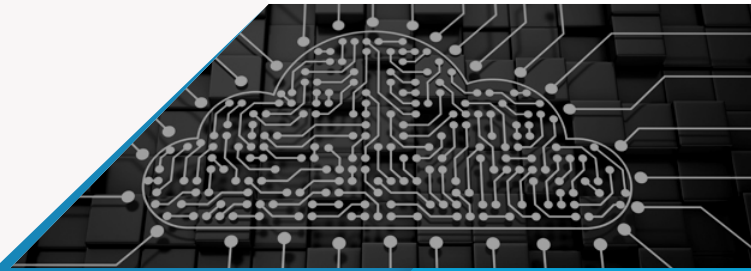


# ENSURING SECURITY AND COMPLIANCE IN HYBRID ENVIRONMENTS USING COLORTOKENS



## Use Case Analysis

**E**nterprises adopt hybrid cloud deployment strategies for a variety of reasons.

Hybrid deployments help enterprises to scale up their data center, cloud burst into a public cloud when demand peaks, and enable disaster recovery. Hybrid deployments also provide cost agility as enterprises can adapt and move forward with the changing business, technology and application requirements.

The most important challenge faced by enterprises while doing hybrid deployments is maintaining a uniform security posture. The IT team is under pressure to ensure that the security policies and compliances remain the same for applications and workloads, be it on their private cloud, or on several public clouds.

ColorTokens software-defined, platform-independent solution enables enterprises gain in-depth visibility across hybrid deployments, reducing the attack surface and improving the overall security posture of the data center.

**58% of the enterprises have a hybrid-cloud strategy, and that's the future<sup>1</sup>**

## | ColorTokens Technology

ColorTokens Unified Security Platform 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, virtual machines, and private and public clouds.

User access to applications spread across hybrid clouds, and communication between workloads, within and across these diverse environments, is facilitated using robust security policy templates. The policies are defined using abstractions, and not by IP addresses or VLAN memberships. ColorTokens provides superior security to hybrid deployments, and adapts to dynamic application movements, providing unparalleled operational ease.

### Use Case Benefits

- Secure, compliant cross-cloud data center extension
- Full security visibility across hybrid clouds
- Continuous protection from APTs and zero-day malware attacks
- Reduced attack surface

<sup>1</sup>Cloud Computing Trends: 2017 State of the Cloud Survey

## | How Does ColorTokens Work?

ColorTokens has two main components – **ColorMaster** and **Trust Agent**.

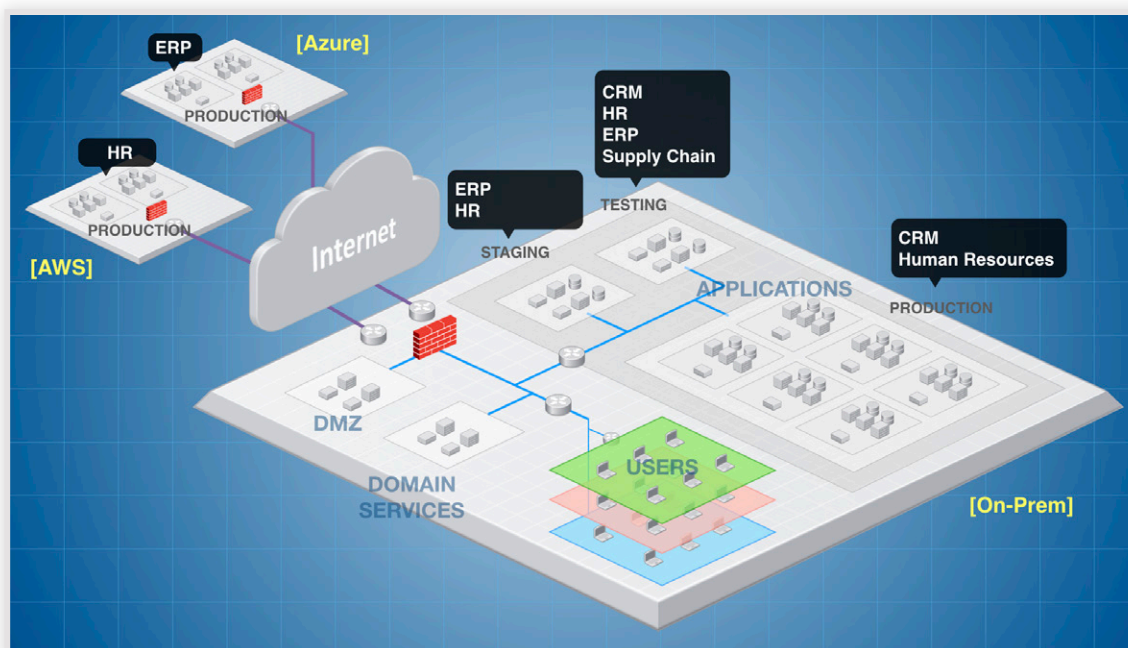
**ColorMaster** provides a single-pane of glass for your hybrid data center, and it is the main console that provides all administrative functions including cross-segment traffic visibility, analytics, and security policy simulations and enforcement.

