COLORTOKENS

Use Case Brief

Granular visibility and contextual analytics for your hybrid datacenter.

Use Case Benefits

- Get 360° security views with infinite granularity.
- Identify indicators of compromise (IoCs) ahead of the actual threats.
- Simplify compliance and audits for your, multi-cloud environments.

Visibility is the underpinning of any cybersecurity strategy, and increasing complexity of distributed enterprise networks makes this extremely challenging.

Most organizations today deploy multiple solutions to gain visibility across cloud workloads, on-premise database, distributed endpoints and users. This quickly results in a fragmented view of the enterprise. And with all the static dashboards and scattered information, you have no way to co-relate logs, that can flag a malicious user, a lateral threat or suspicious activity across your distributed network. Without comprehensive visibility, how do you identify and protect high risk, critical assets?

ColorTokens Technology

ColorTokens can provide comprehensive visibility across the hybrid data center. The technology is vendor agnostic and can work with any server, database, workload, endpoints, special purpose systems among others. At the core, is the state-of-the-art analytics engine that collects telemetry data from managed resources and provides contextual information and protection even from the well-orchestrated modern attacks.

ColorTokens has a built-in vulnerability assessment tool integrates with a market leading threat intelligence feeds to provide a multidimensional risk posture of your enterprise. This helps enterprises protect from zero-day threats and make get proactive.

How Does ColorTokens Work?

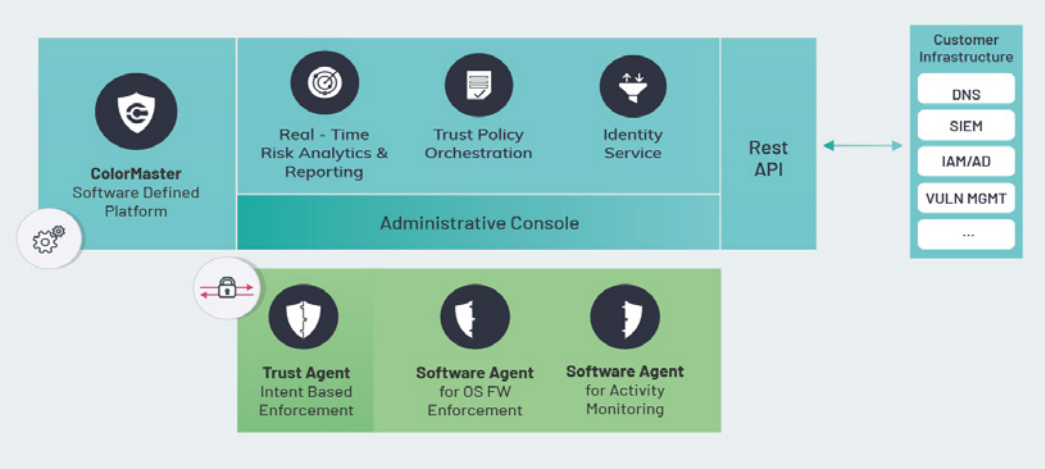
ColorTokens has two main components – ColorMaster and Trust Agent.

