several months to just two or three weeks.”

The success of Vault’s initial implementation has Robert and Benjamin dreaming of the future. “Now that we’ve proven out the tools and processes for team-based credentials management and its impact on security and productivity, we’re having many conversations internally about how we spread this mentality and model to the rest of the organization,” Robert says. “It’s an exciting time.”

Outcomes

Eliminated equivalent of 400 full-time employee hours per year by automating credential cycling and key management

Accelerated security set up and service delivery from several months to 2-3 weeks

Reduced the number of human touchpoints and interventions to lower the risk of security incidents or other reputation-harming occurrences

Solution

ManTech uses HashiCorp Terraform, Vault, and Boundary to securely and automatically provision essential digital infrastructure, manage essential keys and secrets, apply granular role-based access, and accelerate service and product delivery within a zero trust environment.

ManTech Partner

Robert Lara
Technical Director for Cybersecurity Programs, ManTech

Robert Lara is the Technical Director for Cybersecurity Programs at ManTech. He serves as the lead for mission and enterprise IT talent management, roadmap development, and solution delivery and integration for multiple IT capabilities across DHS and federal civilian agencies. Prior to joining ManTech, Robert held several technical services and automation leadership roles. He holds a bachelor's degree from Southern Illinois University and a master's degree in cybersecurity management from Purdue University – Global.

Benjamin Lara
Automation Engineer, ManTech

Benjamin Lara currently serves as an automation engineer at ManTech, where he plays a pivotal role in defining and executing critical organizational strategies for workflow automation, continuous integration and continuous delivery (CI/CD), API development, and DevOps. He joined ManTech in 2019 after receiving a bachelor's degree in Cloud Computing and Solutions from Purdue University — Global.

Technology Stack

- **Infrastructure:** Multi/Hybrid Cloud (AWS, Azure, GCP, OCI, VMware)
- **Workload type:** Containers, VMs, Microservices
- **Container runtime:** Containerd
- **Orchestrator:** Kubernetes
- **CI/CD:** GitLab CI/CD
- **Version control:** GitLab
- **Provisioning:** HashiCorp Terraform
- **Security management:** HashiCorp Vault

HashiCorp

www.hashicorp.com