Zero Trust Security for the Pharmaceutical Industry

Protecting Information Technology and Operational Technology Systems

According to the research firm ABI, the pharmaceutical industry is forecast to spend $4.5 billion on digital transformation alone by the year 2030, with the goal of supporting faster therapeutic innovations and improved production processes for the benefit of patients.1 The International Society for Pharmaceutical Engineering (ISPE) is helping to chart a path to implementation of the "smart factory" Industry 4.0 roadmap for the through its Pharma 4.0 community of practice:

"The Pharma 4.0 Digitalization…will connect everything, creating new levels of transparency and adaptivity for a "smart" plant floor. This will enable faster decision-making and provide in-line and on-time control over business, operations, quality, and regulatory compliance. Notably, this new connectedness will require higher levels of security, since linked systems heighten vulnerability." [our emphasis]2

ColorTokens can help you implement cyber security technology and practices to eliminate the vulnerabilities resulting from this trend towards digital transformation. The goal is to reap the benefits of digitalization, while at the same time constraining the attack surface exposed in the new digitalized systems. This will allow pharma companies to:

- Protect intellectual property, from Electronic Lab notebooks (e-lab) to Laboratory Information Management Systems (LIMS), to Production Systems.
- Protect all phases of the product lifecycle, from discovery to development, manufacturing, sales, and supply chain. (Protect the research, the recipe, and partner and customer data.)
- Protect production systems controlled by the Operational Technology network
- Increase resilience by stopping ransomware and malware propagation.
- Prove compliance with regulations, and to increase their sustainability and ESG score substantially.

The Technical Challenge: Lack of Visibility Over Complicated and Diverse Networks in Both IT and OT

The IT networks in the pharmaceutical industry encompass on-prem data centers, multiple clouds, containers, and even employees' homes and third-party networks. Now, because of convergence and digital transformation, this diverse IT environment is increasingly connected to systems which previously were isolated: the Operational Technology network.

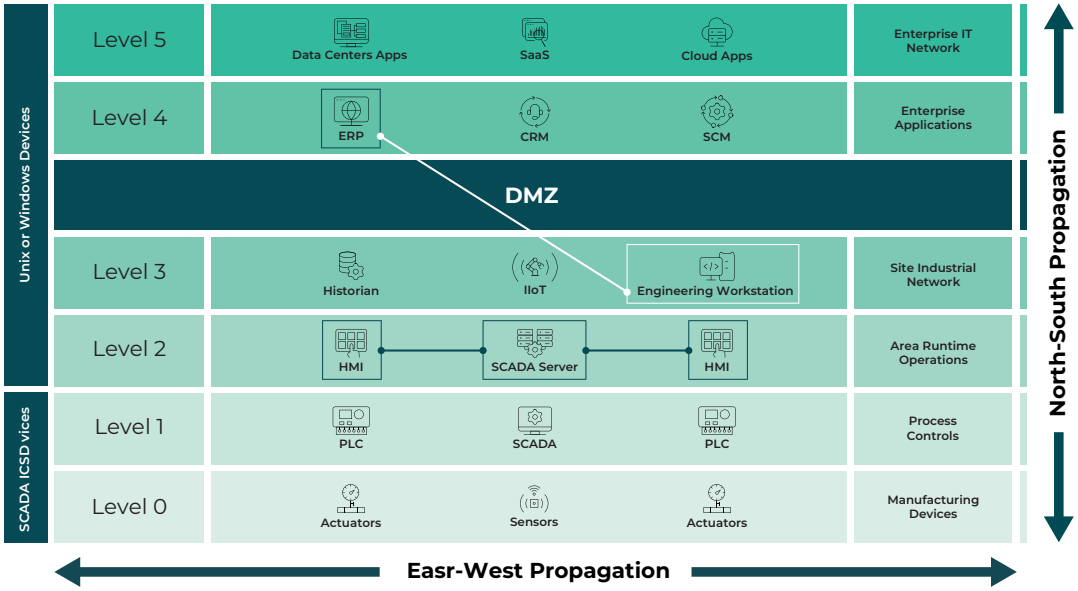
Technological progress in industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems have provided pharma companies with unparalleled industrial productivity increases. Their ability to monitor and manage operations with automation has increased efficiency and agility. To protect this new technology architecture, the industrial network configuration design called the Purdue Model was conceived, as shown in the figure below. It was meant to keep vital industrial control systems segregated from the enterprise IT 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.

1 Pharma Industry to Spend $4.5 Billion on Digital Transformation by 2030 (abiresearch.com)

2 Pharma 4.0 Operating Model | Industry 4.0 | ISPE | International Society for Pharmaceutical Engineering

In recent years the trends of digital transformation and convergence have been pursued so that pharma organizations can fully leverage their enterprise data and applications to achieve cost savings, increase productivity and gain the ability to react to market needs with agility. This has broken down the protective separation between IT and OT. Data sharing is now commonplace across the north-south axis, between enterprise IT systems and the OT industrial network. In addition, lateral movement of attacks occur within the Operational Technology layers along the east-west axis.

