COLORTOKENS

Use Case Brief

Protect workloads from lateral threats in any public, private or hybrid deployment.

Advanced Persistent Threats (APTs) circumvent enterprise security by using "advanced" malware that exploits the system or network vulnerabilities.

APTs stealthily perform reconnaissance and move laterally through the network. The "threat" is orchestrated by a human or software (called the command and control), actively camouflaging to the environment.

Most organizations struggle to reduce dwell time for APTs that manage to penetrate in the enterprise environment. IT transformation further complicates hybrid cloud deployments that include multiple administrators, platforms, and partner/guest environments, thus expanding the surface area of the attack.

Technologies such as micro-segmentation reduce the spread of lateral APTs. An APT that successfully penetrates the network remains aware of the environment, and a CNC may choose to try and re-infect the network at a later time.

Use Case Benefits

- Disrupt lateral threats in the hybrid data center.
- Reduce dwell time.
- Negate operational overhead.

ColorTokens goes one step further and makes resources inaccessible. And by doing so, it ensures that both the APT and any external threats (like the CNC) cannot reach the network resources.

ColorTokens Technology

ColorTokens disrupts APTs and reduces dwell time by preventing the malware from migrating beyond the initial attack surface to other adjacent networks or resources. It goes further and stops any CNC communication halting data ex-filtration.

ColorTokens micro-segmentation can help in reducing the lateral spread of APTs, but since the APT is still aware of the network environment, micro-segmentation may not be sufficient since the CNC may choose to try and re-infect the network. ColorTokens escalates security by making resource inaccessible. Stopping any on-going communications between the APT and external threats (like CNC), this halts data ex-filtration.

Resulting in on-time containment and expediting remediation. Smaller APT footprint further eases root cause analyses and forensic investigations.

How Does ColorTokens Work?

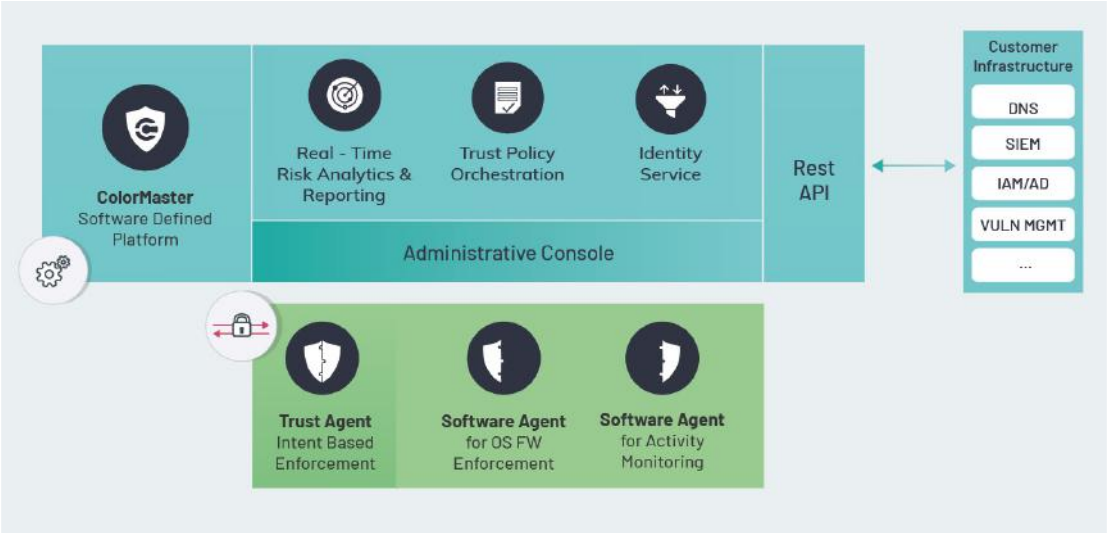
ColorTokens has two main components – ColorMaster and Trust Agent.

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.



