appgate | COLORTOKENS

# COLORTOKENS INTEGRATES WITH APPGATE SDP FOR COMPLETE ZERO TRUST PROTECTION

## Defend your digital operations with Zero Trust Microsegmentation and Zero Trust Network Access (ZTNA).

ColorTokens' microsegmentation enables organizations to set zero trust policy controls for all lateral traffic inside the network perimeter. Appgate SDP enables secure access controls for users and machines from the external network.  Together, they provide coverage for north-south traffic (between external entities and internal resources) and east-west traffic (between internal resources), allowing organizations to enforce zero trust principles across all directional flows of network traffic.

### Microsegmentation is a foundational part of your zero trust strategy

ColorTokens Xshield provides the ability to define zero trust traffic policies that can stop the lateral spread of malware or ransomware within an enterprise landscape. It creates isolated segments that are smaller than traditional VLAN network segmentation. This prevents attackers from easily moving laterally within the environment and accessing critical resources. By reducing the attack surface and limiting access to sensitive data, microsegmentation substantially minimizes the potential damage from a breach.

Appgate SDP provides the ability to establish a "segment of one" network by dynamically creating individualized, encrypted tunnelling between users and the specific resources they are authorized to access. Unlike traditional network security models that rely on broad, static segmentation, Appgate SDP continuously enforces granular access controls based on real-time context including user identity, device posture, location, and risk profile. Each user is isolated within their unique segment, mitigating the risk of unauthorized lateral movement, and reducing exposure to threats.

### Complete Zero Trust protection for your diverse enterprise landscape

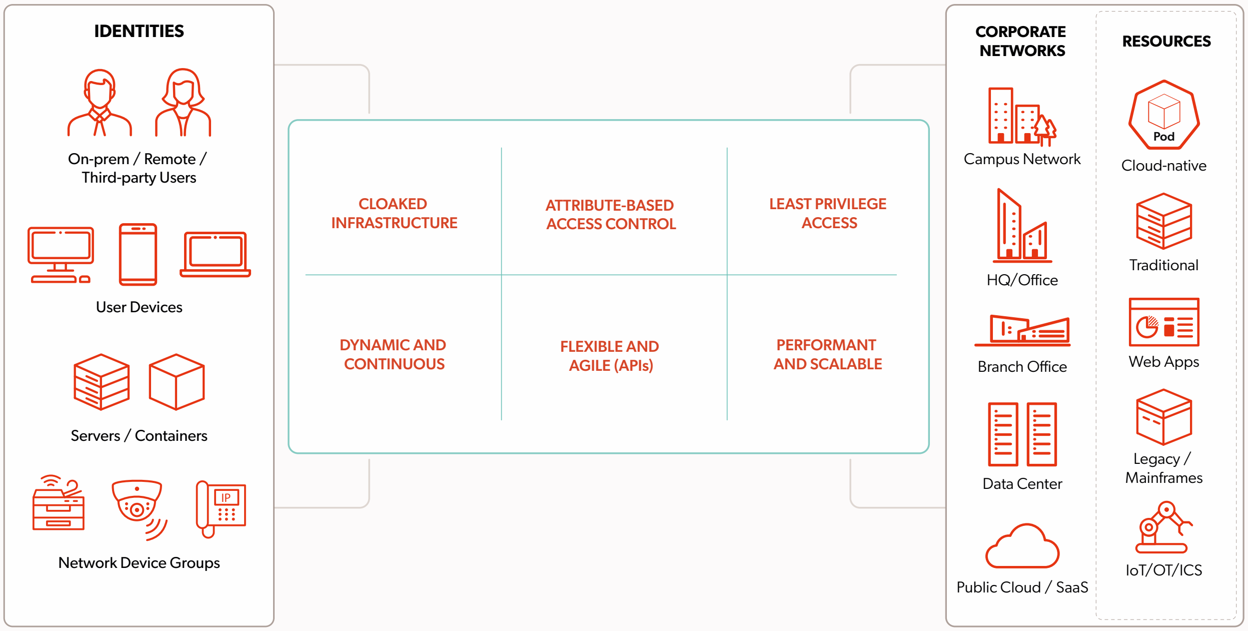
**ColorTokens Xshield Enterprise Microsegmentation Platform** enables organizations to manage multiple types of zero trust policy enforcement points, both agent-based and agentless, from one central console. This decreases complexity and saves time and money on training and staffing. This is an advantage over other microsegmentation solutions that do not support endpoints on which their agent cannot be installed. The multiple types of policy enforcement points include:

1. **Data Center Servers and VMs:** A lightweight agent that senses telemetry and pushes firewall rules to the host-based firewalls in Windows, Linux and macOS
2. **Kubernetes containerized microservices applications:** agentless enforcement at the API level (L7) using integration into the Open Policy Agent (OPA) in the service mesh
3. **Operational Technology, Industrial Control Systems and IoT devices:** an agentless Gatekeeper appliance that enforces policy as the default gateway adjacent to the switch

ColorTokens Xshield stops lateral movement for all types of assets so there are no "soft spots" in your cyber defense.