In the new converged, digitally transformed landscape, a single infected device can propagate ransomware or malware throughout both the OT and 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 challenge with this approach is that the adversary needs 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.

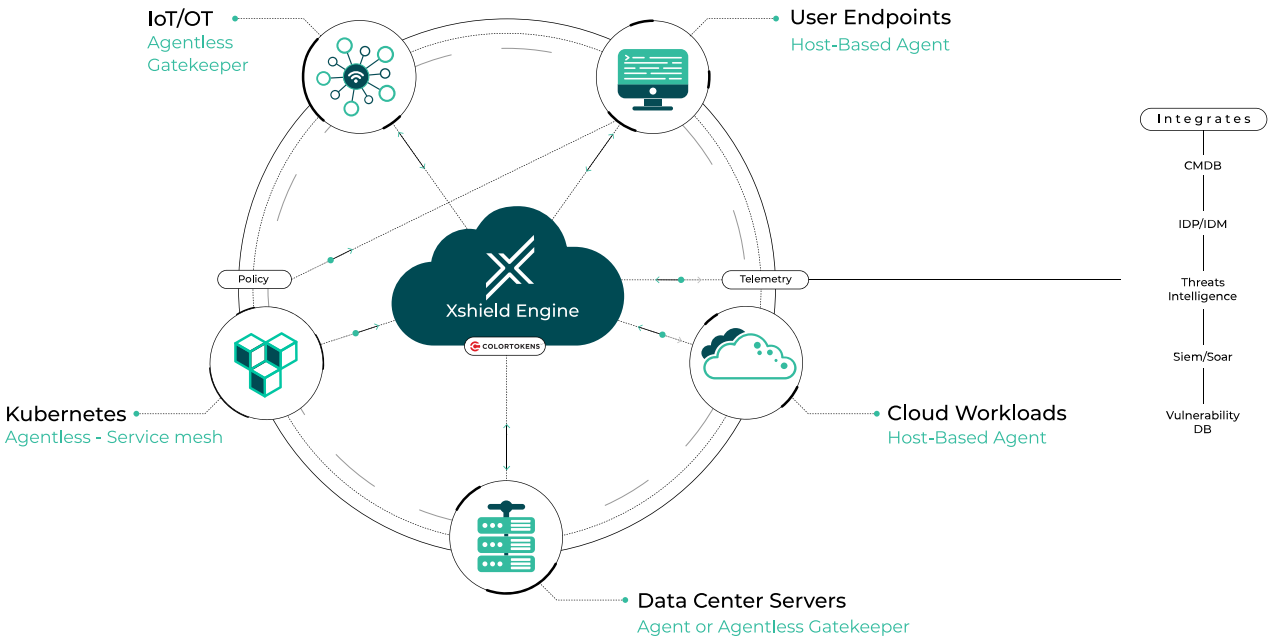
In contrast, the zero-trust security approach assumes the perimeter has been breached; internal users, programs and devices are not to be trusted by default. Traffic between network resources is controlled, and user access is granted only on a leastprivilege-needed basis. The goal is to reduce attack surface and blast radius—the points of entry and the possible effect of any breach.

The Solution: Network Segmentation and Secure User Access for IT and OT

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. ColorTokens has unified the disjointed pillars of network security—network segmentation and zero trust user access — into a single, simple platform. This allows a unified approach to visualizing and controlling network traffic in all modes: workload-to-workload, workload-to-user, and user-to-user. User access to granular microsegments is controlled with context beyond mere log-on credentials, and our Zero Trust Network Access (ZTNA) SaaS engine replaces your VPN servers with greater scalability.

Colortokens Simplifies Your Journey to Zero Trust Architecture

For the IT network, ColorTokens 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 and Internet-of-things network In the new converged, digitally transformed landscape, a single infected device can propagate ransomware or malware throughout both the OT and IT network.



A “Single Pane Of Glass” Solution is Crucial for Visibility and Management of Zero Trust User Access and Network Segmentation

If separate point solutions are used for secure user access and for network microsegmentation, administrators would need to manually maintain coherence between policies defined in different tools and different management consoles—one set of policies for workload-to-workload traffic in the enterprise network, and another for user-to-workload secure access. Managing policies in separate tools is an administration headache and is more expensive, with greater personnel and training needs. It can lead to increased risk because of policy errors. An integrated solution gives you a comprehensive approach to zero trust policy definition and enforcement, so that the greatest reduction in attack surface is achieved.

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**