ColorTokens' Zero Trust Security Platform

2022 Release R9

☑ 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

Container Segmentation

- Container based applications a.k.a Microservices are highly dynamic in nature and they communicate with each other on a well defined set of APIs. Traditional network based segmentation will not help prevent lateral movement as the attack surface in microservices are APIs rather than individual ports & protocols.
  As part of ColorTokens' Zero Trust Security Platform's unified segmentation, users will now be able to prevent APT threats & breaches by visualizing the API communications between the micro services, creating zero trust API policies without any business disruption. ColorTokens' Zero Trust Security Platform's solution for containers' micro segmentation is infrastructure agnostic and will integrate with popular service mesh like Istio to provide visibility and policy enforcement.

Resolved Issues

- **CTSP-31903** → Users were unable to access their emails & other URLs through domain since the DNS was not getting resolved. This issue has now been fixed. Users to note that the DNS resolution for Internet domains (non-customer domains) will be sent to the Internal DNS servers (accessed through ZTNA).
- **CTSP-30671** → Users were unable to configure multiple DNS servers. The missing support for configuring multiple DNS servers has now been added to fix this issue.
- **CTSP-29688** → Outbound connections to some services were affected due to duplication of enforcement rules on AIX machines running agent version - 8.10.6.1. This issue has been fixed.
- **CTSP-32159** → Memory leak was observed in agent versions 8.22.10.1, 8.22.8.21 and 8.22.9.4. The issue has now been fixed in all 3 mentioned builds.

Known Issues

- **CTSP-32658** à Custom tag creation currently does not allow the usage of spaces in between the words
- **CTSP-31972 à** All the details of the blocked traffic are currently not captured in the alert generated or the email notification. Missing details include number of connections, process path, source & destination hostname, etc.
- **CTSP-32418 à** SAML certificate present in one of the clusters is incorrect, due to which the

integration of admin users (Spectrum login) via ADFS is failing in that particular cluster

- **CTSP-25794 à** Currently FQL search happens upon clicking the search button given rather

  than pressing the ‘Enter’ key, across the ColorTokens’ Zero Trust Security Platform
- **CTSP-26228 à** Certain group names that users are part of, at the AD end are not reflecting in the dashboard of the platform.
- **CTSP-23949** à Users are not prompted for re-authentication when their password is changed at the Azure Active Directory or any other SAML IDP end
- **CTSP-32445 à** DNS reachability check is not triggered upon a network switch, resulting in the resource location to remain the same even post the network switch
- **CTSP-31986 à** Slowness has been observed at the application level & while making RDP connections when certain terminal servers are pushed to enforced state
- **CTSP-31399 à** In certain cases, traffic may be denied to a few public domains & UDP-137 despite the presence of domain based allow policy.
- **CTSP-31132 à** Agent upgrade is failing from Ver. 8.22.7.7 to Ver. 8.22.7.10
- **CTSP-30291 à** Agent is getting hung and not reporting to the dashboard on a particular server
- **CTSP-29872 & CTSP-27853 à** Memory leak is suspected in 8.11.0.41 Agents, both with & without turning on Firewall Fusion
- **CTSP-26440 à** Due to the processing limitation of 25K domains, traffic related to a specific domain group is not visible in the visualizer when the filter "Categories" is selected under discovered resources unless the domain is recently accessed. However, the same traffic is visible when the filter 'Domain group" is selected under discovered resources since there is no processing limit in the case of domain groups

Changes to Public APIs

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

Bulletin

Heads-up: Xcloud integration with Xshield and discontinuation of vFeed

In view of Xcloud integration with Xshield in 8.22.7.12 agent release, the current vulnerability solution with third party vFeed will be discontinued starting 1st January 2023. All capabilities of vFeed are supported with Xcloud with greater accuracy.

Customers using older agents are recommended to upgrade to 8.22.7.12 version by 31st Dec 2022 to continue to get vulnerability updates. Failing to upgrade to 8.22.7.12 version by 31st December 2022 would result in **vulnerabilities not being updated** for assets running older agents. This essentially means the vulnerabilities discovered as of 31st Dec 2022 will be reported without any further updates!