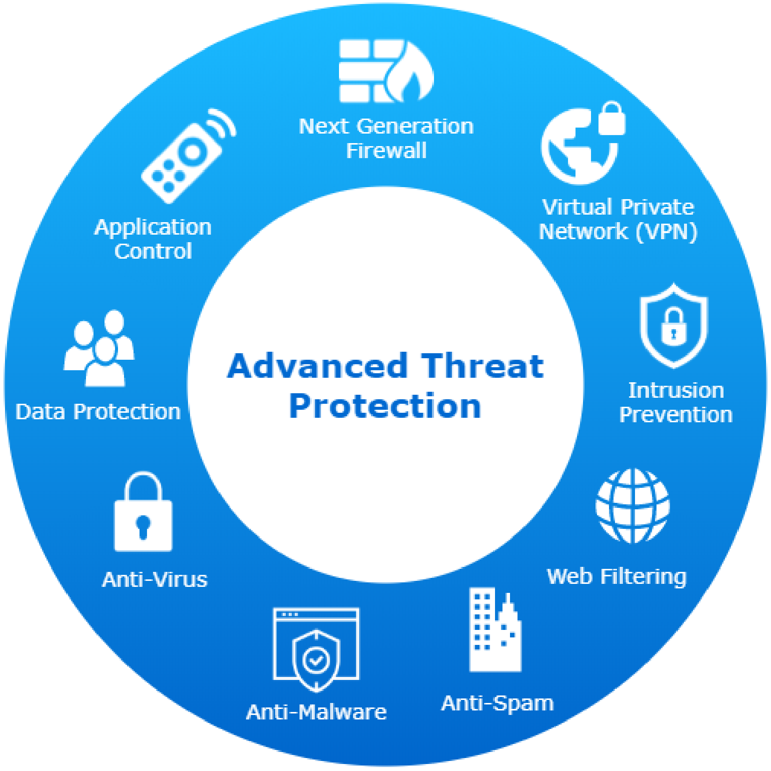
FirstComm℠

MANAGED SECURITY

UNIFIED THREAT MANAGEMENT

Today's organizations can't be too careful when it comes to network security, access, and connectivity, especially when customer data and regulatory compliance are at risk. Many layers of security are required to keep attackers out and to keep sensitive data from falling into the wrong hands. At the same time, achieving strong security shouldn't come at the expense of overloading busy network staff or affecting application or network performance. Unified threat management (UTM) systems consolidate security technologies into a single, dedicated device with a single management interface.



Virtual Private Network (VPN) - VPN creates a private, encrypted "tunnel" through the Internet.

Intrusion Prevention System - Network's watch-dog, looking for patterns of network traffic and activity & records events that may affect security.

Application Control - It gives visibility into applications that generate traffic on the network, along with the ability to control those applications.

Data Loss Protection - It looks for confidential, proprietary, or regulated data leaving the network. It can prevent the accidental "leakage" of data.

Anti Spam - Spam filtering can block threats like viruses and bots, which arrive in users' email boxes.

Anti Malware - It applies protection to file transfer protocol (FTP) traffic, instant messaging (IM), and web content at the network perimeter.

Web Filtering - It blocks traffic to and/or from a network by IP address, domain name/URL, type of content (for example, "adult content") or payload.

Anti Virus - It protects against the latest viruses, spyware, and other content-level threats. It also uses advanced detection engines to prevent both new and evolving threats