CLAROTY EDGE ASSESSMENT

Claroty Edge is a highly flexible, Windows-based edge data collector that delivers 100% visibility into industrial networks in just minutes without requiring network changes, utilizing sensors, or having any physical footprint whatsoever.

ES&E

A Fast, Easy, Simple Solution that Delivers 100% Visibility into Industrial Networks in Minutes

Discover all OT assets on your manufacturing network!

1. Provides asset information (identification & details)
2. Identifies known security risks for each asset
3. Built for OT/manufacturing networks & assets - speaks the correct protocols, targeted for these devices.
4. Zero infrastructure – nothing to install
5. Strongest offering according to Forrester Wave

CLAROTY
Clarity for OT Networks

Risk Assessment Report
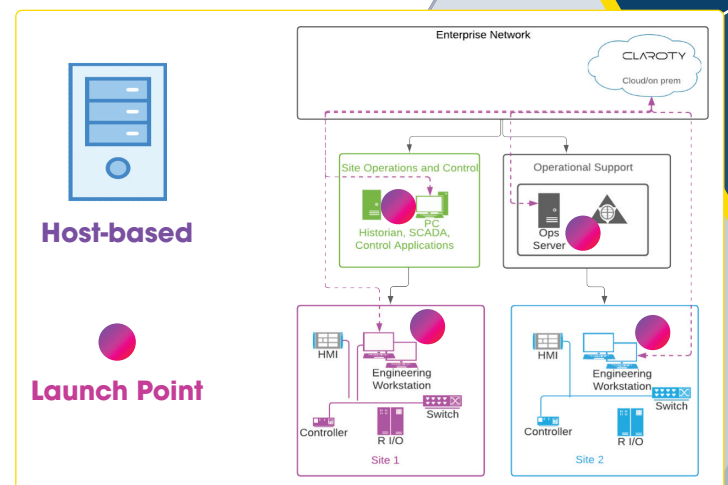**Default**
November 23, 2021

NETWORK HYGIENE SCORE	75%

ⓘ *The calculation represented in the Hygiene Score indicates the cumulative risk level the alerts, insights, and assets pose to the system. A low value means your system is more vulnerable to attacks.*

KEY FINDINGS

- 1 asset was communicating with 5 external IPs
- 14 assets have 160 unpatched vulnerabilities – FullMatch
- 2 assets are using 1 unsecured protocol: TELNET
- 1 asset has 281 unpatched vulnerabilities – Windows Full Match
- 2 PLCs are exposed to remote program changes or have stopped
- 1 asset has 1 unpatched vulnerabilities – Vendor and Model Match
- 5 assets have multiple network interfaces
- 1 asset has 31 vulnerabilities in its installed programs

ASSETS

ASSET INFORMATION

Asset Name	Type	Site	Vendor
Data_Transfer	PLC	Default	Rockwell Automation

Model	Firmware	IP	MAC
1756-EN2TR/B	V4.004	10.1.30.2	00:1D:9C:BD:A9:4F
		10.1.30.30	00:1D:9C:C3:88:9E

FULL MATCH CVES

This table lists assets that run vulnerable software versions and can be leveraged by attackers for various malicious purposes such as, remote code execution, DDOS, etc.

Vulnerabilities are matched against these assets' vendor name, model (family and number) and software version

CVE-2012-6441	10.0	Vulnerability could allow Information Exposure	24/01/12	25/01/12	23/11/21

Access Type: Network

An information exposure of confidential information results when the device receives a specially crafted CIP packet. Successful exploitation of this vulnerability could cause loss of confidentiality.

Related CVEs: ICSA-13-011-03, RA-470154, RA-470155-, RA-470156

Link 1   Link 2   Link 3   Link 4   Link 5

Host-based

Launch Point

Enterprise Network

CLAROTY
Cloud/on prem

Site Operations and Control
PC
Historian, SCADA, Control Applications

Operational Support
Ops Server

HMI
Engineering Workstation
Switch
Controller
R I/O
Site 1

HMI
Engineering Workstation
Switch
Controller
R I/O
Site 2

ES&E Services & Solutions
Call now to get more information or to schedule a demo of our Claroty Edge Assessment.
800.632.0268 | sales@ese-co.com | www.ese-co.com