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.



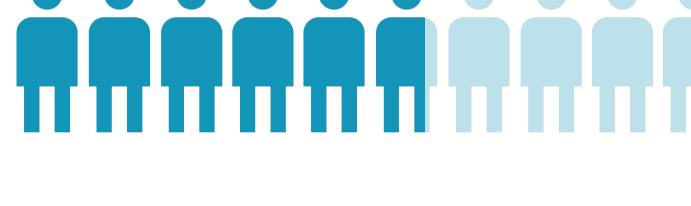
generating accurate, automated policy recommendations.

48%

27%

of organizations are using a hybrid cloud model today.

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



of respondents say cybersecurity has become

59%

more difficult than it was 2 years ago.

>> Top five results of security incidents



Lost productivity

51%



personnel needed for remediation

Significant IT time/



business process



availability



Breach of

confidential data

>> Application availability and security is a top priority



33%

Ensuring secure & available apps is our **TOP** cybersecurity priority,

Ensuring secure & available apps is a <u>TOP 3</u> 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.

89%

>> Zero trust adoption

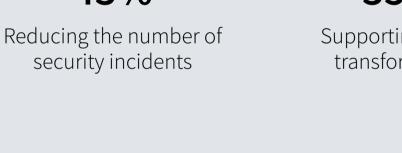
have implemented or begun to implement zero trust

>> Key business drivers for zero trust adoption

across the organization and/or for specific use cases.



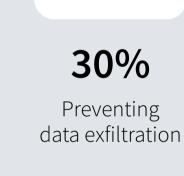








>> The importance of microsegmentation is well understood, but adoption is somewhat limited today



36% 91% of organizations of organizations plan to



PREVENTING LATERAL

MOVEMENT

>> Microsegmentation can address both business and security use cases

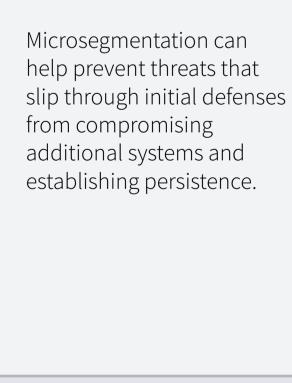
are currently using

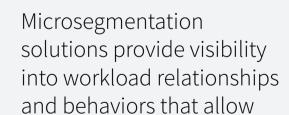
microsegmentation.



use microsegmentation

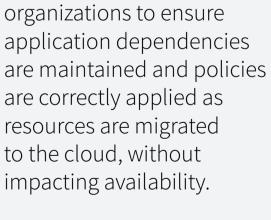
in the next 12-24 months.



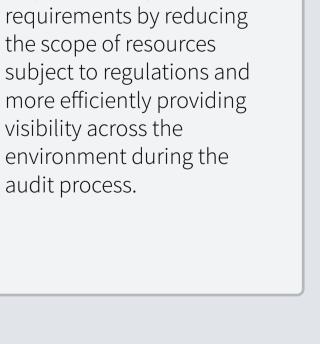


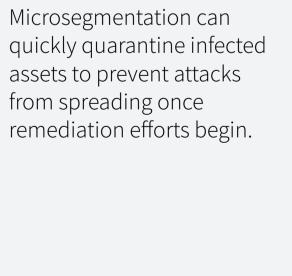
ACCELERATING CLOUD

MIGRATION









IMPROVING INCIDENT

RESPONSE EFFICIENCY

resources are migrated audit process. to the cloud, without impacting availability. Deployment Flexibility, Deep Visibility, and Ease of Use

but cloud-native application architectures and development practices. This typically requires support for both agent-based and agentless deployment models.

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



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

DEEP VISIBILITY

EASE OF USE

Management should be intuitive and highly visualized, with policies dynamically updated as the

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

Microsegmentation solutions should address not only public cloud and on-premises locations,

trustworthiness of applications change.

Microsegmentation tools should automatically recommend policies based on the visibility they provide.

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.



