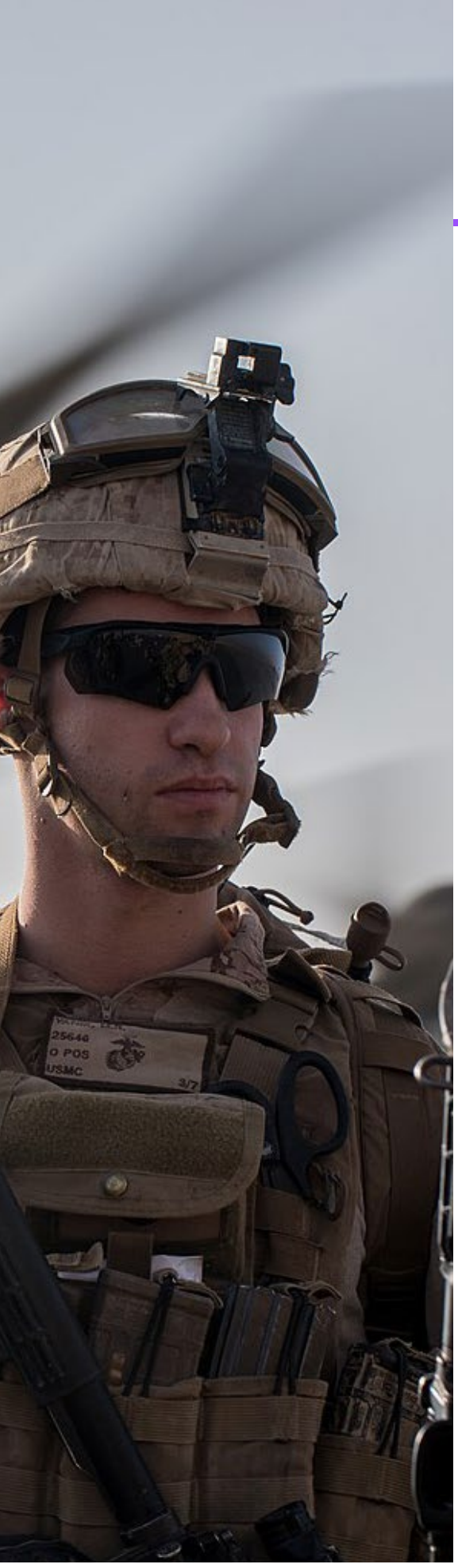
software AG
GOVERNMENT SOLUTIONS

API-Led Hybrid Integration is Key to Successful Implementation of DoD Data Strategy

Table of Contents

1

INTRODUCTION



Introduction

When the U.S. Department of Defense (DoD) announced its new data strategy in September 2020, much of what the department is aiming to do sounded familiar to people with experience in private sector information technology.

The DoD plans to transform into a data-centric organization and use data to help the department fulfill a number of missions, from better preparedness and improved outcomes on the battlefield to more efficient operation and procurement.

To help accomplish these goals, the DoD recognizes the importance of being able to locate, access, and make available data at speed and scale. This is a significant challenge because the DoD is the largest agency in the U.S. government and certainly one of the most complex organizations in all of the world. With 1.3 million active-duty troops across its branches, 750,000 civilian employees, and 811,000 National Guard and reserve troops, the DoD is the largest employer in the nation.

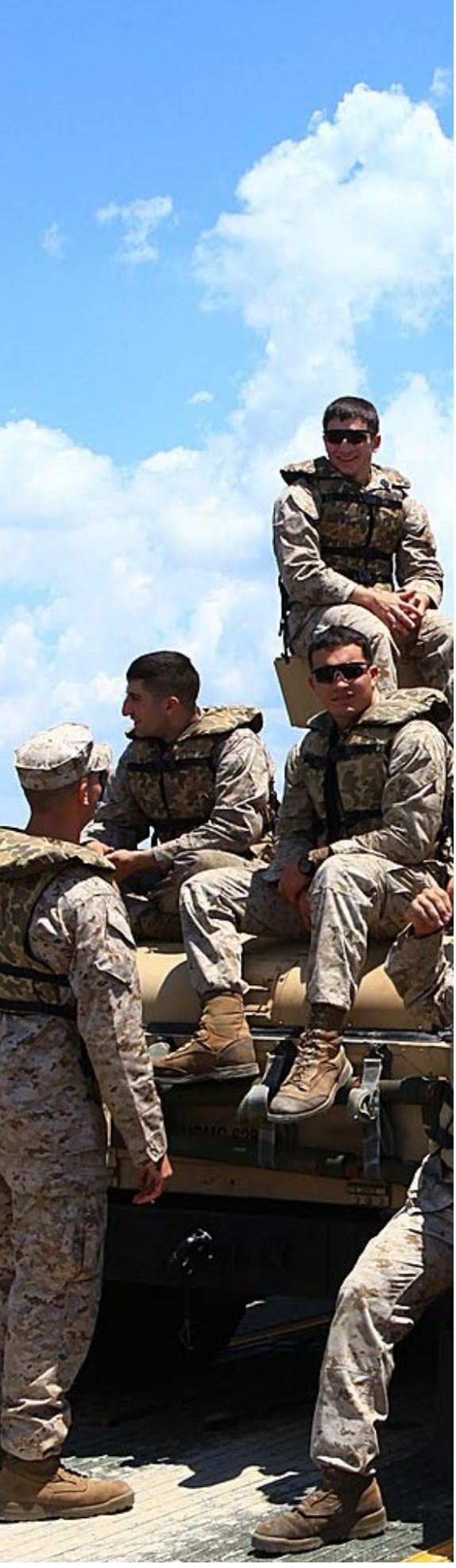
The DoD's strategy outlines guiding principles, which include data governance, stewardship, ethics, collection, compliance, and data for artificial intelligence training. It also lists four essential capabilities: Architecture, Standards, Governance, and Talent and Culture.

