



DATASHEET

Secure Remote Access to Enterprise Applications, Workloads, and Cloud Services

Product Overview

Digital transformation has enabled a new era of connectivity between users, devices, applications, and infrastructure. With remote work here to stay and cloud migration accelerating, more users, endpoints, and applications are connecting outside the traditional perimeter, making the attack surface larger and more difficult to secure. Enterprises today need to enable secure access and protect users, devices, and applications all while managing cybersecurity risk in distributed networks with few if any boundaries. Traditional, legacy VPNs are ill-suited for the scale and security requirements of modern hybrid networks. In these modern environments, the appliance-based, network-centric VPN approach only adds cost and complexity, widens security gaps, and results in inefficiencies at multiple levels.

Xaccess, a cloud-delivered, SaaS-based secure access solution within the ColorTokens Xtended ZeroTrust™ Platform, enables secure access for remote employees, third parties, and contractors from distributed locations as they connect with their cloud or datacenter-based applications. Designed to scale for public clouds, and software-defined with no hardware or architecture constraints, Xaccess allows granular, authenticated access only to specific, authorized applications. Network-wide access is never required to open an application. Further, applications remain hidden at all times, and are never exposed to the internet or bad actors, creating a dark cloud. As a result, the enterprise attack surface is drastically reduced, preventing lateral movement and minimizing breach risk.

Based on a distributed cloud architecture, Xaccess can be quickly deployed anywhere to protect applications and services, whether on-premises or in the cloud. Xaccess delivers the right level of access for many hybrid IT use cases, from users accessing cloud services to providing controlled access to legacy applications in the data center to setting up access policies for their data fabric and workload segments. Customers can define restricted levels of access for specific crown-jewel applications or sensitive company datastores or enforce process-level controls for less-trusted accessing devices. As a true Zero Trust-based solution, Xaccess brings a rich context of threats, reputation feeds, and vulnerabilities into the access decision. Its ML-based access engine dynamically auto-generates access policies based on risk, usage, and disruption metrics.

