EMA IMPACT BRIEF

COLORTOKENS

ColorTokens' Microsegmentation Brings Zero Trust to Virtualized Containers

Abstract

ColorTokens, an American company specializing in zero trust cybersecurity, recently announced the addition of microsegmentation for virtualized containers to their portfolio of capabilities. The new feature provides security for containerized workloads running in private data centers as well as public cloud environments, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

Background – Virtualized Container Security Challenges

Traditional zero trust segmentation strategies work by IP address, but virtualized containers require a more granular approach. Containers running in private data centers as well as the cloud need to be isolated from each other on a per-microservice level to prevent lateral movement of threats. Because of this extra granularity and multiple microservices running on a single IP address, implementing network segmentation for containerized workloads can be complex and challenging, requiring a well-designed and well-implemented microsegmentation strategy.

In response to these challenges and the growing adoption of virtualized containers, ColorTokens announced microsegmentation capabilities for containers as part of their zero trust security platform. This solution provides organizations with enhanced security, improved visibility, and more secure container management.

Key Ramifications

The following are the key ramifications of ColorTokens' release of their virtualized container security offering:

- Discovery & Visualization – Automatic discovery and classification of microservices allows better visibility of your organization's true attack surface. This enables customers to discover containers that may have been created without proper authorization and identify containers that are no longer needed, which can help reduce the attack surface.
- Learning & Policy Recommendation – By observing API usage and not network traffic, ColorTokens can make better, more intelligent decisions regarding security policies and access control.
- Zero Trust Enforcement – ColorTokens' container microsegmentation solution is based on a zero trust security model, which means it enforces strict access controls and verifies every user and device attempting to access a container. This approach helps organizations prevent security breaches by minimizing the attack surface and reducing the risk of lateral movement of threats.

Overall, ColorTokens' solution can help organizations improve their security posture, enhance control over their network, and achieve better visibility of their true virtualized container footprint.

EMA Perspective

ColorTokens' container microsegmentation solution provides organizations with enhanced security, improved compliance, and simplified container management. By using machine learning to analyze container behavior and enforcing zero trust access controls, the solution can help organizations stay ahead of emerging security threats and protect their containerized workloads more effectively.

EMA believes that embracing a zero trust security model is critical for securing virtualized containers because of the unique challenges containerized workloads present. Zero trust security for containers provides granular access controls, auditing, and monitoring capabilities, reducing the attack surface and minimizing the risk of unauthorized access or lateral movement of threats. ColorTokens is desperately needed for today's virtualization-focused enterprise.