There are seven goals outlined in the DoD Data Strategy. If adopted correctly, the DoD strategy will make data:

1. Visible: Allowing data consumers to locate the data they need.

2. Accessible: Meaning consumers of data can retrieve the data they need.

3. Understandable: So data consumers can recognize the content, context, and applicability.



4. Linked: Enabling data consumers to exploit data elements through innate relationships.

5. Trustworthy: Meaning data consumers can be confident in all aspects of data for decision-making.

6. Interoperable: Which means data consumers have a common representation/comprehension of data.

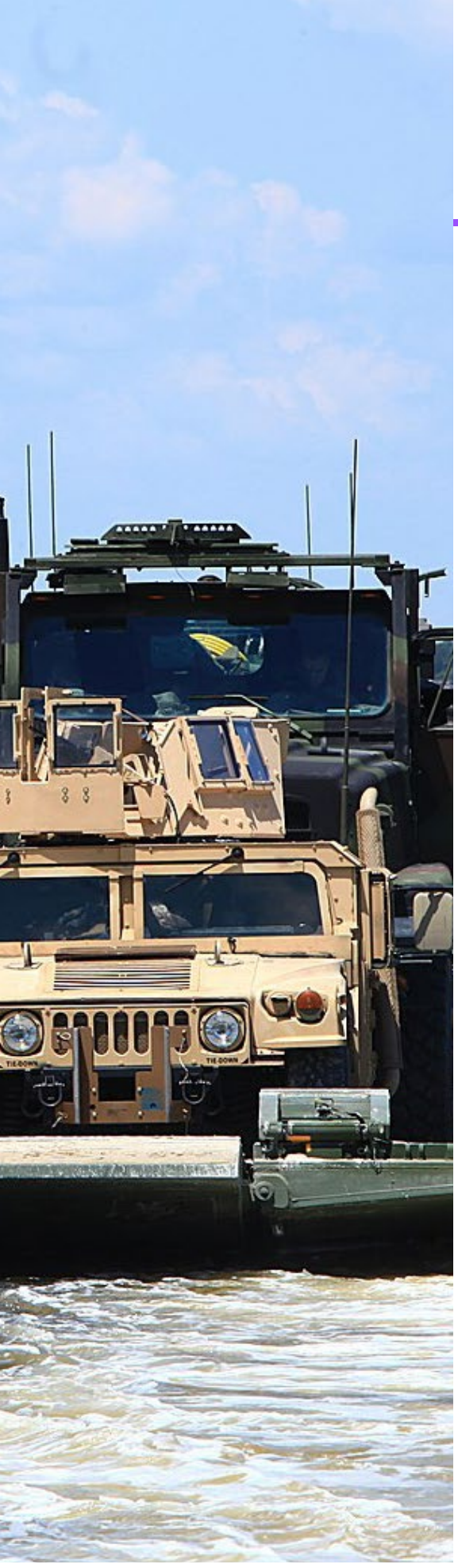
7. Secure: Protecting data from unauthorized use/ manipulation.

Like many digital transformation projects in the private sector, the DoD cannot rip and replace systems and build from the ground up to support its data strategy. Legacy systems are commonplace in the department, and when they say they are "mission-critical," they are exactly that – supporting missions and activities that protect service members and civilians alike.

This paper explores four technical challenges facing the DoD data strategy: Accessibility, discoverability, security, and scalability. These challenges are not insurmountable, but they need to be met while working within the capabilities of legacy systems that were not designed for the type of interoperability and connectivity required to meet the goals of the new data strategy. The size of the DoD, the breadth of its ecosystem of partners and contractors, and the criticality of its missions add additional layers of complexity to the challenge of data integration and security.

2

DATA ACCESSIBILITY



Data Accessibility

Data accessibility is the ability to retrieve data from the systems where it is stored. It's more than accessing data and saving it elsewhere or viewing it. To achieve its goal of becoming a data-centric organization, the DoD needs to empower data consumers to access data and use it in other platforms and combine it with data from various sources to be analyzed and interpreted. Today, this might mean putting the data into an analytics tool or using it to create artificial intelligence or machine learning models.

The problem organizations face when it comes to data accessibility is that data is never a one-size-fits-all proposition. In an organization the size of the DoD, the volume of data and the many forms it takes can be truly staggering. Large organizations like the DoD are dealing with data that is structured (e.g., data stored in a relational database), unstructured (e.g., data stored in productivity tools like spreadsheets and documents, as well as sensor data from mission environments), stored within on-premise applications, stored in legacy systems like mainframes, or stored in a cloud-based application (i.e., SaaS).

In many of these instances, the data is stored in an application or environment where its accessibility was not a concern at the time it was designed. Mainframes, for example, were designed for stability and very high hardware utilization rates but not to connect with cloud-based applications to share data.

