The Cross Domain Dilemma:
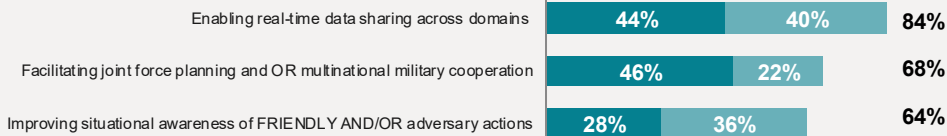## Gaps, Risks, and Roadblocks in Defense Systems

Modern multi-domain operations require fast, adaptable, and secure information sharing across multiple security levels, environments, and commands. Cross domain solutions (CDSs) are essential to enabling this capability—but current systems aren't keeping pace with mission demands. A survey of defense leaders reveal a clear picture: fragmented data flows, system incompatibilities, and rigid architectures are limiting mission effectiveness. As contested environments intensify and resources tighten, defense leaders are calling for CDS capabilities that are secure, interoperable, and designed for real-time adaptability—at every echelon of command.

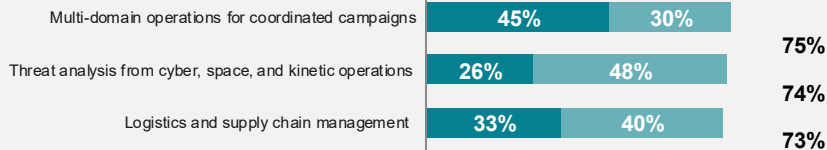## What matters most for cross domain decision making

A successful CDS must balance speed and security with real-time data sharing across domains and with coalition partners: lives depend on it. Respondents most often rate enabling real-time data sharing across domains, ensuring rapid communication between different operational forces, and the ability to access full-motion video (FMV), structured, and unstructured data in the field as critical/very important benefits of CDS.

▶ **Q: How important are the following potential benefits of cross domain systems for decision-making at each level of command? (Top 3 in each category.)**

Strategic Level (National & Theater Command)

Benefit	Very important	Critical	Total
Enabling real-time data sharing across domains	44%	40%	84%
Facilitating joint force planning and OR multinational military cooperation	46%	22%	68%
Improving situational awareness of FRIENDLY AND/OR adversary actions	28%	36%	64%

Operational Level (Theater Joint Task Force Command)

Benefit	Very important	Critical	Total
Multi-domain operations for coordinated campaigns	45%	30%	75%
Threat analysis from cyber, space, and kinetic operations	26%	48%	74%
Logistics and supply chain management	33%	40%	73%

Tactical Level (Unit & Mission Execution)

Benefit	Very important	Critical	Total
Ensuring rapid, secure communication between different operational forces	20%	61%	81%
Ability to access FMV, structured and unstructured data in the field	47%	30%	77%
Providing real-time data for mission execution	23%	54%	77%
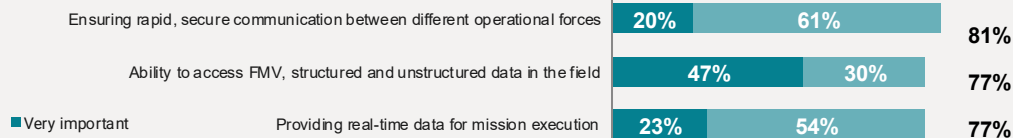
■ Very important
■ Critical

Percentage of respondents, n=100

Over three quarters of respondents say the ability to access FMV, structured, and unstructured data in the field and providing real-time data for mission execution are important.

61% of respondent's report that ensuring rapid, secure communication between different operational forces is critical at the tactical edge.

