SEAMLESS CLOUD MIGRATION WITH COLORTOKENS XSHIELD

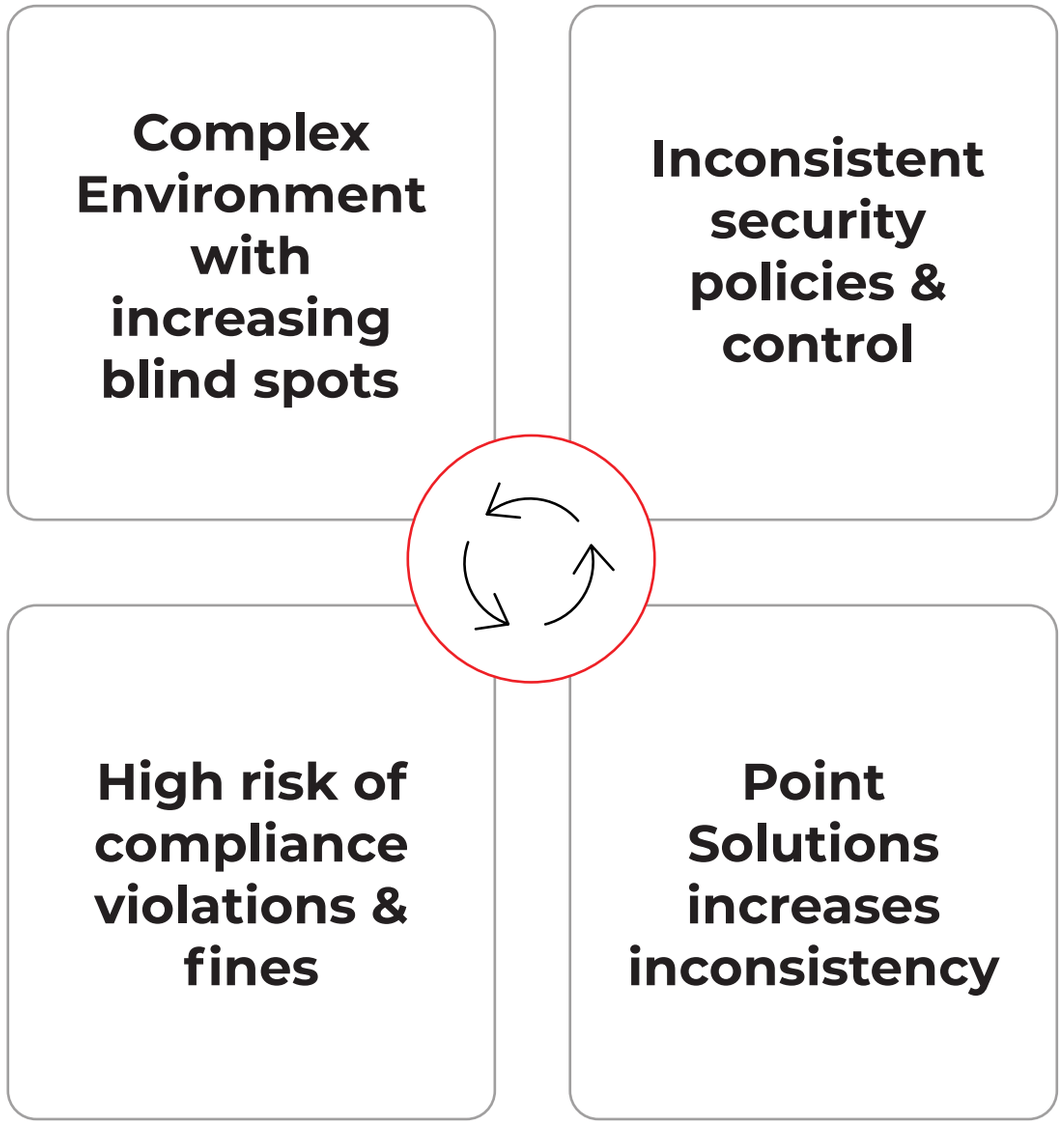
Scalability, increased flexibility and cost agility, and ubiquitous access are key factors behind the rapid rise of cloud migration. To securely navigate the network transformation to cloud, security transformation must also take place. As organizations accelerate their journeys to the cloud but still have a good portion of their assets in on-premises data centers, maintaining a uniform security posture across such hybrid environments becomes a challenge, increasing their risk and exposure to data theft. IT teams are under pressure to ensure that security policies remain the same for applications and workloads, whether in the private cloud, data center, or multiple public clouds.

