graphiant

Graphiant for Department of Defense – Secure and Scalable Networking for Defense Critical Infrastructure

SOLUTION BRIEF

The Department of Defense (DoD) requires a highly secure, scalable, and resilient networking solution to connect bases, command centers, and remote operations across the globe.

Traditional MPLS and VPN-based networks struggle to deliver the agility, cost efficiency, and security required for modern military operations, especially when supporting cloud adoption, real-time data sharing, and edge computing.

US DoD military bases are often like small towns and are typically equipped with many Operational Technology (OT) solutions to monitor and control "Defense Critical Infrastructure" (DCI): water and electric utilities, physical security systems, traffic controls, etc. Critical infrastructure must be highly robust, with average downtime measured in mere minutes per year. Connectivity to remote control systems and operators must be similarly reliable and secure from cyber threats and data exfiltration.

Graphiant's next-generation Network as a Service (NaaS) platform is uniquely suited for DCI connectivity. Graphiant enhances Zero Trust security with global reach and carrier grade performance. As a software solution, Graphiant requires no proprietary hardware and runs on "Commercial Off the Shelf" compute platforms.

Challenges in the DoD Space

1. **Downtime**
    a. Critical infrastructure must be highly robust, with average downtime measured in mere minutes per year.
2. **Resiliency and Security**
    a. Connectivity to remote control systems and operators must be similarly reliable and secure from cyber threats and data exfiltration.
3. **Cost Efficiency and Operational Simplicity**
    a. Reducing costs associated with legacy MPLS and other traditional network models.
    b. Managing growing data demands from IoT devices and advanced analytics.

Graphiant's NaaS for DCI Connectivity Solutions

1. **Security:** Patented Data Assurance capabilities with hyper-scaled threat mitigation.
2. **Privacy:** Edge-Edge encryption with no possibility of decrypt in transit.
3. **Reliability**: Self-healing Core with carrier-grade performance SLAs.
4. **Simplicity**: Delivered As-A-Service – no networking expertise required.
5. **Reach**: Connect to the global private backbone over any "last mile" access.

Why Graphiant for DoD?

Graphiant empowers DoD with a future-ready networking platform designed to support:

- High-performance connectivity for high-demand and high-risk situations.
- Secure and compliant operations to protect valuable data while in motion.
- Global scalability and agility to adapt to the organization's fast-paced and ever-changing demands.

For more information or to schedule a demonstration, visit https://graphiant.com/schedule-a-demo.

Graphiant Demo

Use Case:

Real-Time ISR (Intelligence, Surveillance, and Reconnaissance) Data Transport

Challenge

A joint task force operating in multiple regions and requires real-time ISR data transmission from UAVs and satellites to decision-makers.

Solution

The company adopted Graphiant's Network as a Service to replace its legacy MPLS connections and to modernize their defense critical infrastructure while ensuring their data is secure while in motion.

Results

- *Reduced Costs:* The organization saw a reduction in networking costs, thanks to the consumption-based pricing and elimination of MPLS circuits.
- *Reliability:* Graphiant's Core implements Site Reliability Engineering concepts consistent with advanced hyper-scaler networks to enable AI-driven self-healing behaviors in the event of actual or projected service degradation.
- *Enhanced Security:* Each location's network was segmented and secured, ensuring that any potential breach would be contained without impacting other locations or systems.

Conclusion

Defense Critical Infrastructure requires extreme attention to security and reliability. Physical and network access to DCI equipment and related control systems must be protected from cybersecurity intrusions and abuse. Graphiant offers unique, forward-looking global networking capabilities that satisfy the demands of DCI networking use cases for the DoD, such as private connectivity and isolation from internet threats, network path control with application visibility, global threat detection with reporting and mitigation, a Post-Quantum "encryption plane" for ultra-secure data privacy, and high-performance cloud and security services gateways.