COLORTOKENS

Enabling highly-secure environment separation using colortokens.

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 can also happen when development teams have access to the sensitive data on a production environment due to misconfigurations.

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 just a hundred applications or thousands of applications spread across several 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 on the same page to ensure data security, privacy and compliance.
ColorTokens enables software-defined, platform-independent environment separation in minutes, reducing the attack surface and improving the overall security posture of your data center.

Use Case Benefits

- Rapid, platform-independent environment separation
- Zero-trust architecture with continuous cross-segment traffic visibility
- Privacy, compliance and security assurance
- Reduced attack surface

ColorTokens Technology

ColorTokens Xshield for Workload Protection is a software-defined micro-segmentation solution that enables easy environment separation for modern data centers. Xshield is a part of the award-winning ColorTokens Xtended ZeroTrust Security Platform.

Xshield provides a paradigm shift in data center security by shifting the focus to the end-user and the application. This operational principle makes ColorTokens agnostic to firewalls, virtual machines, private and public cloud infrastructure, enabling security to dynamic application workloads spread across bare-metal and cloud data centers.

User access to applications spread across development, testing and production environments, and communication between workloads, within and across these environments, is facilitated using security policies.

The policies are defined using abstractions instead of IP addresses or VLAN memberships. This makes ColorTokens environment separation adapt to dynamic application environments, providing unparalleled operational ease and security.

How Does ColorTokens Work?

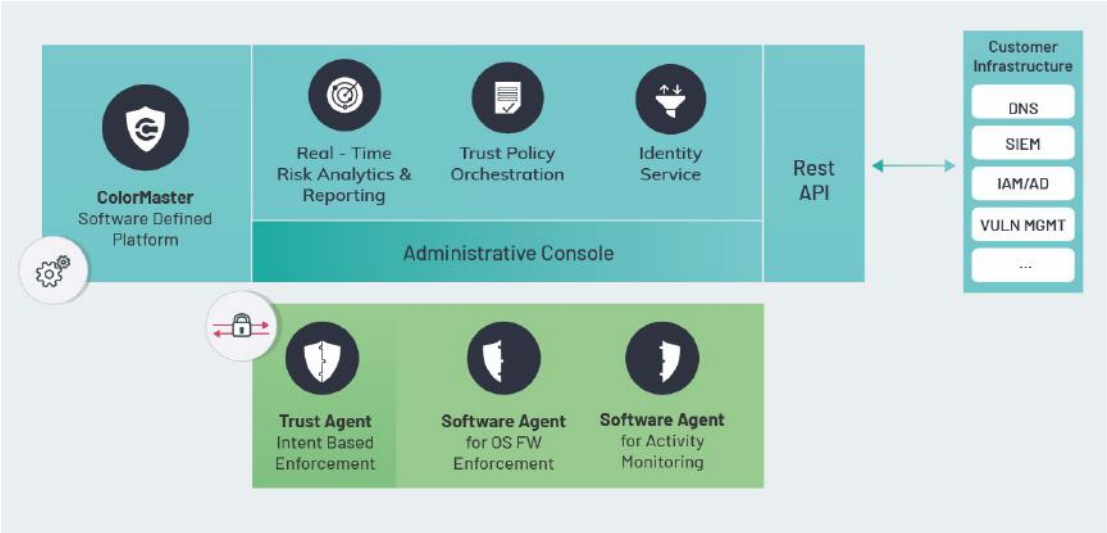
ColorTokens has two main components – ColorMaster and Trust Agent.

Trust Agent

Software that is deployed on each resource to be protected/managed that will enforce the ColorMaster policies as well as collect telemetry for the ColorMaster to analyze.

Colormaster

Provides a single-pane of glass for your hybrid data center. It is also the main console that provides all administrative functions including cross-segment traffic visibility, analytics, and security policy simulations and enforcement.



Environment Separation Using ColorTokens Xshield

Let's consider a scenario where you want to create a separate environment for your HRM production application in your hybrid data center.

With Xshield, you can segment your network by tagging resources and hosting workloads or applications. Tags can be associated with specific workloads or applications, and the required security policies can be automatically enforced.

