COLORTOKENS™

Be Breach Ready

Xshield ENTERPRISE MICROSEGMENTATION PLATFORM

Fast results & stronger security, with minimal configuration & maintenance effort

Security leaders want microsegmentation to protect their enterprise from cyberattacks, but using the wrong tool can create friction between the infrastructure, security, and application teams, inflating policy complexity and pushing measurable results years down the road, often times with several disruption events.

At ColorTokens, we reimagined what microsegmentation should be. Xshield delivers all the capabilities you expect from leading solutions – application, process-based, cloud-native, IT and even OT/IoT segmentation. However, our mission is to make microsegmentation faster and simpler to deploy and enforce. We focus on removing the adoption and implementation barriers associated with implementing enterprise-wide microsegmentation so you can successfully defend your enterprise.

Customer value	Metrics	ColorTokens' Innovation	Other Vendors
Speedy implementation & ease of maintenance	• 10-minute deployment • 60 minutes to pan-enterprise visibility of assets & traffic • 0-minute maintenance of agents	• Integrated with already deployed EDR systems—no additional agents needed on workstations or servers • Supports CrowdStrike, SentinelOne, and MDE	• New agents (or segment servers) must be qualified, deployed & maintained • Some Install new proprietary firewall on every host • Others: ACL configuration on switches
Continuous awareness & mitigation of up-to-date lateral attack tactics	• 48 hours for initial lateral movement risk assessment report • 24-hour updates for MITRE lateral attack TTPs & CISA threat advisories	• Has continuous integration and updates in the admin console on the latest threat advisories MITRE TTPs (Lateral Movement attack Tactics, Techniques and Procedures) TTPs and CISA Threat Advisories	• Not aware of lateral movement TTPs • Manual effort for the SOC team to analyze threat advisories and TTPs
Immediate risk reduction for fast ROI	**60-90 days to**: • Full policy enforcement • 50%-80% breach impact reduction • 90% of MITRE lateral movement attack TTPs addressed	• Progressively enforce hierarchical zero-trust policies at the host level, independent of apps • Security team sets enterprise-wide policies for the most exploited, inactive, and privileged ports • AI-assisted environment interrogation and policy definition	• Must define all policies for a segment. • Cross-departmental policy review and long validation cycles can take weeks for each enterprise application • Months (to years) to enforcement
Zero-disruption to business processes during implementation and enforcement	• Low (< .1%) likelihood that the implemented traffic policies will cause a significant outage • 0 disruption/outage resolution hotline calls	• 30 days of historical traffic simulation checks • Real-time traffic policy testing	• Simulation is limited to a few days and not real-time, allowing disruption • Testing specific policy changes requires unsecuring the entire asset
Reduction in tool proliferation, simplification of staffing & training, coherent security policies	• Unified, single-pane-of-glass visualization and policy definition enforced for all environments--IT, IoT, OT, containers, legacy, and Cloud	• Agentless Gatekeeper for OT, IoT, and Legacy OS • Service mesh integration for container microsegemtation • Agent (EDR or Xshield) for servers & workstations • Native cloud controls for cloud workloads and serverless compute	• ACLs on switches for OT segmentation require hardware dependencies & potential upgrade costs • CNI integration for containers-L3 controls, not API level

ColorTokens, Inc. Confidential and Proprietary