Remote and Roaming User Security

The number of remote and roaming users has increased exponentially in just a few short years.

Key benefits

- Broad, reliable security coverage across all ports and protocols
- Security protection on and off network
- Rapid deployment and flexible enforcement levels
- Immediate value and low total cost of ownership
- Single dashboard for efficient management

LOCKNET
AN EOJOHNSON COMPANY

locknetmanagedit.com » 844-365-4968

The way people work has changed dramatically. So have the risks.

Today, it's estimated that 40% of employees are working outside of their central office and often outside of its network's security. Concurrently, applications that once resided on premise have become more flexible and accessible through the cloud. As a result, businesses are having to adopt direct internet access to deliver greater flexibility to meet the demands of this new virtual work model. However, direct internet access presents a new set of security challenges and leaving businesses to figure out how to extend security to cover this new norm.

Security today needs to be on the move.

The increase of the virtual workforce is driving transformation in the way enterprise and networking security are delivered, leaving the centralized, on-premise security model to become less practical. But there is a way to better protect users, the growing number of devices they carry as well as their data.

Protect users anywhere they work.

Remote and Roaming User Security by Locknet Managed IT is a cloud-native security platform that secures internet access and cloud application usage anywhere users go. Remote and Roaming User Security unifies firewall, secure web gateway, DNS-layer security, cloud access security broker, and threat intelligence solutions into a single platform to help businesses of all sizes secure their network. As more organizations embrace direct internet access, Remote and Roaming User Security makes it easy to extend protection to your virtual workforce. By enforcing security at the DNS and IP layers, Remote and Roaming User Security clocks requests to malware, ransomware, phishing, and botnets before a connection is even established and before they reach your network or endpoints.