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

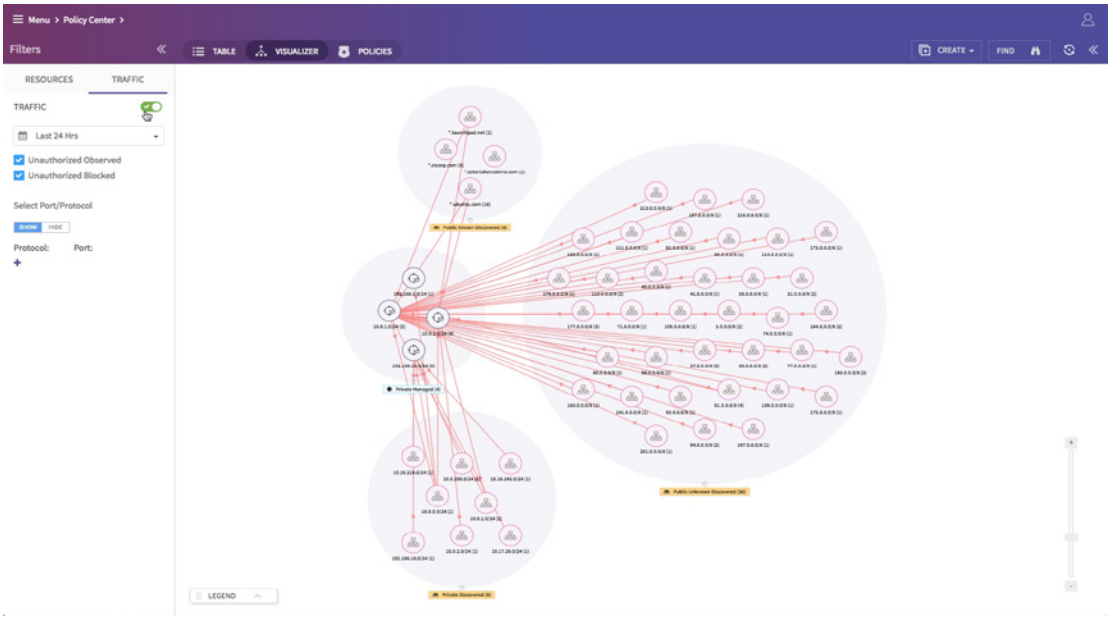
Provides a single-pane of glass for your hybrid data center. It is also the main console that provides all administrative functions including cross-segment traffic visibility, analytics, and security policy simulations and enforcement.



Comprehensive visibility using ColorTokens

ColorTokens provides granular visibility, in every communication between the network, applications, processes, and workloads. ColorMaster's centralized dashboard collects telemetry data from all the ColorTokens managed resources. Security operator can enable traffic view and get a comprehensive network view, without the use of traditional technologies such as network taps or probes.