There are security benefits via internal safeguards provided by the cloud provider and a shared responsibility model. While cloud service providers will take responsibility for the security of their cloud, security of the data in the cloud remains the responsibility of the enterprise.

Security Barriers for Adoption of Cloud Migration

- Lack of visibility
- Compliance violations
- Lack of skilled resources
- Misconfigurations and accidental errors
- Insider threats
- Data exposure to cyber threats

An adhoc approach to cloud migration, or blind cloud adoption, frequently results in more complexity which compounds the problem even further:



Key Requirements for Cloud Migration:

- **Workload identity based micro-segmentation:** Cloud-based systems follow a shared responsibility model. For enhanced security of enterprise data in the cloud, workload micro-segmentation and policy controls are required. Lack of access control remains a key challenge in the cloud and is a key factor in the rise of breaches such as Ransomware.
- **Uniform security posture:** Lack of consistent security policy can cause security gaps, resulting in malicious activities going unnoticed until there is a breach in the cloud by which time the damage has already occurred. Security policy inconsistencies also result in compliance violations, lengthening the audit cycle and creating barriers to a successful cloud migration.
- **Comprehensive visibility:** To properly address vulnerabilities and create sound security policies that meet business and compliance needs, IT security teams need to see how data communicates in cloud environments. Organizations often cite lack of business-level visibility as one of the key challenges they face in the cloud. Comprehensive, application-level visibility of cloud assets is a key requirement for defining cloud workload security policy.

ColorTokens: Modern approach to Cloud Migration

ColorTokens Xshield delivers an industry-leading, Zero Trust micro-segmentation solution for seamless cloud migration and protection of distributed workloads in hybrid environments. The key solution components in Xshield are described below:

Provides Real-time Visibility into Network Assets

- Provides real-time visibility into cloud workload traffic and system processes, along with a unified view of all assets and network traffic across data centers and the cloud
- Instantly discovers cyber-risks due to misconfigurations, vulnerabilities, and malicious communications
- Delivers granular visibility into domains with poor reputation, including IP traffic and C2 traffic
- Enables isolated application views for deeper, drill-down views
- Decouples IP addresses and takes an application-centric approach to visibility

