COLORTOKENS

Unified Zero Trust Platform

# Comprehensive Zero Trust Security to Protect Your Critical Systems and Stop Cyberattacks in Their Tracks

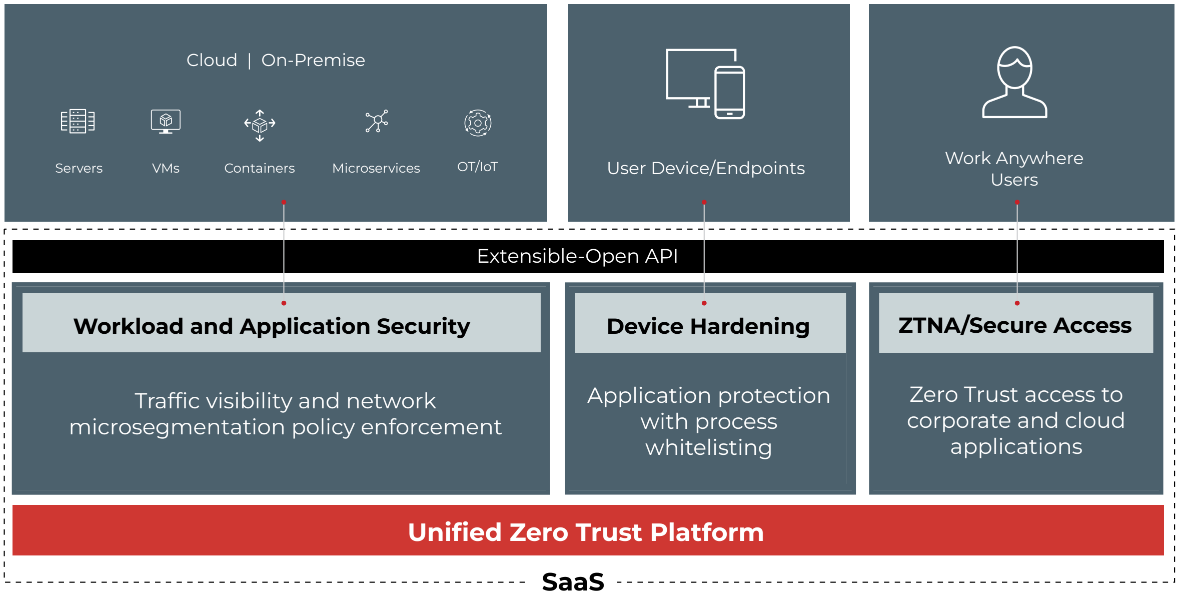
Microsegmentation
Zero Trust Network Access
Device Hardening

→ **IN ONE UNIFIED PLATFORM**

Enterprises are moving to the zero trust model to secure their network from modern cyber threats. With a network perimeter breach considered imminent in practically all enterprise networks, organizations must be able to reduce the damage or "blast radius" of an attack to enable their business to operate uninterrupted. Various components of Zero Trust are being employed by organizations from microsegmentation to remote user access (Zero Trust Network Access).

Organizations, however, are struggling to piece together disparate zero trust architecture solutions resulting in added complexity, security gaps between solutions, and deployment delays. The wide range of network topologies employed by today's enterprises, including cloud, on-premise, hybrid, containers, and OT/IoT networks, all add complexity if an organization is managing multiple security solutions.

ColorTokens has architected the zero trust solution as a unified platform from the ground up. It supports several key security capabilities of zero trust as well as supporting integration with 3rd-party security solutions. The unified approach of the solution architecture ensures the protection of a wide range of network topologies without the complexity of managing multiple solutions.


Cloud | On-Premise
Servers
VMs
Containers
Microservices
OT/IoT
User Device/Endpoints
Work Anywhere Users
Extensible-Open API
Workload and Application Security
Traffic visibility and network microsegmentation policy enforcement
Device Hardening
Application protection with process whitelisting
ZTNA/Secure Access
Zero Trust access to corporate and cloud applications
Unified Zero Trust Platform
SaaS

**Zero Trust Microsegmentation** groups endpoints, servers, applications, and devices into granular logical groups with least-privilege-needed polices that restrict access to them from users and from other microsegments. These policies, while allowing valid traffic to pass, prevent the lateral movement of malware or ransomware that has slipped through the perimeter antivirus and firewall defenses.

**Zero Trust Network Access** (ZTNA) uses encrypted tunnelling for "work anywhere" users' connections, replacing VPNs, and it asserts your policies for user access to microsegments. ZTNA integrated into the unified platform provides seamless secure access, policy configuration and enforcement, and controls access to granular workload segments.

**Zero Trust Device Hardening** uses whitelisting to stop malicious programs and processes from running. It is proactive, not reactive like traditional endpoint detection and response. Its stops novel attacks that have slipped through traditional perimeter defenses. Device hardening can be deployed even on legacy systems with unsupported operating systems which typically cannot run EDR.