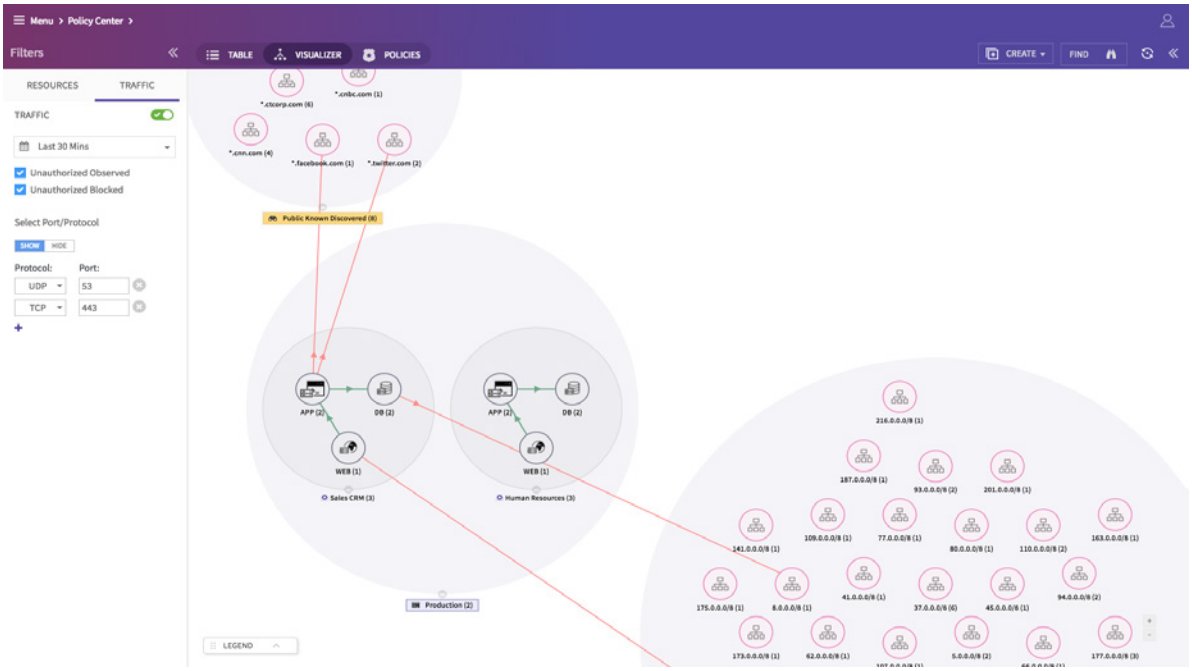
Comprehensive network visibility



The traffic lines provide clear visibility into how resources are communicating among themselves, inside or outside the enterprise boundary. You can also group resources by attributes for better cross-cloud visibility and to identify compliance violations.

The portable policy templates can be applied to resources to validate compliance violations, such as misconfigured DNS servers or unauthorized access of production servers to the public internet.

Audit network traffic

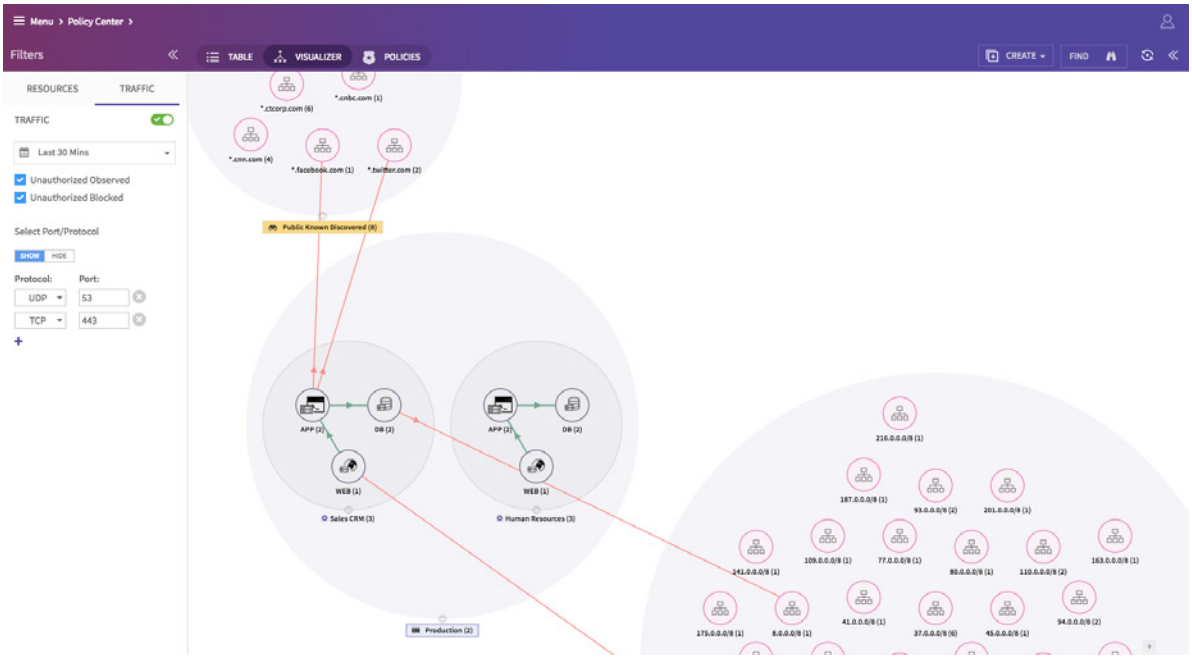


Detect threats with advanced analytics

Identify indicators of compromise (IoCs) and vulnerabilities making potential future threats unsuccessful.

ColorTokens has an inbuilt vulnerability assessment tool; also, there is integration with threat intelligence feeds. This capability provides a multidimensional risk posture analysis. With ColorTokens organizations can stop zero-day attacks, mine telemetry data with powerful, filtered search across 20 plus parameters. This capability makes threat analysis powerful. Besides, customize notification, show where to focus and reduce security vulnerabilities across the far end of your hybrid enterprise.

