COLORTOKENS

Use Case Brief

Xshield

Cloud Workload Protection for Public Cloud

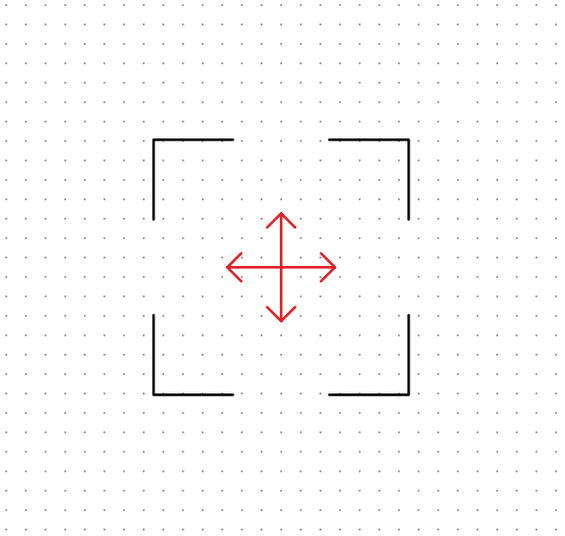
A zero trust approach to securing cloud workloads to strengthen security posture

Request a Demo

Overview

Enterprises implementing “cloud-first” initiatives need complete visibility into and protect application workloads in their dynamic public cloud infrastructure. Compliance with industry regulations demands consistent security policies for cloud workloads. In addition, a breach could affect one of the host clouds, increasing security risks to other applications and workloads. Enterprises need cybersecurity solutions that help reduce the risk of data breaches due to unauthorized workload access within a multi-vendor public cloud environment.

Xshield delivers complete network visibility and security for enterprise workloads in a public cloud environment based on zero trust architecture. It is platform-independent and provides workload protection in minutes. Xshield reduces the attack surface, improves the overall cloud security posture, and secures dynamic workloads as they move across a multi-vendor cloud environment and data centers. Xshield enforces least-privilege zero-trust policies that dynamically adapt to cloud environment architecture changes and updates, while remaining compliant.

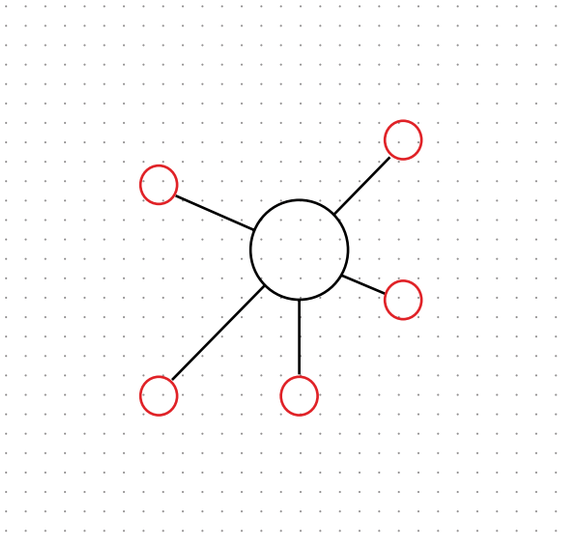


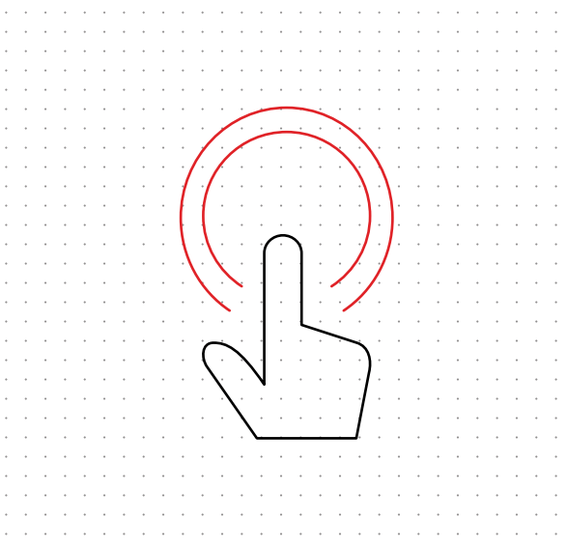
Deploy a Unified Solution

Xshield is vendor-agnostic and can protect resources across a multi-cloud environment. Protected assets can be a cloud-hosted virtual machine, container, or instance. Xshield's ultra-lightweight agent is deployed easily with a centralized dashboard that collects telemetry data from workloads to deliver instant visibility into risk posture and enable fast implementation of dynamic policies.

Achieve Micro-Segmentation

Micro-segmentation significantly reduces cloud workload exposure by protecting against East-West lateral attacks, residual risks, and other insider threats, a key pillar of zero trust architecture. Least-privilege security policies applied individually to every cloud workload minimize the attack surface by limiting communication to only trusted entities so they can function and provide services.





Gain Application Process Control

Process control extends the zero-trust architecture from network to workload processes. Cloud workloads can lock down to allow authorized operations needed for the application to function. Any other operation, regardless of its nature, is prevented from executing within the workload.

Xshield

Software-Defined Micro-Segmentation

VS

Traditional

Hardware (Network) Based Micro-Segmentation

Accelerated Implementation with Automated Policy Recommendation

Gain reusable security policy templates, server roles, and resource access parameters. Create a corporate policy template to enforce faster implementation.

Scalability

Map business applications to server roles, security, and connection information across the multi-cloud and hybrid environment. Dynamic policy tools adapt faster to the changing IT environment

Interoperability

The platform-agnostic implementation runs across bare-metal servers, end-user computers (Mac, Windows, Legacy OS),or cloud-hosted virtual machines,containers, or instances. It seamlessly integrates with identity apps, SIEM apps, and vulnerability tools.

Resource-Intensive

Segment using subnets, Hypervisor, and firewalls. Not scalable with a multi and hybrid cloud environment. Configuring new assets is resource-intensive and can create challenges in implementation.

Unnecessary Complexity

VMs located on the Hypervisor are not platform agnostic and do not communicate with other resources in a multi-vendor environment. The Hypervisor needs protection to comply with the enterprise security policy.

High Cost and Integration

Capital-intensive advanced firewalls are required to segment the network and ensure no performance degradation in data throughput. It requires creating and managing thousands of firewall rules. Multi-vendor resources may not be compatible with these firewall rules.

ColorTokens Inc., a leader in proactive security, provides a modern and new generation of security that empowers global enterprises to singlehandedly secure cloud workloads, dynamic applications, endpoints, and users. Through its award-winning cloud-delivered solution, ColorTokens enables security and compliance professionals to leverage real-time visibility, workload protection, endpoint protection, application security, and Zero Trust network access—all while seamlessly integrating with existing security tools. For more information, please visit www.colortokens.com.