Tags help you identify all the resources, applications and their roles, so that environment separation can be done in minutes, with no manual errors.

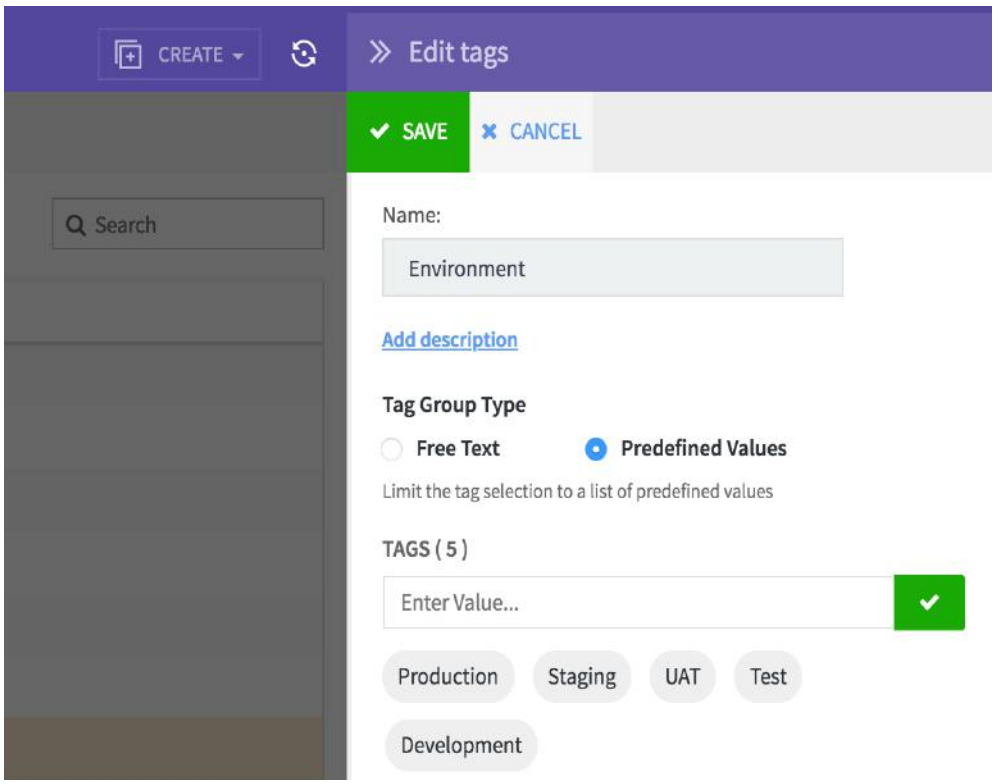
ColorTokens Xshield has three predefined, customizable tags:

Environment:
It defines the operating environment of a resource, with the values being production, staging, UAT, and others.