**Appgate SDP** provides a direct-routed architecture that delivers comprehensive zero trust protection across complex and diverse enterprise environments by securely connecting users to the resources they need without routing traffic through a vendor's cloud. This approach provides secure, direct access and enables consistent policy enforcement across all network segments, reducing complexity and enhancing performance. Appgate SDP supports a wide range of use cases and environments, including:

- **Hybrid and multi-cloud deployments:** Seamlessly integrates with multiple cloud providers and on-premises data centers, ensuring unified zero trust policy enforcement across all corporate networks and resources.
- **Universal ZTNA:** Secures all users, devices, and locations-whether on-campus or remote-by through a unified policy model that replaces traditional technologies such as VPNs, MPLS, and NAC.
- **Local devices:** Secures all LAN devices, including IT, OT, and IoT devices such as IP-based printers, VoIP phones, physical access control systems, IP-based cameras and surveillance systems. (AD), LDAP certificates, OIDC, RADIUS and SAML IdPs.

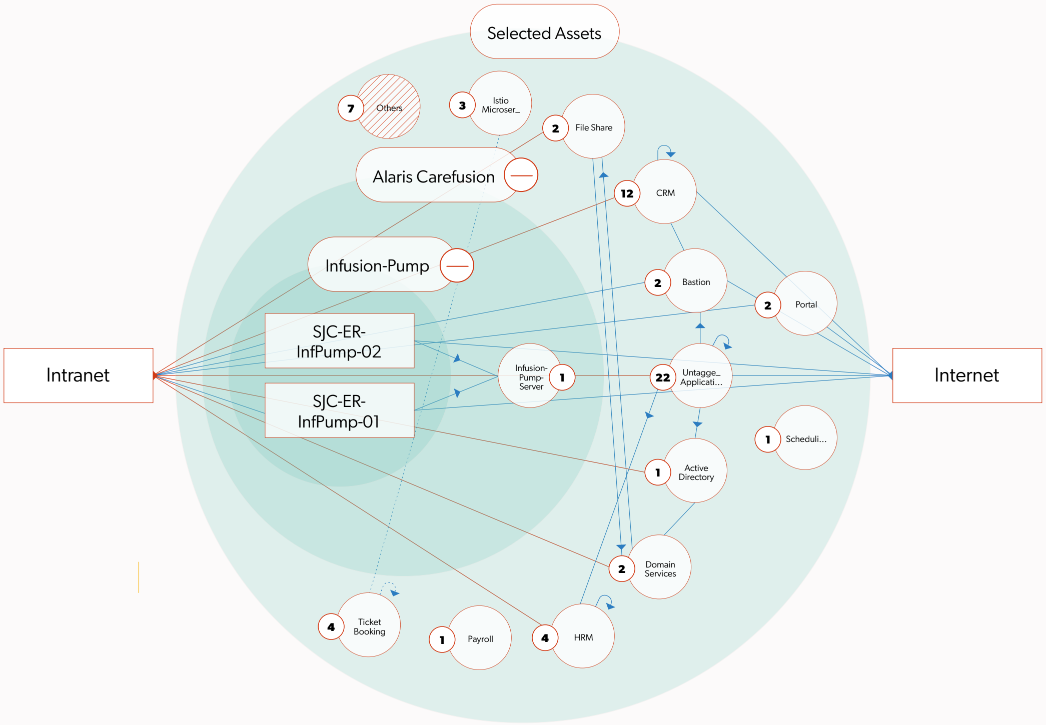


Appgate SDP's unified policy model.

## Flexible, multi-dimensional visibility

ColorTokens' network map visualization interface enables admins to view assets and traffic in the environment using over 20 drill-town dimensions, such as assets, applications, dependencies, physical location, custom attribute tags and others.

This means that different user personas, such as the security, application, and infrastructure teams, each have their own view of the environment that best fits their needs. The Xshield mapping user interface provides multi-level visibility into the whole enterprise environment across IT, IoT, and OT. It provides a focal point for traffic analysis and zero trust policy design. Using it, administrators can easily identify misconfigurations, deprecated protocols, and dangerous communications.



