EVERFOX

Defending the Digital Battlespace

CYBER360

2026

Foreword

Digital transformation has redefined the battlespace, with today's conflicts now being fought across networks more than borders. Government, defense, and critical services are all operating in a highly contested digital arena. The decisive asset is not necessarily firepower: it is data.

Every mission now depends on the ability to move, protect, and trust information at speed. Yet, this dependency has created a new vulnerability: adversaries are exploiting legacy systems, insider threats, and interoperability gaps to degrade mission assurance and pre-position attacks on critical infrastructure.

The numbers tell a stark story. Cyberattacks on U.S. government and defense organizations, and critical services surged 25% year-on-year, with organizations in both the U.S. and UK now facing an average of 137 attacks per week.

Leaders recognize the challenge: 84% agree that sharing sensitive data across networks heightens risk, and nearly half still rely on manual processes, even as AI accelerates the pace of operations.

To counter this, organizations must embrace a new strategic foundation built on a cybersecurity trinity that forms the foundation of mission assurance of the digital battlefield: Zero Trust Architecture (ZTA), Data-Centric Security (DCS), and Cross Domain Solutions (CDS). These three interacting frameworks enable an integrated, data-driven and sovereign force, ensuring that information can flow securely across domains without compromising mission speed or operational resilience.

Our latest CYBER360 report examines what these trends mean for operational resilience and outlines the strategies required to adapt. It is designed to help leaders anticipate the next phase of digital conflict and make informed decisions to protect sovereignty, enable interoperability, and maintain mission speed.

The question is no longer **if** these challenges will impact operations, but **how quickly organizations can respond before adversaries exploit the gap**.

Dave Wajsgras

Chairman and Chief Executive Officer | Everfox

Contents

Methodology

CYBER360: Defending the Digital Battlespace is based on research conducted on behalf of Everfox by Censuswide, among a sample of 500 Security leaders and IT security decision makers working in government, defence, and critical services industries in the UK and US (250 per market). The data was collected in October 2025. All quotes included have been given with express permission from the individual and are based on the findings of this report.

Introduction: The Rise of **Digital Warfare**

Modern warfare is no longer fought in separate domains; it's digital, physical, and human, all connected by data. Operational success now depends on trusted data that moves securely across domains and allies at mission speed.

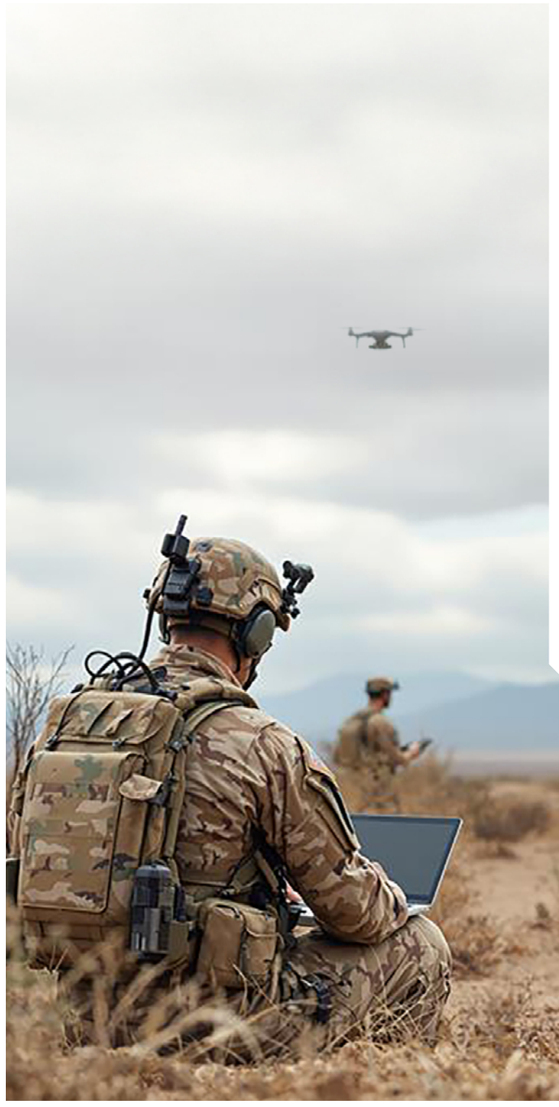
Every drone feed, sensor, and tactical report now flows through a digital backbone that links people, platforms and partners.

This increasing scale, interconnectedness and criticality of data has given rise to an unprecedented challenge for governments, critical agencies and defense organizations:

How to share mission-critical information securely while preserving sovereignty, speed, and trust.