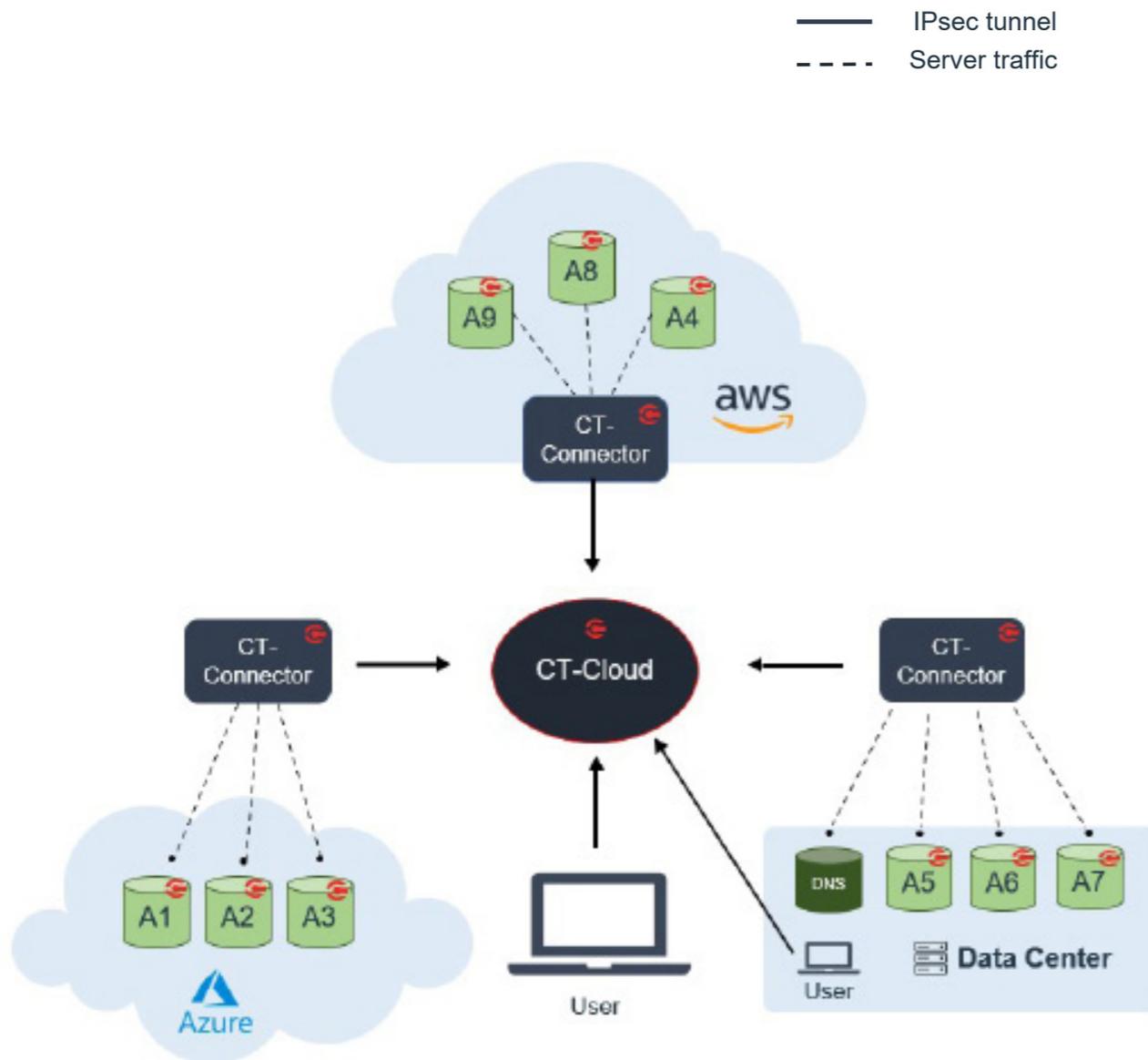


Figure 1. Seamless on-prem/off-prem secure access to applications and cloud workloads

- Public cloud-based SaaS solution for maximum flexibility, scalability, and global availability
- Deployable across data centers, VPCs, and public clouds in a few clicks with readily available Connector images
- Up and running in minutes via seamless guided and self-service deployment experiences via the configuration wizard
- Easy to operate and manage at scale with zero-config Connectors, single pane of glass visibility and control, and auto policy recommendations
- Integrated support for multiple IdP (identity provider)/SSO – LDAP, SAML/SCIM, Azure AD
- Continuous and customizable device hygiene checks and auto-quarantine templates
- Deep integration with Xshield identity-based segmentation for seamless on-prem/off-prem access, policy configuration and enforcement, and access to granular and dynamic workload segments
- Easy to deploy side-by-side with VPNs or replace VPNs
- Data fabric or application access



Features & Benefits

Features	Benefits
100% cloud-delivered, SaaS-based remote access solution	Xaccess is a 100% cloud-delivered, service-initiated secure access solution that can scale to meet customer needs in any location across the globe; there are no user, application, or bandwidth constraints.
Granular application-specific access	Users are allowed least-privilege access only to specific applications that they are authorized to access. Applications are never exposed to the internet and shielded from bad actors, reducing the attack surface and breach risk.
Configuration wizard with in-app guided deployment	The Xaccess configuration wizard makes deployment and activation quick and simple. Customers can deploy Xaccess across their data center, Virtual Private Clouds (VPCs), and public clouds and go live in hours, not weeks.
Easy user on-boarding and delightful user experience with zero configuration and zero hassle end-user app (agent)	There is no learning curve for end-users, nor any user device configuration changes needed to install and start using Xaccess. IT can push the end-user app to user devices (MacOS, Windows 7 and above) using the Mobile Device Management (MDM) tool or users can download and install Xaccess like any other desktop app. Once installed, users only need to authenticate with the CT-Cloud to start using Xaccess for secure remote access. Xaccess integrates seamlessly with enterprise identity providers for user authentication and SSO (single sign-on). There is no need to create VPN profiles or select from a list of multiple VPN gateways to connect to for optimal performance.
Globally available CT-Brokers with support for bespoke CT-Broker deployment	Globally distributed CT-Brokers (connection brokers) deliver high-speed, low-latency connectivity with no Points of Presence (POP) constraints. ColorTokens CT-Brokers are cloud-based and available in multiple geo-regions. Additional CT-Brokers (akin to POPs) can be deployed in minutes anywhere in the world to service customer needs and locations.
CT-Connector autoconfiguration	CT-Connectors (proxy for the app or resource) are autoconfigured and can be deployed in any cloud or data center with just a few clicks.
Support for multiple Identity Providers (IdP) and SSO	Easily onboard users and import user properties such as departments and groups by integrating multiple directory services, identity providers, and SSO without needing to create new user profiles. Administrators have the additional flexibility to create new user groups and end-point groups in the Xaccess console. Xaccess supports advanced use cases of conglomerates with fragmented enterprise networks and multiple SSOs, along with MSPs hosting multiple customers and businesses that employ third-party contractors, each with a separate SSO.
Device security posture check and auto-quarantine	Easily create and enforce device security posture check rules using system attributes and risk score to verify device status before allowing the connection.
Out-of-the-box support for VoIP applications	Xaccess provides out-of-the-box support, with little to no configuration, for static user IPs and policies to enable VoIP services for remote employees.
Integration with workload-to-workload segmentation for identity- and role-based access to workload segments and cloud services	Integration with ColorTokens Xshield Zero Trust segmentation solution provides automated remote user access to cloud services and workload segments, for static and dynamic workloads in the data center or public cloud.
Intelligent, ML-based automated access policy recommendations	Operates at cloud scale with ML-based intelligent policy recommendations to maximize security and minimize the attack surface and risk. Administrators have the flexibility to customize recommended policies or create new ones from scratch.
Centralized dashboard for visibility and control	All the vital stats, actionable recommendations, and controls are available in an intuitive, easy-to-use dashboard.