Protection from Advanced Persistent Threats using ColorTokens

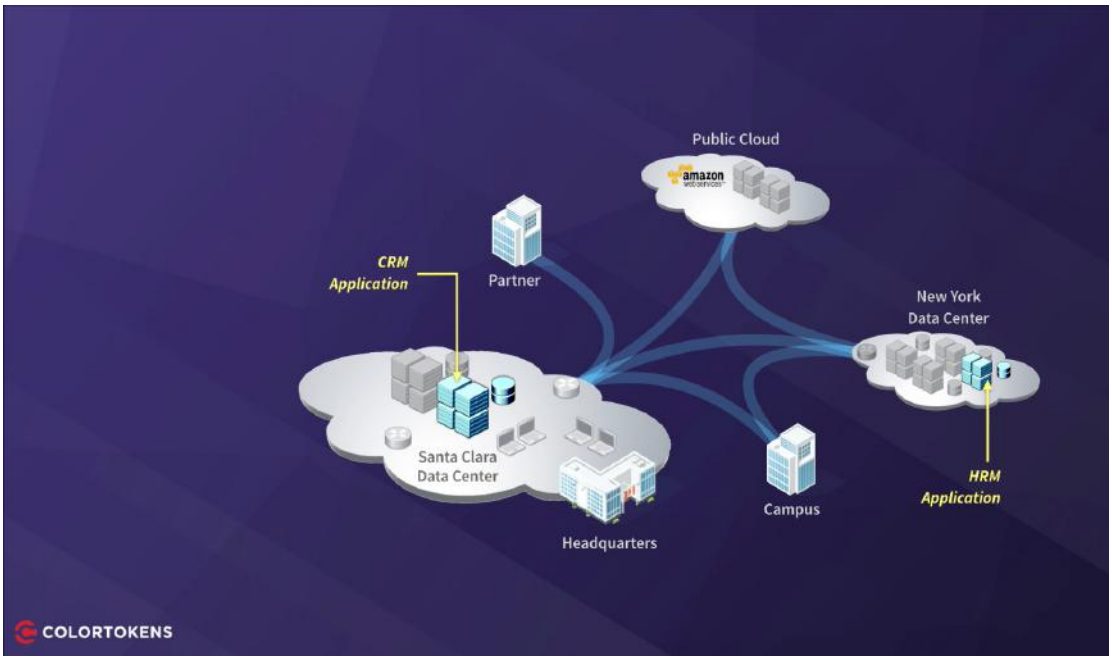
The ColorMaster is a management console that provides a comprehensive inventory of essential enterprise resources. From the console, the security operator can define logical segments and allocate resources to each logical segment. This operation can be done using GUI or automated using API. The security operator can then define security policies that govern connectivity within and across the segments.

Once added to a segment, a resource remains in the segment regardless of its network attachment or location. For example, a resource may be physically moved from one data center (or cloud) to another and will remain in the same segment. The security policies are defined at the segment level and follow the resource regardless of location or platform. This is critical since most solutions, even with micro-segmentation, rely on static definitions of segmenting resources (e.g., VLAN, Internal firewall, etc.) which means as the resource moves (as in the case of a hybrid workload), it may be again exposed to a lateral threat.

Post resource segment assignment, all resources within a network/application segment are made inaccessible and invisible to other segments, inside and outside the segment. This, effectively, makes targeted resources invisible and inaccessible to reconnaissance and other tactics that APTs may try to regain from an infected resource in the future.

