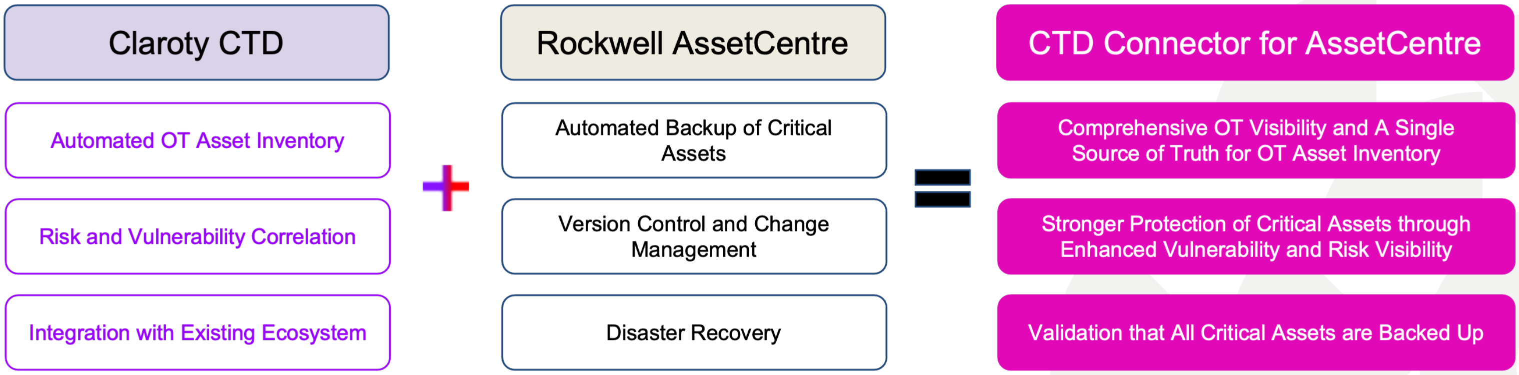
Integration Brief

Claroty CTD Connector for Rockwell FactoryTalk® AssetCentre

Automatically Discover, Protect, and Manage Your Industrial Network's Most Critical Assets

Overview

The Claroty Continuous Threat Detection (CTD) Connector for Rockwell FactoryTalk® AssetCentre fuses CTD's operational technology (OT) visibility with AssetCentre's data management capabilities to automate, optimize, and centralize inventory. The integration brings together CTD's risk and vulnerability assessment and correlation with AssetCentre's backup and recovery coverage for industrial networks.



Claroty CTD		Rockwell AssetCentre		CTD Connector for AssetCentre
Automated OT Asset Inventory	+	Automated Backup of Critical Assets	=	Comprehensive OT Visibility and A Single Source of Truth for OT Asset Inventory
Risk and Vulnerability Correlation		Version Control and Change Management		Stronger Protection of Critical Assets through Enhanced Vulnerability and Risk Visibility
Integration with Existing Ecosystem		Disaster Recovery		Validation that All Critical Assets are Backed Up

Key Benefits & Capabilities

- **Delivers comprehensive OT visibility** and a centralized, fully automated OT asset inventory across the entire OT environment. Insight includes the hardware, firmware, model, rack slot, IP, vendor, and related details for all assets – even tough-to-identify nested devices and those located at levels 0-2
- **Protects your most critical assets** and helps minimize downtime by continuously assessing risks and monitoring for vulnerabilities, automatically correlating this information with the assets in your OT environment to provide tailored mitigation and remediation guidance for all risks and vulnerabilities affecting those assets
- **Expands disaster recovery coverage** by revealing any critical assets not included in your disaster recovery plan, enabling you to add those assets and equipping you to validate asset backup
- **Increases efficiency and effectiveness of governance, risk, and compliance** initiatives and overall decision-making by enabling centralized access, streamlined management, and actionable reporting for all asset, risk, and vulnerability data

How it Works

Highly flexible on-premise, cloud, and hybrid deployment options are available for the CTD Connector for AssetCentre. All deployment options support the following use cases:

Automated OT Asset Inventory

The CTD Connector for AssetCentre uses Claroty's AppDB asset discovery mechanism to ingest project files from AssetCentre, extract the OT asset information present on those files, and populate and organize it within CTD. The result is a fully automated, completely centralized, and always up-to-date OT asset inventory and a single source of truth for OT asset information.

