COLORTOKENS

DATASHEET

Xshield

# SIMPLIFIED ZERO TRUST MICRO-SEGMENTATION FOR HYBRID ENVIRONMENTS

Today enterprises develop and deploy applications in increasingly hybrid or multi-cloud environments, and 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 and internet need a Zero Trust security model to meet this requirement.

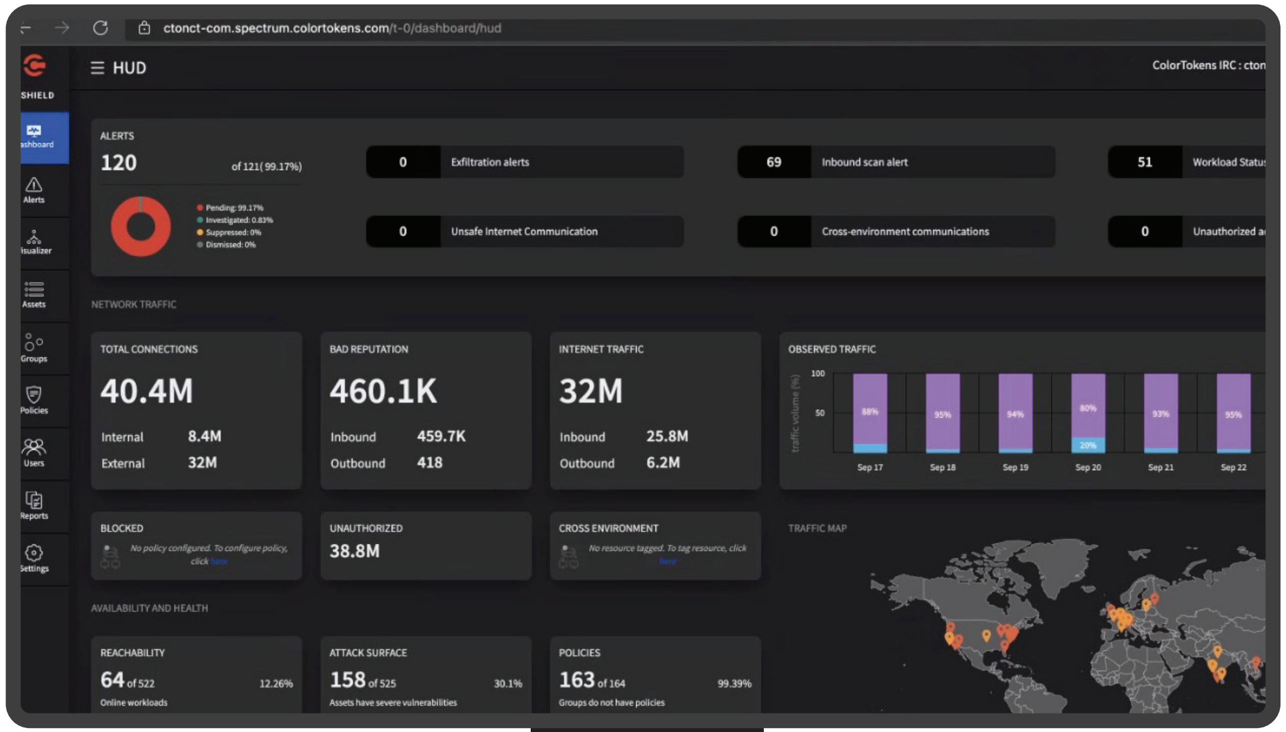
ColorTokens Xshield is a cloud-delivered micro-segmentation solution based on a Zero Trust platform that secure critical corporate assets, including applications and workloads. Our solution provides remote access user control for micro-segments within a single platform. The infrastructure-agnostic platform simplifies and accelerates the enterprise journey for distributed 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) through automation 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 by auto-creating system tags reducing the administrative burden, and creating access policies.

