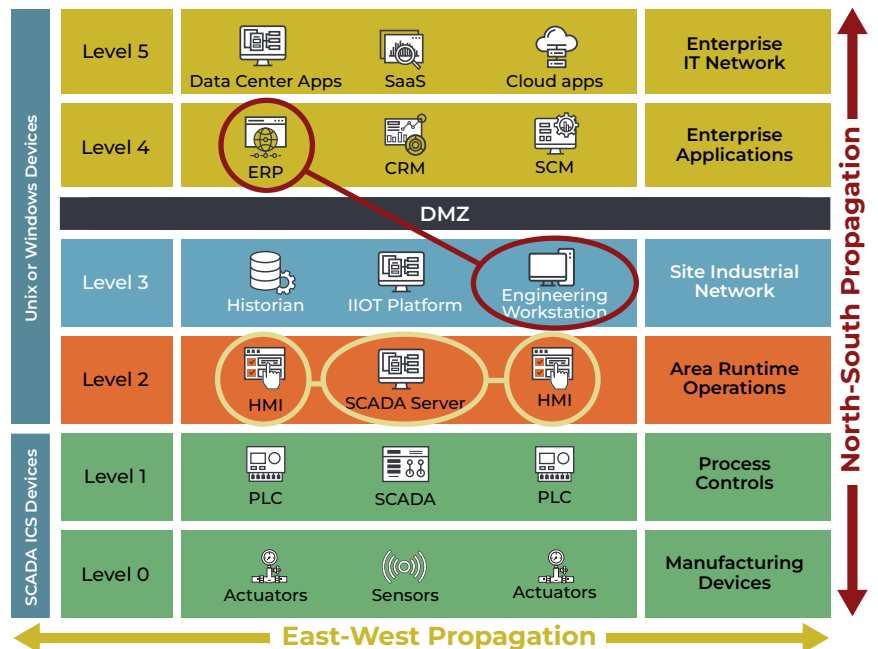# Cybersecurity for Operational Technology

Technological progress in operational technology (OT), industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems have produced unparalleled industrial productivity increases in recent decades. Their ability to monitor and manage operations with automation has increased efficiency and agility. To protect this new technology architecture, an industrial network configuration design called the Purdue Enterprise Reference Architecture (Purdue Model) was conceived, as shown in the figure below. It was meant to keep organizations' vital industrial control systems segregated from the enterprise Information Technology systems, as well as having discrete layers of separation within the OT network itself. It assumed that the industrial control systems were the "crown jewels" of the enterprise and that they would be disconnected and inaccessible to both internal networks and the outside world.

## Layered Architectures and Perimeter Defense Are Not Enough

In recent years the trends of digital transformation and hyper-convergence have been pursued so that organizations can fully leverage their enterprise data and applications with Operational Technology Systems to achieve cost savings, increase productivity and gain the ability to react to market needs with agility. This has broken down the protecting separation between IT and OT. In addition, lateral movement of attacks occur within the Operational Technology layers along the so-called east-west axis. **A single infected OT or IoT device can propagate ransomware or malware throughout the industrial systems and the IT network.**

Traditional methods of securing the network perimeter using firewalls and anti-virus detection seek to protect against attacks from the external internet—the north-south axis. The challenge with this approach is that the adversary need only be successful once; the defender must be right every time. All successful ransomware or malware attacks in the past have, by definition, penetrated the perimeter defenses. It's a question of when, not if.

In contrast, the **zero-trust security** approach assumes the adversary is already inside your perimeter; internal users, programs and devices are not to be trusted by default. ColorTokens allows you to group devices and servers into micro-segments in a much more granular way than VLAN segmentation would allow. This lets you control the east-west movement of data and programs in both your IT and OT systems. The goal is to reduce "attack surface" and "blast radius"—the points of entry and lateral movement in your network and the extent of the damage that can be caused by malware or ransomware.



