Zero Trust Security for Operational Technology

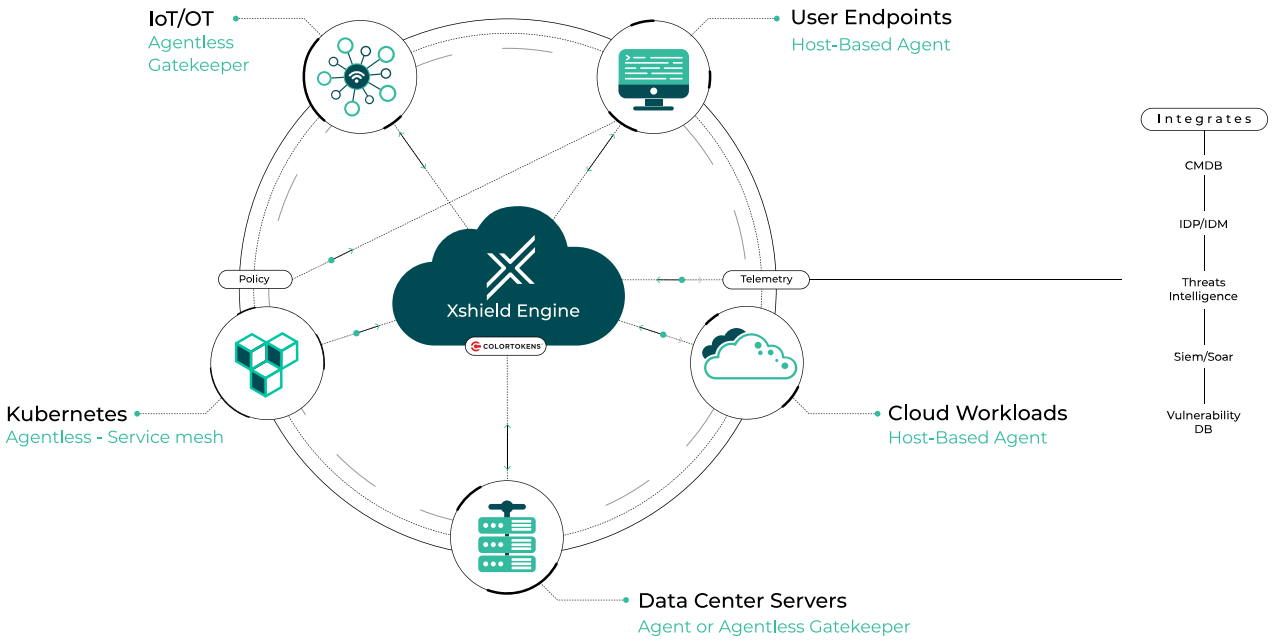
Technological progress in operational technology (OT), industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems have produced unparalleled industrial productivity increases in recent decades. Their ability to monitor and manage operations with automation has increased efficiency and agility. To protect this new technology architecture, an industrial network configuration design called the Purdue 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 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 socalled 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 create microsegments 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.



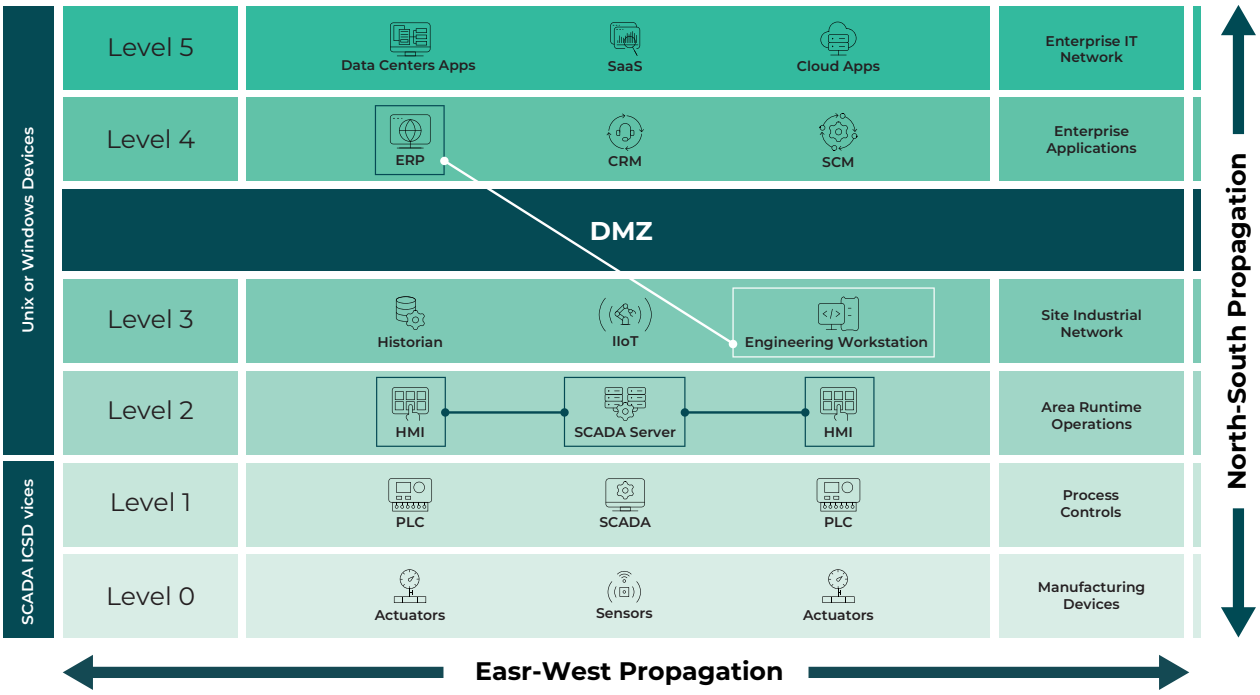
The Solution: Micro-Segmentation for Both IT and OT Systems

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 valid traffic.

With ColorTokens Xshield, both OT and IT assets are separated into micro-segments, and only traffic between those microsegments that should be communicating as part of valid business processes are permitted, in accordance with the zerotrust 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, Xshield leverages the hundreds (or thousands) of host-OS based firewalls you already have in your environment. We provide the central policy engine which configures these native firewalls on Windows, Linux, Unix, and Mac operating systems so you can easily manage them as policy enforcement points. For the OT network Xshield uses an access gatekeeper to enforce your traffic and access policies.

The gatekeeper 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 management console, and those policies are then expressed as rules in the proper format for the host-based firewalls in your IT network, proxies for containerized applications, and for the access gatekeeper appliance for OT devices. This gives you a comprehensive approach to segmentation for your whole environment.



About ColorTokens

ColorTokens is a leader in delivering innovative and award-winning cyber security solutions. It is a US corporation headquartered in Silicon Valley with offices in the US, the UK, Europe, the Middle East, and India serving a diverse client base in both the public and private sector. For more information, please go to **colortokens.com**