

CREATING SECURE, AD HOC NETWORKS OVER PRIVATE, PUBLIC & HYBRID CLOUDS

Use Case Brief

Purpose-built, on-demand networks are a great way to support the dynamic needs of today's enterprises. Most ad hoc networks are built by leveraging hybrid infrastructure, and this brings in significant security and network management challenges.

Use Case Benefits

- Secure micro-segmentation
- Centralized policy management
- Obscure critical assets

Traditionally, network management tools, like VLANs and firewalls, have been used to segment networks. This becomes extremely cumbersome as your IT network grows and is highly error prone. Every time a user moves from one location to another or changes roles, the VLAN or firewall policies need to be rewritten, increasing unnecessary operational overheads.

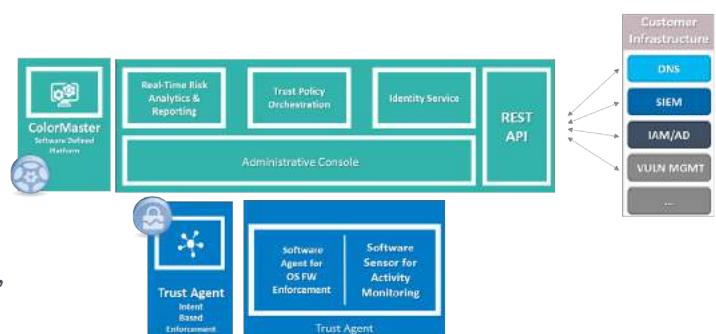
To compound this challenge your IT security teams, have little or no knowledge and control on underlying infrastructure of your public cloud. This raises questions on how you secure the data, that is leaving your enterprise perimeter. Most public cloud providers work on a shared-security model. This means, in a multi-vendor environment, enterprises must work with all public cloud providers to ensure, uniform security policy effectiveness across private and public clouds when creating ad hoc networks. User access is also another critical aspect in ad hoc networks and it's imperative to ensure authorized users retain access to assets independent of their location.

| 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.



| Ad hoc Network using ColorTokens

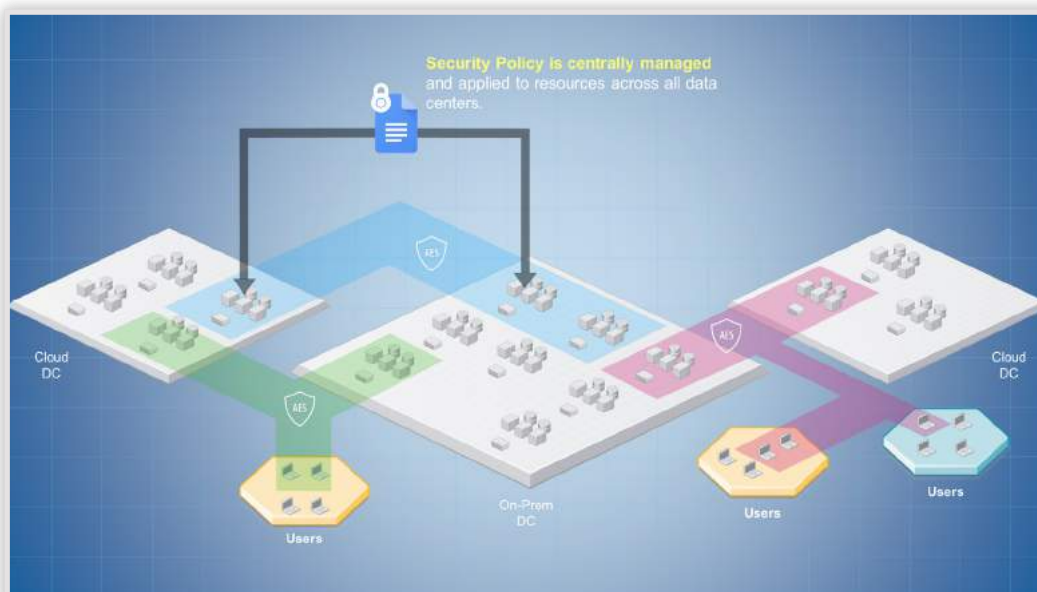
ColorTokens provides software-defined security across private, public and hybrid clouds. The ability to secure networks, independent of the underlying infrastructure, is useful for enterprises and armed forces. This is achieved through secure micro-segmentation that helps in creating secure segments in hybrid clouds and assist IT departments to overcome number of deficiencies that exist in traditional segmentation tools such as VLANs and firewalls.

ColorTokens reduces the attack surface by making critical resources inaccessible. This approach simplifies the execution of zero-trust network by pro-actively eliminating potential targets.