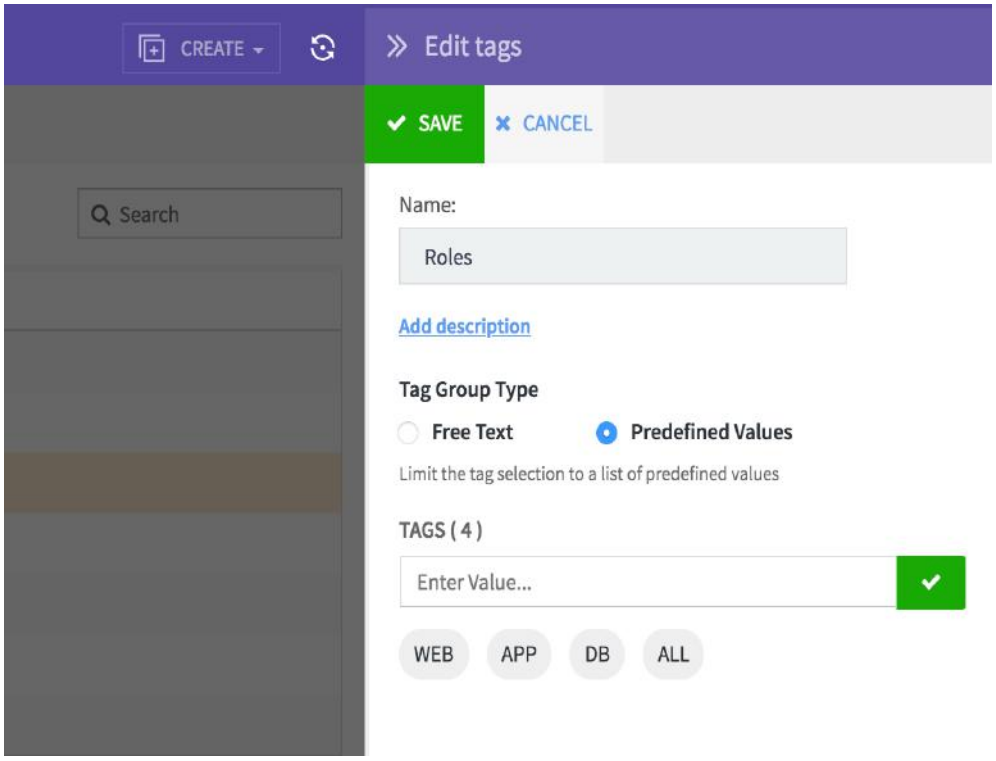
Role:
It defines the function and purpose of a resource. Xshield provides some predefined values like Web, App and DB.

Application:
Create and associate an application with a server role and business impact. For example, assign the HRM app to the production environment, and mark the impact as medium.