Delete text and image



With ColorTokens residual risk metrics, enterprises can strategically assign resources to safe-guard high value, high-risk assets.

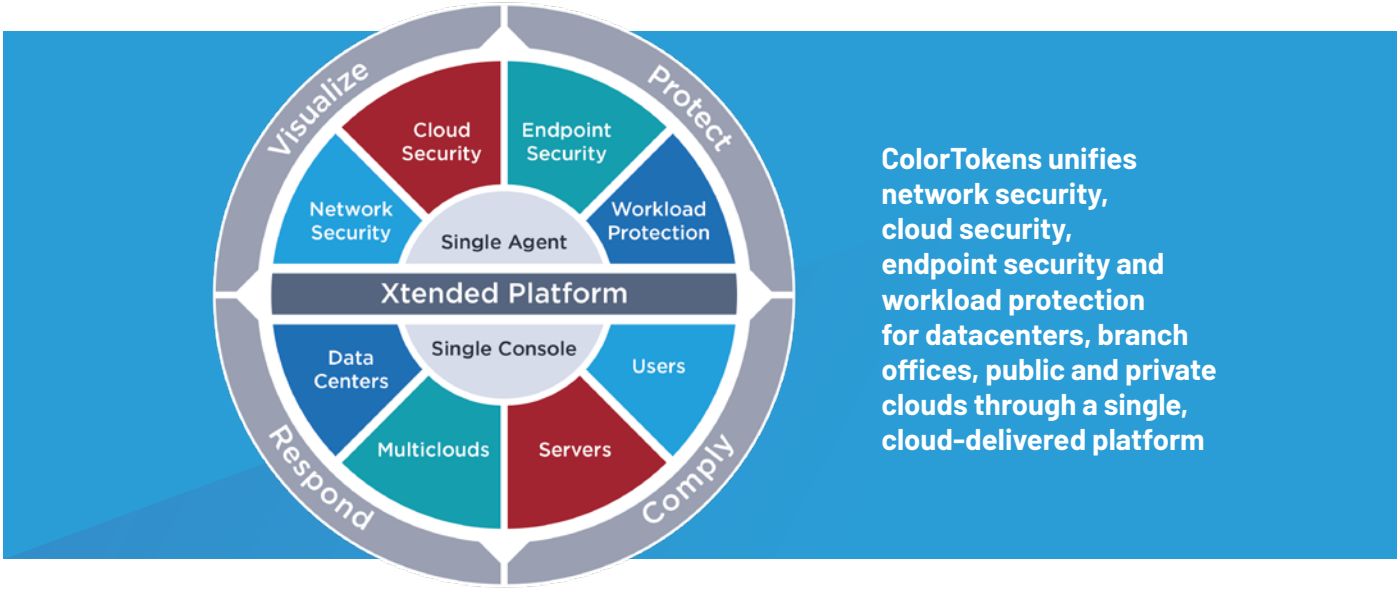
Comprehensive visibility and contextual analytics — Traditional vs ColorTokens

The table provides a list of key differences between thet raditional vendors and ColorTokens approach in providing a comprehensive and contextual visibility.

Traditional	ColorTokens
Usually layer-specific and either network-centric or server-centric. Unable to provide an application-based view of the enterprise data center.	Application-focused, and topology view displays workloads and devices regardless of whether container, VM, server or end-user device.
Typically require separate installations to visualize each datacenter and public and private cloud resources. No integrated view.	A unified solution that is vendor agnostic. Managed resources can be on-premise or in the cloud. It doesn't matter!
Not security focused. Cannot detect IOCs or zero-day threats. Leaves high-risk, high-value assets exposed to threats for a longer time.	Built-in vulnerability assessment tools and full integration with market leading threat intelligence feeds. Allows security teams to detect threats in advanced and deliver proactive security.
Complex installation, longer deployment time and a slow ROI.	ColorTokens can be deployed in minutes across your hybrid infrastructure. The centralized dashboard can start collecting telemetry data instantly – providing faster value.

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:



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