COLORTOKENS

Use Case Brief

# Xshield

# Crown Jewels Security for Hybrid Environments

Complete protection of sensitive assets in complex hybrid environments

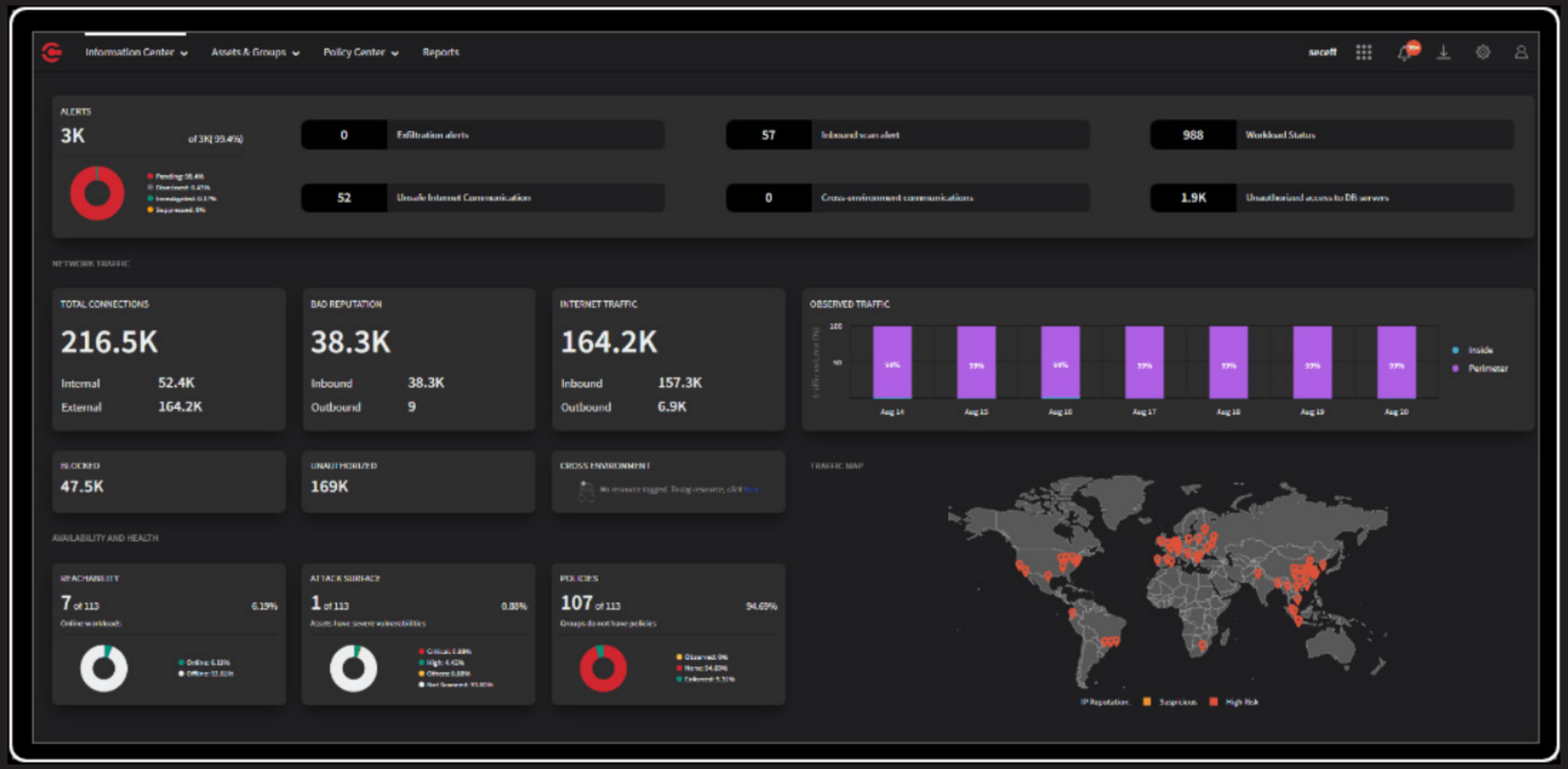
**Request a Demo**

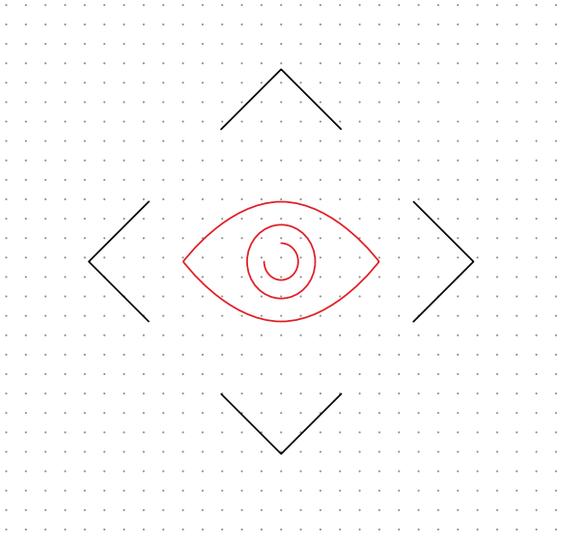
# Overview

Enterprises migrating to the cloud have assets distributed across hybrid environments. These assets could range across a bare-metal server, an end-user computer, or a cloud-hosted virtual machine, container, or instance. Enterprises need a platform-agnostic, easy-to-deploy solution that prevents lateral movement and contains breaches in an environment with no defined perimeter.

ColorTokens Xshield's zero trust solution is a cloud-delivered, vendor-agnostic security solution for hybrid networks that is simple to implement. It provides comprehensive visibility into network traffic and deployed assets, while preventing breaches and unauthorized East-West movement. Xshield delivers 360-degree visibility and network flow analysis identifying vulnerabilities and dependencies between applications, servers, and databases. With just a few clicks, it creates zero trust secure zones (micro-perimeters) around critical assets with least-privilege policies to enable a zero-trust micro-segmentation solution.

## Unified dashboard to achieve 360-degree visibility



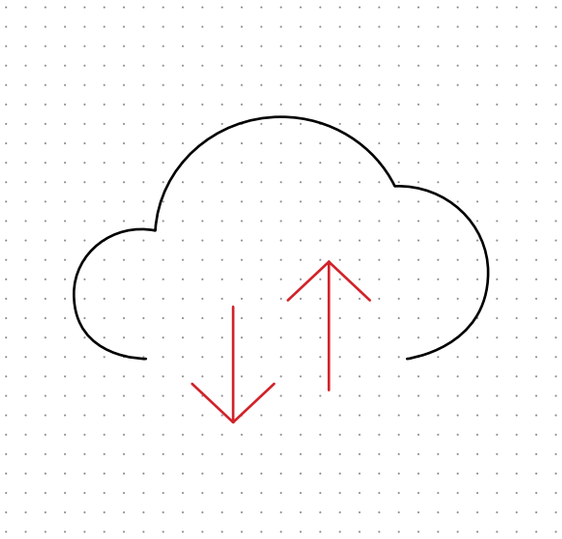


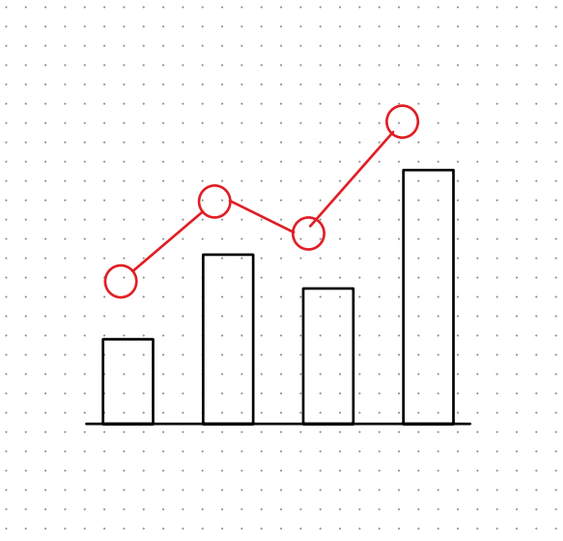
## Gain Complete Visibility

Xshield provides granular visibility into every communication between the network, applications, processes, and workloads. Its centralized dashboard collects telemetry data from all the ColorTokens managed resources. Security operators can thus achieve a comprehensive view of all traffic without using traditional technologies such as network taps or probes.

## Audit Network Traffic for Compliance

The traffic lines help administrators clarify how resources communicate amongst themselves, inside or outside the enterprise boundary. Attributes help to group resources for better cross-cloud visibility and to find compliance violations. Administrators can apply portable policy templates to resources and confirm compliance violations, such as misconfigured DNS servers or unauthorized access of production servers to the public internet.





## Detect Threats with Advanced Analytics

Xshield has a built-in vulnerability assessment tool, and integrations with a threat intelligence feed, that provide a multi-dimensional risk posture analysis. The robust threat analysis helps organizations stop zero-day attacks using telemetry data with powerful, filtered searches across more than 20 parameters. Customized notifications show where to focus on and reduce security vulnerabilities across a hybrid enterprise. Xshield's residual risk metrics help enterprises strategically assign resources to safeguard high-value, high-risk assets.

# 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.