Global security and defense initiatives, such as the U.S. Combined Joint All-Domain Command and Control (CJADC2) initiative, the UK MOD's Strategic Defence Review and The North Atlantic Treaty Organization (NATO) Data Strategy for alliance (DaSA), all point to the same truth: data is now a strategic asset that must be protected and made interoperable across classifications and partners. Yet securing that data across allies classification levels, and operational boundaries remains one of the most complex challenges for security leaders.

Based on insights from 500 Security leaders and IT security decision makers working in government, defense, and critical services industries in the UK and U.S., CYBER360: Defending the Digital Battlespace reveals what senior security professionals are really facing, and fearing, in 2026. These are real-world insights, drawn from those tasked with defending the data, systems, and people that underpin national security.



45% cite **managing identity and authentication** across multiple domains as the biggest challenge to securing access to mission data across different domains.

The findings expose the immense challenge they face in this era of digital conflict and the limitations of isolated Zero Trust strategies, where failure to quickly transfer and secure data means compromised intelligence, degraded mission assurance, slowed mission speed and ultimately mission failure.

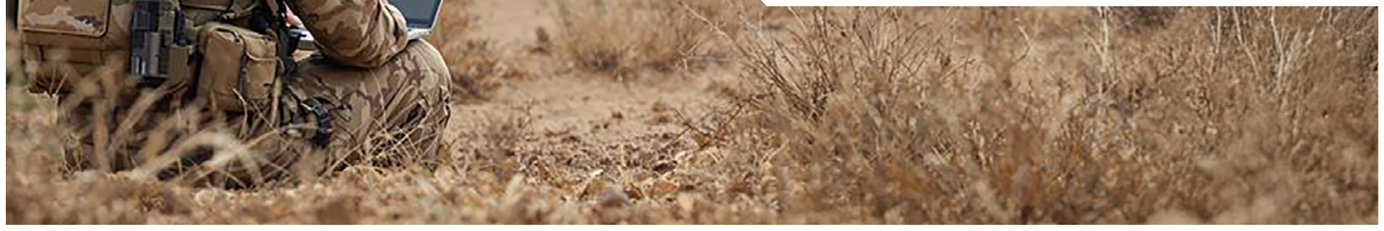
54% believe that data tampering or theft is the most serious consequence of failing to securely access and transfer data across networks and organisations.

The findings expose the immense challenge they face in this era of digital conflict and the limitations of isolated Zero Trust strategies, where failure to quickly transfer and secure data means compromised intelligence, degraded mission assurance, slowed mission speed and ultimately mission failure.

49% cited ensuring **data integrity in transfer** as one of their greatest challenges.

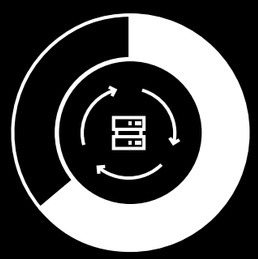
The CYBER360 Report reveals that cyber resilience is now defined not only by secure network perimeters, but by the trustworthiness, integrity, and mobility of data.

Zero Trust alone is no longer enough. The cybersecurity trinity of Zero Trust Architecture (ZTA), Data Centric Security (DCS) and Cross Domain Solutions (CDS) are now mission imperatives for governments, defense organizations, and critical services.



64%

believe secure data movement is the greatest barrier to Zero Trust strategies



89%

have adopted or are implementing data-centric security

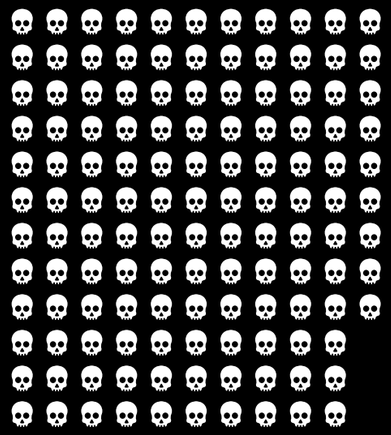
The Consequences of Failure

For organizations, the consequences of failure in cyberspace extend far beyond data loss. National security, operational readiness, and physical safety are all on the line.

And risk to these organizations is rising. CYBER360 reveals a:

7% year-on-year increase in successful or attempted cyberattacks across the US and UK.

2024



127 attacks per week

2025

137 attacks per week

This escalation exposes a harsh truth about the current global cyber landscape. Adversaries are intensifying their focus on U.S. government and defense organizations, and critical services, which have experienced a:

25% surge in attacks year-on-year.

To ensure mission success, leaders need to commit to securing critical data. Failure to act could impact interoperability and lead to an operational standstill.