**Trust Agent** is a light-weight software agent that is deployed on resources to be protected. These agents are hardened, non-disruptive, and never come in the traffic path.

## | Secure Hybrid Deployments Using ColorTokens

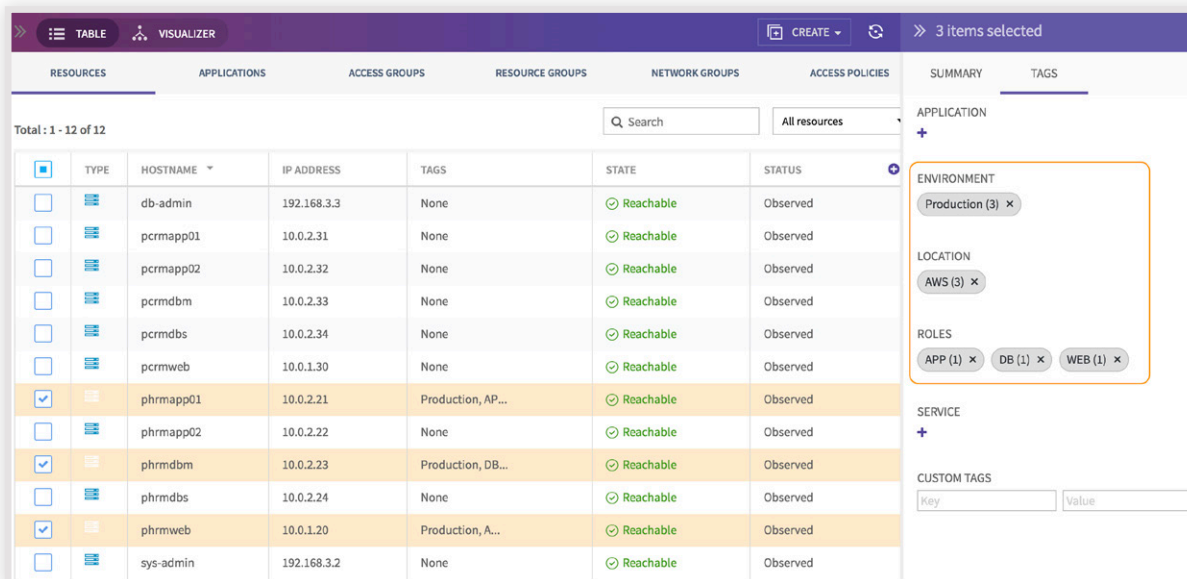
Let's consider a scenario where an HR application is being developed, tested and deployed in your hybrid data center. You want to create the *production* environment on the cloud (for example, on AWS) and the *testing* environment in your on-premise data center.

*Application production and testing environments across on-premise and cloud data centers*