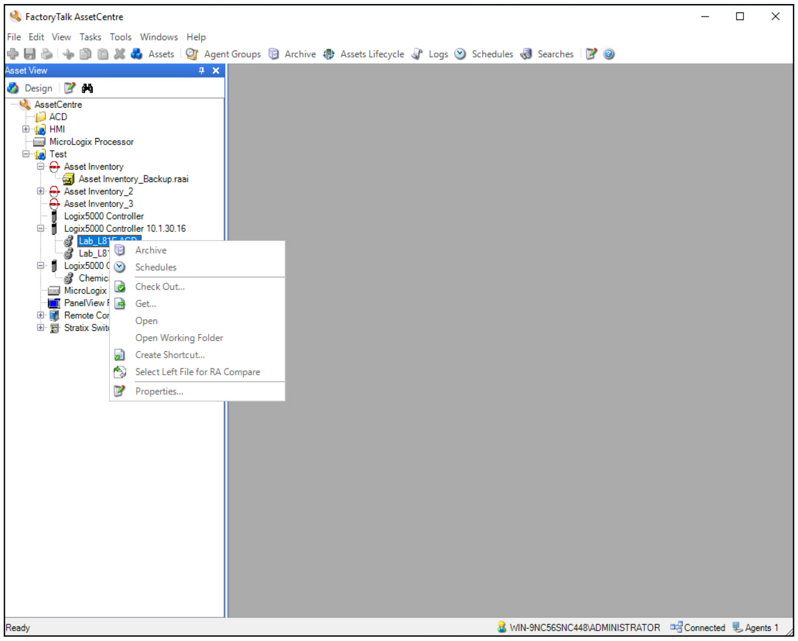
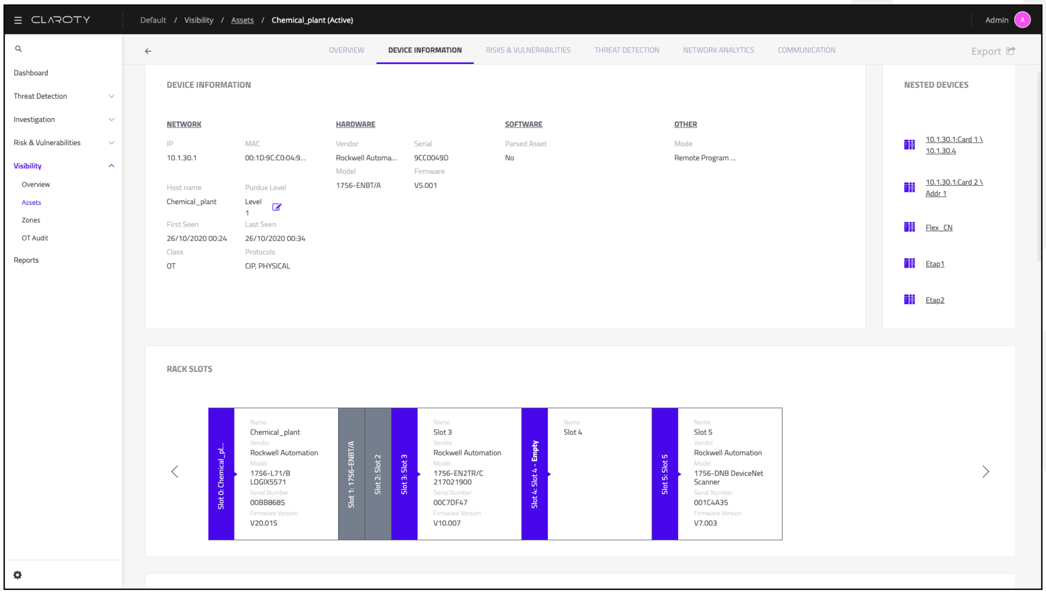


Image 1: *View of the change history and backups of an asset identified as a component of a project file in AssetCentre*



DEVICE INFORMATION

NETWORK
IP: 10.1.30.1
MAC: 00:1D:9C:C0:04:9...
Host name: Chemical_plant
Purdue Level: Level 1
First Seen: 26/10/2020 00:24
Last Seen: 26/10/2020 00:34
Class: OT
Protocols: CIP, PHYSICAL

HARDWARE
Vendor: Rockwell Automa...
Serial: 9CC0049D
Model: 1756-ENBT/A
Firmware: V5.001

SOFTWARE
Parsed Asset: No

OTHER
Mode: Remote Program ...