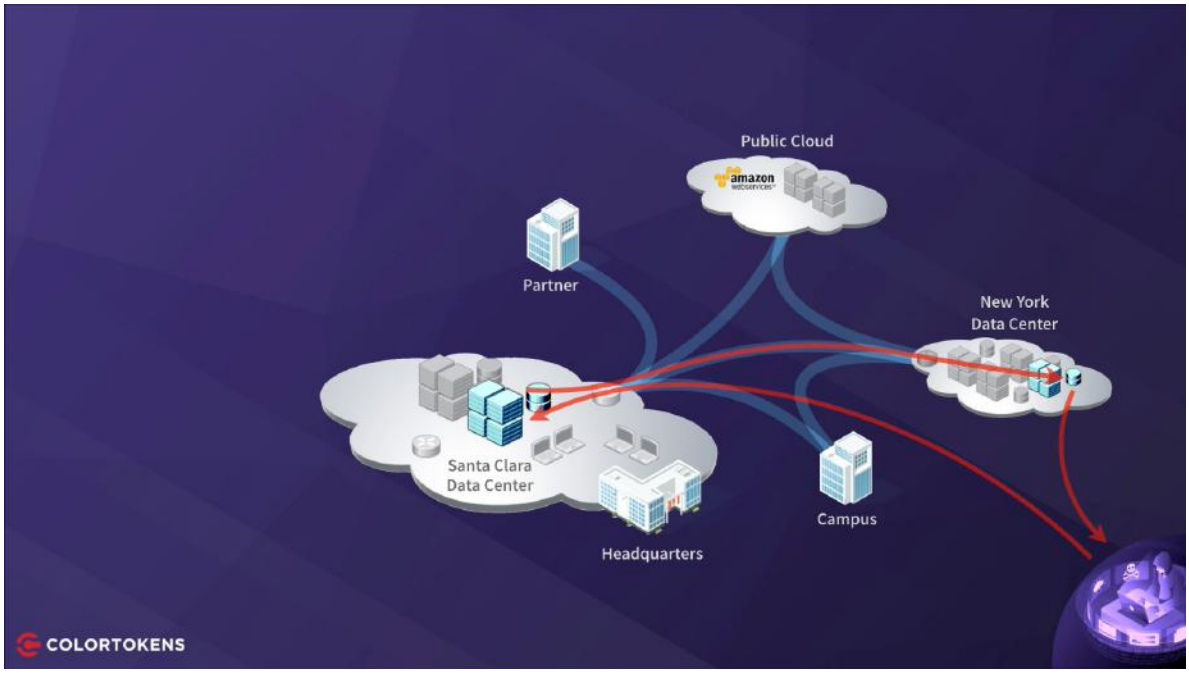
Finally, with ColorMaster, security operators can visualize application interactions to understand APTs traversal in the network and its point of origin. This helps pinpoint users, devices, applications, or workloads resulting in faster containment and remediation.

Enterprise application deployment across a data centers



Consider data centers with two production application: CRM application used by the sales employees, HRM application used by the HR employees. Both applications have development versions that are accessed by R&D employees. Now let's review the simulated attack, the red lines indicate the ongoing APT attack.

