ColorTokens' Zero Trust Security Platform

2022 Release R8, Version 8.22.8.11

What's Included?

Products' Brief..... 2
Xshield..... 3
Xaccess..... 3
Enhancements..... 4
Resolved Issues..... 5
Changes to Public APIs..... 6

Product's Brief

The ColorTokens' Zero Trust Security Platform is a multi-tenant Software As A Service (SaaS) security platform built to manage key security functions for an enterprise.

Xshield

Xshield Core is a cloud-delivered micro-segmentation solution based on a Zero Trust platform that secures corporates' critical assets, including applications and workloads. The infrastructure-agnostic platform simplifies and accelerates the enterprise journey to hybrid environments, driving full cloud adoption with a Zero Trust security model. It deploys seamlessly and enables enterprises to visualize and define secure micro-segment boundaries (micro-perimeters) for their application workloads.

Xaccess

Xaccess is a Zero Trust Network Access (ZTNA) platform that provides customers a secure Zero Trust remote access to employees, third parties and contractors while accessing cloud or datacentre-based applications. Xaccess allows customers to define intelligent and user identity-based access while handling more common and complex use cases such as enabling remote IT admins with deeper access specifications or session-based access needed for multi-user terminals. Its AI-based access engine dynamically autogenerates access policies based on risk, usage, and disruption metrics. Xaccess is easy to deploy, and it operates with no infrastructure or architecture constraints, no network or firewall configuration changes. It provides seamless On-Network and Off-Network user onboarding experience. It comes with built-in integrations for multiple identity providers for authentication and single sign-on.

Enhancements

Network Firewall Integration - Policy creation & enforcement

- ColorTokens' Zero Trust Security Platform will now support creation of policies between a managed network group (Group of servers where ColorTokens' agent cannot be installed, which are protected by user's firewall, integrated with ColorTokens' platform & configured with microsegmentation policies) and other public or private network groups. The enforcement cycle for a Managed Network Group has also been brought in line with the normal enforcement cycle of Observed, Observed (Blocked) & Enforced.

Ability to add description for policies

- Users will now be able to add a description to the policies that they create. Description, if added, would ease the usage of these policies across the user's environment without having to open each policy and understand the context of creation. This field will not be mandatory to fill, however, users can add, update, read & delete the description, as deemed necessary.

Audit logs & alerts at respective asset & group level

- Audit logs & alerts will now also be displayed under the associated asset and group page. Users will be able to correlate any audit log or alert with the respective asset or workload group and fasten their time to action, when necessary.

Enablement of re-direction to untagged assets post asset approval stage

- Upon approving an asset while onboarding, users will now be redirected to the assets page which will display the approved & custom-untagged asset list to the user for simplifying the further process of tagging those approved assets particularly.

Warning on the possible impact upon modification to tags

- ColorTokens' Zero Trust Security Platform will now warn its' users of the impact of adding & deleting tags before the tag modifications made by users are applied to the groups & their respective assets. This warning will help users understand how many assets and their respective memberships are getting affected upon their custom tag updates.

Search query Updates

- ColorTokens' Zero Trust Security Platform is continuously enhancing its search queries in order to support its users for enhanced searches. In this release, users can expect the following updates to the search queries on the platform's hosts', workload group & endpoint group listing pages respectively :

1. Users will now be able to exclusively search for assets with no custom tags assigned via the search query " asset.custom_tagged=FALSE" on the Hosts page. A filtered view of only those assets where tagging is pending can be obtained using this search query, rather than scrolling through the list of assets for the same.
2. Users will now be able to search for groups based on the state of the firewall fusion using the query "group.firewallFusion" on the group listing page on the platform
3. ColorTokens' Zero Trust Security Platform will now allow users to perform a search for their respective endpoint machines on the endpoint group listing page using the search query

"User.email". This search query will enable users to reduce their time to find the intended endpoint and take faster actions while troubleshooting issues or upgrading agents, etc.

Re-labelling of Hosts & Users

- Hosts or assets would be re-labelled to "Servers" & Users to "Endpoints" across the ColorTokens' Zero Trust Security Platform for ease of users' correlation of the labels & their respective functionalities.

Blocked traffic details to be sent in the email notification

- Users will now receive informative emails to their configured mail IDs when there is a certain network traffic observed, which is blocked by defined policies on the ColorTokens' Zero Trust Security Platform. This email would be generated with information regarding the source, destination, port & protocol of the blocked traffic, in order to alert the users for a policy violation attempt.

Resolved Issues

- **CTSP-31421 -** Duplicate policies were observed to be appearing when user created a policy manually and accepted the same policy from the policy recommendation. A check for duplicate port policy has been established for a user accepting duplicate port protocol through recommendations.
- **CTSP-30405 -** Issues reported of the ColorTokens' Xshield Splunk application have been fixed in the latest build and the updated version of this application is now available on Appstore (splunkbase) for users to download.
- **CTSP-30150 -** Search option on the access policies page was not producing any result for policies created with a space in their source/destination names. This issue has now been fixed to allow space character between words while searching.
- **CTSP-30143 -** While searching for destination group names on the Create Policy page, there was a delay observed in displaying the list of groups. When those group details are fetched, the counts of matrix information like (i.e. subnets, geo_location, policieis, assets, endpoints, users etc.) for a group are also displayed using the info icon, which was the cause for the delay in display of the information. This issue has now been fixed to enhance the response time to few milliseconds.
- **CTSP-30055** - There was a mismatch reported in the count of policies visible on the workload group's security page & the csv download of the same page. This issue has now been fixed to match the count of policies on the security page as well as the csv download of the page.
- **CTSP-29726 -** Policy recommendation & ignored policy count was not updated until refreshed, if user ignored certain policy recommendations. This issue has now been fixed to reflect instantaneous updates to the respective counts, when policy recommendations are ignored.
- **CTSP-29716 -** Upon addition of a CPT template to a workload group, duplicate CPT policies were observed to be created instead of updates to existing ones. This duplication of policy

issue has now been fixed to ensure that existing policies are checked & updated upon insertion of CPT template for the same.

- **CTSP-29467 -** IP based search in the Assets page was reported to display subnet details instead of the host details. This issue has now been fixed to display the right information.
- **CTSP-27807 -** While using "Tag-Assets" API the hostname to be keyed in was case-sensitive, which has now been made case in-sensitive to induce ease of use of the API.
- **CTSP-27714 -** On visualizer page, user was unable to view the traffic lines for private & public networks when network groups filter was selected. Additionally, if option to “only show groups with traffic" was enabled, both public and private networks bubbles were not getting displayed. This issue has now been fixed.

Changes to Public APIs

There were no changes made to public APIs in this release.