Built-in Security with Join Network-as-a-Service

Stay in compliance with our no-compromise network security, from infrastructure to Zero Trust architecture.

In the ever-evolving landscape of networking being sold as a service, Join Network-as-a-Service (NaaS) offers unparalleled flexibility, scalability, and efficiency. By shifting the burden of network management and operations to Join, organizations can focus on their core business while leveraging cutting-edge networking technologies. However, all enterprises require the best possible security capabilities across the network and, with Join, there are no compromises when it comes to security. Join completely complements and enhances all existing security mechanisms in place.

With Join NaaS enterprises can embrace innovation without compromising on security. By harnessing the power of automation and advanced AI-driven analytics, organizations can proactively identify and respond to security threats in real-time and fortify their networks against evolving cyber threats.

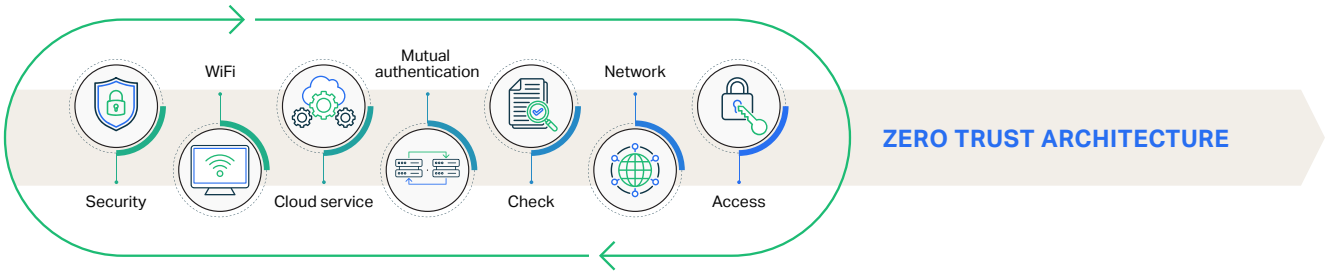
A MORE HOLISTIC APPROACH TO NETWORK SECURITY, ZERO TRUST, AND AIOPS —

There are many aspects associated with securing networks and understanding the threats, vulnerabilities, and best practices of this new way of deploying, managing, and operating networks. From data integrity to access control, and threat detection to compliance, each aspect demands careful attention to ensure the confidentiality, integrity, and availability of critical enterprise resources.

The foundational principles of NaaS security include authentication and authorization to safeguard the network and robust security policies and procedures to mitigate risks and ensure regulatory compliance.

Join designs and implements a holistic security framework that protects against threats and minimizes the risk of unauthorized access. Zero Trust security for user authentication, least privileged access, and continuous authentication ensures that access to the network is controlled. Once the network is operational, real-time threat detection with oversight of network activity and anomaly detection is utilized to protect the network. Enhanced network protection is enabled by micro-segmentation by device and/or user and strict security policies help isolate and protect sensitive information while guaranteeing the integrity of data.

Security is a key consideration for organizations embarking on the NaaS journey, and with Join NaaS enterprises can embrace innovation without compromising on security. By harnessing the power of automation and advanced AI-driven analytics, organizations can proactively identify and respond to security threats in real-time and fortify their networks against evolving cyber threats. With this holistic approach to NaaS security, organizations can unlock the full potential of this revolutionary networking approach while safeguarding their digital assets against a myriad of threats.



ROBUST SECURITY FEATURES OF JOIN NAAS —

- Network/Service Microsegmentation
- Strictly Enforced Wireless Access Point Isolation
- Identity-based Authentication for Network Access
- DNSSEC and DNS over TLS (DOT) Protection
- Restricted access to Network Equipment for Management
- Malicious Threat Filtering
- IoT Security
- Integration with Industry-Leading Enterprise Cybersecurity Solutions

Don't leave your network vulnerable to cyber threats. Partner with Join and fortify your networks with our cutting-edge NaaS security solutions.

join™

Visit joindigital.com/security-guide to learn about our NaaS security solution.

Or contact sales@joindigital.com to get a guided walkthrough.