New applications present another accessibility challenge. Thanks to cloud-based applications and services, no-code/low-code programming platforms, and the DoD's commitment to Continuous Integration / Continuous Delivery software development practices, it's never been easier or faster to deploy new applications. These applications come online quickly, and they rapidly scale to generate new data sources and repositories. Like every

organization, the future of data and IT at the DoD is not static, so any strategy around accessibility requires the ability to quickly accommodate new data sources.

Any solution to the data accessibility challenge needs to focus on more than basic interoperability. Complex IT environments have data that is stored in different formats and in different types of databases. Raw data moved from one application to another only solves part of the problem. To become accessible, that data needs to be translated, transposed, and contextualized. Accessing quality data requires that the data be understood and cleaned up, not just imported into a new application.

Consider the personnel records at the DoD, which is the nation's largest employer. Now think about the different ways names can be entered, even into a structured database: last name first; first name first; middle initial optional; middle initial required; and unique identifiers like Social Security numbers or serial numbers for enlisted personnel. A data store of this size will certainly include duplicate data, such as the names of people who have served in multiple branches of the armed forces.. Accessing all of that data from various systems and trying to create a single format presents a potentially monumental task. What's needed is an intelligent approach to accessibility that can be put in place quickly without a lot of manual coding.

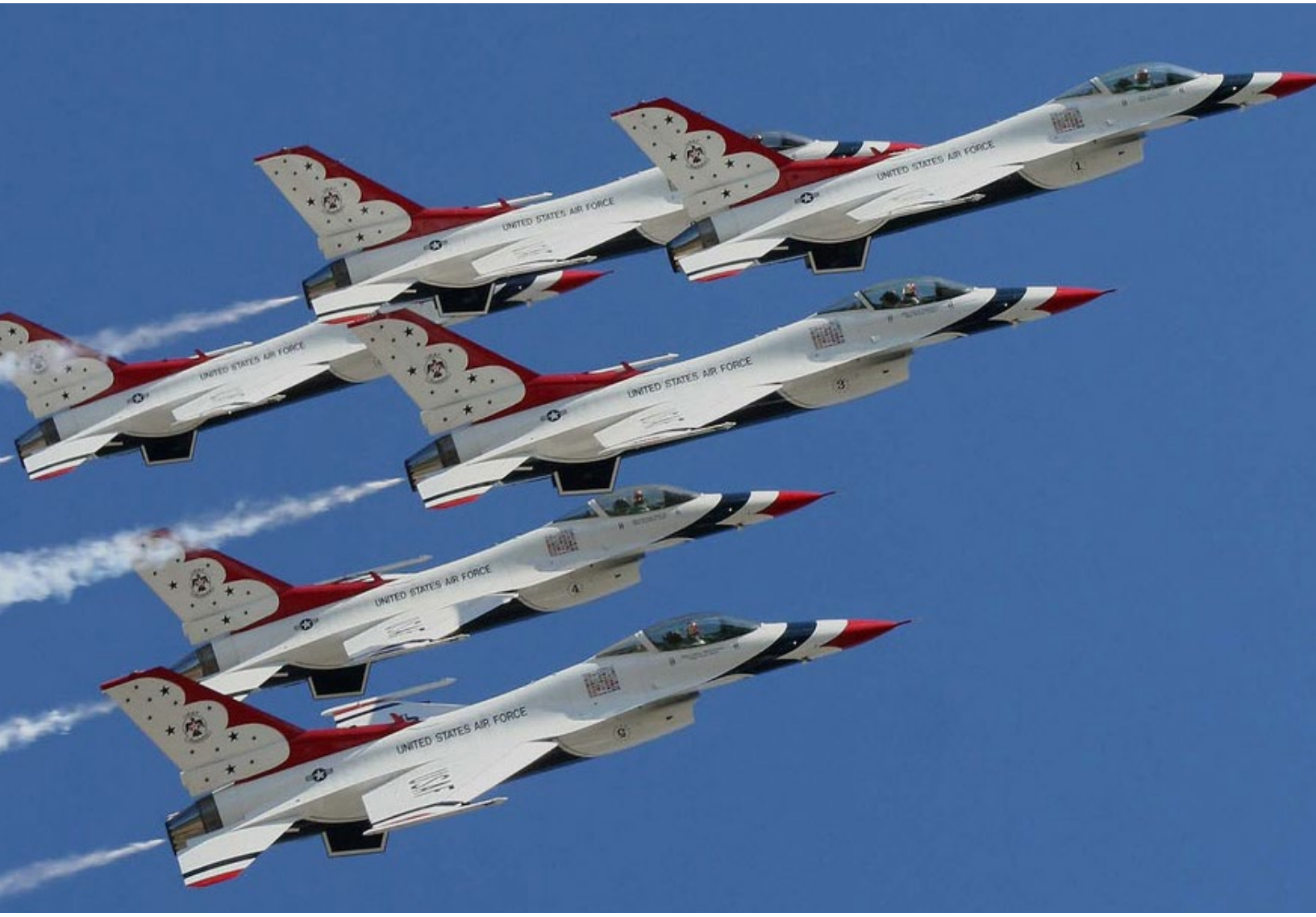
Relying solely on teams of developers to solve data accessibility issues is not practical. There is often intense competition for application development resources, making projects both lengthy and costly.

