Leverage Micro-segmentation To Build A Zero Trust Network

Micro-segmentation through network virtualization enables improved agility, security, and compliance

Both external attacks and internal incidents pose credible threats

Most common sources of security incidents over the past 12 months

- External attack: 74%
- Internal incident: 21%

The average organization has experienced three to five security incidents within the past year.

Organizations are overconfident in their security capabilities

Self-assessed computing infrastructure security rating

- 1 to 4 rating: 13%
- 5 to 6 rating: 7.6 avg.
- 7 to 10 rating: 84%
- Extremely vulnerable: 1%
- Extremely secure: 1%

Despite high security ratings, just 23% have full confidence in IT’s ability to stop data breaches.

Network virtualization enables micro-segmentation

Most important attributes of network virtualization

- Micro-segmented security controls: 21% (Very important)
- Improved automation: 21% (Very important)
- Faithful representation of networks in software: 23% (Very important)
- Management by business units: 26% (Very important)
- Horizontally interconnected components: 27% (Very important)

Network virtualization yields improvements in security, agility, and compliance

Top-ranked business benefits of network virtualization

- Improve security: 58%
- Easier network segmentation: 48%
- Improve agility/speed: 44%
- Better meet data compliance standards: 16%

Micro-segmentation provides the network visibility and control needed for making security ubiquitous throughout the network. Organizations can more effectively control and protect their data as they move toward building a Zero Trust model.

Methodology

For this study, Forrester conducted an online survey of 210 IT and risk and compliance decision-makers at organizations in the US, EMEA, and APAC with 500 or more employees.

Source: A study conducted by Forrester Consulting on behalf of VMware, June 2015