The Owl Cyber Defense™ Insight

Advancing Mission Success Through Resilient Cross Domain Solutions

As multi-domain operations grow more complex and adversarial threats escalate, the ability to securely move mission-critical information across domains is not optional—it's foundational. This survey set out to understand how CDSs are being used across the U.S. armed forces, and where today's systems are falling short. The results are clear: rigid architectures, fragmented data flows, and integration hurdles hinder mission agility. In this environment, defense leaders need more than just compliance—they need CDS capabilities that are adaptable, interoperable, and purpose-built for the speed and scale of modern missions. Owl Cyber Defense™ is committed to delivering the trusted, mission-aligned technologies that meet these evolving demands—ensuring decision dominance at every level of command.
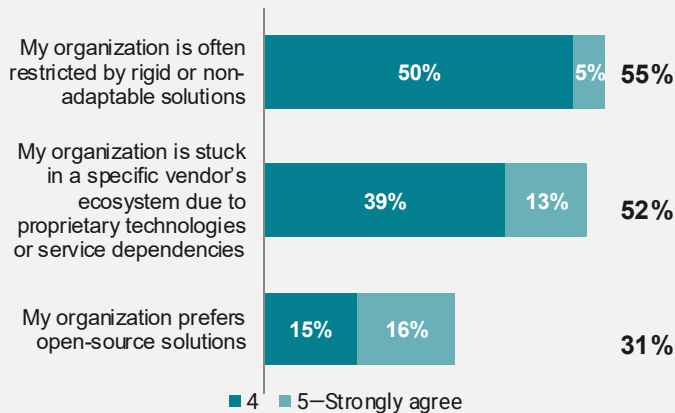
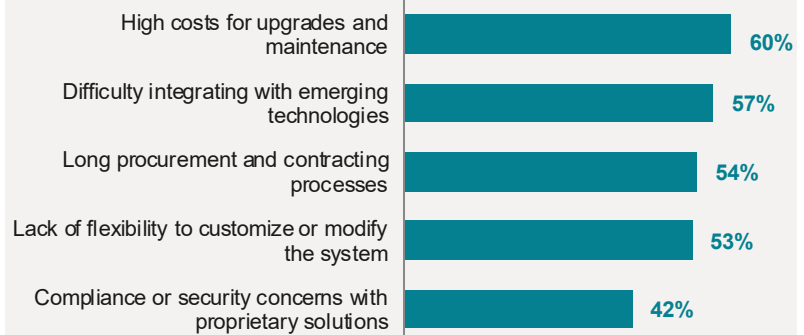## Finding the right solutions: fast, secure, and adaptable

Over half of respondents agree that rigid or non-adaptable solutions often restrict their organization, and/or that their organization is stuck in a specific vendor's ecosystem. **Vendor lock-in is a challenge:** 60% encounter challenges with high costs for upgrades and maintenance and well over half have experienced difficulties integrating with emerging technologies, long procurement and contracting processes, and a lack of flexibility to customize or modify systems.

▶ **Q: How much do you agree or disagree with each of the following statements?**

My organization is often restricted by rigid or non-adaptable solutions
- 50% | 5% — **55%**

My organization is stuck in a specific vendor's ecosystem due to proprietary technologies or service dependencies
- 39% | 13% — **52%**