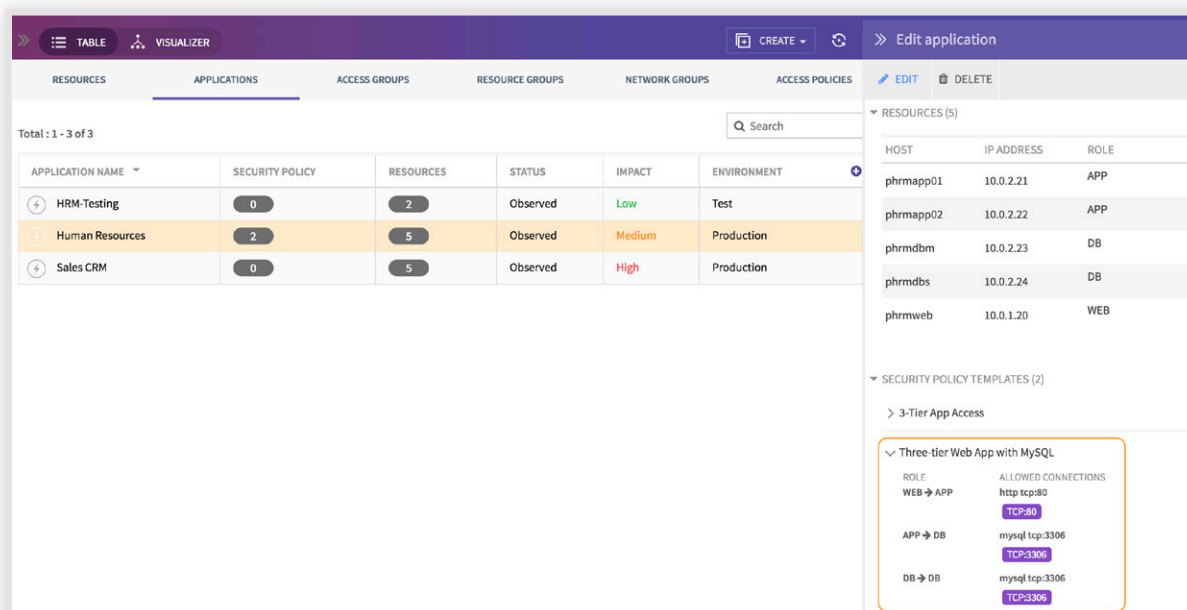
Using ColorTokens central console, you accomplish this by creating the production and test HR business applications. You assign the predefined WEB, APP and DB server roles to the appropriate HR servers (Web, application and database) hosted on the AWS production and on-premise test environments.

HR application, database and Web servers on AWS production environment



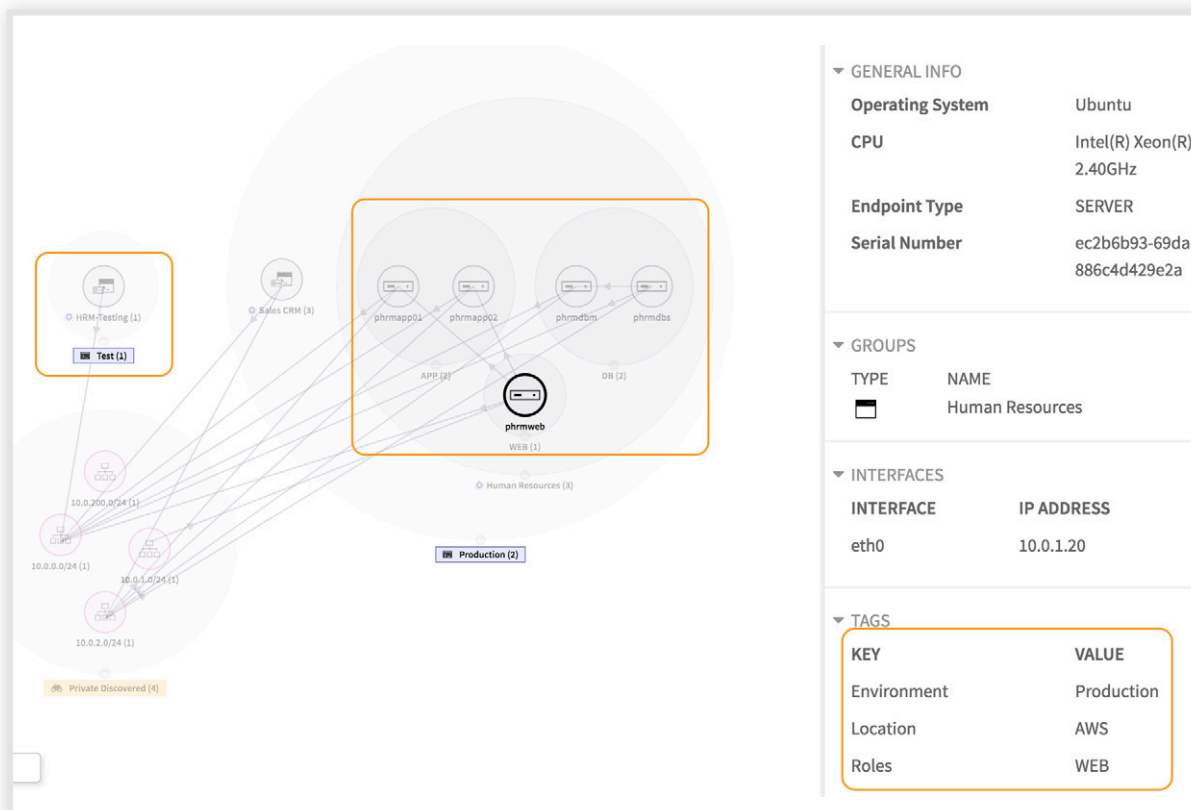
Create and apply reusable security policy templates that suits the compliance and data privacy requirements of the HR applications on the AWS production and the on-premise testing environments. Avoid data privacy issues by securely isolating the production data from testing and development environments across clouds without the need for internal firewalls.

