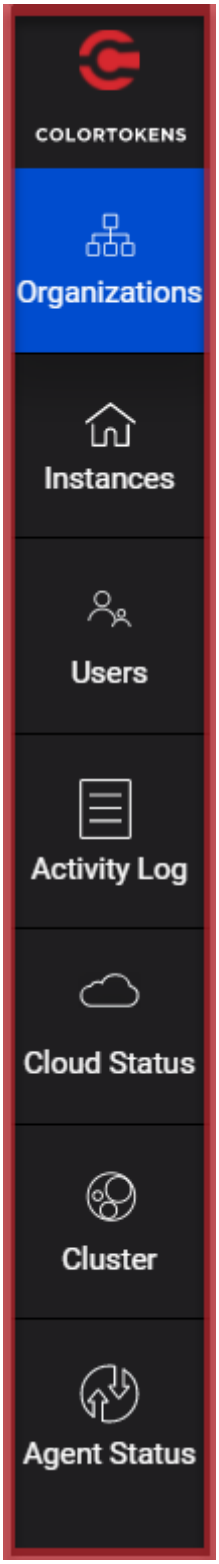

Release Notes

Xshield, Xaccess

2022 Release R5, Version 8.11.2.5

What's Included

About the products

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 datacenter-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.

What's New in Xshield and Xaccess

New capabilities in Xshield:

- Xshield supports process-based policies. The multiple flavours supported are as follows:
    - Policy to accept network traffic destined to a specific port only if the specified process is listening on that port
    - Policy to allow a specified process to accept traffic on a list of ports
    - Policy to allow only a specified process to initiate a connection to a specified destination port
- Xshield can now automate tagging of assets with Tag Rules using hostnames.
- Visualizer can provide a single pane of glass interface to view groups, assets, policies, traffic flows and perform CRUD operations without switching to multiple pages back and forth.
- Policy recommendation can now reconsider previously ignored flows in the next recommendations. Flows that were once considered harmful can now be considered as trusted.
- Agents running on Virtual Machines hosted on cloud instances (AWS and Azure) can now discover and deliver associated cloud tags to Xshield. These tags can then be used to appropriately group the asset based on cloud tags.
- Alerts can be easily searched now with FQL. Multiple keywords are supported like alert id, alert category, alert type, alert severity, alert status, alert description, asset hostname, asset ip, and group name.
- The Zero Trust Security Platform will consolidate traffic data associated with traffic originating from the internet towards a workload. These raw inbound flows from the internet are not very useful for granular flow visualization and hence are summarized.
- The Zero Trust Security Platform now supports an alert generation that notifies operator on the failure to write flow data to S3 bucket(s).
- The software now allows administrators to modify user role without having to delete and recreate the user.
- The upgraded version of server agent will now be supported on Debian 9, Debian 10, Amazon Linux AMI, Amazon Linux 2 AMI and Windows Server 2022

Changes to Public APIs:

The changes made to public APIs as a part of this release are mentioned in the table below.

Changes have been made in the terminology to make it more intuitive to the user. These changes are not backward compatible.

API Name	Previous API	New API
GET_ASSETS	/public/api/v1/<TenantName>/resources	"/public/api/v1/<TenantName>/assets
QUARANTINE_RESOURCE	/public/api/v1/<TenantName>/resources/<asset id>/quarantine	/public/api/v1/<TenantName>/assets/<asset id>/quarantine
SECURITY_INFO	/public/api/v1/<TenantName>/probe/security-info/<asset id>	/public/api/v1/<TenantName>/assets/<asset id>/security-info
UNQUARANTINE_RESOURCE	/public/api/v1/<TenantName>/resources/<asset id>/unquarantine	/public/api/v1/<TenantName>/assets/<asset id>/unquarantine
MANAGE_TAGS	/public/api/v1/<TenantName>/resources/<asset id>/tags	/public/api/v1/<TenantName>/assets/<asset id>/tags
POLICY_TAMPERING	/public/api/v1/<TenantName>/policy/tampered-details?resource_id=<asset id>	/public/api/v1/<TenantName>/assets/<asset id>/tampering-info
MANAGE_AGENTS	/public/api/v1/<TenantName>/resources/<asset id>	/public/api/v1/<TenantName>/assets/<asset id>
MANAGE_HEALTH_LOGS	/public/api/v1/<TenantName>/resources/<asset id>/healthlogs	/public/api/v1/<TenantName>/assets/<asset id>/healthlogs
MANAGE_QUARANTINE	/public/api/v1/<TenantName>/resources/quarantine	/public/api/v1/<TenantName>/assets/quarantine/public/api/v1/<TenantName>/assets/quarantine