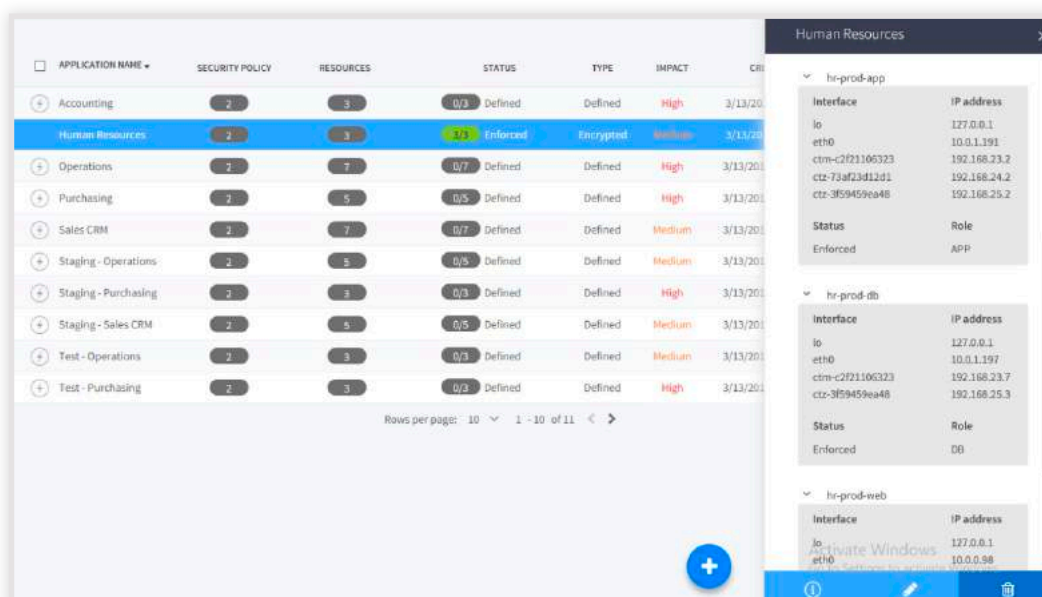
ColorMaster provides a comprehensive inventory of all enterprise resources. Security operators can define the logical segments and allocate resources to these segments across private, public and hybrid clouds. The Security operators can, then, define security policies that govern connectivity within and across the logical segments in the ad hoc networks.

Once added to a segment, a resource remains in the segment regardless of their location or the underlying infrastructure. For example, armed forces can simplify complex IT procedures when soldiers and equipment are temporarily reassigned from their primary battalion or brigade. As the security policies are defined at the segment level, they follow the resource regardless of their location or platform. This is critical since most solutions, even with micro-segmentation capabilities rely on static definitions to segment resources (e.g. VLAN, VxLAN, etc.) which means that when a resource moves from one location or battalion, he or she may be exposed to threats again.

Centrally manage security policies across the ad hoc network



ColorTokens further enhances security by making resource inaccessible and invisible to unauthorized users within and outside the segment. This ability of obscuring resources provides exceptional security to ad hoc networks which is completely independent of the underlying infrastructure.

Escalate security with ColorTokens

Finally, with ColorMaster, security operators can visualize resource interaction and manage policies with ease resulting in enhanced cyber security.


ColorTokens simplifies creation of ad hoc network and management of mobile workforce and resources independent of the underlying infrastructure from a single unified management control with ease.


| Ad hoc Network - Traditional vs ColorTokens


Traditional	ColorTokens
Highly dependent on networking tools to create segmentation, which is complex and cumbersome. Segmentation using VLANs in an ad hoc network is a huge operational burden and error prone.	Achieve host based micro-segmentation which is more effective than network-based segmentation. This provides granular view and control for defining policies and securing access to critical assets.
Coordinate with multiple public cloud providers to define security policies. Security operators must ensure that these policies are consistent across the ad hoc network that spans over public, private and hybrid deployments.	Security operators can test and manage security policies across the ad hoc networks. The changes in security policies are propagated automatically and simultaneously across the hybrid infrastructure in the ad hoc network.
Traditionally, ACLs have been used to control access to critical resources, but this is extremely tedious.	Rogue or malicious users in another segment cannot see critical resources in the same or other segments. Critical resources are rendered inaccessible to unauthorized users by leveraging, ColorTokens technology.

| ColorTokens Security Platform Delivers Technical Innovation Through

ColorTokens Unified Security Platform, based on a 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)** – Critical layers of security and compliance visibility for all workloads and users. The layers provide actionable information: topology and interaction of apps and the underlying infrastructure, a security risk posture showing security vulnerabilities and their impact on the rest of the network, and automated exploit testing to show the impact of potential threats on the environment.

 **ColorTokens Unified Intent Based Enforcement (ColorTokens Intent Enforcement)** – Zero-trust environment through the enforcement of resource actions, collection of telemetry information stops policy violations and determine malicious intent. With policy modeling and policy-based war gaming, organizations can visualize “what-if” scenarios for accurate policy deployment and probe resiliency.

 **ColorTokens Unified Secure User Segmentation and User Access (ColorTokens Secure User)** – ColorTokens Secure User securely enables users to access only those apps they are authorized to access. This goes beyond simple identity and access management and looks at the risk level the user provides to the workload. By combining the user risk and ensuring the user has only access to the specific apps required, insider theft or compromised resources/credentials no longer pose a threat to the workloads.

| 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.

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