# ColorTokens Xshield Dashboard / Architecture

## ColorTokens Xshield Dashboard / Architecture



ctonct-com.spectrum.colortokens.com/t-0/dashboard/hud

SHIELD

☰ HUD

ColorTokens IRC : cton

ALERTS

120 of 121( 99.17%)

- Pending: 99.17%
- Investigated: 0.83%
- Suppressed: 0%
- Dismissed: 0%

| | |
|---|---|
| 0 | Exfiltration alerts |
| 0 | Unsafe Internet Communication |
| 69 | Inbound scan alert |
| 0 | Cross-environment communications |
| 51 | Workload Statu |
| 0 | Unauthorized a |

NETWORK TRAFFIC

TOTAL CONNECTIONS

40.4M

| | |
|---|---|
| Internal | 8.4M |
| External | 32M |

BAD REPUTATION

460.1K

| | |
|---|---|
| Inbound | 459.7K |
| Outbound | 418 |

INTERNET TRAFFIC

32M

| | |
|---|---|
| Inbound | 25.8M |
| Outbound | 6.2M |

OBSERVED TRAFFIC

BLOCKED

*No policy configured. To configure policy, click here*

UNAUTHORIZED

38.8M

CROSS ENVIRONMENT

*No resource tagged. To tag resource, click here*

TRAFFIC MAP

AVAILABILITY AND HEALTH

REACHABILITY

64 of 522 12.26%

Online workloads

ATTACK SURFACE

158 of 525 30.1%

Assets have severe vulnerabilities

POLICIES

163 of 164 99.39%

Groups do not have policies

**Figure: Cloud Console**

NIST NVD (National Vulnerability Database)

Vulnerability

BrightCloud / AlienVault

Threat Intelligence

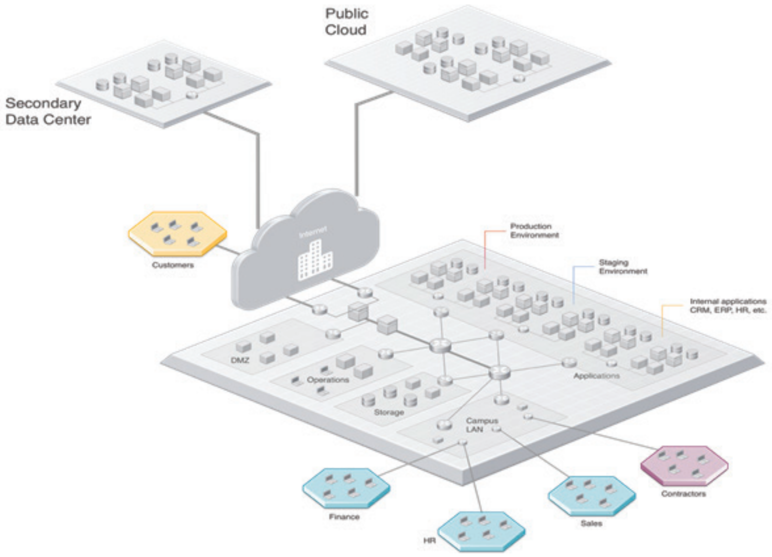
Connectivity to Cloud Providers (AWS, Azure, GCP and others)

Visualization Policy Management Reports

Agents collect Telemetry

Policy

Identity Feed (SIEM Integration)



# Xshield Features & Benefits

| Features / Capabilities | Benefits |
|---|---|
| **Skyview Visualizer** | • Simplified console eases log collection drives better debugging and reduces the need to collect firewall logs manually<br>• Rich, contextual visibility into network flows from the most significant trend to individual workload service<br>• Simulate each security change to minimize business disruption<br>• Instantly correlating threats from risk, malicious flows, processes, and vulnerabilities, and users<br>• Perform powerful searches using tags, addresses, names, and asset types based on natural language processing capabilities<br>• Manage cloud workloads with pre-assigned tags, reducing the time to identify cloud workloads, including resource name, type, configuration |
| **AI Segmentation Engine** | • Effortlessly segment and save time using the Xshield deep learning engine to, recommend tags and Zero Trust segments across your hybrid cloud environments<br>• Reduce, the attack surface, minimize business risk and prevent lateral movement of threats<br>• Seamlessly clone policies within workload groups and automatically recognize asset metadata to apply and create a flexible grouping with custom tags based on business needs<br>• Policy templates for enterprise applications and build custom policy templates for known applications |
| **ML Policy Engine** | • Automate and optimize policy recommendations based on software identity, user identity, application awareness, historical network, threat, and vulnerability data<br>• Progressively create policies to secure applications externally and internally that extend to protect against intra-application threats and user access<br>• Understand the policy impact before enforcement to minimize any<br>• View entire policy state from policy creation to firewall rule on the workload from the console |
| **Dynamic Policy Graph** | • Translate and apply natural language policies automatically to workload-specific policies across environments (physical servers, virtual machines, cloud, and containers) and operating systems (Windows, Linux, Solaris)<br>• 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<br>• 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** | • Fasten security operations by responding to operational issues and security incidents by integrating Xshield API to SIEM console using our Splunk and Azure apps<br>• Zero-touch agent rollout via integration with existing IT automation tools like Ansible, GPO across distributed infrastructure without manual intervention<br>• Extend identity-based segmentation to users by integrating with your identity provider<br>• Consume audit logs with log type and time range |

**Segmentation Readiness and Compliance**

- Accelerate compliance by simplifying audits and reporting on compliance needs such as PCI
- Receive notifications instantly for any unauthorized changes to the environment
- Streamline Xshield administrative workflows using RBAC
- Assess segmentation progress through a readiness score and find gaps in security posture.