My organization prefers open-source solutions
- 15% | 16% — **31%**

■ 4 ■ 5—Strongly agree

Percentage of respondents, n=100

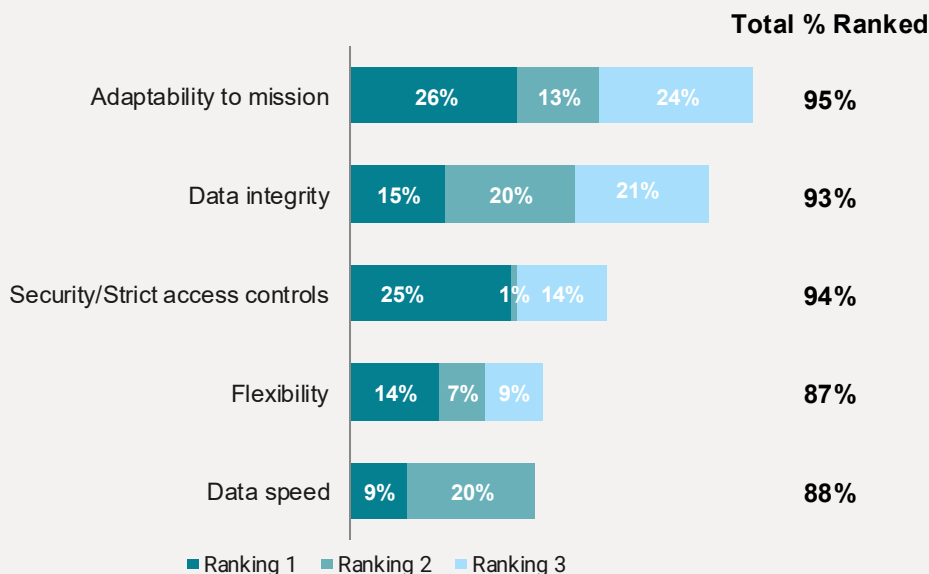▶ **Q: What challenges have you encountered with vendor lock-in when procuring or managing cross domain systems? Select all that apply. (Top 5)**

High costs for upgrades and maintenance — **60%**

Difficulty integrating with emerging technologies — **57%**

Long procurement and contracting processes — **54%**

Lack of flexibility to customize or modify the system — **53%**

Compliance or security concerns with proprietary solutions — **42%**

Percentage of respondents, n=100
Note: Respondents allowed to select multiple responses

Given the challenges with vendor lock-in, what are respondents really looking for in a partner? They believe everything is important. However, some features rank higher than others. Nearly all respondents rate adaptability to the mission, security/strict access controls, and data integrity as their top priorities in cross domain solution providers. Of those, adaptability to mission and security/strict access control are the number one priorities.

▶ **Q: Please rank the following in order of highest priority to lowest priority when partnering with a cross domain system solution provider. (Top 5 #1 ranking)**

Total % Ranked

Adaptability to mission
- 26% | 13% | 24% — **95%**

Data integrity
- 15% | 20% | 21% — **93%**

Security/Strict access controls
- 25% | 1% | 14% — **94%**

Flexibility
- 14% | 7% | 9% — **87%**

Data speed
- 9% | 20% — **88%**

■ Ranking 1 ■ Ranking 2 ■ Ranking 3

Data integrity ranks as a top-three priority for

56%

of respondents when selecting a cross domain system provider.

One quarter of respondents rank security and adaptability as their #1 priority when partnering with a CDS provider. Only 9% rank data speed #1.
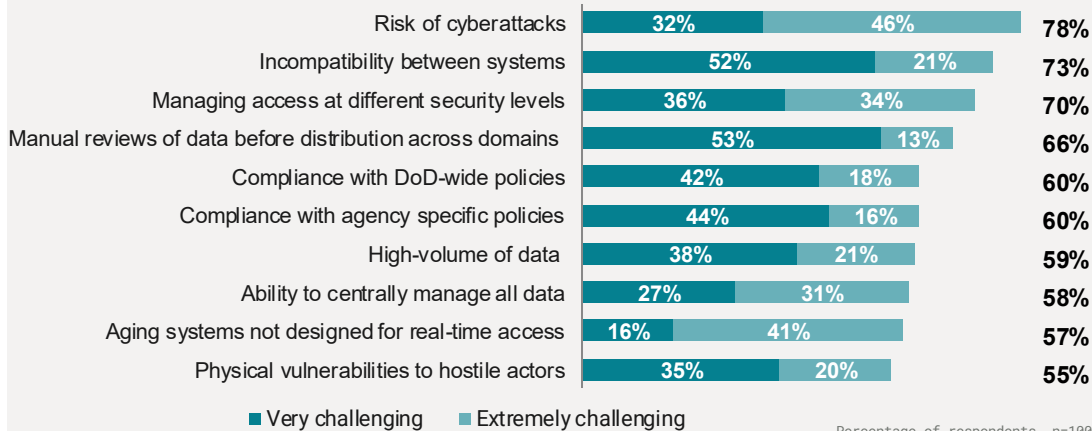
Challenges to overcome