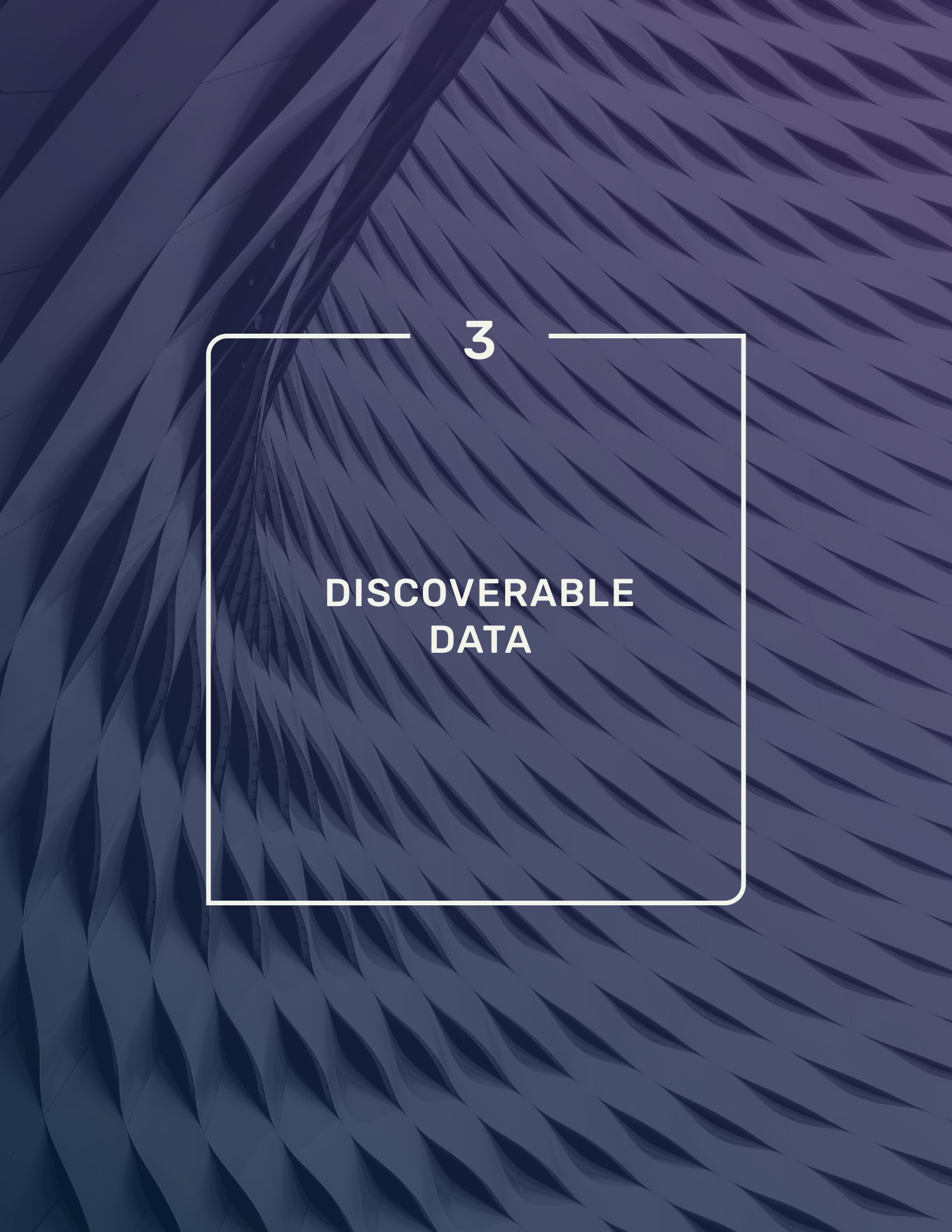
A better approach to data accessibility is to employ a platform designed for data integration that makes use of no-code/low-code environments. Rather than creating a lengthy queue for application development resources, no-code/low-code environments help democratize data integration and accessibility by empowering business process owners.

Deploying a platform with out-of-the-box connectors for the most common applications and platforms and the ability to graphically map and transform data can also help

overcome accessibility challenges. Finally, exposing the data locked in various applications and silos as APIs will make it truly accessible to users and applications in the shortest amount of time, as users can leverage re-usable APIs rather than writing one-off integrations.

APIs are a great leap forward for addressing data accessibility challenges, but taken alone, the creation of APIs can give rise to almost as many problems as they solve for IT organizations. As we'll see in the coming sections, properly managing and securing APIs will improve accessibility while meeting the governance requirements of the overall DoD data strategy.





3

DISCOVERABLE DATA

Discoverable Data

Improving data accessibility opens up the data in an organization to data consumers and applications. But in an organization the size of the Department of Defense, understanding the types of data that exist, how they can be used, and who can use them can be a significant challenge.

Consider how critical it is to the DoD's mission to track supplies and equipment: What the agency has, where it's stored, how it can be transported, etc. Making data easily discoverable serves a similar function. Making fast, accurate decisions based on data requires an understanding of what data is available to consumers. If data consumers are aware of what's available, they won't waste time and resources trying to find data or creating a data source to access information that already exists.

Achieving a return on the investment in data accessibility requires data discoverability. APIs need to be exposed and published in order to break down data silos and provide value.

