COLORTOKENS

Use Case Brief

A platform-independent approach to micro-segmentation

The threat landscape is constantly evolving. Data centers running business-critical workloads need proactive security solutions to protect themselves from hidden and emerging threats.

Segmenting data centers, improving security, and ensuring compliance constitute the best strategy to protect against threats, but implementing this strategy can be time-consuming and challenging.

Over the past decade, enterprise IT environments have grown from bare metal servers into hybrid setups consisting of public and private clouds. Even after investing in several high-capacity firewalls and intrusion detection systems, enterprises constantly worry about Advanced Persistent Threats (APTs) and security breaches that may be lurking 'undetected' in the data center.

ColorTokens enables software-defined, platform-independent application micro-segmentation in minutes, reducing the attack surface and improving the overall security posture of your data center.

Use Case Benefits

- Zero-trust network with full visibility and control
- Proactive protection from APT, malware, and insider threats
- Reduced attack surface
- Interoperability with legacy and cloud systems

ColorTokens Technology

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

It brings the focus on end-users and applications. This operational principle makes ColorTokens agnostic to firewalls, virtual machines, and private and public cloud infrastructure, and capable of securing dynamic application workloads spread across bare-metal and cloud data centers.

User access to applications and communication between workloads, within and across segments, is facilitated using security policies.

The policies are defined using abstractions, and not by 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?

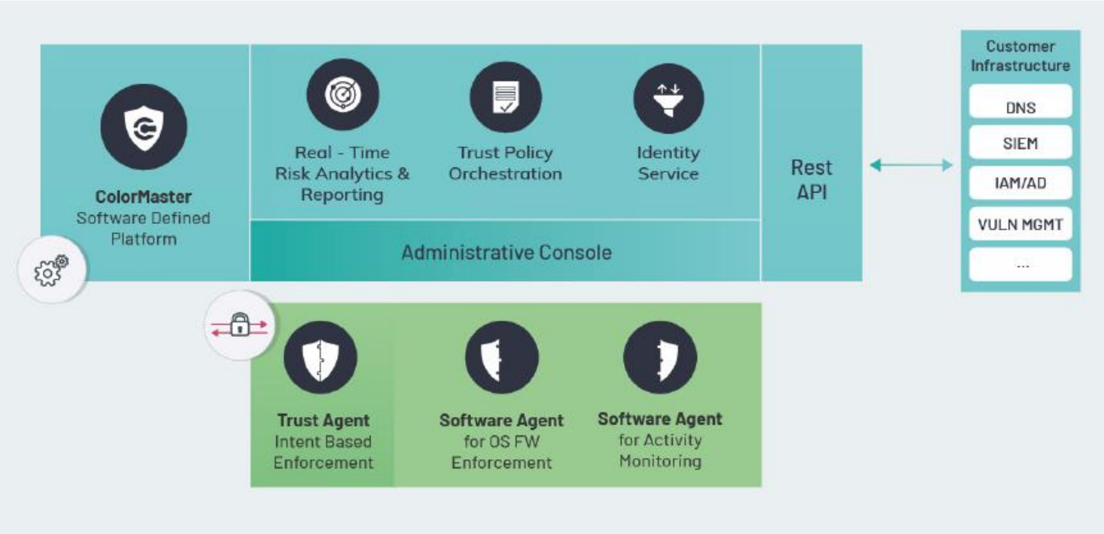
ColorTokens has two main components – ColorMaster and Trust Agent.