When choosing whether to use CDS, respondents say their top challenges are risk of cyberattacks, incompatibility between systems, and managing access at different security levels. **Cross domain solutions need to successfully address these challenges to ensure mission success.**

▶ **Q: How challenging are each of the following in utilizing cross domain solutions to ensure mission-critical decision-making happens at the right level of command? (Top 10)**
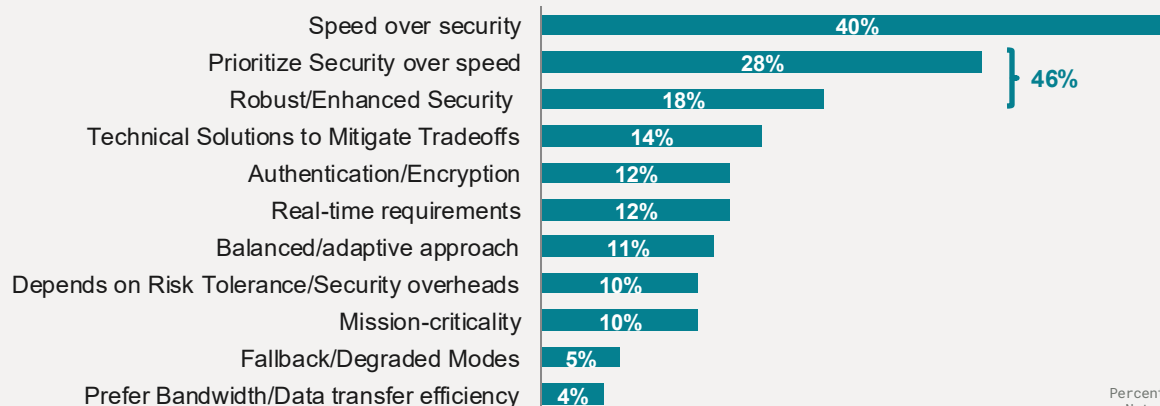
	Very challenging	Extremely challenging	Total
Risk of cyberattacks	32%	46%	78%
Incompatibility between systems	52%	21%	73%
Managing access at different security levels	36%	34%	70%
Manual reviews of data before distribution across domains	53%	13%	66%
Compliance with DoD-wide policies	42%	18%	60%
Compliance with agency specific policies	44%	16%	60%
High-volume of data	38%	21%	59%
Ability to centrally manage all data	27%	31%	58%
Aging systems not designed for real-time access	16%	41%	57%
Physical vulnerabilities to hostile actors	35%	20%	55%

■ Very challenging ■ Extremely challenging

Percentage of respondents, n=100

41%

Of respondents are extremely challenged by aging systems not designed for real-time access.

Over a third of respondents are extremely challenged by managing access at different security levels.

Trading one important feature for another is always a challenge. While respondents say speed over security is their primary consideration (40%), a combined 46% noted security related themes as their primary consideration. Given how closely matched these priorities are, it raises a more fundamental question: is choosing between speed and security even an option—when organizations today must have both?

▶ **Q: What are the tradeoffs you consider between security and speed when transferring data in high-threat environments?**

Speed over security	40%
Prioritize Security over speed	28%
Robust/Enhanced Security	18%
Technical Solutions to Mitigate Tradeoffs	14%
Authentication/Encryption	12%
Real-time requirements	12%
Balanced/adaptive approach	11%
Depends on Risk Tolerance/Security overheads	10%
Mission-criticality	10%
Fallback/Degraded Modes	5%
Prefer Bandwidth/Data transfer efficiency	4%

(Prioritize Security over speed + Robust/Enhanced Security = 46%)

Percentage of respondents, n=100
Note: OPEN ENDED, Coded Themes