COLORTOKENS

DATASHEET

Xshield

Zero Trust Microsegmentation

Simplifying Your Journey to Zero Trust Microsegmentation

Microsegmentation Protects Against Modern Cyberattacks

Perimeter security will eventually be breached. The speed at which this occurs is dependent on the attackers' determination and the latest techniques employed. Based on this fact, the zero-trust security approach assumes all internal users, assets, and applications are not to be trusted. To increase resiliency and protect critical systems and data, organizations must group them into granular microsegments with polices that restrict traffic to and from each microsegment. The policies, while ensuring valid traffic are allowed to pass, prevent the propagation of malware or ransomware that has slipped through the perimeter defenses, drastically slowing down or stopping the cyberattack. Organizations can also detect and stop lateral movement of data before it can lead to exfiltration.

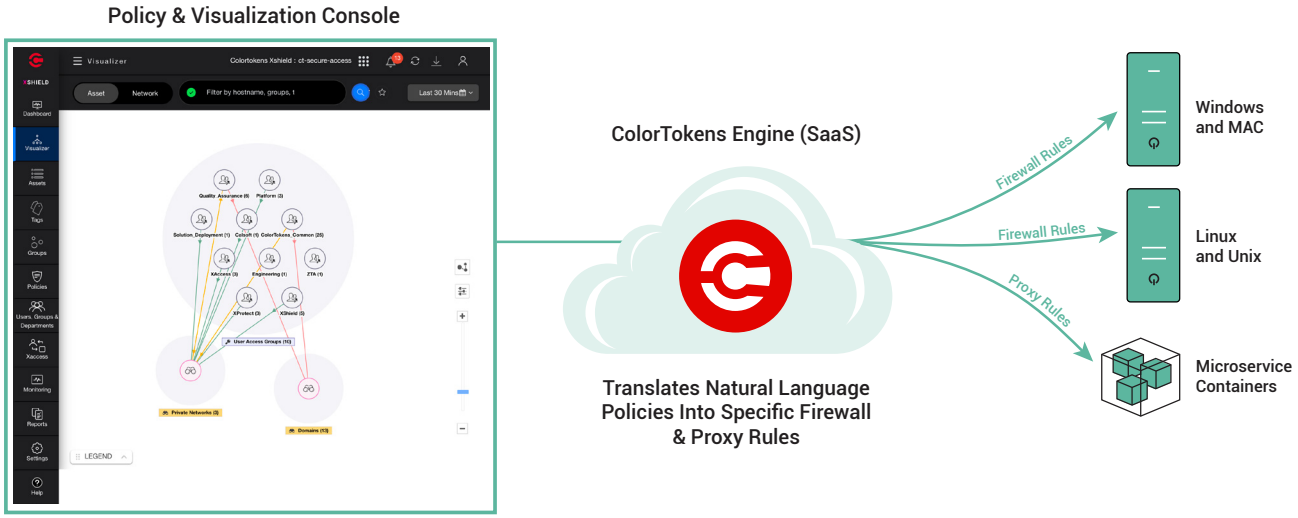
Discover, Visualize and Monitor Your Total Environment

Xshield's visualizer shows servers and applications running on any infrastructure: on-premise data centers, cloud deployments, and containerized microservices applications. It shows the traffic occurring between your internal assets, as well as to the external internet. Color-coded lines indicate traffic that is in policy and out-of-policy.

Unified Policy Management

The policy management console lets you define microsegmentation policy for users, both remote and on-campus, and all asset types. You write policies once, using natural language, and the policy engine translates them into firewall rules for your servers, and sidecar proxy rules for containerized microservices.

Write Policies Once, Deploy Everywhere



Automated Microsegmentation Implementation

Identifying all your assets to configure microsegments is a daunting task. Configuration Management Databases (CMDB) are often incomplete or inaccurate. To solve this, Xshield scans your environment to discover assets and allows you to classify and tag them using automated and manual methods. It uses heuristics to recommend polices based on communication traffic in your normal business processes. Your team doesn't have to spend days or weeks trying to infer appropriate policies. In a very short time, you can begin enforcement to block propagation of ransomware and lateral movement of data.

PATH TO ZERO TRUST MICRO-SEGMENTATION

	Deploy and Maintain Platform	Discover Assets and Deploy Agent	Categorize and Classify Assets	Create Segments and Groups	Create, Observe, Enforce Policies
XSHIELD	SAAS CLOUD - Instant on-boarding - Zero maintenance	AUTO DISCOVER/DEPLOY - Inventory in minutes - Pre-approved deployment	AUTO TAGGING - Auto-generated system tags - Program tag rules	DYNAMIC GROUPING - Infinite group rules - New member with tag rules	FULLY AUTOMATED POLICIES - Contextual recommendation - Progressive enforcement
COMPETITION	ON-PREM CLUSTER - Weeks to deploy - Ops team to maintain	MANUAL DISCOVERY - Inventory in hours - Manual install keys	MANUAL TAGGING - Manual fixed tags - No automation	STATIC GROUPS - Static REAL tags - Members with static tags	LIMITED AUTOMATION - No context recommendation - Disruptive enforcement

Secure Your Environment Quickly

Because it is a software-only solution, delivered as SaaS, Xshield eliminates the time and costs of capacity planning, hardware provisioning, installation and configuration, as well as the on-going upgrades and maintenance effort needed by other solutions. Xshield offers a low on-boarding scope-of-effort, and zero maintenance.

When You Are Ready, ColorTokens Will Be There

Microsegmentation is one pillar in the Zero Trust Maturity Model defined by the Cybersecurity & Infrastructure Security Agency and NIST. ColorTokens can help as you progress along the maturity model with components for endpoint & server hardening/ whitelisting, zero trust network access (ZTNA), cloud configuration application protection, and container security. With ColorTokens, you can implement zero trust incrementally, without disruption to your business.

For more information, please visit **colortokens.com**.

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**