LEGACY RISKS IN A MODERN LANDSCAPE

Nation-state-backed threat actors such as Volt Typhoon and Salt Typhoon are exploiting the gaps, not only to steal intellectual property, but to pre-position attacks on the networks and infrastructure that underpin modern defense and national life.

Across both nations, outdated infrastructure is cited as a **primary source of vulnerability by 78% of cyber professionals** and it introduces a widening gap between adversary capability and institutional agility.

> “Nation-state adversaries are not just probing our networks, they are working aggressively to embed themselves in the infrastructure of our national defense and critical services. When outdated systems remain in place, we **hand them the opportunity to disrupt missions** and erode public trust. Modernization is not a luxury for government and defense organizations, **it is the cost of maintaining operational readiness.**”
>
> William Evanina,
> former Director National Counterintelligence and Security Center

Securing legacy infrastructure for digital warfare is complicated by outdated analog systems, manual processes, and the urgent need for modernization.

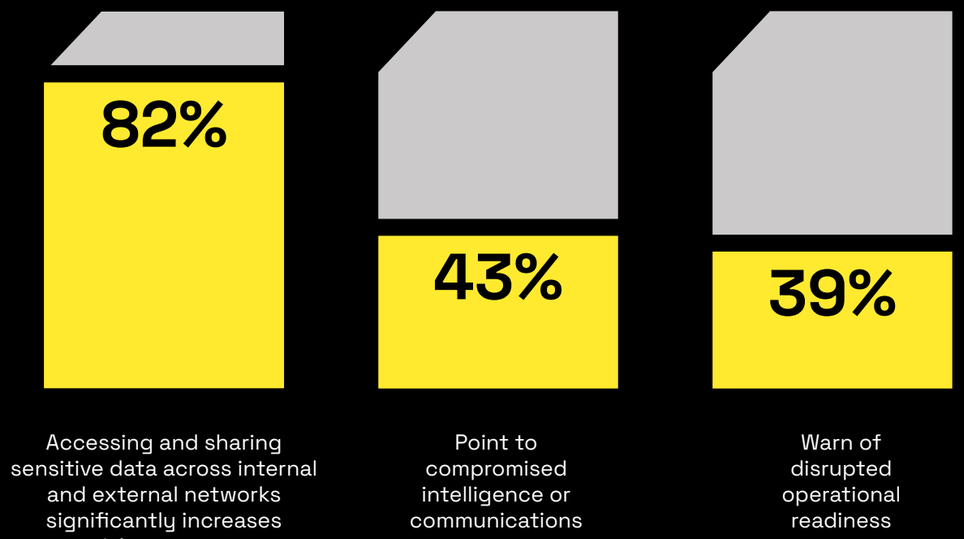
More than half of organizations still rely on paper records or physical data transfer, with minimal security controls.

This reliance often comes from existing systems being built around physical records. This is not only due to the digital transition being costly and disruptive, but in restricted or contested areas, access to high-bandwidth or trusted digital resources may be limited, reinforcing the need for traditional methods.

It’s therefore no surprise that **71% of cybersecurity professionals believe a single successful supply chain attack could bring their organization to a standstill** and **64% expect the next major strike on critical infrastructure to cause physical destruction, not just digital disruption.**

OPERATIONAL FALLOUT OF CYBER RISK

The operational fallout is equally as stark when data cannot be trusted or is inaccessible.



In modern conflict, that translates to delayed decision-making, fractured coalition coordination, and, potentially, mission failure.

This is why even mature Zero Trust Architectures (ZTA) are no longer sufficient on their own. While essential, ZTA struggles to operate across environments with differing levels of trust and classification. In both the U.S. and the UK, respondents most frequently identified as their greatest Zero Trust challenge:

- **58%:** Secure data transfer and Cross Domain access
- **47%:** Network visibility and threat detection
- **42%:** Identity and access management

The findings expose how the inability to move and protect data across networks, partners, and classification levels is the single greatest risk to operational success. Without trusted, integrated data, the digital backbone of the integrated force cannot function safely and efficiently.

Zero Trust Architecture is a security framework that operates on the **"never trust, always verify"** principle, assuming no user or device is safe by default, even those already on a private network.

Cross Domain Access and Transfer refers to the **secure sharing and movement of information between systems** with different security levels.

