Enterprise Strategy Group | Getting to the bigger truth.™

Emphasizing Prevention with Microsegmentation

Cybersecurity has become more difficult as applications become increasingly distributed and the threat landscape continues to evolve. The negative impacts of successful attacks require a preventative approach via zero trust, with microsegmentation uniquely positioned to ensure that the impacts of an incident are limited. To foster broader adoption, solutions supporting microsegmentation must be easy to use and straightforward to deploy, generating accurate, automated policy recommendations.

Security Teams Struggle to Keep Pace with Modern Environments

Application environments are more complex than ever, even as the threat landscape continues to evolve. Further, security incidents can have a variety of negative impacts on security teams, IT teams, and the business overall. This makes ensuring the security and availability of applications a high priority for nearly all organizations.

» The expansion of application environments makes cybersecurity more difficult

88%

support at least 100 business applications.

48%

of organizations **are using a hybrid cloud model today.**

27%

are planning to adopt one over the next 12-24 months.

59%

of respondents say cybersecurity has become **more difficult** than it was 2 years ago.

» Top five results of security incidents

51% Lost productivity

39% Significant IT time/personnel needed for remediation

37% Disruption of business process

31% Disruption of business applications or IT system availability

21% Breach of confidential data

» Application availability and security is a top priority

Ensuring secure & available apps is our TOP cybersecurity priority, 33%

Ensuring secure & available apps is a TOP 3 cybersecurity priority, 54%

Prevention through Zero Trust and Microsegmentation

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.

» Zero trust adoption

89%

have implemented or begun to implement zero trust across the organization and/or for specific use cases.

» Key business drivers for zero trust adoption

51% Modernizing cybersecurity program

43% Reducing the number of security incidents

35% Supporting digital transformation

34% Accelerating cloud adoption

30% Preventing data exfiltration

» The importance of microsegmentation is well understood, but adoption is somewhat limited today

36% of organizations **are currently using microsegmentation.**

91% **of organizations plan to use microsegmentation** in the next 12-24 months.

» Microsegmentation can address both business and security use cases

PREVENTING LATERAL MOVEMENT

Microsegmentation can help prevent threats that slip through initial defenses from compromising additional systems and establishing persistence.

ACCELERATING CLOUD MIGRATION

Microsegmentation solutions provide visibility into workload relationships and behaviors that allow organizations to ensure application dependencies are maintained and policies are correctly applied as resources are migrated to the cloud, without impacting availability.

ENSURING COMPLIANCE

Microsegmentation can help fulfill compliance requirements by reducing the scope of resources subject to regulations and more efficiently providing visibility across the environment during the audit process.

IMPROVING INCIDENT RESPONSE EFFICIENCY

Microsegmentation can quickly quarantine infected assets to prevent attacks from spreading once remediation efforts begin.

Deployment Flexibility, Deep Visibility, and Ease of Use Are Critical for Microsegmentation to Be Successful

While needs will vary from one organization to the next, there are some capabilities to prioritize in microsegmentation solutions that will benefit most organizations.

DEPLOYMENT FLEXIBILITY

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.

DEEP VISIBILITY

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. Overlaying vulnerability information can highlight the attack paths posing the greatest risk to the organization.

EASE OF USE

Microsegmentation tools should automatically recommend policies based on the visibility they provide. Management should be intuitive and highly visualized, with policies dynamically updated as the trustworthiness of applications change.

The Bigger Truth

Application environments have changed dramatically since the first microsegmentation tools were deployed ten years ago. Environments are more distributed and dynamic, and attackers are more motivated than ever before to target these valuable resources. 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.

LEARN MORE

TRUEFORT

Source: ESG Complete Survey Results, Network Security Trends in Hybrid Cloud Environments, December 2021.