Emphasizing Prevention with Microsegmentation

Security Teams Struggle to Keep Pace with Modern Environments

- Zero trust strategies are being prioritized to address these challenges, modernize security, enable the business, and reduce incidents. While zero trust requires the granular policies microsegmentation supports, the practice has not been widely deployed to date, despite its ability to support business and security use cases.

- Microsegmentation tools should automatically recommend policies based on the visibility they provide. Vulnerability information can highlight the attack paths posing the greatest risk to the organization. Overlaying visibility at the application layer into processes and related services identities, supported by analytics, provides context to help establish a baseline for normal behavior and detect anomalous activity.

- Microsegmentation solutions should address not only public cloud and on-premises locations, but cloud-native application architectures and development practices. This typically requires support for both agent-based and agentless deployment models.

- The expansion of application environments makes cybersecurity more difficult, but cloud-native application architectures and development practices are currently using microsegmentation. For all these reasons, organizations should recognize microsegmentation as a critical component of their zero trust strategy and prioritize tools that deliver deployment flexibility, deep visibility, and ease of use.

- Top five results of security incidents
  - 51% of respondents say cybersecurity has become more difficult
  - 48% of generations are using a hybrid on cloud model today
  - 27% are planning to adopt over the next 2-3 years

- Top five use cases for microsegmentation
  - 53% of organizations are secondary to current challenges
  - 39% of respondents say cybersecurity has become more difficult
  - 37% of respondents say cybersecurity has become more difficult
  - 32% of respondents say cybersecurity has become more difficult
  - 21% of respondents say cybersecurity has become more difficult

Prevention through Zero Trust and Microsegmentation

Zero trust is a strategy that recognizes the increased number of challenges, coupled with more visibility into and control over data, and digital assets. To address these challenges and drive the business forward, Zero trust segment the network into smaller, isolated domains to reduce the attack surface and enforce more security at the user, device, session, and application layer.