"Zero Trust provides essential controls, but **it was not designed to solve Cross Domain transfer or coalition data sovereignty on its own.**

In operational settings where classification boundaries and partner policies differ, the missing piece is **assured, policy-driven data movement.**

Without that capability, intelligence sharing **slows**, coalition tempo **drops**, and commanders **lose decision advantage."**

Marianne Bailey,
former NSA Deputy National Manager for National Security Systems

The Data Transfer and Access Challenge

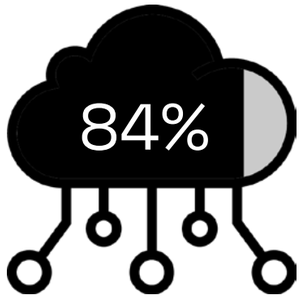
Every organization depends on the ability to move, access, and protect data across domains, networks, and partners without compromising sovereignty, speed, or trust. Yet, the act of sharing and accessing data remains one of the greatest sources of operational risk – particularly when your own people pose amongst the highest threats, whether negligently or maliciously.

Many face barriers such as siloed or overlapping data holdings, inconsistent governance, non-standardized delivery, and critical skills gaps that undermine accountability and recognition of data's value.

Failure to tackle these barriers and secure data movement degrades intelligence, slows operations, and risks mission failures.

SECURING DATA IN MOTION

For organizations and agencies, trust in data is no longer a given; it must be verified, in motion and at rest. But this presents an immense challenge when data sharing is critical to their defenses, with **84% of CIOs and CISOs agreeing that accessing and sharing sensitive data across internal and external networks significantly increases their organization's risk exposure.**



The major barriers include:

Data tampering

Nearly half (49%) of cyber professionals cite ensuring **data integrity** and **preventing tampering in transit** as their single biggest challenge when transferring information across classified or coalition networks.