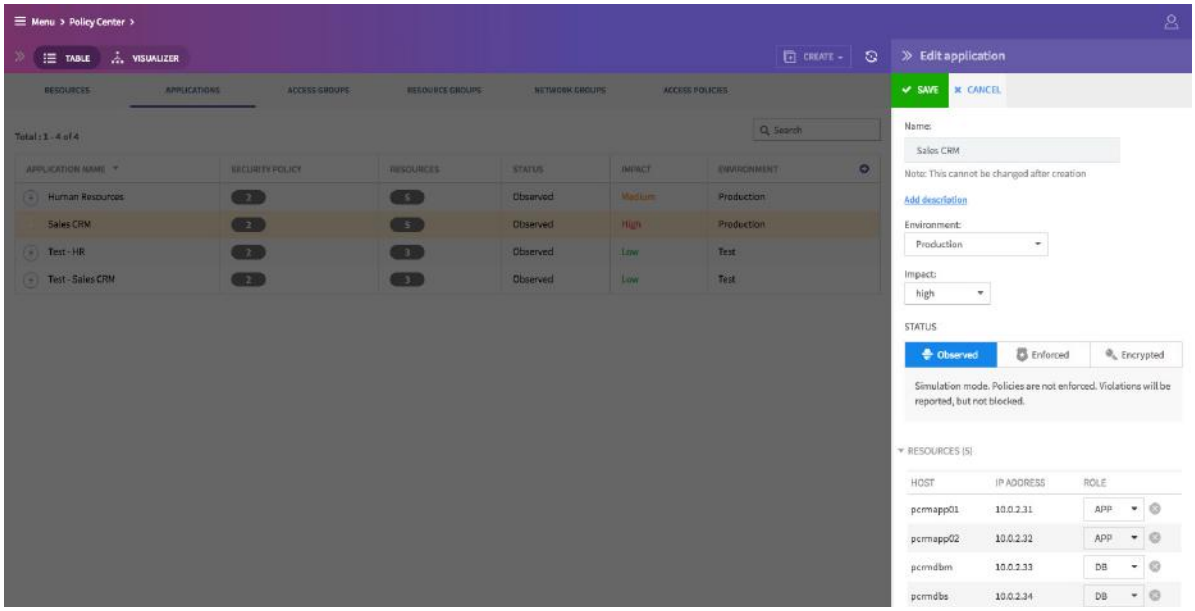
Simulated APT



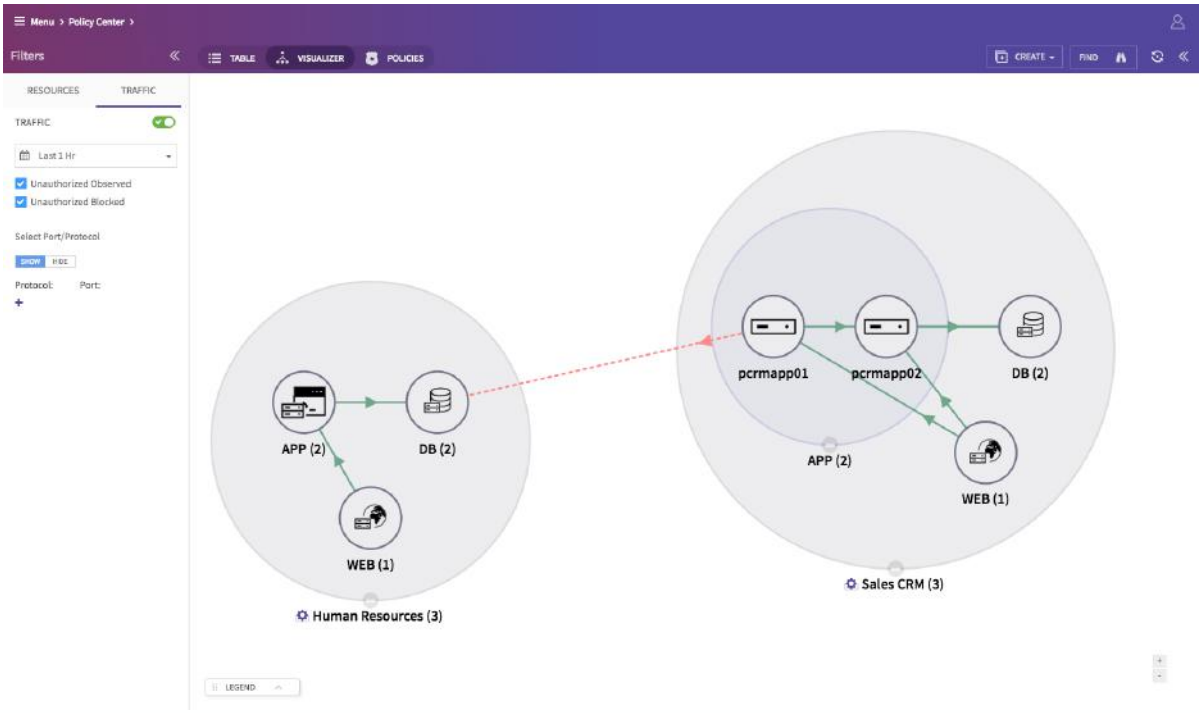
ColorTokens can provide visibility in discovery mode, to see the hackers CNC system communicating with HRM web server and then to the CRM DB server.

Now let's protect the CRM application from the lateral threats. ColorTokens provides simulation and enforcement mode for policy enforcement. In simulation mode, security operators can apply policies detect violations without blocking; this allows administrators to test policies. Post-testing, IT admins are more confident about the business outcome and enforce policies.