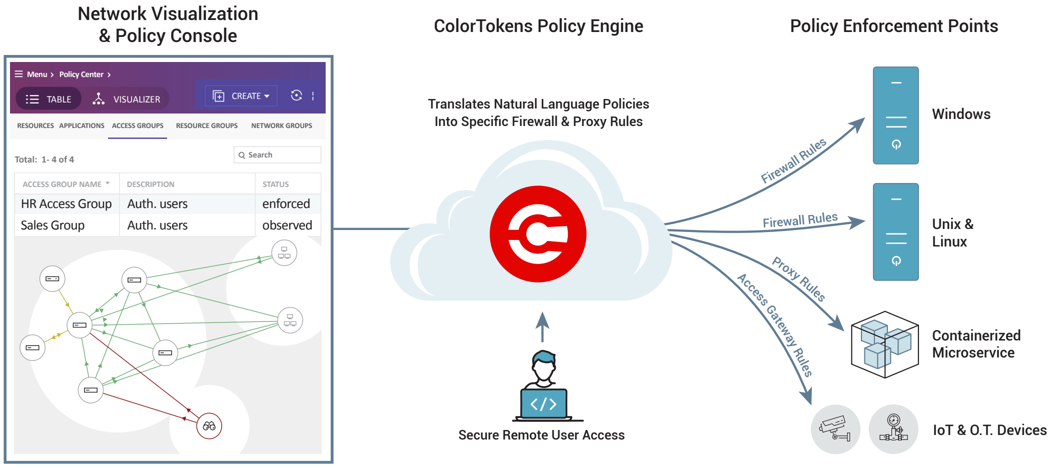
A **UNIFIED ZERO TRUST PLATFORM** is crucial for centralized management of these functions. If separate point solutions are used, administrators would need to manually maintain coherence between policies defined in different tools and user interface consoles—one set of policies for traffic between microsegments in the enterprise network, and another for microsegment access for remote or "work anywhere" users.

In addition to being more expensive and an administration headache, managing policies in separate point solutions requires more personnel & training, and can lead to errors, increasing risk. A common management interface allows for a holistic approach to zero trust policy definition and enforcement, so that the greatest reduction in attack surface is achieved.

- Protect critical systems and data—even when the perimeter is breached.
- Ease of policy management with fewer staff & less training, using a unified interface
- Less chance of risky policy errors across point solutions
- Significant cost savings vs. implementing separate point products
- Simplification through VPN replacement
- Scalability, speed of deployment and ease of management with Software-as-a-Service; deploy modules incrementally as needed to satisfy your critical use-cases
- Seamless integration to your security ecosystem with open APIs to SIEM, SOAR, IdM, SSO, etc. leveraging your existing infrastructure investments

## Write Policies Once, Deploy them Everywhere

Unified Administrator Console for network visualization, microsegment communication policy, and remote user access to microsegments



Total: 1- 4 of 4

| ACCESS GROUP NAME | DESCRIPTION | STATUS |
|---|---|---|
| HR Access Group | Auth. users | enforced |
| Sales Group | Auth. users | observed |

Network Visualization & Policy Console
Menu › Policy Center ›
TABLE
VISUALIZER
CREATE
RESOURCES
APPLICATIONS
ACCESS GROUPS
RESOURCE GROUPS
NETWORK GROUPS
Search
ColorTokens Policy Engine
Translates Natural Language Policies Into Specific Firewall & Proxy Rules
Secure Remote User Access
Policy Enforcement Points
Firewall Rules
Firewall Rules
Proxy Rules
Access Gateway Rules
Windows
Unix & Linux
Containerized Microservice
IoT & O.T. Devices

## Features at-a-Glance

### A unified zero trust platform providing the following functions:

### Zero Trust Microsegmentation

- Asset and traffic visibility
- Automated and manual asset tagging, supporting custom tags
- Microsegmentation policy auto-recommendation
- Translates policies in natural language into specific firewall and proxy rules needed for different policy enforcement points
- Manage multiple types of policy enforcement points:
  - Generates host-based firewall rules for Windows, Linux, and Unix
  - Sidecar proxy rules for containerized microservices
  - Access gateway rules for agentless IoT and O.T. devices
- Open APIs to integrate with SIEM, SOAR, etc.

### Zero Trust Network Access

- VPN replacement with secure tunneling
- User access policy controls to granular workload microsegments
- Open APIs to integrate with SSO, Identity Management (IdM), etc.

### Zero Trust Device Hardening

- Whitelisting of applications and child processes
- Proactively stops malicious processes and programs that have evaded antivirus scanning

### Unified Administration Interface

- Visualize assets and network traffic.
  - Color coded lines for in- and out-of-policy traffic
  - Visualize asset metadata
- Microsegmentation policy console
  - Unified microsegment access policy management for both on-campus and remote users
  - Define policies using natural language

### Simplifying Your Journey to Zero-Trust Architecture

ColorTokens is a leader in delivering innovative and award-winning zero-trust cyber security technology solutions such as network micro-segmentation, endpoint hardening and whitelisting, cloud and container security, and zero-trust network access. ColorTokens is a US corporation headquartered in Silicon Valley, and has approximately 400 employees world-wide, with offices in the United States, the United Kingdom, the Middle East, and India serving a diverse client base in both the public and private sector. For more information, please visit **colortokens.com**