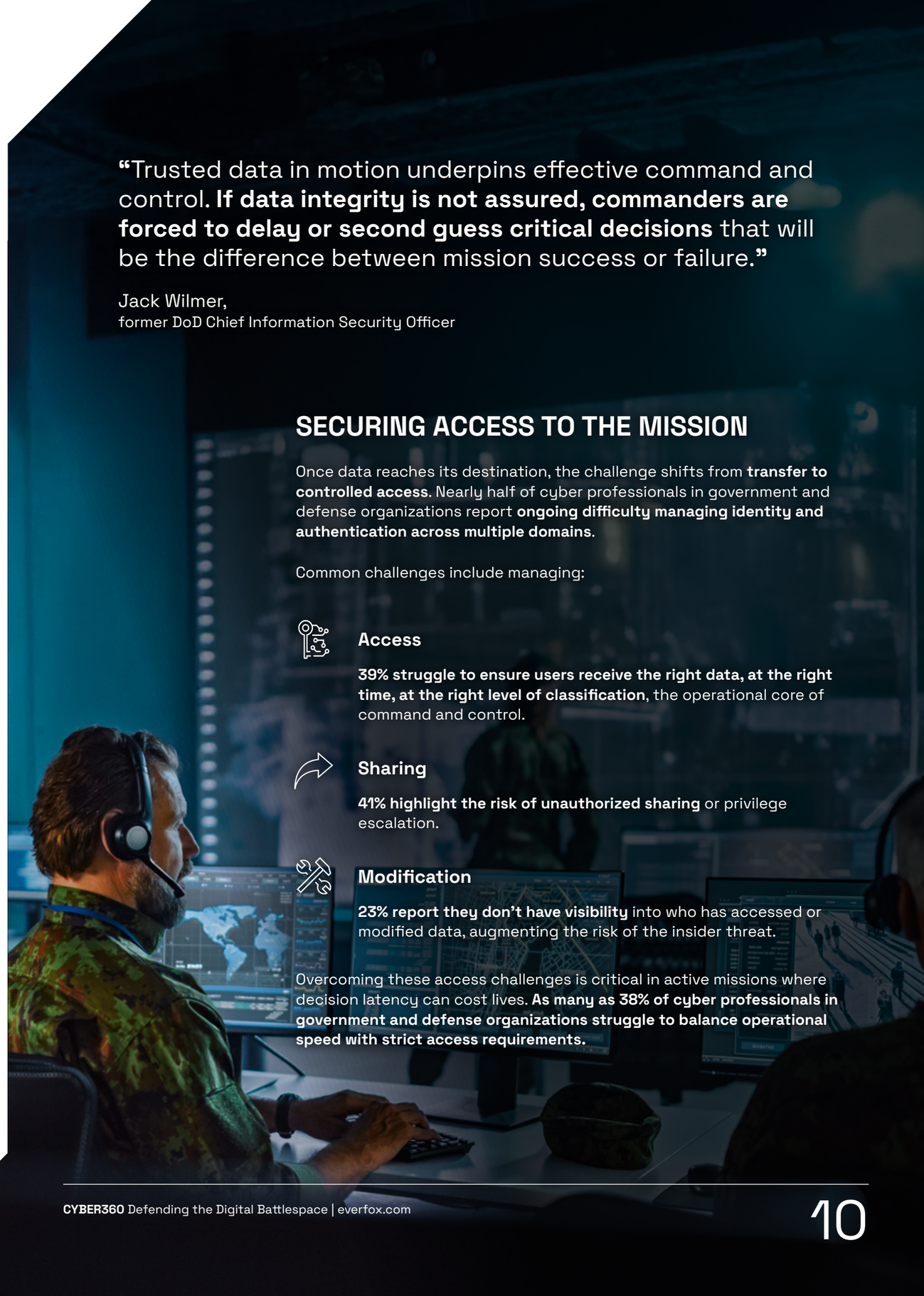
Security policies and controls

45% of cyber professionals struggle to **apply consistent security policies and controls** during transfer.

Embedded threats

41% of cyber professionals highlight **removing potential malware or embedded threats** from data before movement as a major barrier.

That's why technologies like Content Disarm and Reconstruction (CDR) and Remote Browser Isolation (RBI) have emerged as critical safeguards. The ability to exchange safe data between environments while physically isolating them from each other is now fundamental to mission assurance.



"Trusted data in motion underpins effective command and control. **If data integrity is not assured, commanders are forced to delay or second guess critical decisions** that will be the difference between mission success or failure."

Jack Wilmer,
former DoD Chief Information Security Officer

SECURING ACCESS TO THE MISSION

Once data reaches its destination, the challenge shifts from **transfer to controlled access**. Nearly half of cyber professionals in government and defense organizations report **ongoing difficulty managing identity and authentication across multiple domains**.

Common challenges include managing:

Access

39% struggle to ensure users receive the right data, at the right time, at the right level of classification, the operational core of command and control.

Sharing

41% highlight the risk of unauthorized sharing or privilege escalation.

Modification

23% report they don't have visibility into who has accessed or modified data, augmenting the risk of the insider threat.

Overcoming these access challenges is critical in active missions where decision latency can cost lives. **As many as 38% of cyber professionals in government and defense organizations struggle to balance operational speed with strict access requirements.**

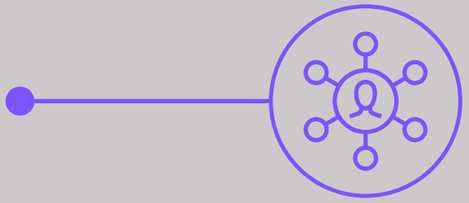
SECURING THE PEOPLE BEHIND THE NETWORKS

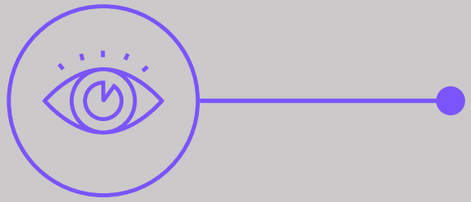
Technology may form the digital backbone of national security, but people remain both the first line of defense and one of the greatest points of vulnerability.

84%

of CIOs and CISOs report that **insider threats**, whether malicious or accidental, are a **critical vulnerability to their organization's data**.

In environments that rely on trusted individuals operating within classified networks, **even a single compromised credential or mishandled file can have cascading effects**. The consequences range from **data exfiltration and privilege escalation** to **accidental policy breaches** that erode coalition confidence and disrupt operational readiness.





Advanced monitoring and integrated threat intelligence are therefore essential to **identify and contain** these risks without hindering legitimate operations.

SECURELY SHARING WITH ALLIES

As global threats deepen, the ability to **share intelligence and operational data securely**, both nationally and with allied nations, has become a strategic imperative. Yet **poor interoperability is constraining this ability**.

Cybersecurity professionals working in defense report that the greatest challenges are:

INCONSISTENCY ACROSS AGENCIES

- **49%:** Differing security classifications and data handling policies
- **40%:** A lack of common data standards and formats
- **38%:** Inconsistent access and authorization models

were cited as the biggest barriers to interoperability.

MISMATCHED CAPABILITIES

Inconsistent technical capabilities posed the next greatest barrier. These included a **lack of Cross Domain Solutions (35%)** and the **implementation of legacy systems that can't integrate (31%)**. Notably, **differing levels of Zero Trust maturity between partners** also posed an issue for nearly one-third of respondents.

NATIONAL SOVEREIGNTY

Despite ambitions for greater interoperability of data and systems across allied environments, **data sovereignty remains a key challenge for defense organizations. 82% of cyber professionals working in defense** highlighted that balancing data sovereignty requirements with the need for coalition information sharing is an ongoing challenge for their organization.

