COLORTOKENS

SOLUTION BRIEF

3 Tenets of a Successful Microsegmentation Project

Microsegmentation has gained mainstream adoption as the security architecture to address the most common and latest cyberattacks. When implemented effectively, it helps organizations quickly prevent propagation of cyberattacks such as ransomware, insider exploits and data exfiltration. It also serve a critical role in meeting organization's compliance requirements. Despite the market adoption, many organizations struggle to operationalize microsegmentation in their environments. Here are three principles organizations should abide by to ensure a successful microsegmentation project:

Always Have Full Visibility of Applications

The network and security teams responsible for implementing microsegmentation and other cybersecurity solutions often differ from the team managing applications. Hence, the security team do not have visibility into application architecture, dependencies, and the services or data it must access. This lack of visibility is by far the most common barrier to timely and successful microsegmentation projects. Some of the critical information the security team rely on includes:

- Application asset details including association with other applications and users
- Acceptable and standard communication to/from applications
- Underlying vulnerabilities or exploits that must be considered

Security teams are heavily dependent on these details to not only generate segmentation policies but also methodically plan organization's microsegmentation or Zero Trust journey.

To overcome this challenge and to avoid being bogged down, organizations should consider microsegmentation solution that addresses the following:

- Self-learning capabilities of applications to further simply future deployments
- Automatically categorize and classify applications at scale
- Identify vulnerabilities, exposures, and attack surfaces for applications
- Integrate with existing asset management tools
- Integrate with existing enterprise workflows to simply asset onboarding process
- Generate context-based application communication map based on organization's unique business requirements

Divide and Conquer

Organizations deploy applications across a wide range of environments ranging from datacenters and hybrid to cloud and microservices. The applications themselves also exhibit various uses cases such as standalone apps, multi-tiered apps across several datacenters, and infrastructure apps that power the business across departments as well as external partners or customers. The attempt to create a single segmentation strategy across all these use cases and unique requirements often fails. The resulting policies are often overly complex, and at the same time ineffective since many rules are not relevant for a select application or department.

A practical way to tackle this challenge is to divide and conquer. Organizations must map business requirements to logical application segments. Hence, relevant policies should consider specific applications, its use case and business requirements it supports. For organizations to take this approach, however, they need to do their "homework" or implement microsegmentation solution that supports:

- Flexible logical segmentation framework based on organization's unique business requirements
- Identify different segmentation types that support the business (e.g., applications, environments, and locations)
- Hybrid infrastructure such as datacenter/cloud applications, users, OT, containers and cloud

Eliminate Application Downtime with Simple Policies

Any policies, simple or complex, can be enforced. However, in practice, many overly complex policies are not enforced. In microsegmentation deployments, complex policies are often used for passive monitoring purposes since enforcement can result in application outage. While monitoring provides valuable insight, it doesn't protect against the propagation of the latest cyber-attack in real-time.

Despite their best efforts, security teams often fall into the trap of creating very complex policies. They often take an ad hoc and manual approach to creating policies or aim to cover all communication and applications – both approaches leading to gaps in policies. Other reasons for falling into this trap stems from past experiences in which they enforced policies without sufficient testing or prematurely deploying across entire organization, resulting in flood of support calls.

Organizations can avoid this pitfall and successfully implement segmentation controls by considering microsegmentation vendor who can:

- Automate policy management through continuous learning of traffic flows, applications, and other security parameters
- Select microsegmentation solution that supports continuously test and validate policies before enforcement
- Automatically update policies with changing network and application environments
- Enforce policies progressively

Path to a Successful Microsegmentation Project

Microsegmentation is a powerful architecture to protect organizations from modern cyberattacks. To avoid delays and in some cases postponement of the deployment, organizations require careful planning and execution. It is important for organizations to keep the top 3 tenets in mind to avoid falling into common traps others have encountered – application visibility, divide and conquer, and simple policies. Accordingly, organizations should partner with the right microsegmentation vendor to help overcome some of the common challenges and ensure your strategy and deployment plans are successful.

Simplifying Your Journey to Zero-Trust Architecture

ColorTokens is a leader in delivering innovative and award-winning zero-trust cyber security technology solutions such as network micro-segmentation, endpoint hardening and whitelisting, cloud and container security, and zero-trust network access. ColorTokens is a US corporation headquartered in Silicon Valley, and has approximately 400 employees world-wide, with offices in the United States, the United Kingdom, the Middle East, and India serving a diverse client base in both the public and private sector. For more information, please visit **colortokens.com.**