KnectIQ®

CAPABILITY COMPARISON

Enhancing Cross-Domain Security in Defense:

Zero Trust vs. SelectiveTRUST™

This guide is for decision-makers in the defense sector, comparing the conventional Zero Trust cybersecurity approach against SelectiveTRUST™ by KnectIQ. The two approaches differ in how they advance operational capabilities in cross-domain data sharing and communication at various classification levels, a critical aspect of modern U.S. and Allied military operations.

Conventional Zero Trust Cybersecurity

- **Framework Overview:** Adheres to the "never trust, always verify" principle, emphasizing constant verification within a network.
- **Key Features:** Multi-factor authentication, continuous monitoring, micro-segmentation, and strict access controls.
- **Relevance to Cross-Domain Operations:** Provides a secure framework but can be rigid, potentially hindering fast data exchange and collaboration across different classification domains.

VS.

SelectiveTRUST™ by KnectIQ

- **Advanced Approach:** Zero Trust based with enhanced capabilities including dynamic trust decision-making and data operational agility.
- **Innovative Features:** Quantum-safe data protection through agile, adaptive, modern, and ephemeral cryptographic operations.
- **Alignment with Cross-Domain Needs:** Specifically designed to ensure operational agility and confident, combined operations by facilitating ultra-secure, real-time data sharing and communication across various security domains.

Recommendation

In the context of modern military operations and intelligence sharing, where speed, flexibility, and secure cross-domain communication are paramount, SelectiveTRUST™ by KnectIQ offers significant advantages over conventional Zero Trust models. Its ability to dynamically manage trust, safely advance data operational agility, and provide quantum-safe security makes SelectiveTRUST™ particularly suited for the complex and varied communication and data sharing needs of the U.S. military and its Allies.

Conclusion

The evolving landscape of global defense operations requires advanced capabilities that not only adhere to but exceed modern security standards while promoting operational efficiency and adaptability. SelectiveTRUST™ is the solution, particularly in scenarios demanding secure, operationally agile cross-domain communications and data sharing.

Comparative Use Cases

1. Cross-Domain Tactical Communication

Zero Trust provides secure communication channels but may impede real-time data flow due to encryption secrets management protocols.

SelectiveTRUST™ enables more fluid and responsive communication at speed of relevance across different classification levels, vital in joint operations and coalition warfare.

2. Intelligence Sharing with Allied Nations

Zero Trust ensures high-security data protection but may slow down the sharing process due to compartmentalized controls.

SelectiveTRUST™ facilitates faster and more secure sharing of intelligence, respecting the necessary classification levels, enhancing combined operations and collaborative decision-making.

For more information, please contact your KnectIQ representative or visit us online.

T: +1.651.447.4264 | E: secure@knectiq.com | www.KnectIQ.com | 724 Bielenberg Drive, St. Paul, Minnesota 55125