| | | | | |
|---|---|---|---|---|
| | Level 5 | Data Center Apps   SaaS   Cloud apps | Enterprise IT Network | |
| Unix or Windows Devices | Level 4 | ERP   CRM   SCM | Enterprise Applications | North-South Propagation |
| | | DMZ | | |
| | Level 3 | Historian   IIOT Platform   Engineering Workstation | Site Industrial Network | |
| | Level 2 | HMI   SCADA Server   HMI | Area Runtime Operations | |
| SCADA ICS Devices | Level 1 | PLC   SCADA   PLC | Process Controls | |
| | Level 0 | Actuators   Sensors   Actuators | Manufacturing Devices | |

East-West Propagation

# The Solution: Micro-Segmentation and Secure User Access for Both IT and OT Systems

Zero Trust network segmentation, when done right, can completely block lateral movement and kill ransomware and malware. It involves applying a firewall "micro-perimeter" around every asset in both the OT and IT networks, allowing only necessary traffic. But Zero Trust is not just about the network—it's not really Zero Trust unless it controls user access to applications, data and devices in those microsegments. ColorTokens has unified the disjointed pillars of network security—segmentation and zero trust user access—into a single, simple platform.

With ColorTokens, both OT and IT assets are separated into micro-segments, and only traffic between those micro-segments that should be communicating as part of valid business processes are permitted, in accordance with the zero-trust security paradigm. This prevents malicious code from freely traversing the environment and affecting your critical Operational Technology systems and enterprise IT systems.

For the IT network, the ColorTokens' visualization & policy engine centrally manages the configuration of the OS-based firewalls in Windows, Linux, Unix and MAC operating systems. For the OT network, to protect devices on which a software agent cannot be installed, ColorTokens uses an access gatekeeper to enforce your traffic and access policies. The access gateway software can be deployed as a virtual machine, or as a discrete hardware appliance. As shown below, you can easily configure traffic and user access policies using natural language in our central policy administration user interface, and those policies are then expressed as rules in the proper format for the host-based firewalls in your IT network, and for the access gateway for OT devices.
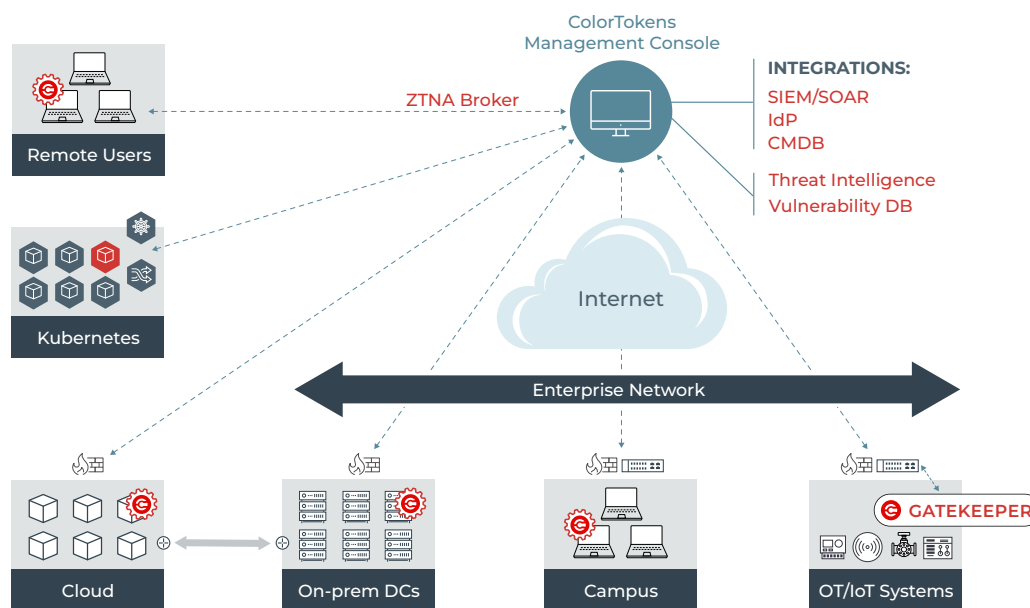


## Simplifying Your Journey to Zero-Trust Architecture

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**