Making security manageable

Cyberattacks are increasing in frequency and sophistication.

Data breaches can be costly and can negatively impact an organization’s reputation.

Cybercrime damages around the world continue to skyrocket.

Organized cybercrime is a real threat to the enterprise:
80% of cybercriminals are affiliated with organized crime.

Network segmentation contains cyberattacks.

Network segmentation is an accepted best practice by security experts and industry regulators.

DHS: network segmentation is a necessary step in an organization’s network security strategy.

Forrester recommends the Zero Trust Model of Cybersecurity: external and internal networks can’t be trusted.

Firewalls can be used to segment the network.

Firewall policies are a must-have to ensure agility and security, and are an essential part of network segmentation.

Security policies:
- Will eliminate the threat of going too much access to the network, or giving the wrong people access they don’t need.
- Having strong security policies in place will tighten the overall security posture.

In the hybrid network:
Firewall policies are very complex to manage, and as a result, segmentation is too complex to manage.

- An enterprise could easily have hundreds of firewalls.
- Many organizations are managing firewall policies and network segmentation manually, which can lead to misconfigurations.
- Misconfigurations can widen the attack surface and result in security holes.

Visualization and enforcement segmentation from a single console across vendors and platforms.

Keep your organization protected against today’s sophisticated cyber threats.

Maintain continuous compliance with industry regulations.

Tighten the overall security posture of the network.

Avoid exposing unnecessary security risks.