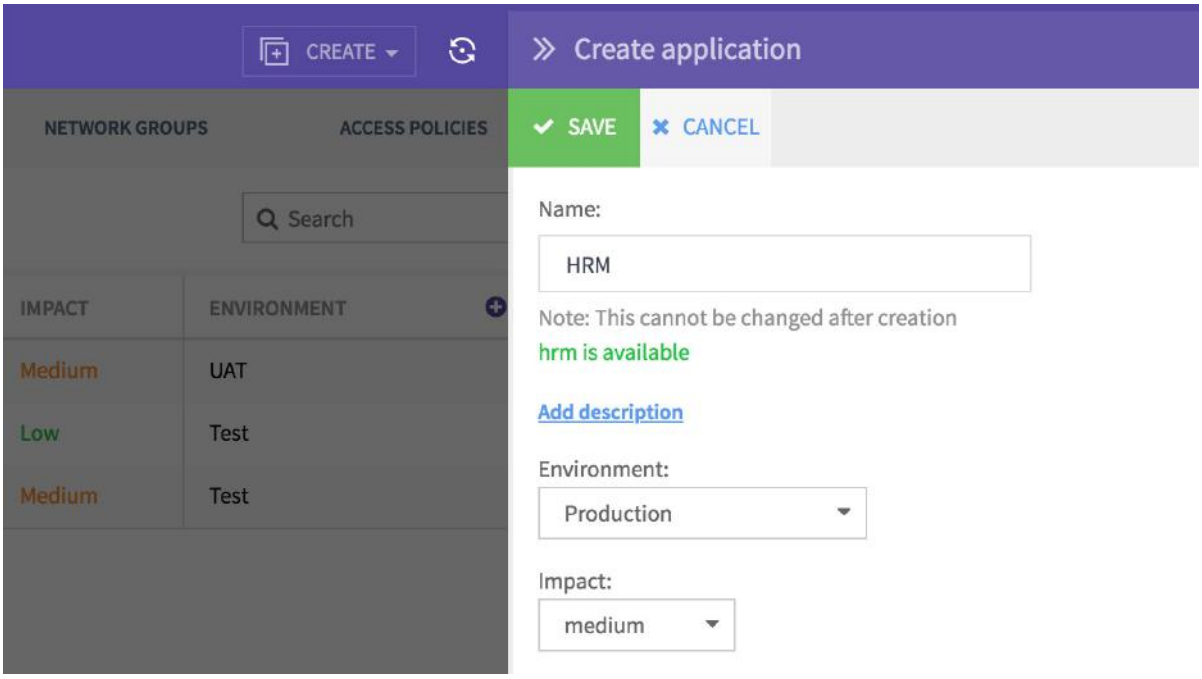
Environment



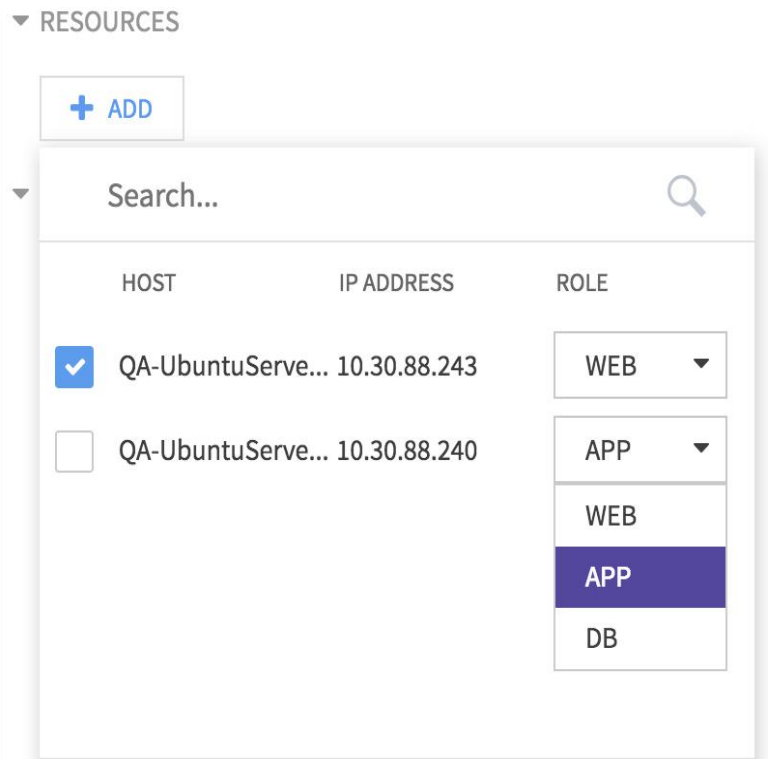
Role



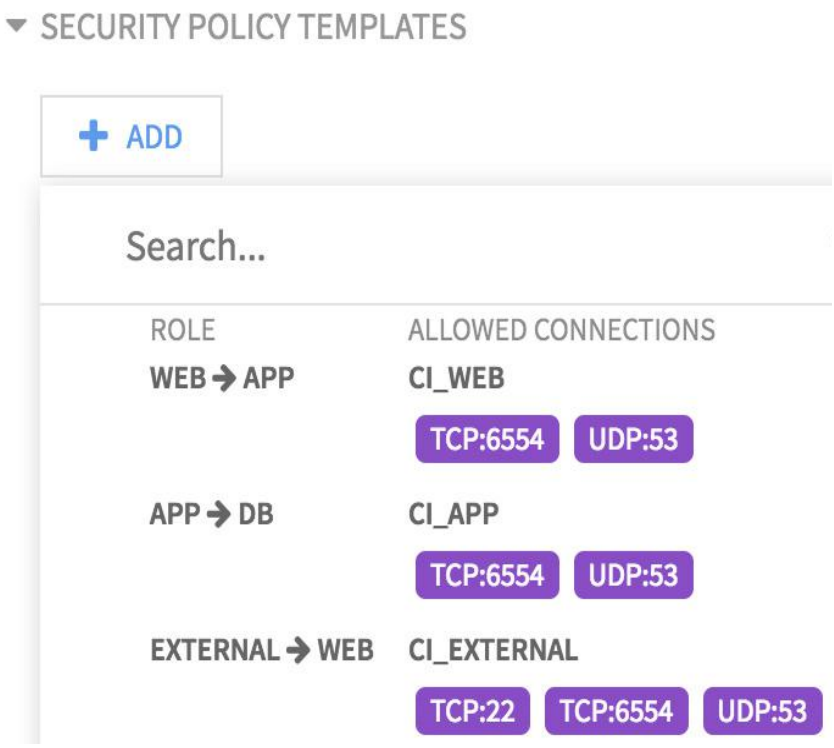
Application



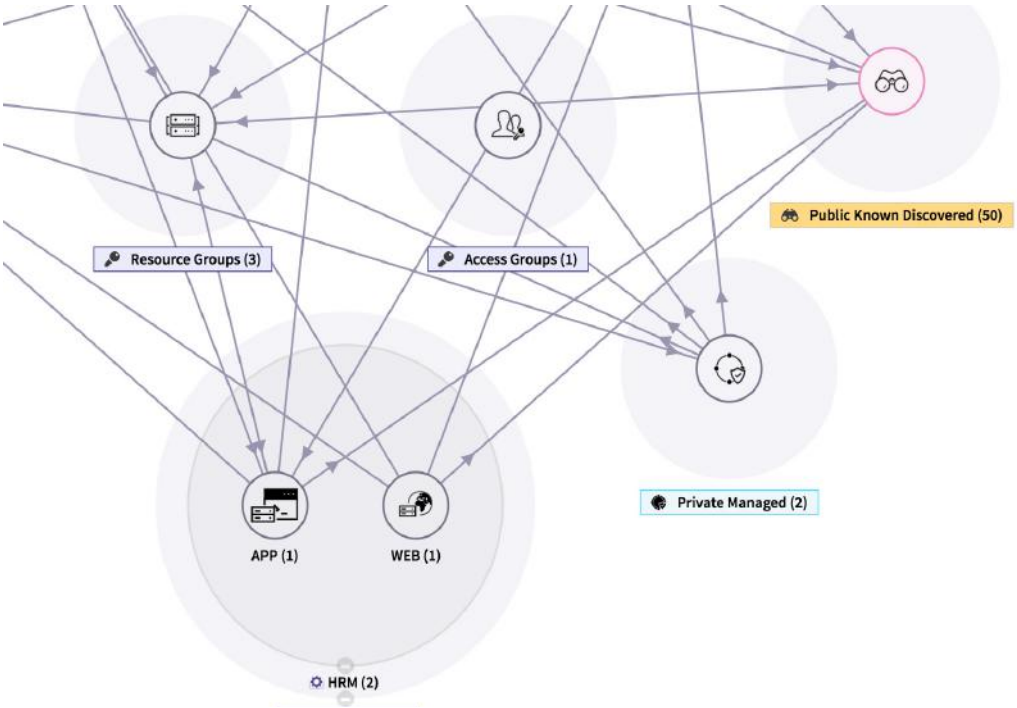
Assign the roles to the appropriate server resources; WEB, APP, or DB.



You can apply the correct security policies required for this environment and complete the environment separation of the HRM production application.



