Holistic security for connected critical infrastructure, Industrial Control Systems (ICS) and SCADA networks

Weak underbelly of ICS/SCADA networks and key security challenges

- Designed for segregated networks, ICS/SCADA systems lack adequate security
- Security vulnerabilities overlooked for integration benefits with corporate IT networks
- Risks include unauthorized access, unpatched systems, poor or no authentication, exploitation of ICS component vulnerabilities (Project SHINE), inadequate visibility
- Over half a million ICS devices exposed on public Internet
- Traditional firewalls do not understand ICS/SCADA protocols

Cyberoam bridges the security gap, improves visibility into ICS/SCADA networks, offers integrated threat protection and enables business continuity

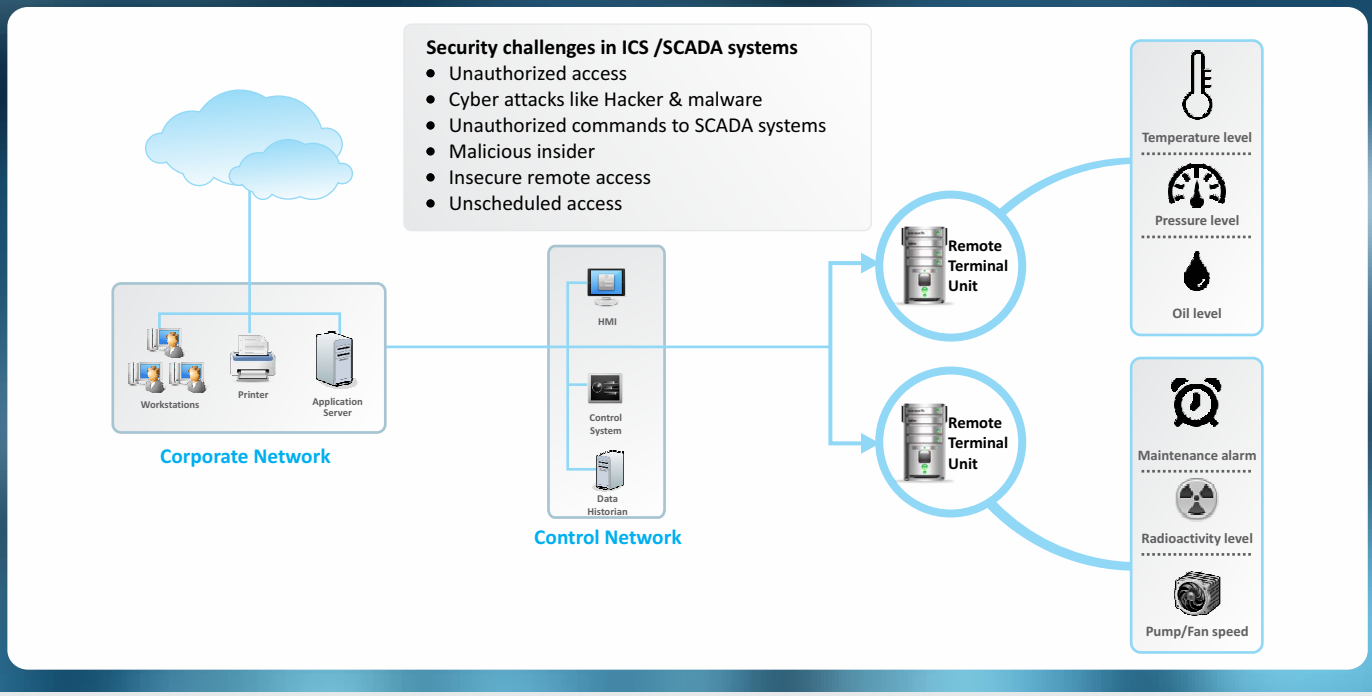
- DPI Firewall to inspect ICS/SCADA traffic
- Layer-8 and Layer-7 security capabilities to strengthen user authentication and understand /filter ICS and SCADA commands
- Intrusion Prevention System & Web Application Firewall to protect against exploitation of ICS component vulnerabilities including web-attacks
- Real-time logging and reporting enabling situational awareness
- VPN protection to enable secure remote access to entities like operators and engineers
- Centralized security management & visibility of distributed security installations in ICS networks

Cyberoam®
A SOPHOS Company

From yesterday's closed silos to today's open networks

ICS systems used for controlling critical infrastructure and processes in verticals such as Oil and Gas, Nuclear Power Plants and other Energy Generation & Distribution units, Manufacturing, Chemicals & Pharma, Water Treatment / Waste Management and the like are no longer isolated, but integrated with corporate /IT networks. Originally designed for segregated environment, Industrial Controls Systems run on legacy communication protocols that were made keeping in mind continuity of key processes and operations and lacked focus on security. As a result, ICS environments have remained fraught with inadequate security such as lack of user integrity check, unencrypted (simple or no encryption) traffic, seldom patched SCADA applications, servers and operating systems.