Returning to the analogy of military materiel, supplies in a warehouse aren't very valuable when no one knows where they are. At the same time, soldiers cannot simply show up at a warehouse and request any piece of equipment. There need to be policies in place to authorize who can access supplies and ensure the equipment is current and in working order. The same goes for data.

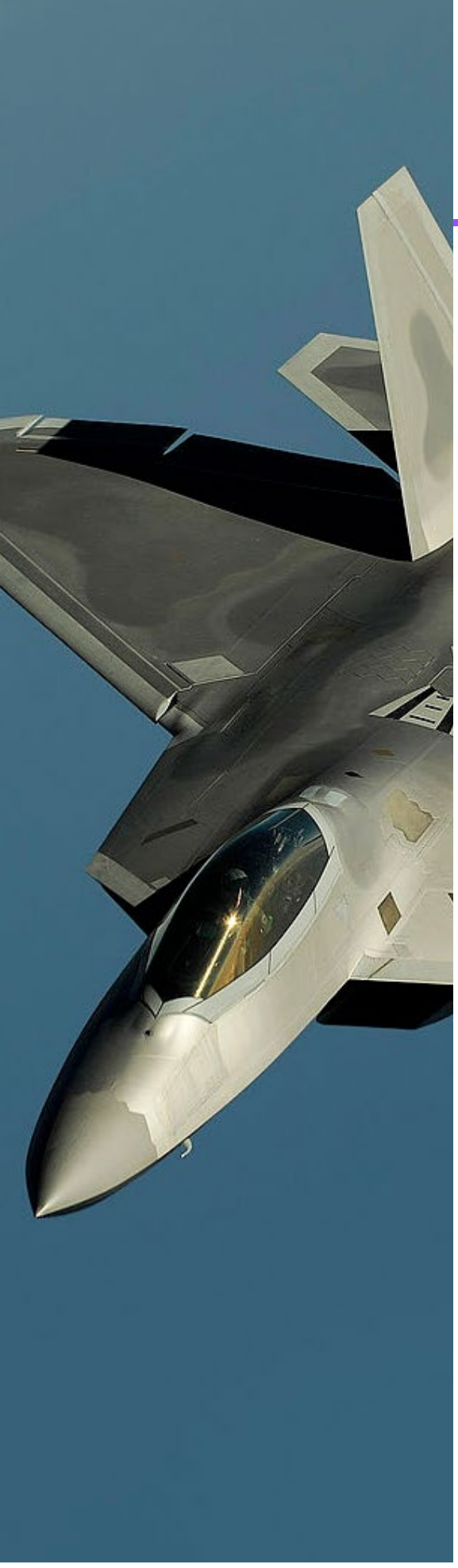
Cataloging APIs helps with data discovery, but the catalog cannot be static because data is not static. APIs have a lifecycle, from inception to retirement, and they need to be managed and updated along the way. APIs need to be monitored to understand who is using them and how, which is useful information for planning around new API creation, API retirement, and more.

Finally, APIs need policies that govern who or what can access them and how the data can be used. This is especially critical in an organization like the DoD, where sensitive information is commonplace and the sheer amount of data creates challenges around managing and monitoring APIs.

Security is paramount to everything that happens at the DoD, where sensitive information ranges from military intelligence to personnel files.

4

DATA SECURITY



Data Security

The goal of data accessibility is to unlock data from silos and legacy applications and put it to use. It's an important step in any organization that wants to become more data-centric. Exposing and publishing the data as APIs helps data consumers understand the data available to them and how they can use it in their own applications. Openness is critical to both accessibility and discoverability.

Data security seeks to impose limits on that openness out of necessity. An agency of the size and scope of the Department of Defense generates a great deal of data, and some of that data needs to be restricted to authorized users.