**Public APIs**

- Availability of public API for assets, tags, groups, policy creation, flow, audit logs, alerts, and quarantine.
- Gather data for assets, including policy tampering, vulnerability exposure, and network exposure
- Search FQL-based keywords for filtering assets with asset API filter

# Key Use Cases

## Zero Trust Security for Crown Jewels

| Challenges | ColorTokens Solution |
|---|---|
| Enterprises host critical applications across bare-metal, traditional servers, cloud-hosted virtual machines, containerized workloads, and other host systems. Organizations lack visibility into what assets are in their network, where data exists in their distributed environment, who has access to data, and how to secure the data from malicious or unauthorized access. Regulatory requirements enforce heavy penalties to secure data. However, the critical assets (crown jewels) have security risks from east-west communications within the data center or cloud. Enterprises need a platform-agnostic, easy-to-deploy solution that protects their crown jewels from unauthorized east-west communications and lateral movement. | Xshield ensures that customers have complete visibility into their assets through a visual dashboard, gain insight into data-related business risk, and are continuously aware of the security posture of their crown jewels. The security policy is close to the data, and it moves with the assets as they shift from on-premises to the cloud. ColorTokens provides a simplified, Zero Trust ("never trust, always verify") approach to securing an enterprise's most valuable crown jewels against cyberattack. ColorTokens Xshield is based on the NIST Zero Trust framework to address evolving threats and compliance requirements. 100% cloud-delivered, SaaS-based for fast time-to-value, Xshield enables granular visibility, security, and control over applications and network assets to reduce the attack surface and the impact of breaches significantly. Customers benefit from increased resilience to attacks, rapid containment, and minimal business disruption or downtime. |

## Environment Separation

| Challenges | ColorTokens Solution |
|---|---|
| Properly configured environment separation reduces the risk of data breaches arising due to unwanted or unmonitored movement of production data into a development environment. Data breaches also happen when development teams have access to sensitive production data in the development environment. Secure environment separation, ensuring compliance and data privacy, is the best strategy to prevent data breaches. However, this can become time-consuming and challenging in distributed and hybrid data center environments. The biggest challenge to any enterprise IT-consisting of multiple applications spread across development, testing, and production servers – is enabling secure environment separation. For every movement of a resource or an application in the data center, all stakeholders, from the CIOs to the network and system engineers, must be aligned to ensure data security, privacy, and compliance. | ColorTokens Xshield helps create Zero Trust Secure Zones™ (micro-perimeters) around applications with just a few clicks to prevent lateral movement and the spread of breaches. With environment separation, the security boundary moves with the application, reducing the attack surface and preventing the spread of violations in a hybrid and multi-cloud environment. It enables customers to isolate and protect their critical applications in development, staging, and production environments from one another. Xshield fits into any stage of an enterprise's cloud journey by enabling security policies to follow the application environment as they move to and from the moment a new workload is born. |

## Cloud Workload Protection

### Challenges

Enterprises on an accelerated journey to cloud adoption need to gain complete 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 Solution

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.

## Proving Compliance

### Challenges

Whether your organization is a brick-and-mortar business or has an online presence with e-commerce, achieving PCI compliance can be challenging. Merchants process cardholder data and store it across data centers and cloud platforms to the point of sale (POS) systems, PCs, and in-store kiosks. To avoid PCI violations, IT teams need to understand precisely where cardholder data flows, minimize access by users and applications, and scan their environments for vulnerabilities and unprotected paths to confidential data. To protect PII (Personal Identifiable Information) processing and storage servers against vulnerabilities and streamline PCI compliance, micro-segmentation is the right solution.