"Interoperability has both **technical and political considerations.**

Allies must be able to **act on shared intelligence** while also **preserving sovereignty** over their own sensitive data."

VADM Nancy Norton, RET.,
former Director, DISA

The Key Drivers to Being **Battle Ready**

Securing the modern battlespace requires more than defending networks. It demands the ability to share, trust, and act on data across domains, allies, and operational environments at mission speed. But the persistent challenges cybersecurity professionals face when securing data, access, transfer, and people expose a hard truth:

“Zero Trust on its own is **no longer enough.**”

Dave Wajsgras
Chairman and Chief Executive Officer | Everfox

THE ZERO TRUST REALITY CHECK

Zero Trust has become a universal standard across government and defense organizations, but cyber professionals are struggling with its limitations.

The biggest challenges they face in developing or enhancing a Zero Trust strategy:

Secure Data Transfer & Cross Domain Access: ensuring the safe movement of data between networks or domains while maintaining security controls — 64%

Network Visibility & Threat Detection: achieving continuous insight into traffic, anomalies, and potential intrusions — 47%

User Behavior Monitoring & Insider Risk Management: detecting anomalous activity and addressing the human attack surface — 41%

Endpoint & Device Security: hardening, monitoring, and threat prevention/ detection across on-site and remote devices — 41%

Identity & Access Management: unifying identity governance and privileged access control across systems — 40%

These findings confirm what many cyber leaders will already know to be true:

Zero Trust alone cannot secure operations that span multiple domains, partners, and classification levels.

THE RISE OF DATA CENTRIC SECURITY

In response, organizations are pivoting from network-centric to data-centric models, protecting the information as well as the environment around it.

Recognizing the need for a fundamental mindset shift, **nine in ten organizations** have already adopted or are in the process of implementing a data-centric security approach.

Data-Centric Security protects data by **applying security controls directly to the data itself**, rather than relying solely on network or perimeter security.

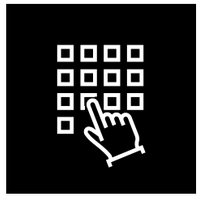
Fully adopted and operationalized

In progress but not fully implemented

Early stages or planning

Data-centric security (DCS) enables intelligence to **move securely across coalition networks**, ensuring that **sovereignty and assurance are preserved**, even when systems or partners differ in classification or trust level.

By focusing on the data itself, **organizations can achieve two outcomes** that Zero Trust cannot guarantee without it:



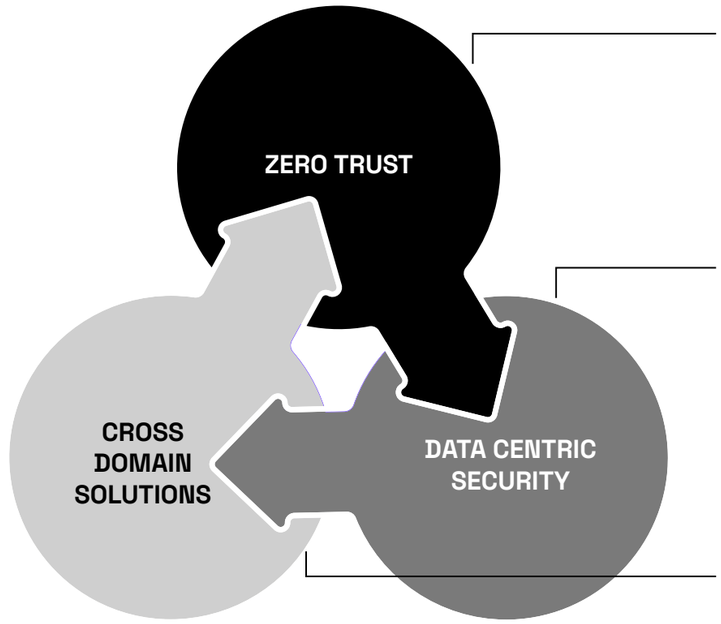
Trusted access for those who need it, even in contested or disconnected environments.

Persistent protection wherever the data moves, across sensors, command systems, or allies.

CYBERSECURITY MODEL FOR THE DIGITAL BATTLESPACE

The benefits and limitations of each framework aside, organizations in government, defense and critical services cannot overcome the challenges they face in securing data access, transfer, and sharing with a single framework. **Success depends on combining multiple layers of protection. This is why integration matters.**

Only by bringing together three interacting cybersecurity frameworks, Zero Trust Architecture (ZTA), Data-Centric Security (DCS), and Cross Domain Solutions (CDS), can organizations enable secure, **near-real-time cross domain data sharing and access across mission systems.**



The guiding principle. It assumes a breach and enforces continuous verification, ensuring that no user or system is trusted by default.