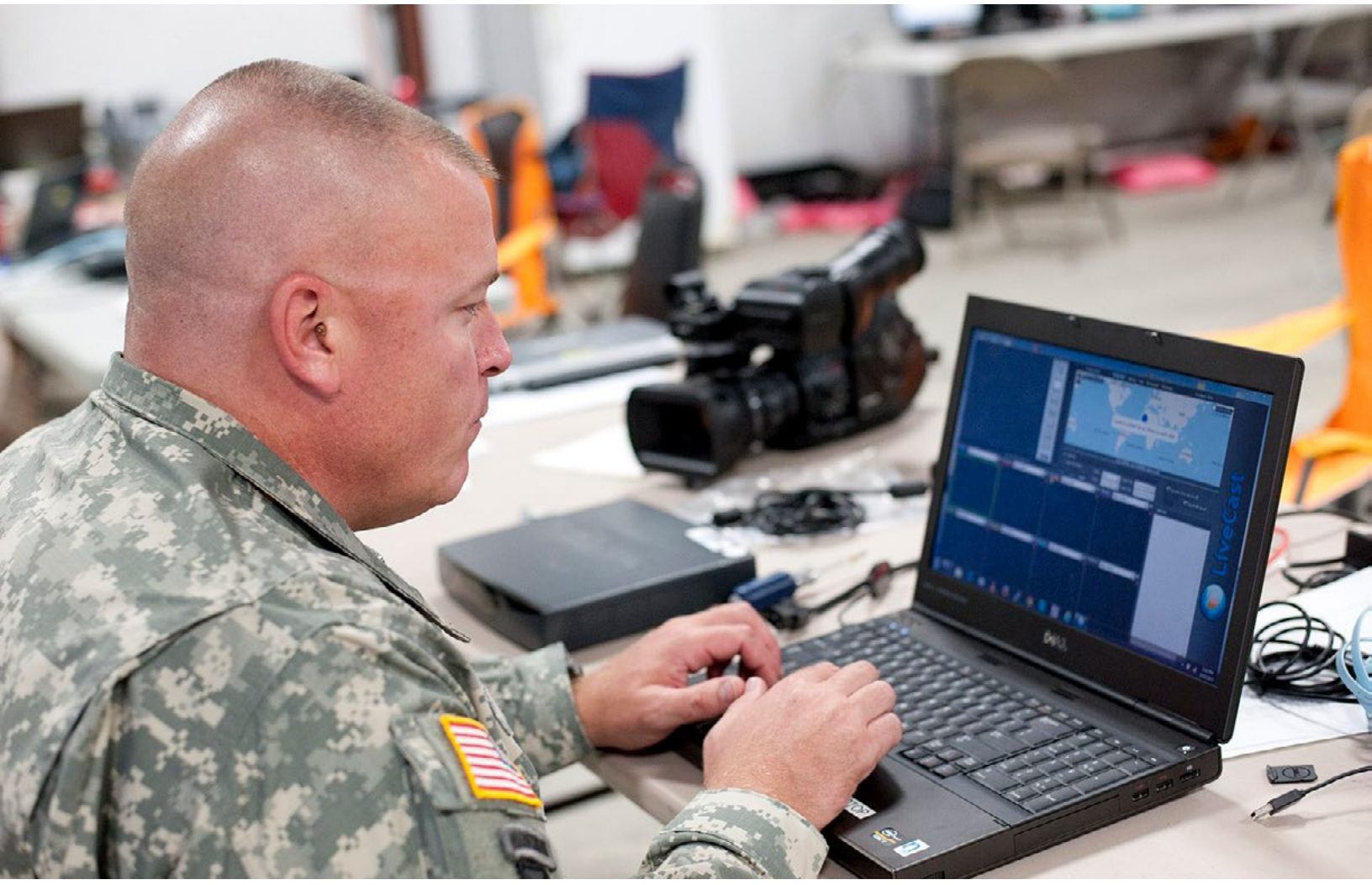
The data security challenge at the DoD is twofold. First, who can access the data available via the APIs? The size of the DoD and the number of contractors and partners make issues of access more complicated than in many private sector enterprises. Second, how is access to data controlled? Data consumers in both military and civilian roles in the DoD see their responsibilities and clearances change as they move among jobs, ranks, and commands. Governing access needs to be a relatively easy task to meet the DoD data strategy's mandate for speed and scale.

A policy-driven approach to APIs will help restrict access as needed. This is part of the aforementioned API lifecycle and management. Another popular data security strategy that can be applied to APIs is zero trust, which treats every user and application as a threat until proven otherwise. Because of the granularity of access required in an organization like the DoD, policies like zero trust need to govern not just "north-south" traffic, but also "east-west" traffic to control access to data.

API monitoring will help track access to and usage of APIs. API gateways function as the secure access point to data, rather than communicating directly with the data

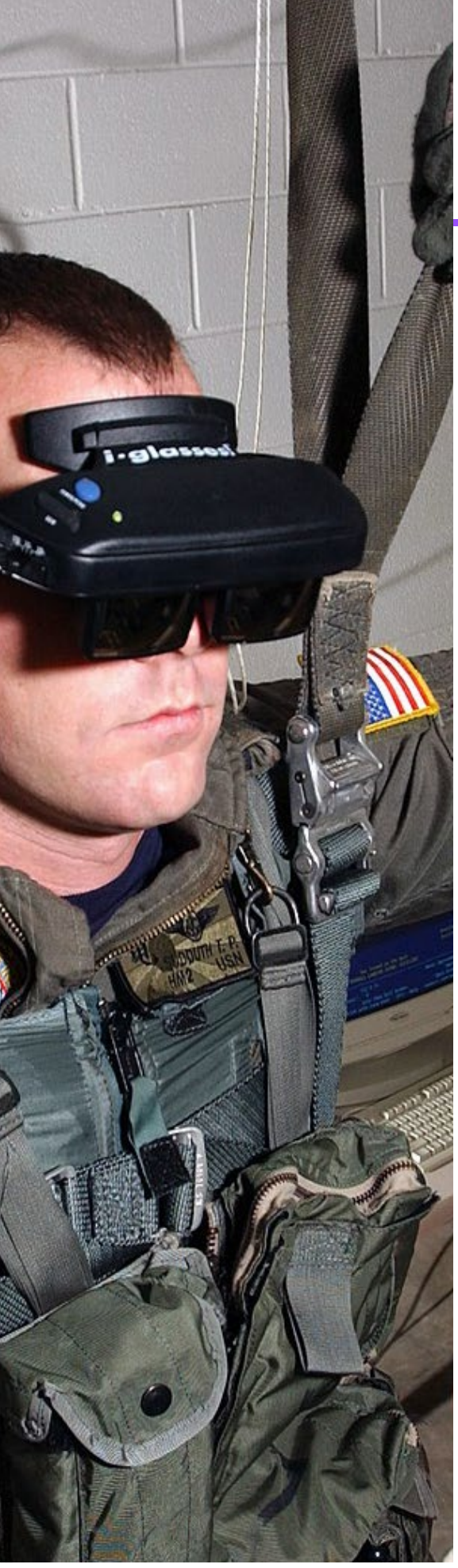
source. They protect data and applications by securing access to APIs and applying runtime governance. Microgateways, which have a smaller footprint, perform a similar function in distributed environments. They can be used to manage API access and prevent the main gateway from being overloaded. Microgateways can help manage, minimize, and secure the east-west traffic in distributed environments.