Resolved Issues

The following issues are resolved:

Bug ID	Description
Xshield	
CTSP-26917	The asset vulnerability data is not shown when the page level is set to more than 100.
CTSP-26436	In group page the blocked flows and the corresponding counts do not match often. Also, the flows fail to display when the page is refreshed.
CTSP-26314	In policy recommendation, the port numbers disappear while editing the assigned policies.
CTSP-26230	In the policy recommendation page, the help button overlapped the policy save button thus blocking the user from saving the recommended policies.
CTSP-25859	Agent marks the direction of the TCP flows incorrectly due to out of order SYN and RST packets
CTSP-25845	When the user clicks the “Learn more” option in the Alert configuration page, the “Page Not Found” message was displayed.
CTSP-25747	Rule type is shown as blocked in the downloaded Corporate Policy Template (CPT), while it should be shown as allowed.
CTSP-25645	The “Download and Deploy” option was not redirecting to the Agent Download page. This is resolved now.
CTSP-24564	UDP outbound traffic is shown as inbound in flow explorer and visualizer. This happens whenever the response packet is delayed.
CTSP-22950	Audit logs page was taking time to load data. This is resolved now.
CTSP-20648	The Helpcenter link in the Spectrum portal was broken. The link for the Helpcenter icon did not work and displayed the HTTP 414 error when clicked for the first time. However, the link worked when it is clicked the second time.
Xaccess	
CTSP-24891	High memory usage observed with a few user agents running with the version 8.10.4.3
CTSP-18454	Incorrect e-mail notification was received for a user account that was not created.

Known Issues

The following known issues are present in this release:

Bug ID	Description
Xshield	
CTSP-27989	High CPU utilization was observed on the agent due to large number of firewall rules applied on the system
CTSP-27774	Domains which are already part of a domain group are displayed under ungrouped bubble in the visualizer.
CTSP-27714	In the visualizer page the traffic lines for private and public networks are not visible when “network groups” filter is selected. Additionally, when the option “only show groups with traffic" is selected, the public and private network bubbles do not get displayed.
CTSP-26057	In tag rules tab, the asset hyperlink only displays server assets ignoring the user assets. Ideally it should display both server and user assets as matched by tag rules.
CTSP-26052	While creating a corporate policy template (CPT), we can see that the CPT creation is successful, and the pop-up is shown along with the increase in count. However, the created CPT is not visible in the CPT list.
CTSP-25794	FQL should have ability to stick the whole query instead of individual blocks within the query. Also, the query should be executed upon enter key is pressed.
CTSP-25287	The list of folders/paths and executables are not allowed for the Colortokens agent to work with the application control products like Airlock for the Windows 2003 server.
CTSP-24866	The traffic status is shown as blocked /denied or authorized for same traffic at different time intervals. This is expected because domain polices create a rule dynamically after resolving the domain group into IP address leading to inconsistencies.
CTSP-23446	The Windows firewall services and the LGM services do not restart after a server reboot due to hypervisor crash. The user must restart the server manually. In few servers, when the user tried to enable the firewall, “1068 service dependency error” was displayed.
CTSP-23378	The traffic from untagged assets is shown as blocked in the flow explorer.
CTSP-22446	When Xprotect agents are installed along with Xshield agents, the control data generated by Xprotect are marked as unauthorized. As a workaround, an exception policy could be added to allow traffic from Xprotect agent to its orchestration service.
Xaccess	
CTSP-26796	Domain based policy does not work for the Xaccess use case.
CTSP-26228	User group information is not fetched from AD for some users after they have logged in to the application.
CTSP-25414	Connection drops observed while accessing RDP using Xaccess
CTSP-24751	Continuous failed logs are observed in audit logs for multiple users.
CTSP-23949	The user agent does not re-authenticate when the password for a user has changed in active directory.
CTSP-16983	Unauthorized access count shown on the Xaccess dashboard does not match with the flow explorer count.