Policy enforcement



Blocked APT attack



Protection from Advanced Persistent Threats - Traditional vs ColorTokens

Functionally, in a static environment, a firewall can accomplish several benefits as discussed earlier. The challenge occurs with a dynamic environment (hybrid workloads, dynamic applications, moving users or workloads) and the integration of a partner or semi-trusted network.

Micro-segmentation, as a response to the static VLAN/ACL approach has some benefits but has its own limitations. Commercial micro-segmentation products require significant setup and deployment time. In addition, many of these tools are not very easy (if at all) to use in a hybrid cloud environment where the cloud provider may not have the same segmentation platform as the enterprise.

Traditional

Security in some sense from initial compromise, but expensive and difficult to mitigate laterally propagated threats. Cannot secure cloud-based (or hybrid) workloads. Specialized skills or analysis may be required.

Longer time to analyze threat-trail proves lethal, resulting in the lateral spread and data exfiltration. This lateral spread further delays investigations and the ability to limit the blast radius.

Traditionally enterprises are compelled to invest in multi-point tools to protect from APTs, increasing operational burden and costs.

ColorTokens

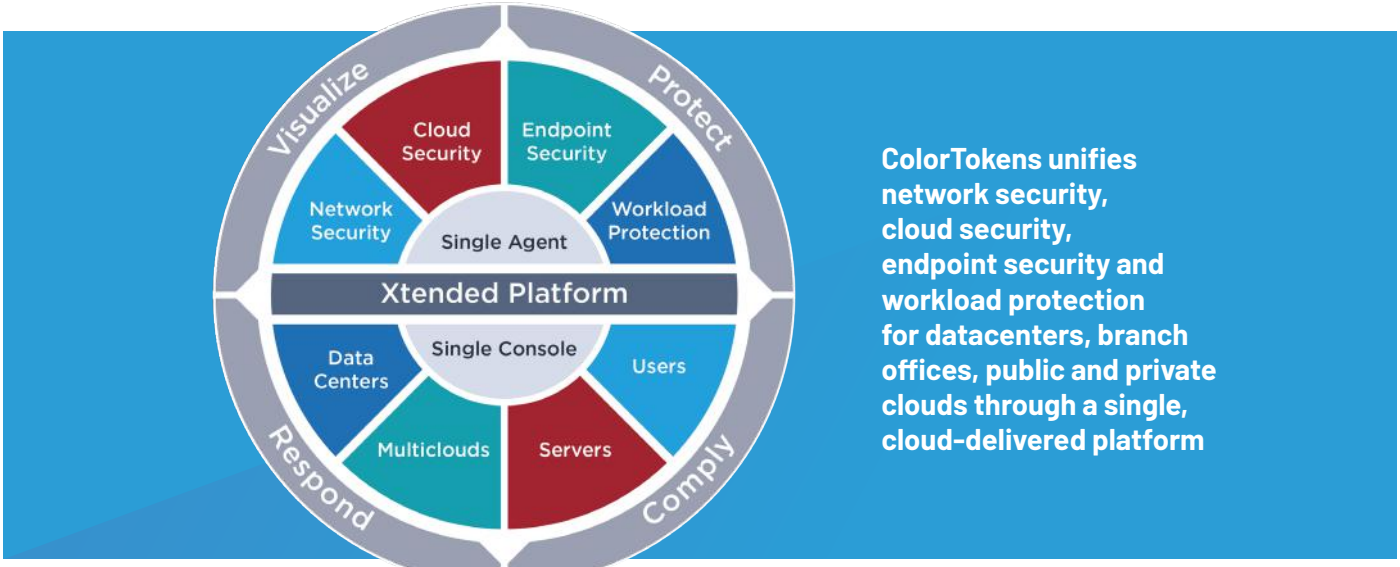
Existing advanced threat protection solutions can remain. For new cloud workloads or for internal networks, and business applications ColorTokens can work in conjunction.

Correlation using telemetry data with access to most granular level of information - IP, topologies, ports, processes, across the threat-trail will provide swift actionable intelligence.

Eliminates the need for traditional, security solutions. Visualize lateral threats and impact to business instantly without ATP solution/sandboxing.

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