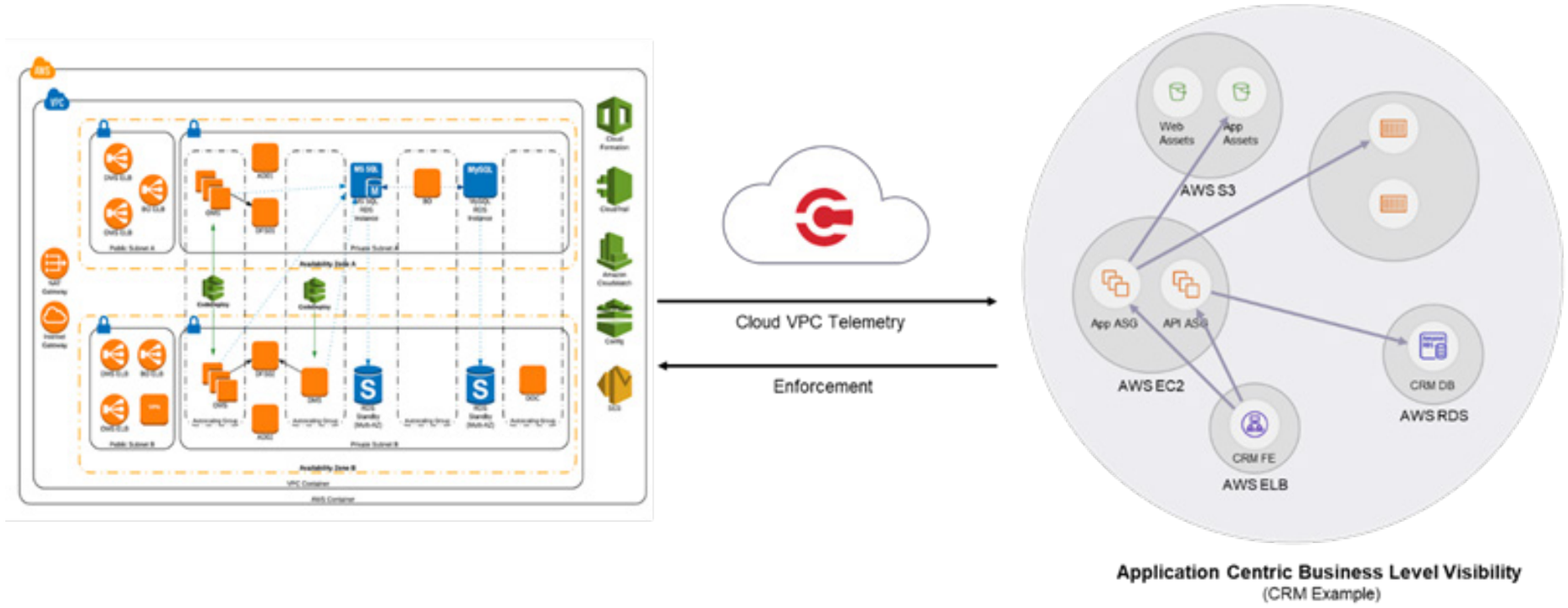


Figure 1. Business level views of LOB applications enable faster construct of policy definition

How ColorTokens Xshield supports a seamless migration to the cloud

- ColorTokens Xshield enables rapid implementation of a three-step Zero Trust-based approach for establishing a baseline for policies in the on-premises data center. IT and security teams can undertake this activity during the initial stages of the cloud migration journey.
- Visibility is the first step. Xshield's cloud-based console provides comprehensive visibility into all assets, with color-coded views of network traffic that enable critical insights into vulnerabilities and dependencies among the different applications and systems.
- Xshield's AI/ML-based policy engine automates the creation of policies based on business need, which is followed by simulating and observing policies to validate that the traffic path, segments, and access privileges don't violate business policy and compliance.
- Xshield blocks unauthorized traffic via single-click enforcement in the host firewall and only allows authorized traffic based on least-privilege policies.
- ColorTokens' Xshield policies are infrastructure-independent, making the policy transition to the cloud easy to implement. Dynamic in nature, the policies follow the workloads as they migrate from the on-premises data center to the cloud, ensuring comprehensive security during the move.
- After the migration, depending on business requirements, previously defined microsegments can remain as is or be redefined based on the new application architecture, and previously proven policies can be leveraged.
- For multi-cloud deployments, Xshield provides a single pane of glass for visibility and policy management across all clouds.

Reduces the attack surface, blocks lateral movement, and enforces Zero Trust access policies

- Host-based micro-segmentation based on workload identity and least-privilege access policies
- Zero Trust Zones based on application architecture, compliance needs and environment
- Contains the lateral movement of an attack between departments, functions, applications and workload segments
- Blocks C2 traffic/bad-domain traffic

Uniform and consistent security policies across data center and cloud workloads

- AI/ML-based policy engine learns traffic patterns and auto-recommends policies; customized tag-based policies can be quickly defined based on recommendations
- Fast tracks micro-segmentation with simplified, automated policy deployment that allows policy simulation (observe mode) before one-click enforcement
- Granular, dynamic policies based on workload identity and attributes eliminates the dependency on underlying network
- Infrastructure-agnostic approach enables uniform security policies across cloud and data center

ColorTokens Xshield Advantages for Cloud Migration

- Infrastructure- and platform-independent; can be deployed in minutes, not weeks
- Effortless deployment, with business-level application visibility from day one
- Single pane of glass visibility and policy management from one console
- Granular context awareness and visibility of each workload across on-premises and cloud environments
- Works seamlessly in distributed/hybrid environments across data centers and cloud/multi-cloud
- Dynamic software-defined micro-segments that adjust automatically as resources are added or removed
- Automated policy recommendations to simplify Zero Trust policy definition and customization
- Adaptive policies automatically adjust to changes in the network, whether on-premises or cloud
- Born in the cloud, with a flexible approach that supports on-premises and multi-cloud architectures

Xshield

The leading choice for a seamless cloud migration

Xshield is based on a cloud-native architecture to deliver a multi-tenant and agile SaaS offering with fast response times, rapid and continuous release updates with no management burden or disruption, and instant scaling. The solution deploys in minutes, not weeks. There is no Capex or Opex affecting the customer's bottom line and no cloud hosting costs. Customers like the true SaaS advantages of ColorTokens compared to alternative solutions who require that the customer bear the cloud cost on their VPC (virtual private cloud), causing costs to go up as the business starts to grow.

In the cloud, Xshield delivers complete network visibility and cloud workload security based on a Zero Trust platform. It is infrastructure- and network-independent, 100% 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 policies dynamically adapt to cloud environment architecture changes and updates, while staying compliant.

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.**