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

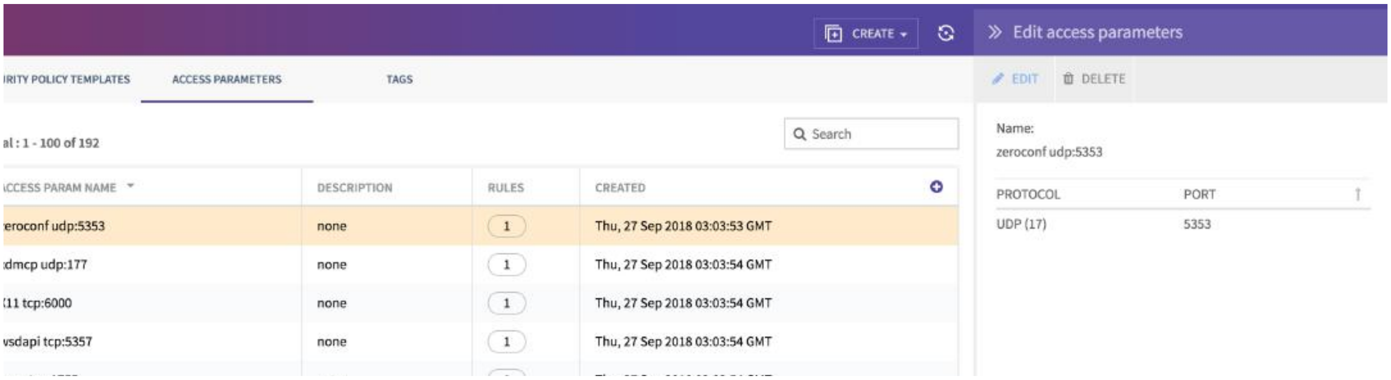
Provides a single-pane of glass for your hybrid data center. It is also the main console that provides all administrative functions including cross-segment traffic visibility, analytics, and security policy simulations and enforcement.



Micro-segmentation Using ColorTokens

Let's consider a scenario where you wanted to segment and isolate the HRM Web, application and database servers located in a production environment. With ColorTokens, you can create reusable security policy templates and access parameters that can be applied on the resources you want to segment and protect.

Access parameters



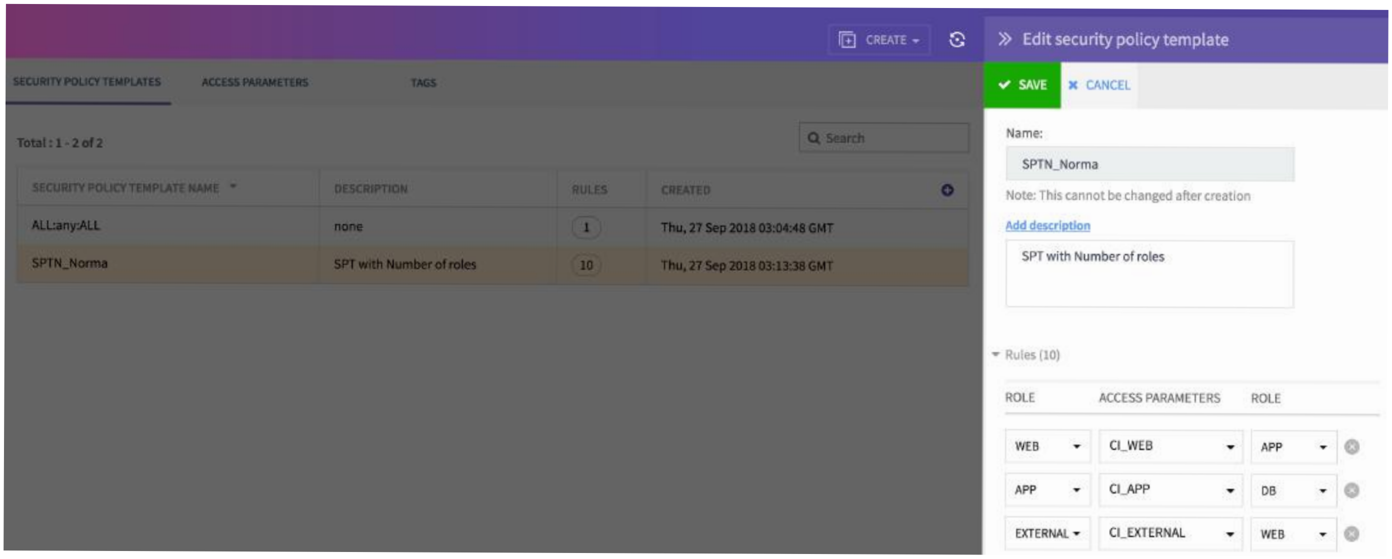
al : 1 - 100 of 192

CCESS PARAM NAME	DESCRIPTION	RULES	CREATED
eroconf udp:5353	none	1	Thu, 27 Sep 2018 03:03:53 GMT
dmcp udp:177	none	1	Thu, 27 Sep 2018 03:03:54 GMT
11 tcp:6000	none	1	Thu, 27 Sep 2018 03:03:54 GMT
vsdapi tcp:5357	none	1	Thu, 27 Sep 2018 03:03:54 GMT