With data exposed, discoverable, and secured via APIs, DoD data consumers will be able to find and use data which they have the privileges to access. But putting data integration to work in a large organization like the DoD requires scalability. There is a requirement to ensure the APIs and applications can deliver the information that's needed in a timely manner.



5

SCALABILITY



Scalability

The DoD generates and stores a tremendous amount of data and supports a massive base of users. Some of the data found in the DoD is similar to what you'd expect to find in a large private sector enterprise: Employee records, benefits information, accounts payable and receivable, procurement information, and more.

Other types of data directly related to national defense are more unique to the DoD, such as information about weapons systems, intelligence, and logistics.

Finally, there are the types of data few would expect to find included in the DoD's mission, such as weather data, which comes from the DoD's collection of the most sophisticated weather satellites in the world; river traffic data, which is collected and managed by the U.S. Army Corps of Engineers as part of its mission to maintain dams, locks, and levees across the country; and Global Positioning System (GPS) data, because GPS is run by the U.S. Air Force.

Not all of this data needs to be treated the same, but it all needs to be accessible, discoverable, and secure. But the sheer volume of data means that any strategy to make it easily available to consumers needs to scale in terms of the amount of data, the number of concurrent users, and the time it takes to access data. This latter point is especially important in systems used for command and control, or C2, where timely access to data is a matter of life or death.

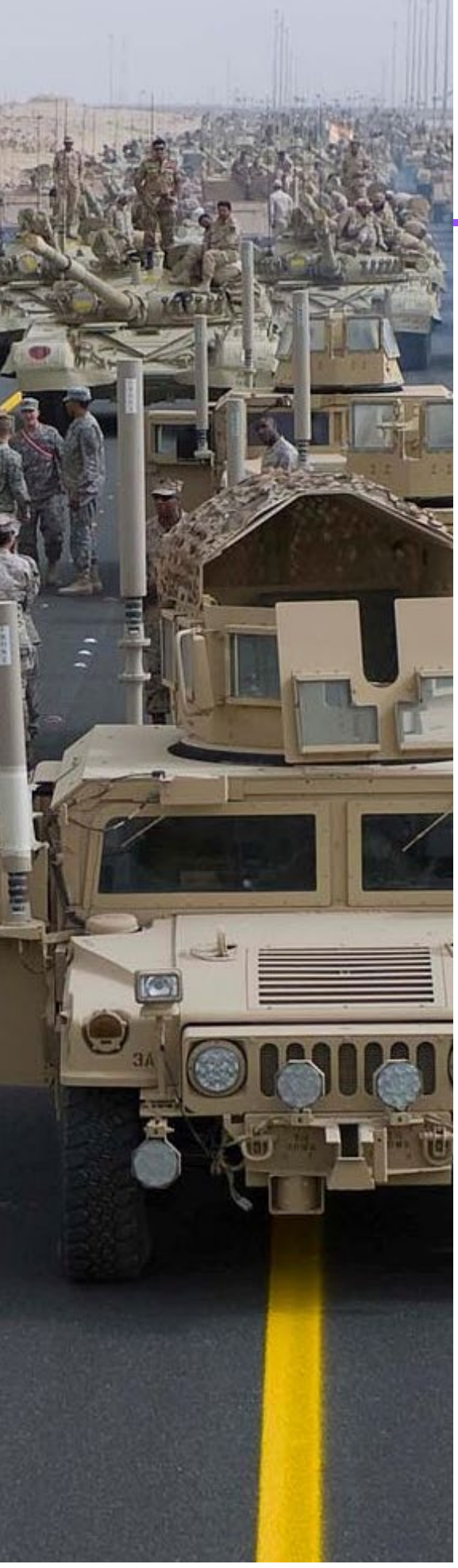
When the DoD says it wants to become data-centric and put data at the center of its decision making, there is no room for downtime. Integration solutions need to deliver real-time access to the most important data and remain highly available, even in far-flung locations where connectivity is limited or unreliable. They even need the ability to provide access to data when disconnected.

Flexibility is actually a key to scalability. Flexible architectures and hybrid deployment models, including the use of cloud-based systems, will help create integration solutions that match the use case and recognize the difference between command and control systems and those accessing river traffic data. In-memory data caching helps provide the timely access to data that many mission-critical systems in the DoD require.

In the next section, we'll explore one platform that is designed to overcome many of the challenges vendors will face as they help the DoD meet the goals of its data strategy. An API-led approach to accessibility, discoverability, security, and scalability is both proven and capable in scenarios like those required by the DoD. But an API-driven approach will only succeed with proper governance, real-time access, flexible deployment models, and more.