Integration with IT has exposed ICS to Internet risks and insider threats and has revealed inherent security shortcomings in ICS infrastructure. Several attacks like Stuxnet, Flame, Duqu, Red October and other threats have made news while initiatives like project SHINE, SHODAN search engine and The Internet Census that expose the database of SCADA & ICS devices on the internet, shed light on the sad state of SCADA /ICS security.

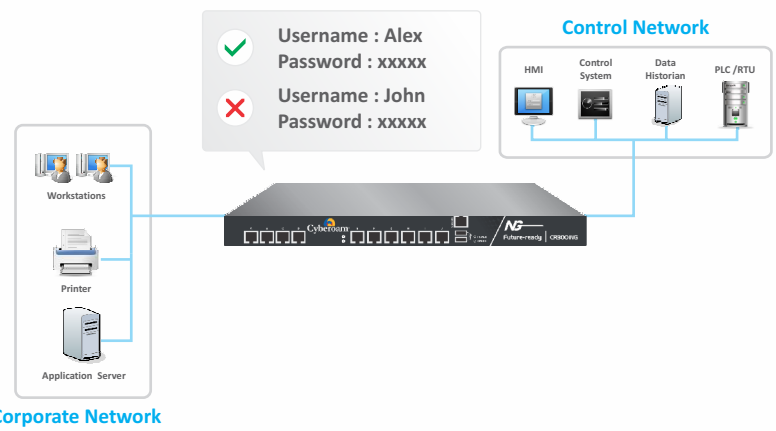


Cyberoam secures ICS and SCADA infrastructure

Cyberoam network security appliances available as Unified Threat Management and Next Generation Firewalls offer integrated security over single platform to ICS and SCADA devices, protecting them from internal and external threats. Security features include DPI Firewall, Layer 8 Identity-based security, Intrusion Prevention System, Application Visibility & Control, Web Application Firewall, Gateway Anti-Virus /Anti-Spyware, Virtual Private Network, Web Filtering, High Availability & more. Cyberoam appliances can be deployed at control centers, remote stations and in enterprise networks to protect them from threats. Cyberoam also enables organizations to centrally manage security of distributed security deployments and get centralized visibility with Cyberoam Central Console and dedicated iView appliances.

1 Adding user authentication for ICS/SCADA systems with Cyberoam's Layer 8 Technology

Cyberoam with its patent-pending Layer 8 technology adds a human layer over the OSI stack providing user-identity based controls. It enables setting user or role-based access allowing only authorized users to access ICS/SCADA systems. Moreover, access to ICS can be linked to a combination of user and device as well. This prevents unauthorized access to ICS using methods such as IP spoofing, malicious login attempts.



2 Visibility & Control over SCADA commands with Cyberoam's Application Filter (Layer 7 security)

Cyberoam firewalls come with app-aware (layer-7) capabilities that understand and filter ICS and SCADA protocols.

Supported protocols include
Modbus DNP3 Bacnet IEC Secure DNP3

Cyberoam enables fine-grained control over individual commands and functions like Modbus read, write, diagnostic. It also enables setting up of schedule-based control on SCADA commands.

Available Modbus Functions		
Modbus - Read Coils	Modbus - Diagnostics	Write Multiple Registers
Modbus - Read Discrete Inputs	Modbus - Read FIFO Queue	Modbus - Write Multiple Coils
Modbus - Read Holding Registers	Modbus - Mask Write Register	Read/Write Multiple Registers
Modbus - Read Input Registers	Modbus - Write File Record	Read device Identification
Modbus - Write Single Coil	Modbus - Report Slave ID	*and more...*
Modbus - Write Single Register	Modbus - Get Comm Event Counter	
Modbus - Read Exception Status	Modbus - Get Comm Event Log	

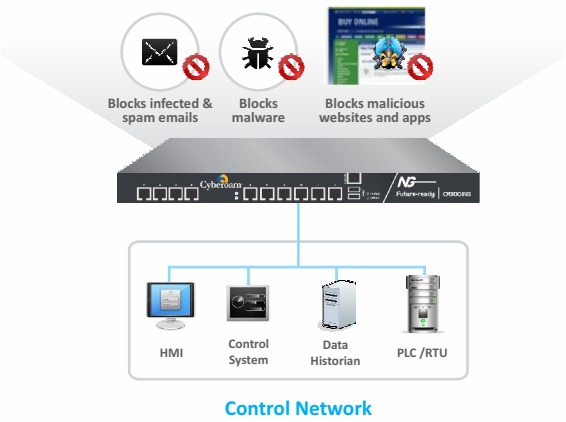
Any application, command or function not covered by Cyberoam app database currently, can be addressed by the Cyberoam Engineering Team. Also, Cyberoam offers customers the ability to create custom signatures

3 Protecting ICS /SCADA systems from malware attacks

To implant malware in the network over web, bad guys use techniques like sending malware infected emails and phishing messages to lure employees to visit an infected website or app, waterhole attacks.

