COLORTOKENS

DATA SHEET

Xshield

Simplified Zero Trust Micro-Segmentation for Hybrid Environments

Today enterprises develop and deploy applications in increasingly hybrid or multi-cloud environments, and application access has expanded beyond corporate offices and networks to remote locations across the internet. The corporate data centers, servers, and networks give customers inherent ownership and control-based trusts. However, the cloud or internet needs a Zero Trust security model to meet this requirement.

ColorTokens Xshield is a cloud-delivered micro-segmentation solution based on a Zero Trust platform that secures critical corporate assets, including applications and workloads. The infrastructure-agnostic platform simplifies and accelerates the enterprise journey to hybrid environments, driving full cloud adoption with a Zero Trust security model. It deploys seamlessly and enables enterprises to visualize and define secure micro-segment boundaries (micro-perimeters) for their application workloads.

Xshield in Action

The ultra-lightweight agents collect telemetry data and enable the security administrator with rich visualization, automated policy management, progress reports, and actionable contextual alerts via a cloud console shown to the right. The cloud platform ingests telemetry data coupled with the vulnerability feed, threat feed, and identity feed to guide the learning engine to automate segmentation and access policies.

ColorTokens Xshield Dashboard / Architecture

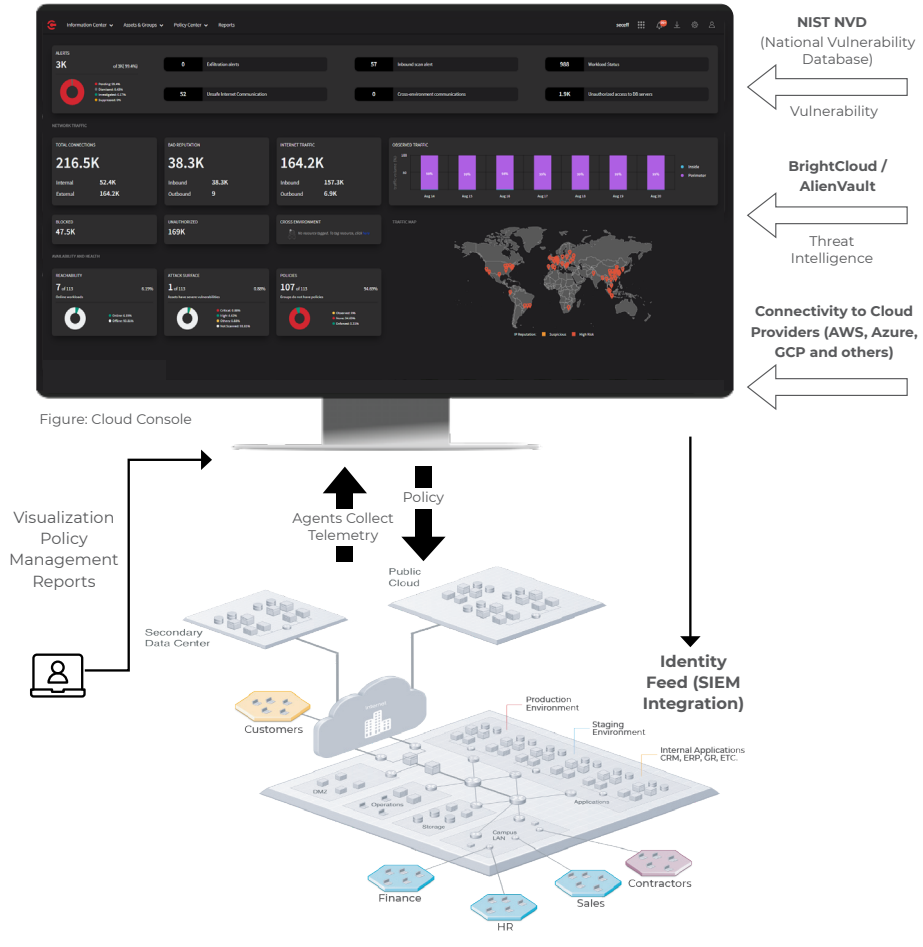

Figure: Cloud Console

Xshield Features & Benefits

Features / Capabilities	Benefits
Skyview Visualizer	• Rich, contextual visibility into network flow from largest trend to workload service. • Instantly correlate threat visibility to see the full chain of threats from risk and malicious flows to processes, vulnerabilities, and even users. • Simulate each security change to minimize disruption to your business. • Perform powerful searches using multiple dimensions like tags, addresses, names, and asset types.
AI Segmentation Engine	• Effortlessly segment and save time using the Xshield deep learning engine, which learns and recommends tags and Zero Trust segments across your hybrid cloud environments. • Reduce the attack surface, minimize business risk, and prevent lateral movement of threats. • Flexible grouping provides the freedom to create segments using different system and cloud attributes with custom tags to suit business needs.
ML Policy Engine	• Automate and optimize policy recommendations based on software identity, user identity, application awareness, historical network, threat, and vulnerability data. • Progressively create policies to secure applications externally and internally that extend to protect against intra-application threats and user access. • Understand the policy impact prior to enforcement to minimize any disruption.
Dynamic Policy Graph	• Translate and apply natural language policies automatically to workload-specific policies across your environments (physical servers, virtual machines, cloud, and containers) and operating systems (Windows, Linux, Solaris, Mac). • Recognize any changes in IP address, auto scaling and removal of workloads, implement policy updates to cover any blind spots, and quarantine the workloads in case of any compromise. • Freedom to selectively enforce policies at your own pace for inbound and outbound traffic, with domain-based policies instead of just IP address.
Native Integrations	• Faster security operations by responding to operational issues and security incidents through integration of Xshield API with SIEM console • Zero touch rollout via integration with existing IT automation tools like Ansible, GPO and rollout of Xshield agents across your infrastructure without manual intervention • Extend identity-based segmentation to users by integrating with your identity provider.
Flow Compliance Auditor	• Accelerate compliance by simplifying audits and reporting on your environment for compliance needs such as PCI. • Receive notifications instantly for any unauthorized changes to the environment. • Streamline Xshield administrative workflows using RBAC.

