COLORTOKENS

SOLUTION BRIEF

Zero Trust Security for the Energy Sector

Protecting Information Technology and Operational Technology

DHS, in their Sector Risk Snapshot has outlined potential vulnerabilities to the OT and IT converged landscape in the oil and gas sector:

> "Oil and natural gas infrastructure is highly automated... Assets may be vulnerable if these industrial control systems are connected to the Internet, either directly or indirectly. For example, control system networks may be connected to the corporate business network, which, in turn, is connected to the Internet. These connections increase the network's vulnerability to direct cyberattacks that could potentially disrupt movement and increase risk to the Sector."[1]

ColorTokens can help you implement Zero Trust security to protect automated systems in upstream, midstream and downstream, chemicals, alternatives, low carbon and other activities, for both the information technology and operational technology landscapes. The goal is to reap the benefits of digital transformation, while at the same time reducing the attack surface exposed in the new digitalized systems. This will allow oil and gas companies to:

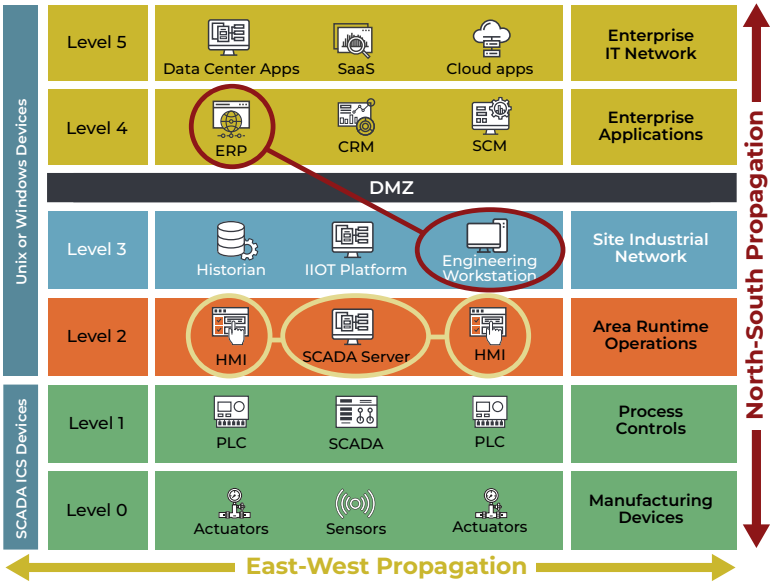
- Protect petabytes of critical business and competitive field data, especially in supply chains from research, exploration, development and production all the way to shipping, terminal operations, distribution and sales.
- Provide network asset and traffic visibility across the entire landscape, mapping dependencies of applications, and monitoring connectivity for policy violations.
- Protect business and operational data and its availability in the production process controlled by the Operational Technology network, while balancing cyber security risk and human safety.
- Have the flexibility to incorporate zero trust principles in cyber security programs, without having to refactor expensive infrastructure in large, distributed landscapes.
- Enforce policies for secure remote and local user access to network resources using the least-privilege-needed paradigm.
- Optimize risk and increase resilience through the ability to stop or delay ransomware and malware propagation.
- Prioritize investments to protect "crown jewels" by focusing on the ability to prevent lateral movement in the event of a cyberattack.

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

The Information Technology network encompasses on-prem data centers, multiple clouds, containers, and even employees' homes and third-party networks. Now, because of the convergence and digital transformation, this diverse IT environment is increasingly connected to systems which were previously isolated: the Operational Technology network. Because of this, visibility is all-important to ensure resilience and continuous operation of digital systems in the energy sector.

[1] OCIA-Sector-Risk-Snapshots.pdf (naccho.org)

In recent years the trend of digital transformation has been pursued so that oil and gas 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 eroded or eliminated the traditional air gap and protective separation between the IT and OT assets. Data sharing is now commonplace across the north-south boundary, 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. As we have seen in the recent WannaCry/NotPetya attack, **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 least-privilege-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: Software-Defined 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. Think of as defining only what should versus everything that shouldn't connect to your digital assets. 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.

Software defined segmentation disallows unapproved network connections by the use of microsegments. Therefore, attempts to connect new computers to existing microsegments require visible approval when required for a valid business process. This results in reducing the technical challenge of visibility in IT/OT convergence.

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 (IoT) network ColorTokens 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 management console, 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 gatekeeper for OT devices.

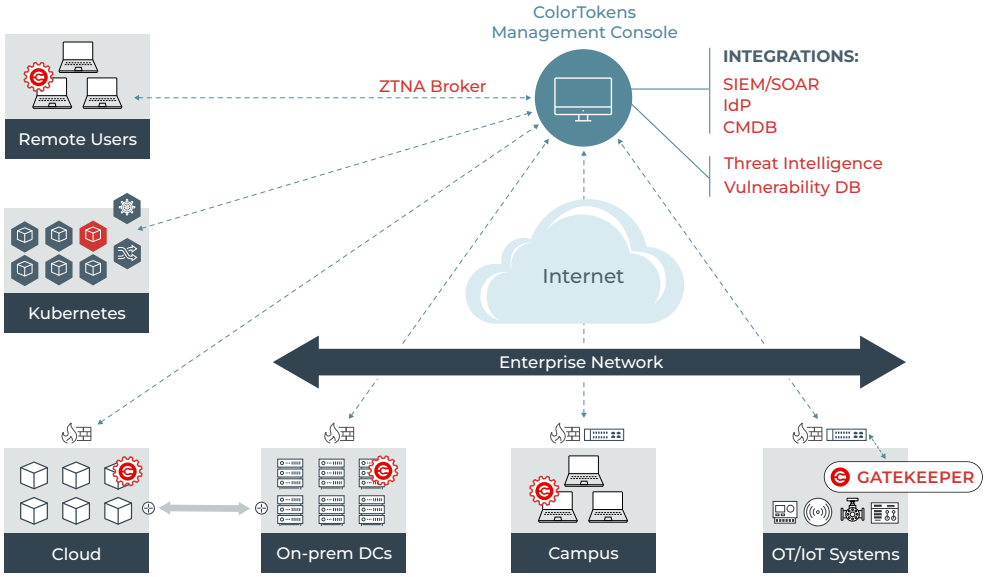


Figure 1: ColorTokens Unified Zero Trust Platform

A Unified 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.

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**