Cyberoam security appliances offer protection against malware implantation in the network with a range of security features that include:

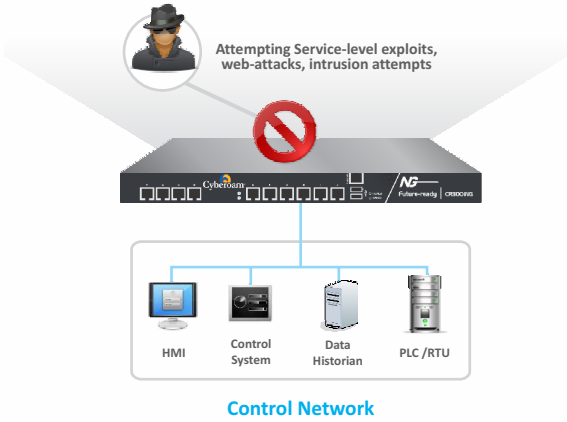
- Gateway Anti-Virus: Blocks infected emails, malware over website from infecting network
- Website and Application Filtering: Blocks access to malicious websites and risky applications
- Anti-Spam: Blocks spam emails



4 Protection from hacking or vulnerability exploits with SCADA-aware IPS and WAF

Hackers exploit vulnerabilities in ICS components including unpatched SCADA systems. Cyberoam security appliances offer SCADA-aware Intrusion Prevention System with a pre-defined category for ICS / SCADA signatures to prevent service-level exploits of vulnerabilities in ICS components. Moreover, its Web Application Firewall blocks web-attacks like exploitation of HMI web-app vulnerabilities.

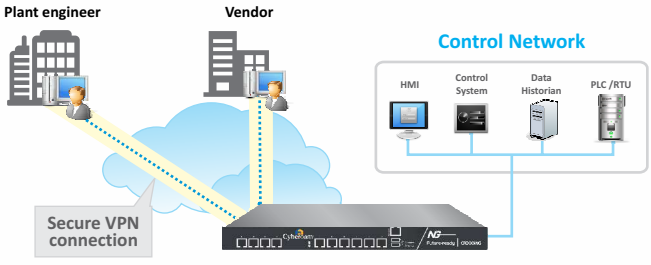
Prevent exploitation of ICS component vulnerabilities and unpatched systems



5 Secure remote access to ICS and SCADA systems with On-appliance SSL VPN (or IPSec VPN)

Operators, plant engineers and vendors require remote access for reasons like monitoring status, running diagnostics and fixing operational issues. An attacker can intercept a poorly guarded remote communication to connect to SCADA network.

Cyberoam enables secure and authorized remote access with SSL VPN (or IPSec VPN) feature available on its security appliances and ensures encrypted communication over Internet to ICS/SCADA systems.



6 Enabling situational awareness with On-appliance Logging and Reporting

Cyberoam offers on-appliance logging and reporting that enables situational awareness with real-time visibility of users accessing ICS, unauthorized attempts, policy violations, ICS commands, IPS alerts and capabilities that help with incident management and forensic analysis. This eliminates the need for an independent reporting solution and minimizes the resultant security investment and operational expense.

- User Reports
- Intrusion Alerts
- Application Reports
- VPN Activities
- Traffic Discovery
- *and more...*

7 Centralized Security Management & Reporting with CCC and iView products

Cyberoam offers centralized security management and visibility for distributed security deployments across ICS and corporate /IT networks through its Cyberoam Central Console (CCC) and dedicated iView appliances. CCC helps security administrators to centrally manage security policies and updates of distributed security appliances. In addition, CCC also allows configuring role-based access for individual or group of Cyberoam security appliances. For centralized visibility, Cyberoam iView's logging and reporting helps with incident management, forensic analysis and compliance management.

Cyberoam product portfolio for securing ICS / SCADA infrastructure:

Network Security Appliances - UTM, NGFW (Hardware & Virtual)	Centralized Management (Hardware & Virtual)	Centralized Reporting (Hardware & Software)

For more information, contact our Sales personnel at sales@cyberoam.com

Awards & Certifications

Cyberoam
A SOPHOS Company

www.cyberoam.com

® Registered Trademark of Cyberoam Technologies Pvt. Ltd.