Key Use Cases

Zero Trust Security for Crown Jewels

Challenges	ColorTokens Solution
Enterprises migrating to the cloud have valuable data and assets distributed across hybrid, on-premises, and cloud environments. These assets could reside on a bare-metal server, an end-user computer, or a cloud-hosted virtual machine, container, or instance. Enterprises need an infrastructure-agnostic, easy-to-deploy, cost-effective solution that prevents lateral movement, minimizes compliance violations, delivers broad and deep visibility, and contains breaches.	Built to protect crown jewels in hybrid networks, ColorTokens Xshield delivers precisely that. Xshield is a cloud-delivered, network-agnostic Zero Trust solution that is simple to implement whether on-premises or in the cloud. It provides comprehensive visibility into network traffic and deployed assets, while preventing unauthorized east-west lateral movement. Xshield delivers 360-degree visibility into network flows, finding vulnerabilities and dependencies between applications, servers, and databases. It creates secure zones (micro-perimeters) around critical applications and assets with least-privilege policies, enabling Zero Trust micro-segmentation to be implemented with just a few clicks.

Environment Separation

Challenges	ColorTokens Solution
Enterprise internal networks are usually flat and often span multi-vendor environments, causing security and compliance concerns because sensitive corporate servers, development systems, and production environments are at risk of being breached and causing business disruption. Segmenting and isolating sensitive assets and environments can improve security posture, contain breaches, and ensure compliance. VLANs and traditional network segmentation techniques are static, hardware-based, and costly to implement in modern networks that are dynamic and distributed. Businesses need agile security combined with simplicity and flexibility when segmenting their distributed systems and environments across different networks.	ColorTokens Xshield creates flexible, dynamic Zero Trust secure zones around protected systems, servers, and environments with just a few clicks. The security boundary moves with the environment, maintaining separation, reducing the attack surface, and preventing unauthorized or malicious access. It allows customers to isolate and protect their critical systems in development, staging, and production without impacting the underlying infrastructure.

Cloud Workload Protection

Challenges	ColorTokens Solution
Enterprises on an accelerated journey to cloud adoption need to gain full visibility into distributed assets, ensure compliance, and protect application workloads in dynamic public cloud networks. Compliance with industry regulations demands consistent security policies for cloud workloads. A breach could also affect one of the host clouds, increasing security risks to other applications and workloads. Enterprises need cloud workload protection solutions that help reduce risk from data breaches caused by unauthorized workload access within a multi-vendor public cloud environment.	ColorTokens Xshield delivers complete network visibility and cloud workload security based on a Zero Trust platform. It is infrastructure and network-independent, cloud-delivered, and enables workload protection in minutes. Xshield reduces the attack surface, improves overall 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 staying compliant.

Supported user OS

Xshield agents for clients (end users) are available for MACOS and Windows OS families.

MACOS	OS 10.10 and above
Windows 64-bit	OS 7 and above

Supported workload OS

Xshield agents for workloads are available for AIX, Linux, and Windows OS families.

OS Family	Supported Versions
Windows 32-bit	OS XP SP3 and above
Windows 64-bit	OS 2003 SP2 and above
MACOS	OS 10.10 and above
Ubuntu	OS 12.4 and above
Redhat	OS 6.7 and above
CentOS	OS 6.7 and above
SUSE	OS 12 and above
AIX	OS 7.1 and above

Start Free Trial

or send your query to info@colortokens.com

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.