6

THE SOFTWARE AG APPROACH TO API-LED HYBRID INTEGRATION



The Software AG Approach to API-Led Hybrid Integration

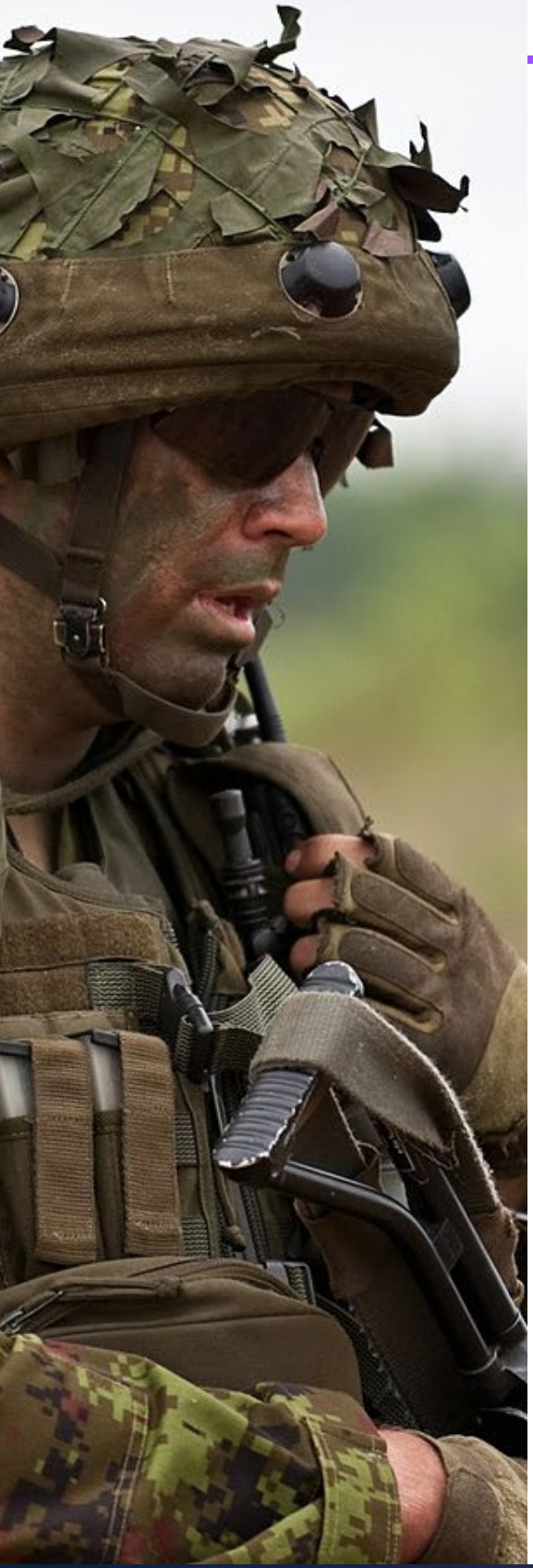
The webMethods platform from Software AG delivers an API-led approach to hybrid integration that will help data consumers and IT leaders at the DoD and its partners align with the agency's data strategy.

In a large IT environment like the DoD, which features everything from legacy systems to new, cloud-based applications, webMethods offers connectivity to everything by making available a number of capabilities, including:

- Connectors built specifically for popular enterprise systems of record make it easy to connect without the time and expense of creating custom, point-to-point integrations. More than 300 out-of-the-box connectors are available.
- A no-code/low-code development environment eases the burden on application development teams, offers faster integrations, and removes application dependencies.
- Mapping and transformation capabilities that create common data formats from data residing in disparate systems.

Once the data sources are connected, Software AG's webMethods makes it easy to expose data as APIs, eliminating the complexity of data accessibility and abstracting the information data consumers need without making them complete numerous steps.

Software AG also provides the management and governance required to secure and monitor the APIs. Macro



and micro API gateways apply run-time security policies in the data center or at the edge, while auditability helps track who and what is using the APIs and how. An API Portal exposes the APIs, giving data consumers a one-stop shop to identify currently available APIs and controlling access to potentially sensitive data. The API Portal allows developers to test out available APIs to help them better understand how they can be used to add value to their applications.

The architectural flexibility of Software AG's webMethods platform helps it meet the many use cases presented in a complex organization like the DoD. It offers cloud-based, on-premise, and edge deployment models each with the highest levels of security. In-memory data caching means fast access to data, and high availability means the data is there for mission-critical applications when they need it.

Software AG's webMethods is a vendor-neutral approach to data integration that offers connectivity to everything a complex environment like the DoD has deployed. It's a single, unified platform that is proven and relied on by some of the largest organizations in the world, where it's used to meet challenges around data accessibility, discoverability, security, and scalability. Software AG's webMethods is already used in classified and unclassified environments within the DoD, including the U.S. Navy ERP program, and in other federal government agencies, such as the Internal Revenue Service (IRS). webMethods is available in the DoD Iron Bank repository as an extension to the baseline Platform ONE capabilities.

Meeting the goals of the DoD data strategy will not be quick or easy. Rapid capability development will be critical. With API-led integration, connectors to common systems, and no-code/low-code capabilities, Software AG's webMethods platform is well-positioned to help overcome some of the biggest challenges facing the overall strategy and its implementation.

For more information please visit **www.softwareaggov.com** or email us at **info@softwareaggov.com**