SCADA ICS/DCS SYSTEM SECURITY

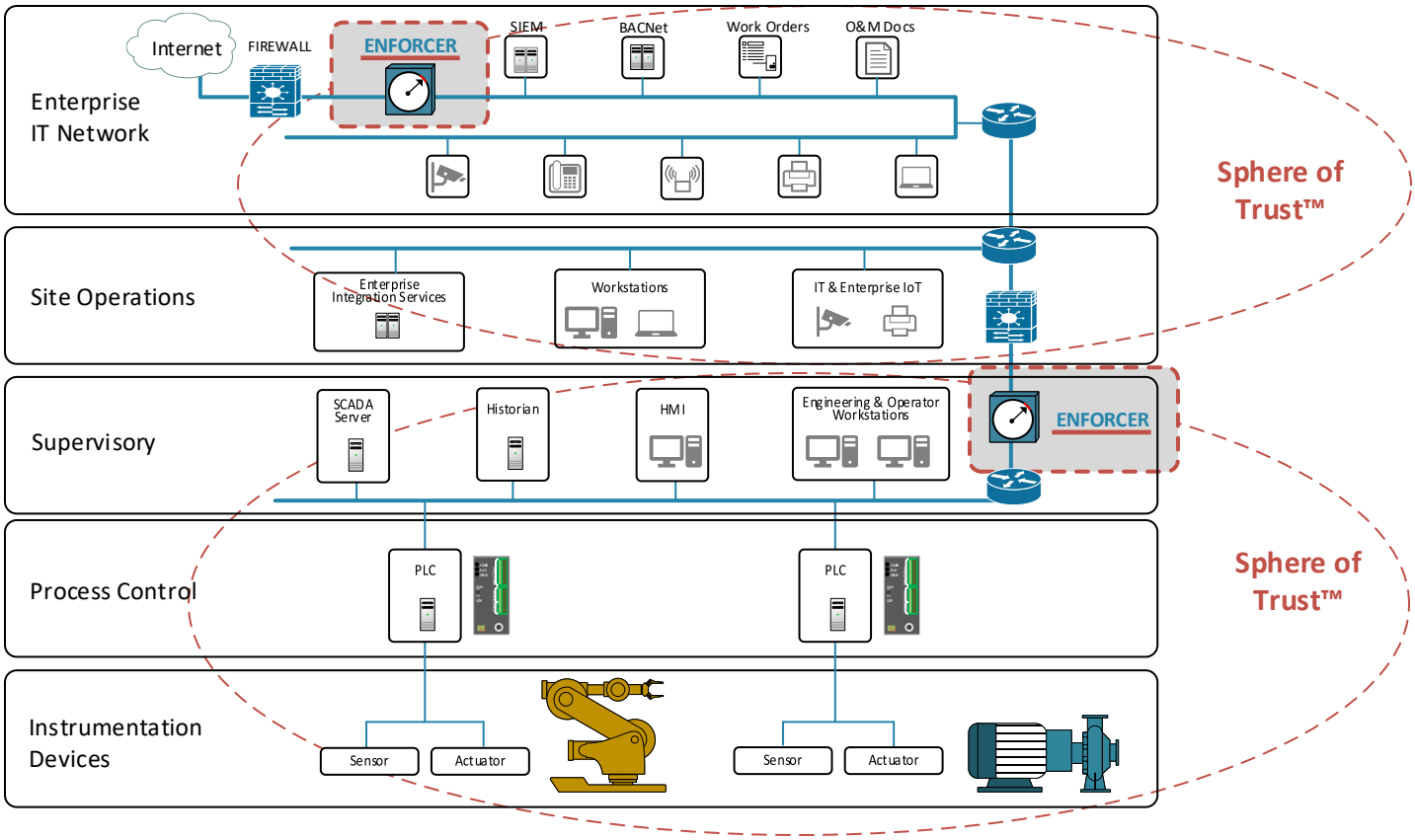
It is good to have real time technology that identifies compromised ICS/DCS systems or open attack vectors on your network. It is even more valuable to proactively prevent the compromise from happening.

Critical infrastructure uses Industrial Control Systems (ICS) to instrument and control process automation. The risk of cyber attacks and achieving command and control (C2) is becoming a prime concern. The rapid conversion of Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCSs) to standard Ethernet networks has created highly interconnected management networks. It is critical that engineers and managers are able to verify that the control networks are isolated from external threats. HOPZERO Security products provide the technology to view the information administrators need in real time and isolate the system from unwanted intruders. Customers can start with a cyber security and risk assessment for SCADA ICS and DCS and receive a comprehensive review of the open threats to the network. The report will quantitatively determine the probability of an attack method, and provide recommendations for reduction of risk.