Name:
zeroconf udp:5353

PROTOCOL	PORT
UDP (17)	5353

Security Policy Templates



Total : 1 - 2 of 2

SECURITY POLICY TEMPLATE NAME	DESCRIPTION	RULES	CREATED
ALL:any:ALL	none	1	Thu, 27 Sep 2018 03:04:48 GMT
SPTN_Norma	SPT with Number of roles	10	Thu, 27 Sep 2018 03:13:38 GMT

Name:
SPTN_Norma
Note: This cannot be changed after creation

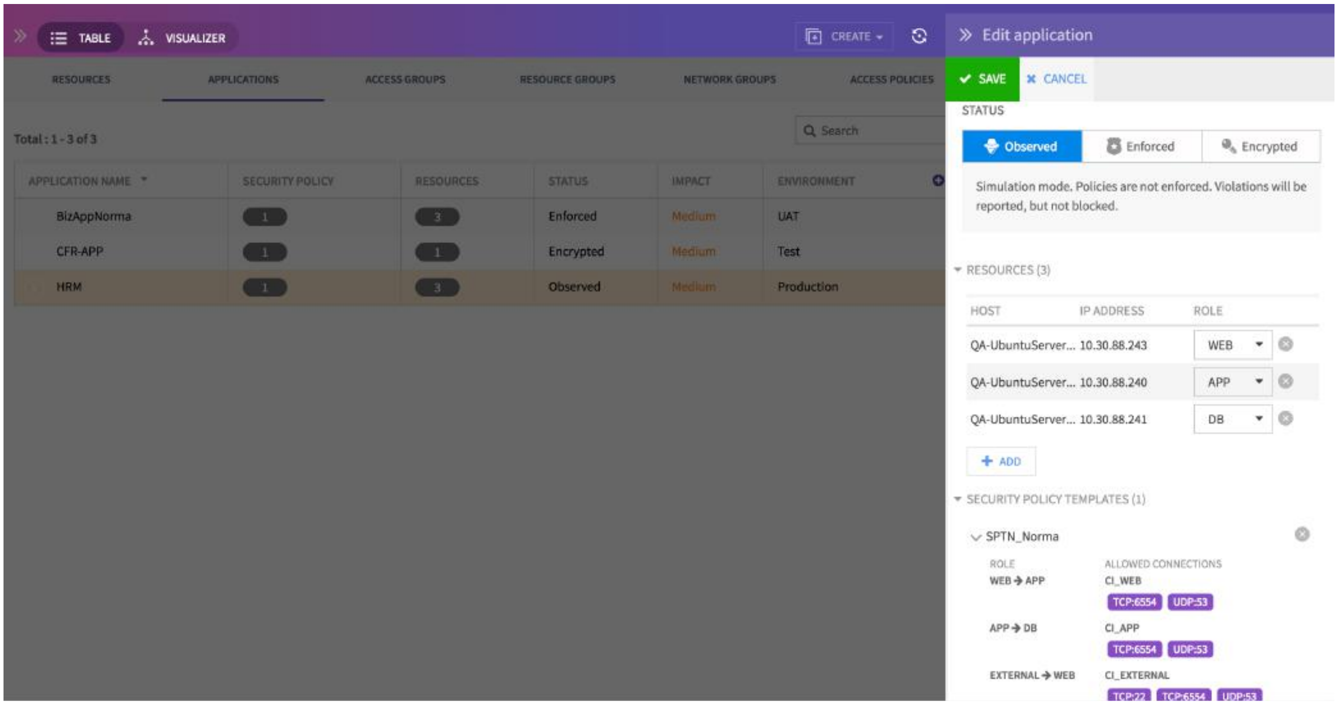
SPT with Number of roles

Rules (10)

ROLE	ACCESS PARAMETERS	ROLE
WEB	CI_WEB	APP
APP	CI_APP	DB
EXTERNAL	CI_EXTERNAL	WEB

After defining the security policies and resource access parameters, you can create an HRM application for segmentation. With ColorTokens intuitive interface, you can assign the corresponding server roles to the HRM Web, application and database servers based on abstractions. You can then apply the three-tier security policy template based on PHP and MySQL over this application.