Reusable security policy templates



Even though the data center technologies are different, ColorTokens gives you in depth visibility into the workloads, traffic and security posture across the Azure, AWS and on-premise data center deployments. Even if these resources move, the security policies previously applied will follow them, maintaining a uniform security posture across enterprise IT environments.

Hybrid deployment of the HR application on the cloud and on-premise data centers







Without ColorTokens, you would have to juggle with several tools to understand what’s happening in different sections of your hybrid application environment.

## | Securing Hybrid Deployment - Traditional VS ColorTokens

Traditional	ColorTokens
Same security and access policies for apps hosted on bare-metal, private or on the public cloud – <b>Cumbersome manual processes.</b>	Promote/remove resources to/from their respective roles – <b>Retain defined security policies.</b>
Deal with a different firewall on the public cloud. Spend hours configuring rules to match the organizational requirements – <b>Configuration errors. Takes hours.</b>	Edit and move business applications across clouds from within a central console – <b>Save time.</b>
Learn and unlearn software from multiple vendors, and deal with IT personnel from multiple departments to achieve the desired security posture, visibility and control – <b>Too many moving parts.</b>	Define roles like Web, App and DB – <b>Reuse across several resources.</b>

## | ColorTokens Products

ColorTokens Unified Security Platform, based on the zero-trust architecture, can see, stop, and predict security and compliance violations across any workload, any deployment, and any user.

-  **ColorTokens Unified Threat Visibility and Analytics (ColorTokens Visibility)**  
Provides comprehensive visibility across all workloads, servers, containers and distributed endpoints and users, including special purpose systems like ATMs and kiosks. This layer provides actionable intelligence: topology and interaction of apps and the underlying infrastructure. Security operators can look at the risk posture, analyze security vulnerabilities and their impact on the network. You can audit traffic from VLANs/ACLs and are more confident about your security posture.
-  **ColorTokens Unified Intent Based Enforcement (ColorTokens Intent Enforcement)**  
Create zero-trust environments by enforcing resource access policies specific to individual network segments. Using micro-segmentation with residual risk metrics, and with policy simulations and enforcement, enterprises can visualize ‘what-if’ scenarios for accurate policy deployments or to even probe the resiliency of the hybrid data center.
-  **ColorTokens Identity based enforcement (ColorTokens Secure User)**  
Implement zero trust based on user identity and control user access to application workloads in a cloud or on-premise servers. Reduce the attack surface on critical infrastructure due to lateral movement of malware that piggybacks on office users and BYOD. Get granular visibility into unauthorized workload accesses or anomalous user behavior. This deep insight further simplifies compliance and forensics investigations.
-  **ColorTokens Radar360 (Advanced Signature-Less Endpoint Security)**  
ColorTokens Radar360 is a signature-less security solution that works at the kernel level to detect, alert and prevent unauthorized processes from running on your end-points, special purpose terminals and critical servers. Radar360 comes as an ultra-lightweight agent and deploys in under five minutes on Windows and Linux desktops and servers, instantly enabling process-level visibility and control for enterprises.

## | About ColorTokens

ColorTokens is a Silicon Valley company, backed by legendary investors and advisors who have helped structure the IT industry over last 30+ years. ColorTokens’ core team brings deep and innovative industry experience from brands such as Cisco, Juniper, VMware, Microsoft, and Zscaler in domain areas including cybersecurity, networking, and infrastructure. With customers and partners worldwide, ColorTokens is headquartered in Santa Clara (Silicon Valley), CA, USA with a major center of development and sales in Bengaluru, India.



For more information about the ColorTokens solution email us at [sales@colortokens.com](mailto:sales@colortokens.com)

Call +1 (408) 341-6030 to speak to a ColorTokens security specialist.