ColorTokens Xshield gives you a single pane of glass view of your hybrid environment. You can operate with speed and accuracy as you visualize the environments and the connections between them at a top level.



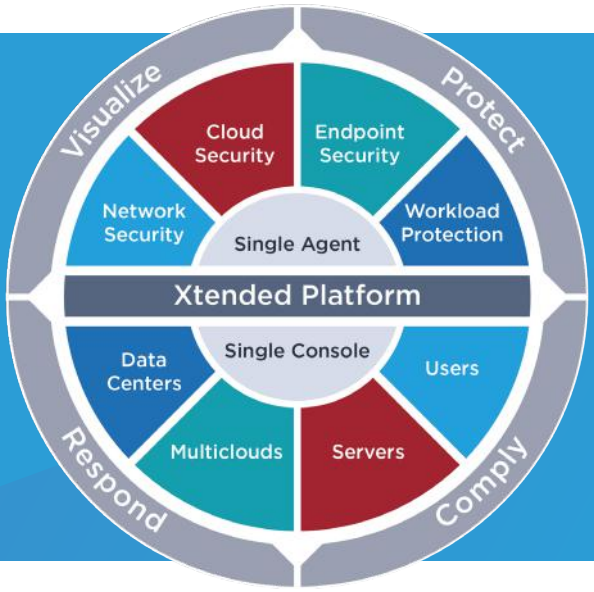
You can drill down each of the specific environments to look at the applications in detail and be confident that the changes are secure and compliant.