### ColorTokens Solution

Achieving and supporting compliance with PCI standards can be challenging for any organization, regardless of size or industry. And even businesses that do manage to meet PCI requirements may find audits expensive, time-consuming, and stressful. ColorTokens helps enterprises address these challenges by simplifying ongoing PCI compliance, identifying changes in compliance scope, reducing the audit scope and time to audit, and accelerating any needed remediation. Our solution supports PCI cloud compliance, can enable merchants and retailers to prepare for their cloud transformation without added security or hardware requirements. ColorTokens Xshield micro-segmentation solution can see, stop, and predict security and PCI compliance violations across any workload, deployment, and user. It delivers a unified approach for organizations to simplify security and compliance across their hybrid infrastructures.

## Preventing Lateral Movement

### Challenges

Organizations have started to realize that perimeter security solutions are ineffective against preventing ransomware. The blurring of the perimeter has resulted in opening new entry points for cybercriminals to exploit. Once inside, ransomware spreads laterally to other endpoints and assets in the network if left undetected. Attackers focus on spreading the malware through lateral movement, making the perimeter security ineffective. Cybercriminals often exploit organizations using remote access tools for their employees and outsourced staff by gaining a more accessible path through a remote connection and crippling the system through lateral movement.

### ColorTokens Solution

ColorTokens Xshield delivers real-time protection against ransomware in core data center and cloud workloads by segmenting and preventing lateral movement. Xshield helps prevent large-scale, costly corporate attacks with a software-defined micro-segmentation solution based on a Zero Trust architecture. The Zero Trust architecture works on the principles of least-privilege access to segment the network. The Zero Trust security model helps secure networks and workloads by restricting internet access, reducing the attack surface, preventing lateral infection, and stopping a ransomware attack efficiently.

# Defending Legacy Systems Against Attacks

## Challenges

Many organizations depend on legacy systems because they are hard to replace and many core enterprise applications still run on these legacy systems. Legacy solutions no longer receive technical support or O.S. patches/software upgrades and are vulnerable to cyberattacks that could compromise the entire network. With the cyber threat landscape evolving faster than security teams' ability to update and replace legacy systems, securing legacy systems against cyberattacks has become a key priority for organizations. Unsupported legacy systems allow attackers to infiltrate the network and move laterally to gain access to sensitive data and critical applications. With no support or patches to address these security vulnerabilities, legacy systems can put businesses at risk for costly data breaches. Hackers make use of the end-of-support dates available online to find zero-day exploits that are unpatched. Organizations must take the correct cybersecurity steps to keep operations running and prevent downtime, potential revenue loss, and regulatory penalties.

## ColorTokens Solution

ColorTokens extends support to data center legacy systems, including vulnerable and unpatched applications running Windows 2003, XP, and above by performing identity-based segmentation and offering comprehensive network visibility. Many cybersecurity vendors do not support legacy systems beyond Windows 7, increasing vulnerability for customer assets that share applications or have traffic flowing in a hybrid environment. Our solution ensures that the customer can manage their unpatched systems without compromising the security of their assets or network. Our solution also investigates security issues while providing complete visibility and reducing lateral movement.

## Supported workload OSes

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 |
| Sun Solaris | OS 10 |
| Oracle Linux | OS 7.8 and above |

## Supported user OSes

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

| OS Family | Supported Versions |
|---|---|
| MacOS | OS 10.10 and above |
| Windows 32-bit | OS 7 and above |
| Windows 64-bit | OS 7 and above |

**Start Free Trial**

or send your query to info@colortokens.com

ColorTokens Inc. is a leading innovator in SaaS-based Zero Trust cybersecurity solutions providing global enterprises with a unique set of products and services for securing applications, data, and users across cloud and hybrid environments. Through its award-winning Xtended ZeroTrust™ Platform and context-aware machine learning-powered technologies, ColorTokens helps businesses accurately assess and improve their security posture dynamically.

As cloud adoption grows, traditional perimeters get redefined, and new attack vectors and threat actors materialize, corporations recognize their security posture needs to reflect their Zero Trust philosophy. ColorTokens' technology allows customers to achieve Zero Trust by utilizing rich, meaningful contextual information about the application, microservice, or protected resource, so customers can apply Zero Trust with as secure of a perimeter as they can. ColorTokens' cloud-based SaaS platform can automatically deploy next-generation security controls and increase security posture dynamically without any new hardware, downtime, reboots, or changes to a client's existing systems.

With a team of over 400 people, ColorTokens has global office locations in Santa Clara, California; New York; London; Copenhagen, Denmark; and Bengaluru, India. For more information, please visit **www.colortokens.com.**