



HUB Networks and Security for Managed Service Providers





Hub Networks and the Security of Managed Service Providers

HUB Networks (HUB) is an advanced telecommunications enterprise that empowers business leaders with a reliable digital connectivity infrastructure to bring innovative services to Puerto Rico, the Caribbean, and the Eastern seaboard of the United States. Hub offers services to critical clients ranging from banking institutions and electricity utilities to local municipalities and small businesses. Businesses require essential services that include cybersecurity protection measures to protect and power their data and the sensitive data of their customers. HUB and other Managed Service Providers (MSPs) who integrate XQ's zero-trust technology are highly sought after in the market. They provide compliant and highly secure services that are more reliable, faster, easier to manage, and increase the RPU of their client base. This is a game-changer for MSPs focused on providing internet connectivity like HUB.

“On Average, MSPs Have Seen A 32% Increase In Revenue Through Offering Security Services”

– Vanson Bourne, 2021

What happens when MSPs fail to offer secure services to protect their clients from malicious actors?

Successful attacks against companies and governments have increased exponentially, suggesting that either service providers lack the tools to protect their clients or cybersecurity measures deployed are ineffective. In June of 2020 alone, Luma Energy LLC, Puerto Rico's most prominent power supplier, suffered a cybersecurity attack before a fire broke out in San Juan ([The Wall Street Journal](#)). The disruption to Luma's network gave hackers access to customer information and made it impossible to report power outages. As a result, thousands of people experienced a power outage for days. MSPs expose their customers to liability and financial loss. Such incidents risk the reputation of MSPs and their ability to be marketed as reliable service providers. Cybersecurity has become an essential component for MSPs to provide reliable services to their customers.



“This year, 56% of SMBs would hold both their provider and themselves accountable in the event of a cyberattack, compared to 39% saying so last year.”

— Vanson Bourne, 2021

Cybersecurity risks that MSPs and their clients face without the proper cybersecurity protections:

- Loss of services
- Loss of client information
- Ransomware
- Increasing liability costs
- Compromised analytics
- Compliance violations
- Loss of income

“Nine Out Of Ten SMBs Said They Would Consider Using An MSP Or Switching MSPs To Find The ‘Right’ Cybersecurity Solution”

— Vanson Bourne, 2021

How does XQ’s Zero-Trust Secure Gateway work to enhance security beyond the network?

XQ has partnered with HUB to bring XQ’s Zero-Trust Gateway as a software-defined replacement for VLAN and VPN. The XQ platform, combined with the Gateway, secures any data from any device, anywhere, and across any shared networks.

XQ's zero-trust secure Gateway enhances protection beyond the network by encrypting individual data at its creation.

Two major differentiation benefits are:

- independent Security Systems for each client on Shared Networks
- independent identity systems for each client on Shared Networks



XQ's plug-and-play Zero Trust Gateway is deployable on devices as small as a Raspberry Pi, an IoT sensor, or a more highly powered server. Our approach allows data to travel across any series of networks from any device, origin, and to any destination safely. Data travels through XQ's secure gateways, encrypting outgoing traffic and decrypting or routing incoming traffic, creating end-to-end encrypted communication channels, and ensuring enhanced reliability and privacy. Given that traditional cybersecurity measures have focused on protecting the entire network, hackers who successfully infiltrate a network gain access to every piece of data. However, XQ's Zero-Trust technology looks beyond traditional approaches to cybersecurity. XQ uses segmented data wrapped with meta-tags to employ authenticated endpoints and incremental event logging systems that provide a data-centric Zero-Trust framework for transmission.

XQ does not stop attacks, but it frustrates hackers as the difficulty of decrypting individual data packets and reconstitution becomes overwhelming. Even if a network or a communication pipe is compromised, the possibility of complete data exfiltration is impossible.

XQ's Secure Virtual Local Area Networks (VLANs) solution is a software-based alternative to hardware VLANs available today. As a breakthrough, XQ's Zero Trust technology allows secure data transmission through Layer 3 IP channels and over Layer 2 VLAN channels managed through a software web interface. Although the traditional use of hardware-based VLANs has allowed the transmission of large amounts of data over a private virtual channel, such hardware-based networks are expensive, difficult to manage, and protect the network link rather than the data. XQ's software-based technology allows the secure transmission of data without risks. Without XQ's Zero Trust technology, communication pipes processing data from the edge and between links are vulnerable to unauthorized infiltration, mismanagement on-site and fundamentally leave the data exposed once it reaches its destination through various communication networks.

Benefits of integrating XQ's Zero Trust Gateway software for MSPs:

- Market differentiation
- Increased RPU
- Simplified management



- Better performance
- Remote management
- Improved safety
- Cost Reductions
 - Less digital maintenance
 - Less physical maintenance
 - Lower FTE
- Increased ROI on existing infrastructure
- Prevent data leakage
- Regulatory compliance
- Protection of citizen personally identifiable information
- Increase in system stability and reliability

**“In 2 Years Data Protection Will Be The #3
Revenue Generator For MSPs”**

— Acronis 2021

MSPs leading the market provide reliable and affordable services. Without the proper integration of cybersecurity measures, clients relying on service providers are left vulnerable to risks and losses associated with malicious events. XQ's secure Gateway empowers data to pass between networks securely, protecting users from catastrophic threats.

By partnering with XQ, Hub is now offering Puerto Rico Electric Power Authority (PREPA), the island's largest electricity supplier, secure services to protect against communication data breaches. As thousands of people depend on PREPA's electricity services, system failures because of data breaches are catastrophic for the enterprise and those living on the island.

By using XQ's secure zero-trust Gateway, Hub is empowering PREPA to meet the electricity needs of their clients by having complete control of their data and, therefore, guaranteeing reliable electricity services. By partnering with XQ to offer zero-trust data protection, Hub is positioned to grow their managed secure services business



throughout their existing customer base and use it as the basis for expanding their client base.

“On Average, MSPs Have Seen A 32% Increase In Revenue Through Offering Security Services”

— Vanson Bourne 2021

[Apply to become an XQ partner to grow your Managed Secure Service practice today!](#)

Contact Us

We'd love to hear from you!

<http://xqmsg.com>

support@xqmsg.com