Role- and Identity-Based Cloud Services Access

Challenge

Hybrid organizations need to provide secure role- and identity-based remote access for employees, contractors, and administrators to enterprise applications and application/workload segments with services and infrastructure distributed across public clouds, VPCs, campuses, and/or data centers. Applications and workload segments can span multi-cloud or hybrid cloud infrastructure environments. Using traditional VPNs is cumbersome and expensive.

Solution

Xaccess enables role- and identity-based secure access to distributed applications, cloud services, and workload segments across any public cloud, hybrid cloud, or data center with zero-complexity deployment and operations. The solution is software-defined, seamless across environments, and makes it easy to define and manage policies at scale across clouds. It is the only remote access solution that is integrated with workload-to-workload segmentation for maximum security of applications and services being accessed by internal and external users.



Third-Party Access

Challenge

Enterprises need to provide third-party contractors, vendors, outlet employees, and partners with secure access to applications in their cloud or data centers, without adding these users to enterprise AD/SSO and without requiring a VPN or DMZ.

Solution

Xaccess enables independent third parties, suppliers, and ecosystem partners to securely access internal applications and resources based on least-privilege Zero Trust access. Xaccess integrates with multiple identity providers (IdP/SSO) for authentication, eliminating the need to add external users to active directory servers or set up VPNs or DMZ for access. Enabling third-party access with Xaccess requires no VPN setup and no changes to NW or FW configurations, while facilitating seamless operations across fragmented networks due to multiple campuses or M&A.



Seamless On-Prem/Off-Prem Access to Dynamic Workloads

Challenge

Organizations with a cloud presence are need to isolate dynamic and ephemeral workloads and applications within the cloud/DevOps environment and affect separation of duties for developer and administrative access, to reduce the risk of insider threats while enforcing dynamic policies. Current bespoke solutions make it challenging to manage and enforce access policies while users transition between on-prem and off-prem, without impacting user experience and ease of use/administration.

Solution

Xaccess integrates seamlessly with Xshield for dynamic workload segmentation capabilities that enable remote access with automated policy enforcement and granular access control to dynamic workloads such as S3 buckets, Kubernetes clusters, containerized applications and services, Lambda functions, and more. With Xshield integration, access policies are enforced automatically and seamlessly whether users are on-prem or off-prem, without requiring any reconfigurations or reinforcements.

 **Application-Specific End-User Access****Challenge**

Enterprises need to provide secure access to specific applications that employees need in order to do their jobs. Traditional VPNs provide network-centric access and are ill-suited to this need, as they cannot enforce per-application end-user access based on identity, thereby exposing large attack surfaces to malicious actors.

Solution

Xaccess provides user identity- and device security posture-based granular and secure direct access to applications, even on the same network segments; this granular access control is enforced irrespective of the user being on-prem or off-prem. Applications are never exposed to the internet, reducing the attack surface and lowering risk. Xaccess normalizes the user experience on and off the corporate network. It is a low-latency, low-complexity, higher-security solution that simplifies deployment and improves the user experience for both end-users and IT admins.

ColorTokens Inc. is a leading innovator in SaaS-based Zero Trust cybersecurity solutions, providing global enterprises with a unique set of products and services for securing applications, data, and users across cloud and hybrid environments. Through its award-winning Xtended ZeroTrust™ Platform and context-aware machine learning-powered technologies, ColorTokens helps businesses accurately assess and improve their security posture dynamically.

As cloud adoption grows, traditional perimeters get redefined, and new attack vectors and threat actors materialize, corporations recognize their security posture needs to reflect their Zero Trust philosophy. ColorTokens' technology allows customers to achieve Zero Trust by utilizing rich, meaningful contextual information about the application, microservice, or protected resource, so customers can apply Zero Trust with as secure of a perimeter as they can. ColorTokens' cloud-based SaaS platform can automatically deploy next-generation security controls and increase security posture dynamically without any new hardware, downtime, reboots, or changes to a client's existing systems.

For more information, please visit colortokens.com

