QUANTUM® NETWORKS

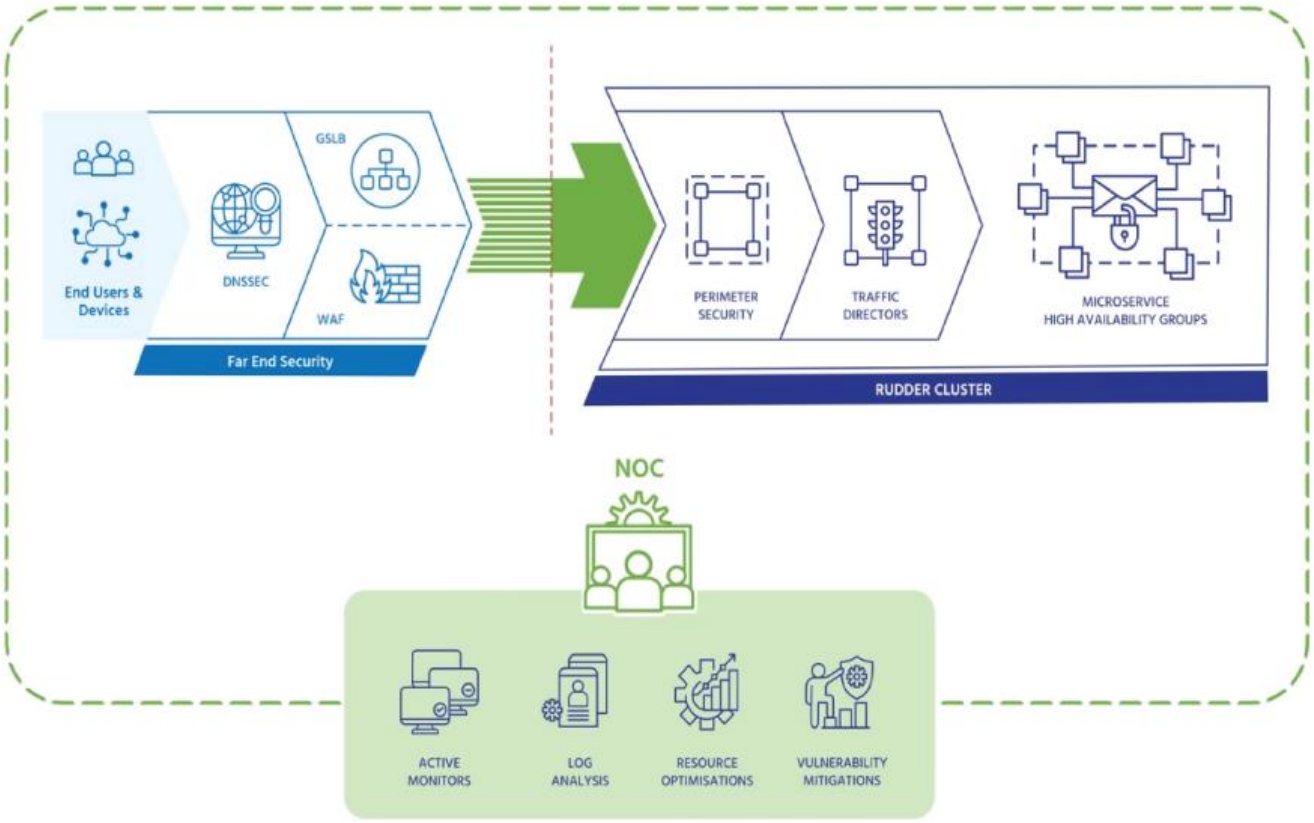
RUDDER SECURITY WHITE PAPER

Wi-Fi Switches Gateways Q-Services

In the current IT landscape, where industries heavily rely on the well-being and operational efficiency of their systems, ensuring the safety and security of servers and networks is crucial to business continuity and growth. Information security faces constant threats, including software attacks, information theft, and malware. While these external threats may not always lead to data loss or physical damage, the unavailability of services caused by such attacks can significantly disrupt operations and hinder progress.

The RUDDER security system is designed to not only address external threats through its robust safety mechanisms but also to keep all types of threats outside the boundaries of the system and servers.

In simple terms, a threat such as a DDoS attack, which can disrupt system operations by jeopardizing server availability, is effectively neutralized by RUDDER's intelligent safety mechanisms. These mechanisms prevent such attacks from even breaching the system's firewall, ensuring seamless operations at all times.



In order to ensure the Data Transmission and Communication behave in expected ways, the system must define what is and is not acceptable behavior. This begins with development of appropriate, reasonable, and applicable policies. Perimeter security sets up functional techniques at the perimeter of the network to secure data and resources. Traffic Director is a managed control stage for application networking. Traffic Director allows to deliver global, highly available services with ultra-modern application networking abilities such as traffic management and observability.

End-to-end Encryption (E2EE)

End-to-end encryption (E2EE) is a method of secure communication that prevents third parties from accessing data while it is transferred between two systems or devices. E2EE ensures data security at both ends and guarantees secure transmission throughout the process.

Screening at the Far-end

Far-end safety protocols secure the system from external threats, resolving issues before they reach the system boundaries. This ensures uninterrupted services and facilitates hassle-free data transmission and communication.

Scalability & Redundancy

RUDDER offers a highly scalable solution for fast-growing industries to manage the rising number of users effectively. The system's redundancy ensures the availability of secondary servers, which are replicas of the primary server and can seamlessly take over in case of a primary server failure.

Proactive Monitoring

Proactive monitoring involves and encompasses multiple observations within the system.

Log analysis is the process of reviewing, interpreting, and understanding computer-generated records. It helps track real-time entries and data logs for smoother management.

Resource optimization is the process of allocating and managing network resources in the most efficient way possible to maximize system performance.

Vulnerability management is the process of identifying, assessing, reporting, and addressing security threats and known vulnerabilities in systems.