Shifts the focus from infrastructure to the asset. It ensures that data remains protected regardless of where it resides or how it moves, preserving sovereignty and mission intent.

The enabler. It provides a secure data exchange between networks - even those with different classifications and security levels - without compromising speed or isolation.

This cybersecurity trinity forms the foundation of the digital battlefield, **the foundation that enables an integrated, data-driven, and sovereign force**.

However, the interoperability between the technologies underpinning these frameworks shouldn't be taken for granted. Historically, for example, Cross Domain Solutions have been viewed as **bespoke, complex, and costly tools**, reserved for the most sensitive environments.

Advances in architecture and assurance have changed that. Today, flexible, high-speed, COTS CDS products deliver trusted, policy-enforced security without the trade-offs of legacy systems. Modern CDS platforms are agile, scalable, and interoperable, capable of operating across allied environments while maintaining isolation, integrity, and performance.

This highlights the need to actively plan and ensure that the three cybersecurity frameworks truly can interact.

The AI Imperative

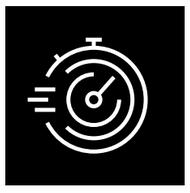
AI is an accelerator of integrated operations and the cornerstone of decision advantage in a battlespace where success depends on sensing, deciding, and acting faster than any adversary.

From autonomous vehicles to next-generation command and control systems, AI is reshaping how forces operate. Next-gen C2, for example, creates a more agile, data-centric, and resilient framework through advanced software and modular architecture, making AI the difference between success and failure.

Cyber professionals agree: **87% say AI is critical** to achieving a fully integrated force, with **42% rating it very critical.**

> "AI is dramatically changing the battlefield and improving decision advantage. **But AI is only as effective as the data pipeline that feeds it.** For defense and government, the priority should not be AI for its own sake, but rather **trusted, labelled, and auditable data** flows that allow AI models to produce reliable, explainable outputs for commanders and policy makers."
>
> Major General Joseph Brendler,
> (U.S. Army, Ret.), former Chief of Staff, USCYBERCOM

When considering the top three areas where AI has the potential to make the greatest impact on government and defense operations and critical services, cybersecurity professionals expect:



Improved cyber defenses and response times

Enhanced threat prevention and situational awareness

Automated data analysis and intelligence fusion

These capabilities are essential to delivering operational advantage and underpin the vision behind CJADC2, a unified approach to accelerate decision-making across land, sea, air, space, and cyber. **At its core, it is a secure data fabric that connects sensors to decision-makers and effectors**, enabling real-time analysis and action.

CDS enables the safe use of AI by allowing **secure data exchange between networks of different classifications**, preserving sovereignty while maintaining speed. Combined with data-centric security, CDS ensures AI can operate confidently within CJADC2.

Yet there remains a stark paradox. Despite organizations in government, defense operations and critical services recognizing the AI imperative, **more than half (53%) still rely on manual data transfer on paper**. In an age of AI, this analogue dependency is a mission risk.

The Path **Forward**

The digital battlespace demands a new mindset where data is not just an enabler, but integral to strategic, operational and mission success.

Every sensor feed, video, chat log, intelligence report, and operational decision depends on trusted, accessible, and secure data.

To achieve mission assurance, organizations must move beyond perimeter defense and adopt an integrated model that combines ZTA, DCS, and CDS. This path forward is built on five critical steps:

1. Protect the data, not just the network

Shift security from infrastructure to the asset itself. Apply controls directly to the data, create clear classification and labelling standards, and establish trust frameworks for intelligence exchanges. **This ensures persistent protection wherever data moves:** across domains, partners, and mission systems.

2. Build interoperability into architecture

Design for coalition and Cross Domain operations from the start. Combine ZTA for identity assurance, DCS for data-level protection, and CDS for secure interoperability. This layered approach enables **dynamic policy enforcement and resilience** without slowing operational tempo.

3. Preserve sovereignty through policy-based control

Interoperability must never compromise national sovereignty. Use policy-based access controls to enforce sharing rules dynamically, maintain compliance with international regulations, and promote transparency and accountability in Cross Domain data flows.

4. Ensure isolation between domains without sacrificing agility

Modernization cannot mean disruption. CDS enables phased transformation by isolating critical data flows while bridging legacy systems with modern platforms. This reduces risk and cost, maintains operational continuity, and supports agile integration of emerging technologies like AI.

5. Enable AI with confidence using CDS

AI depends on trusted, integrated data. CDS provides the secure data fabric that allows AI to operate confidently within CJADC2. Without this foundation, predictive analytics and rapid threat detection collapse.

