As modern IT environments become more distributed, the attack surface and corresponding risk from them increases. Organizations can’t afford to have any blind spots and must leverage data from the network and real-time analysis to enable their zero trust initiatives.

The Importance of NETWORK VISIBILITY AND ANALYTICS

Leveraging SD-WAN for Zero Trust Initiatives

Applications are distributed across private data centers, multiple public clouds, and edge locations. In addition, employees now split their time between the office and home or remote locations. As a result, organizations now have a much larger attack surface to defend. The dynamic nature of modern application environments means services are spun up and down in seconds and applications can be easily moved.

Highly Distributed Environments Create Risk

- 86% currently using two or more public cloud services to some extent (IaaS and/or PaaS).
- 57% state that more than half of their workforce will be roaming users in 24 months.
- 62% cite that 50% or fewer of their production applications/workloads are running in the public cloud.

To overcome the challenges created by the larger attack surface of highly distributed environments, organizations are implementing zero trust initiatives (“never trust, always verify”) to better protect their assets.

More than half (46%) of the organizations surveyed reported having limited success or bumps in the road during deployment.

- The vast majority of organizations (81%) reported that having end-to-end visibility of their IT environment is either very important or critical."
- "The vast majority of organizations (81%) reported that having end-to-end visibility of their IT environment is either very important or critical." - Bob Laliberte, Enterprise Strategy Group Principal Analyst

Visibility and Analytics Are Key Capabilities

- 55% said they identify and inventory all devices on the network.
- 48% said they use analytics to identify anomalous behavior.
- 44% reported their starting point was network segmentation.
- 42% reported analytics was their starting point.

Conclusion

Modern IT environments are highly distributed. As such, these environments are faced with an increased attack surface and increased risk to the business. To ensure a secure zero-trust environment, organizations are adopting deep packet inspection and analytics to monitor and control access to resources that are distributed across various locations. This enables organizations to implement a zero trust strategy that provides for a more secure environment.

© 2023 TechTarget, Inc. All Rights Reserved.