# ColorTokens' Zero Trust Security Platform

2022 Release R10

# ☑ What’s Included?

# 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.

# New Features

### Introduction of Event Viewer

- ColorTokens is introducing an event viewer on its' Zero Trust Security Platform. All non-administrator driven platform events will now be captured in the event viewer. The following existing alert rules (Policy Violation, Policy Tampering, Workload 'offline' status, Agent CPU & Memory & S3 archival alert) would remain as alerts. All other existing alert rules will be converted to events in the event viewer.

  Additionally, users will have the option to convert selective event rules into alerts at their discretion. Upon conversion to alert from an event, the respective rule type would carry the categorization & severity of an alert and reflect in the existing alert page.

  Event Viewer will be available under Monitoring in the main menu alongside the alert & audit log pages.

# Enhancements

### Enhancement to process based policies

- ColorTokens' Zero Trust Security Platform has now enhanced its' recommendation engine to recommend policies based on processes running on a workload. Users can now create an access policy to allow traffic from/to (inbound/outbound) a specific process and port/protocol to a destination or from a source. Benefits of this enhancement include the ability of creating an access policy where users can have granular micro-segmentation at a process, port and protocol level. If the process is dynamic i.e. the process uses dynamic ports, users can have the policy for the process alone.

### Policy direction in a CPT

- Direction field in a Corporate Policy Template (CPT) cannot be modified after it has been assigned to a group.

### Addition of CPT to multiple groups at once

- ColorTokens' Zero Trust Security Platform now provides an option to add a Corporate Policy Template (CPT) to multiple groups at once. Users would be able to select the required groups and pick from the existing CPTs to add the required policies in the template to the selected groups. Any modification to the CPT would automatically translate into the required policy changes on all the groups to which the CPT has been assigned. This option is applicable only to endpoint, user access & workload groups.

### Addition of supported OS on CTSP

- The new version of the server agent can now be supported on CentOS 7.5, Oracle Linux 8.5, 8.6 & 8.7 operating systems.

### Search of policy attributes

- Users will now be able to search policies with the newly introduced FQL on the 'Security' page under each workload group using the following key policy attributes:
  Port, Protocol, Source & Destination group name, Policy status & action.

### Flow to Policy optimizations for standalone assets

- Users will now be able to view recommendations of port ranges and subnets in the flow to policy customization page which they can review, modify and accept. The recommended values will be selected by default while the users will have an option to modify the same, if required, before creating the policy.

### Option to create multiple users at once

- ColorTokens' Zero Trust Security Platform now allows the creation of multiple platform users at once using the newly introduced option of uploading a CSV file with the required details. A downloadable template has been made available on the platform user creation page which would help the users to fill the required details in the CSV file in a said format, before uploading the same for creation.

### Agent upgrade failure notification

- Users will now be notified when an agent upgrade fails via an audit log. The upgrade failure log will also carry the probable reason for failure.

## ✓ Resolved Issues

- **CTSP-33007** → Policy recommendations with a combination of ANY & other ports together for a particular protocol, were not getting added as policies. This issue has now been fixed.
- **CTSP-32418** → Users were unable to configure ADFS SSO due to an incorrect SAML certificate signature. This has now been fixed.
- **CTSP-31972** → Policy Violation alert did not contain sufficient information for users to take corrective actions. This has now been fixed to reflect the required information in the alert description and the email notification for the same.
- **CTSP-31397** → Inconsistency was reported in the number of overall unauthorized connections reflecting in the traffic status for a workload group and the actual unauthorized connections for the same group. This issue has now been fixed to report the exact number in both the places.

- **CTSP-31132 →** Agent upgrade failure from version 8.22.7.7 to 8.22.7.10 was reported. The issue has now been fixed and users will be able to upgrade the agents successfully.
- **CTSP-26228 →** Certain group names that users were part of, at the AD end were not reflecting in the dashboard of the CTSP platform. This issue has now been fixed with a workaround.
- **CTSP-21752 →** Custom tag creation did not allow the usage of spaces in between the words. This issue has now been fixed.

## Known Issues

- **CTSP-32929 →** SSO re-enablement can cause reactivation request emails to be triggered to all registered users of the tenant.
- **CTSP-23949 →** Users on the ColorTokens' Zero Trust Network Access (ZTNA) platform (aka) Xaccess users, are not prompted for re-authentication when their password is changed at the Azure Active Directory or any other SAML IDP end.

## Changes to Public APIs

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