"Achieving mission assurance requires looking beyond just network architecture. **Zero Trust, Data Centric Security, and Cross Domain Solutions** should be aligned to operate as a single, auditable capability. When procurement and architecture are synchronized, governments can deliver **sovereign, high speed information exchange that sustains coalition operations and shortens decision cycles."**

Michael Mestrovich,
former CIA Chief Information Security Officer

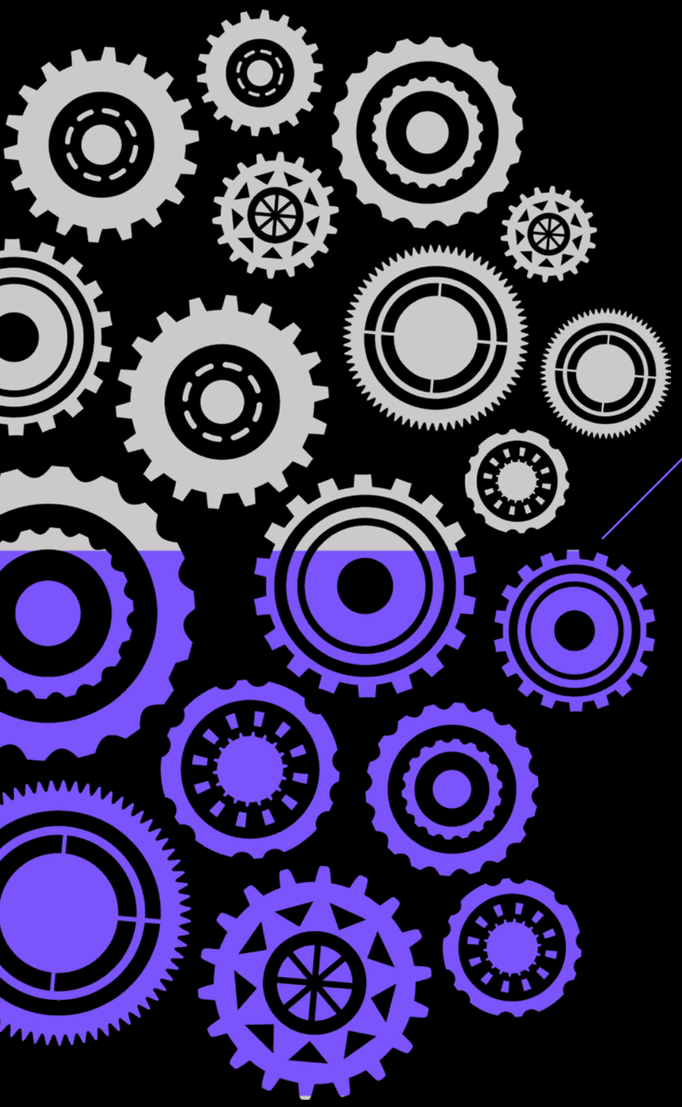
Securing the digital battlespace requires a strategy where data is:

- **Protected,**
- **Trusted**, and
- **Ready to move at mission speed.**

ZTA, DCS, and CDS are not optional frameworks; together they form the foundation for interoperability, modernization, and decision advantage.

Conclusion

The findings are clear: access to and sharing trusted data at speed are now mission-critical. Digital warfare is here, and organizations must plan today to fight tomorrow.



While 90% of organizations have begun integrating data-centric security (DCS),
nearly **half still rely on manual processes**, leaving critical gaps in readiness.

Zero Trust in isolation cannot deliver mission assurance, which is driving a shift toward data-centric security (DCS) and Cross Domain Solutions (CDS) in government, defense, and critical services.

Combined with Zero Trust, these frameworks enable **secure data exchange**, **enforce sovereignty** through policy-based controls, and **lay the foundation for AI-driven decision advantage.**

Data is the decisive asset in the digital battlespace.

It must be protected, moved securely, and made interoperable across domains and partners. **By integrating ZTA, DCS, and CDS and following the path forward outlined, organizations can have confidence in the integrity of their data, enable AI with certainty, and achieve the agility required for mission success.**

EVERFOX

About Everfox

Everfox secures the data, networks, and people that protect national security and global defense, empowering agencies to operate confidently in high-consequence environments, all while realizing efficiencies in cost, capabilities and productivity.

Built for mission-critical operations, Everfox empowers governments, allies, and enterprises to collaborate securely, operate confidently, and act at mission speed.

Unlike traditional cybersecurity vendors, we don't just defend systems, **we defend missions**. Our purpose is clear, protect the data that protects the people that protect us.

2026
CYBER360

Learn More:

www.everfox.com