HRM application defined with the 3-tier security policy template



Total : 1 - 3 of 3

APPLICATION NAME	SECURITY POLICY	RESOURCES	STATUS	IMPACT	ENVIRONMENT
BizAppNorma	1	3	Enforced	Medium	UAT
CFR-APP	1	1	Encrypted	Medium	Test
HRM	1	3	Observed	Medium	Production

STATUS

● Observed ○ Enforced ○ Encrypted

Simulation mode. Policies are not enforced. Violations will be reported, but not blocked.

RESOURCES (3)

HOST	IP ADDRESS	ROLE
QA-UbuntuServer...	10.30.88.243	WEB
QA-UbuntuServer...	10.30.88.240	APP
QA-UbuntuServer...	10.30.88.241	DB

SECURITY POLICY TEMPLATES (1)

SPTN_Norma

ROLE	ALLOWED CONNECTIONS
WEB → APP	CI_WEB TCP:6554 UDP:53
APP → DB	CI_APP TCP:6554 UDP:53
EXTERNAL → WEB	CI_EXTERNAL TCP:22 TCP:6554 UDP:53

Note that when a policy is applied on the application, it is by default in the defined state; all connection attempts and violations are reported (i.e. simulated), but no action is taken until enforced. This state is very useful as you may want to simulate or even test out this security posture before enforcing it – without affecting anything on the network.

Microsegmentation – Traditional vs ColorTokens Xshield

Traditional

Segmenting using subnets – define separate policies for every subnet and configure the VLANs and ACLs.

Cumbersome. Takes hours!

Segmenting using VMs – VMs located on the Hypervisor are not platform agnostic and do not communicate with other resources in a multi-vendor environment. Also, the Hypervisor must be protected to comply with the enterprise security policy.

Too many moving parts!

Segmenting using firewalls – Must provision for capital-intensive advanced firewalls to segment the network and ensure that there's no performance degradation in data throughput. Also, there is no escape from creating and managing thousands of firewall rules.

ColorTokens

Reusable security policy templates, server roles and resource access parameters - **Automate security**

Definable business applications mapped to server roles, security and connection information – **Simplify micro-segmentation**

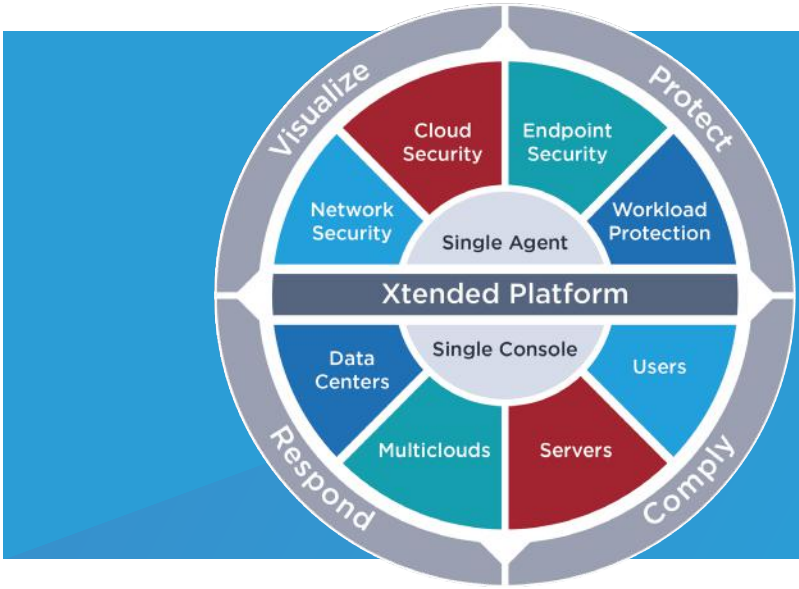
Segmentation across clouds in hybrid deployments – **Future-proof.**

Platform agnostic implementation – **Interoperability.**

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