Environment Segmentation – Traditional vs ColorTokens Xshield

Traditional	ColorTokens
Subnet segmentation: Define separate policies for each subnet and configure the VLANs/ACLs. Cumbersome. Takes hours!	Reusable server role, environment and application tags. Simplify separation.
Segmentation using firewalls. Provision for capital-intensive, advanced internal firewalls to segment the network and ensure that there's no performance degradation in data throughput. Also, there's no escape from creating and managing thousands of firewall rules.	Reusable security policy templates. Automate security.
Manually separate development staging and production segments for every new app. Planning and execution takes time.	Separation across clouds in hybrid deployments. Future-proof.
Manually setup separate environments to meet security and compliance requirements. Takes days. Human errors.	Platform agnostic. Interoperability. Zero disruptions.
Sync with many stakeholders from conception to execution. Reduces execution speed.	Automatic audit trail for every action. Audit-ready.
Multiple tools to record and maintain change information. Not always audit-ready.	Zero-trust network with full visibility and control. Limited attack surface.

ColorTokens Xtended ZeroTrust Platform

Built from the ground up to make zero trust a reality for any enterprise, the ColorTokens Xtended ZeroTrust Platform delivers a refreshing, new-generation of security to provide the following unique benefits:



ColorTokens unifies network security, cloud security, endpoint security and workload protection for datacenters, branch offices, public and private clouds through a single, cloud-delivered platform

Xview for Visualization

Xview – part of the Xtended ZeroTrust Platform – provides unified visibility across on-premises and mulitcloud infrastructure, giving a telescopic view into networks, clouds, applications and endpoints. The Xtended Visualization analytics engine integrates with market-leading threat intelligence to investigate suspicious behavior anywhere in the enterprise—while protecting against zero-day threats. Integrated widgets and canned reports enable security teams to achieve faster time-to-compliance for critical mandates like PCI, HIPAA and GDPR. And, the platform's built-in scanner hunts for vulnerabilities in real-time – providing an immediate return on your security investments.

Xshield for Workload Protection

Xshield – part of the Xtended ZeroTrust Platform – enables enterprises to achieve consistent visibility and control of all cloud workloads – regardless of the location or granularity of the instances. Built from the ground up for unrivaled software-defined micro-segmentation, ColorTokens enables the modern enterprise with instant workload visibility, automated and dynamic policy enforcement, and the ability to control any communications to/from the workload instances.

Xprotect for Endpoint Detect and response

Xprotect – part of the Xtended ZeroTrust Platform – provides enterprises with a robust signature-less approach that works at the kernel level to block unauthorized processes on endpoints, servers and legacy/fixed-function systems. Go beyond signature-based security, that blocks only 'known-bad' threats, with powerful whitelisting, prevent unauthorized software execution on endpoints – even with administrator rights and block malicious processes from spawning and infecting legitimate applications.

CIOs and security teams are frustrated with too many complex, reactive point products—and are still vulnerable to sophisticated threats and attacks. ColorTokens proactively secures enterprises through a single, cloud-based Xtended ZeroTrust Platform. This enables enterprises to instantly visualize and segment their entire IT infrastructure, block advanced malware, contain and respond to APTs and zero-day attacks – all while seamlessly integrating with existing security tools. ColorTokens makes end-to-end zero trust security a reality for any enterprise—covering protection, detection, investigation and response through a single-agent, single-platform architecture. Enterprises can now protect networks, multiclouds, containers, workloads and endpoints with the world's first single agent and platform that unifies network, cloud and endpoint security.

COLORTOKENS

ColorTokens Inc., a leader in cloud-delivered ZeroTrust security, provides a modern and new-generation of security that empowers global enterprises with a proactive approach to single-handedly secure cloud workloads, dynamic applications, endpoints and users. Through its award-winning Xtended ZeroTrust Platform, ColorTokens delivers the only cloud-based solution that combines AV, EDR, workload protection and application control into one ultra-lightweight agent. This enables enterprises to instantly visualize and segment their entire IT infrastructure, block advanced malware, contain and respond to APTs and zero-day attacks—all while seamlessly integrating with existing security tools.

colortokens.com
sales@colortokens.com