COLORTOKENS

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2020

BLACK UNICORN AWARDS 2019 NOTABLE MENTION

INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2019

SOLUTION BRIEF

IT/OT Integration
Achieve Cybersecurity and IT Integration for OT Systems

Operational Technologies (OT) such as Industrial Control Systems (ICS), Supervisory Control and Data Acquisition Systems (SCADA), and Process Control Networks (PCNs) are critical for enterprises to operate effectively. The applications cut across process manufacturing, utility, mining, transportation, healthcare, and medical service providers. But both discrete and continuous industrial processes are vulnerable to security threats.

Disruption to the OT environment can lead to substantial production shortfalls, personal injuries, environmental disasters, and even threats to an enterprise's long-term survival. That's why it's so important that organizations pay close attention to their OT system security.

Traditionally, however, security has been viewed as an IT problem – not an OT concern. That's because many OT systems were never connected to the outside world, so security attacks were internal rather than external. As a result, the frequency and severity of incidents were generally lower, and inadequate consideration was given to the security challenges of migrating OT workloads from on-premises to a cloud platform.

Today, many OT components lack even elementary cybersecurity defenses, and the underlying ICS operating system of many OT installations is at the end of service life. Hence, these systems have no security patches available to prevent security breaches. Patches are available for OS that have not reached end of life, but a well-founded reluctance to jeopardize production schedules and delivery processes by installing updates and patches places many organizations at risk of cyber compromise.

The Fast Track to OT Security

ColorTokens Xtended ZeroTrust™ Platform enables enterprises to protect vital OT systems by simplifying the security of complex OT environments. The platform's versatility and intuitive UI also empower IT security staff to strengthen OT defenses – there's no need to train IT staff on a new, OT-specific security tool.

The platform is based on the NIST Zero Trust framework to address evolving new threats and compliance requirements. Cloud-delivered for fast time to value, it enables granular visibility, security, and control over endpoints, applications, and network assets to vastly reduce the attack surface and prevent breaches.

Reduce the attack surface and monitor suspicious traffic

ColorTokens Xtended ZeroTrust™ Platform analyzes networks and provides a visual map of all IP-based devices. It creates a comprehensive view of all devices and the associated communication traffic between them. And it shows connections between OT components, OT and IT systems, systems on the enterprise IT network, and the internet.

Challenges

- Restricting and controlling access to OT systems from IT systems and the internet
- Protecting systems that are difficult or cannot be patched or updated
- Strengthening and demonstrating security and compliance
- Coping with scarcity of OT security expertise

Requirements

- Controlling and monitoring access to OT systems at network and process levels
- Preventing malware from executing or replicating in OT networks
- Safeguarding unpatched systems
- Simplifying and documenting compliance with standards

This information allows IT/OT security teams to reduce the attack surface of OT environments by:

- Observing real-time traffic (not simulated) communications between systems and components
- Visualizing and identifying risky and unnecessary paths to OT systems
- Enforcing granular access controls

ColorTokens also allows security teams to monitor network traffic in, out, and between OT/IT environments and quickly identify connections that indicate unauthorized activity.

Control access to OT systems with micro-segmentation

ColorTokens Xtended ZeroTrust™ Platform provides the critical visibility organizations need to implement micro-segmentation. ColorTokens enables enterprise customers to block all traffic from systems and users not explicitly authorized to connect to an OT system. The platform also helps organizations design network security that is often absent from many OT components and network devices.

Plus, ColorTokens' straightforward user interface allows users to effectively isolate OT environments at a faster pace, without the need to manage rules on dozens of firewalls or network devices.

Lock down unpatched systems at the process level

ColorTokens Xtended ZeroTrust™ Platform delivers strong visibility into application processes (good, bad, and unknown), including advanced malware running on OT servers and workstations. ColorTokens provides application process controls to protect OT systems from unauthorized operations, including file-less malware, remote access trojans (RATs), and other forms of malware used by cybercriminals and malicious users.

ColorTokens' platform also protects USBs, preventing files from loading and malware from USB thumb drives. Malware is blocked whether running from the USB drive inserted by a malicious intruder or misguided employee. These are particularly critical features for OT environments where it is expensive or simply impractical to patch systems regularly, because they block threats without needing signatures.

Simplify compliance with industrial IoT security standards

ColorTokens Xtended ZeroTrust™ Platform enables industrial enterprise customers to demonstrate compliance with NIST, NERC-CIP, ISA99/IEC 62443, and other standards. The platform allows security teams to:

- Specify the scope and boundaries of OT and IT systems and interzonal traffic
- Demonstrate the compliance of network traffic in real-time
- Monitor and report access to critical systems by users and other applications
- Automate report creation for incidents, suspicious processes blocked, and other activities related to attacks and breaches

Results and Benefits

With ColorTokens Xtended ZeroTrust™ Platform, you can:

- **Simplify protection of vulnerable OT systems** by leveraging your own security experts
- **Reduce the attack surface of OT environments** by identifying and closing down unneeded ports
- **Implement micro-segmentation** to block unauthorized traffic to OT systems
- **Design network security into the OT environment** to compensate for the absence of controls in existing components
- **Lock down servers and endpoints** by preventing unauthorized applications and processes from executing
- **Simplify compliance** with NIST, NERC-CIP, ISA99/IEC 62443, and other government and industry standards

ColorTokens Inc., a leader in proactive security, provides a modern and new generation of security that empowers global enterprises to singlehandedly secure cloud workloads, dynamic applications, endpoints, and users. Through its award-winning cloud-delivered solution, ColorTokens enables security and compliance professionals to leverage real-time visibility, workload protection, endpoint protection, application security, and Zero Trust network access—all while seamlessly integrating with existing security tools. For more information, please visit www.colortokens.com