"SCADA ICS/DCS Exfiltration and C2 Prevention Monitoring with Enforcement "

Passive SCADA/ICS Communications Monitoring & Sphere of Trust™ Enforcement

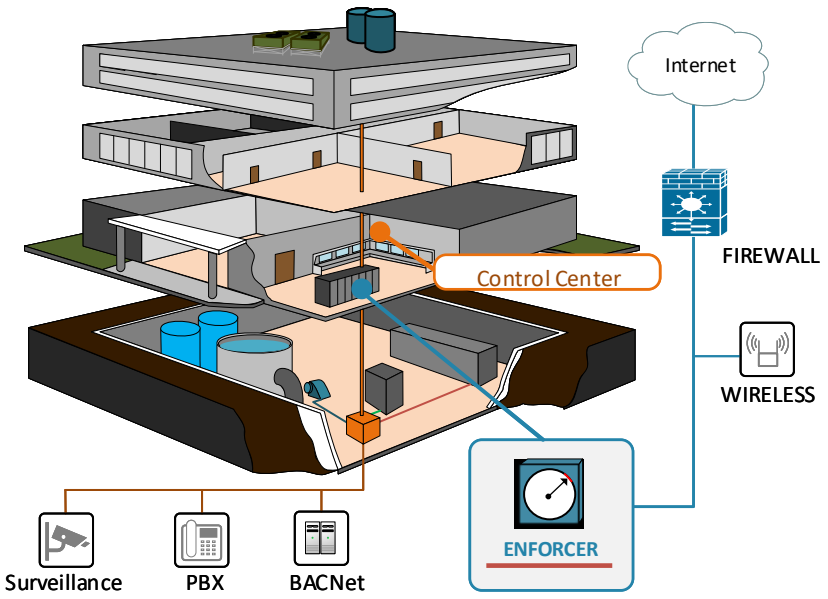
HOPZERO Enforcer technology uses passive monitoring and analysis of every session on the network. The Enforcer identifies thr eats and applies Sphere of Trust™ (SoT™) limits on communications to stop unwanted IP devices from reaching protected SCADA ICS/ DCS systems. This ensures all communications are kept safely within the Sphere of Trust™, undiscoverable by untrusted IP sources.



Smart Building and Data Center Data Containment and Control System Isolation

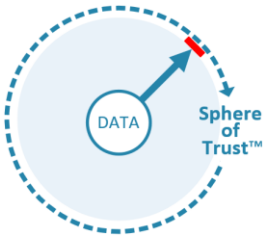
Intelligent Buildings are managed and operated by Smart devices and IoT infrastructures integral to the physical environment. Smart buildings and Data Centers are highly reliant on cooling systems, security systems, data and power infrastructures to keep the building secure and operational. HOPZERO Enforcer technology stands between the control network and other public or open networks. This ensures control and management systems are isolated while delivering verification that the network is protected. Data leaks and command and control attempts against the building are stopped at every attempt.

HOPZERO removes Attack Surface threats using powerful Sphere of Trust™ technology to protect servers and ICS/DCS devices, assuring communications remain inside your network and out of the control of intruders.



Inside the **Sphere of Trust™**

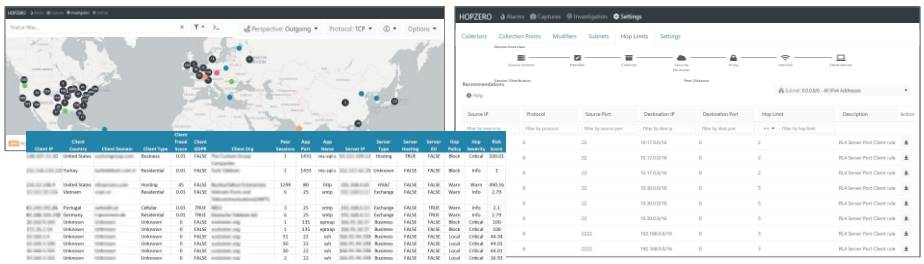
- PLC Devices
- DCS Communications
- C2 Server Protection



Outside the **Sphere of Trust™**

- User Insider Threats
- Command & Control Exploits
- Untrusted Network Risks

The Enforcer learns the Attack Surface of every device, creating numerous SoT™ policies to Block and Limit DataTravel™. An administrator's click authorizes an enforcement recommendation, limiting how far a vital server or ICS device may communicate – keeping it safe inside the Sphere of Trust™. Enforcement works even if a firewall is compromised, allowing exfiltration – even if access credentials to devices become lost to intruders – nothing can connect to the server from outside the Sphere of Trust™. The SoT™ prevents command-and-control and other exploits proactively securing SCADA and ICS systems. Customers can now meet compliance requirements for archiving session information for multiple years with very little storage. Compliance for security standard are provided in HOPZERO software with FIPS 140.2 certification.



Sphere of Trust™ Enforcer includes all the features of the SaaS Auditor and the Smart Session Recorder. Get graphical geo maps and export data to create custom reports.

Learn more about Exfiltration Prevention and Data Containment at https://hopzero.com/Enforcer

HOPZERO
11400 Concordia University Dr.
Austin, TX 78726
833-467-9376
inquire@hopzero.com

About HOPZERO

HOPZERO is an Exfiltration Prevention solutions developer. Audits and proactive security solutions allow companies to protect their private data. HOPZERO products are managed with a unified SaaS management platform providing enterprise wide visibility and safe data containment policy enforcement. HOPZERO security systems eliminates complexity and training gaps normally associated with enterprise systems.

HOPZERO DataTravel™ Security