Xshield's asset and traffic map user interface.

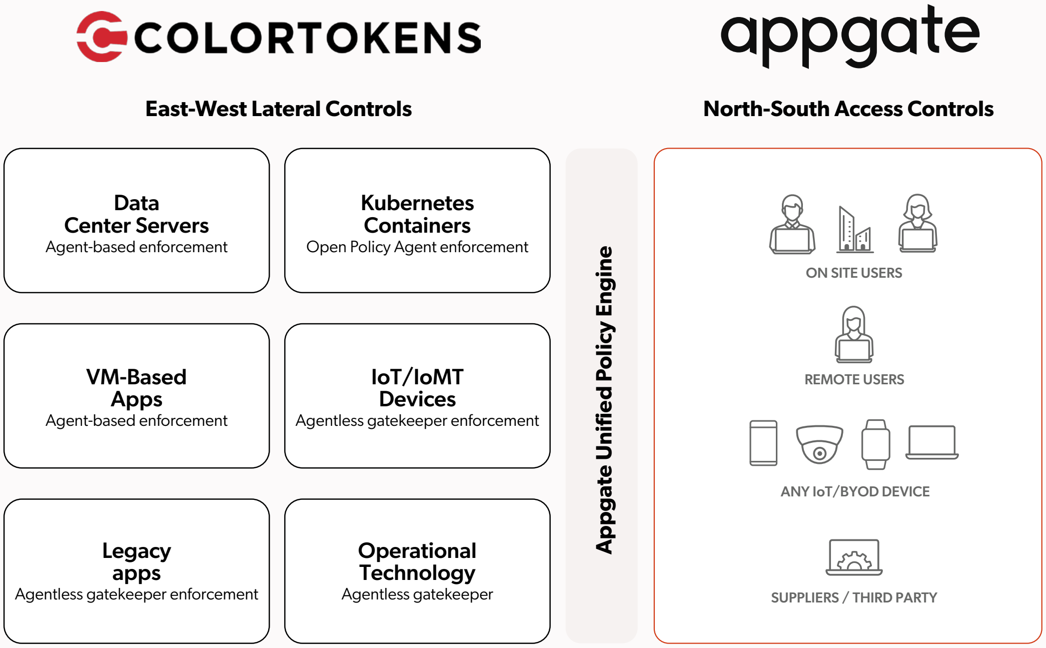
## Simplify your zero trust network access policy definition

ColorTokens tags your assets with attributes that can be used by Appgate SDP to set access policies. Application assets are defined using ColorTokens so that if there are updates to IP addresses, your access policies remain consistent and synchronized through the ColorTokens-Appgate SDP API integration.

## Use Cases for the combined solution

Zero trust architecture is defined by CISA with several pillars[1] – identity, devices, networks, applications and workloads, and data. Risk and infrastructure leaders should consider each capability area individually and how those capability areas interact. The combination of Appgate SDP and ColorTokens provides zero trust controls across the identity, devices, network, and applications/workloads pillars.

1. Remote user least privilege access to authorized applications
2. Least privilege remote access for IT and security personnel to systems or tools
3. Least privilege access for suppliers, third-party contractors, and IT outsourcing partners to specific applications
4. Least privilege access for vendors of IT, IoT, and Operational Technology/Industrial Control Systems infrastructure to applications and devices for patches, maintenance and troubleshooting
5. Ensure secure, seamless access to applications during mergers and acquisition (M&A) activities with continuous least-privilege enforcement
6. Manage secure access between environments with overlapping IP addresses without reconfiguring network settings
7. Provide secure, least-privilege access to IoT and OT devices for maintenance and troubleshooting
8. Securely route and control access to applications and resources spread across multiple tunnels or data centers



Combining ColorTokens and Appgate SDP provides complete Zero Trust microsegmentation and network access protection.

### About Appgate

Appgate secures and protects an organization's most valuable assets and applications. Appgate is the market leader in Zero Trust Network Access (ZTNA) and online fraud protection. Appgate products include Appgate SDP for Universal ZTNA and 360 Fraud Protection. Appgate services include threat advisory analysis and ZTNA implementation. Appgate safeguards enterprises and government agencies worldwide. Learn more at appgate.com.

### About ColorTokens

ColorTokens is a leader in delivering innovative and award-winning zero-trust cybersecurity technology solutions. ColorTokens is a US corporation headquartered in Silicon Valley with offices in the United States, the United Kingdom, Europe, the Middle East, and India, serving a diverse client base in both the public and private sectors. For more information, please visit colortokens.com.

[1] https://www.cisa.gov/zero-trust-maturity-model

appgate