NESTED DEVICES
10.1.30.1:Card 1 \ 10.1.30.4
10.1.30.1:Card 2 \ Addr 1
Flex_CN
Etap1
Etap2

RACK SLOTS

Slot 0: Chemical_pl...
Name: Chemical_plant
Vendor: Rockwell Automation
Model: 1756-L71/B LOGIX5571
Serial Number: 00BB8685
Firmware Version: V20.015

Slot 1: 1756-ENBT/A

Slot 2: Slot 2

Slot 3: Slot 3
Name: Slot 3
Vendor: Rockwell Automation
Model: 1756-EN2TR/C 217021900
Serial Number: 00C7DF47
Firmware Version: V10.007

Slot 4: Slot 4 - Empty
Name: Slot 4

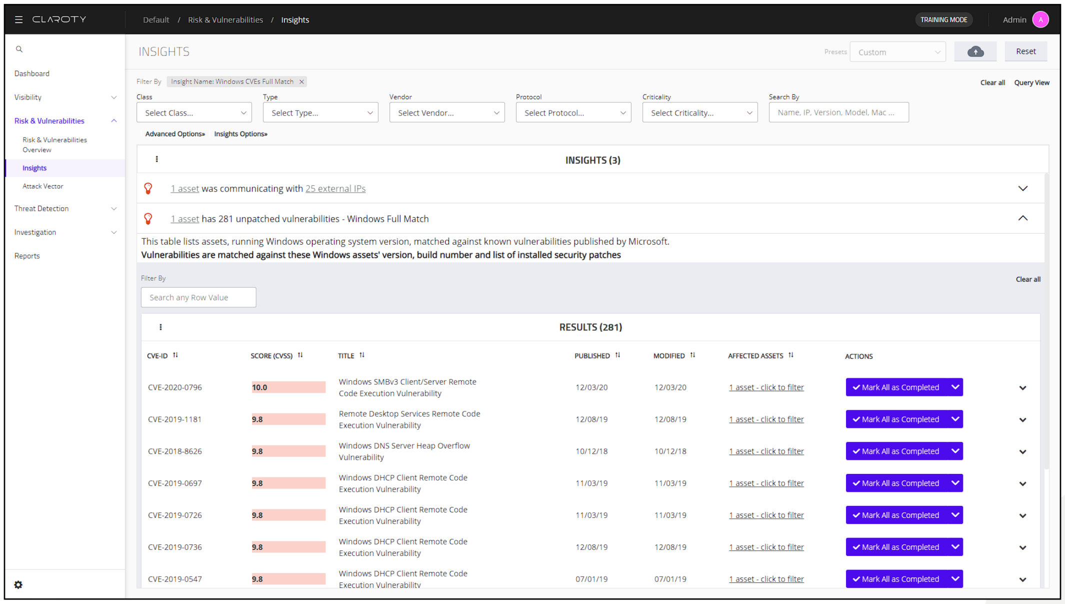
Slot 5: Slot 5
Name: Slot 5
Vendor: Rockwell Automation
Model: 1756-DNB DeviceNet Scanner
Serial Number: 001C4A35
Firmware Version: V7.003

Image 2: *View within CTD of the same asset, which Claroty identified as a Rockwell PLC at level 1 of the network Details such as the asset's rack slot, model, and IP have also been identified and populated here*

Risk & Vulnerability Correlation

After optimizing and automating OT asset inventory, CTD automatically compares the granular details of each asset to the latest common vulnerabilities and exposures (CVE) data and an extensive library of insecure protocols, misconfigurations, and other security weaknesses tracked by the renowned Claroty Research Team.

The depth, accuracy, and timeliness of these details ensures rapid identification of full-match vulnerabilities present in OT assets. The availability of these critical insights also enables CTD to automatically assess and score each vulnerability, affected asset, and the overall industrial environment based on risk, as well as provide actionable guidance on mitigation, remediation, and patch management. All risk and vulnerability data is continuously monitored, automatically correlated, and updated as new risk factors and vulnerabilities emerge. These capabilities are all completely centralized within CTD.



Filter By: Insight Name: Windows CVEs Full Match

Class: Select Class… | Type: Select Type… | Vendor: Select Vendor… | Protocol: Select Protocol… | Criticality: Select Criticality… | Search By: Name, IP, Version, Model, Mac …

INSIGHTS (3)

1 asset was communicating with 25 external IPs

1 asset has 281 unpatched vulnerabilities - Windows Full Match

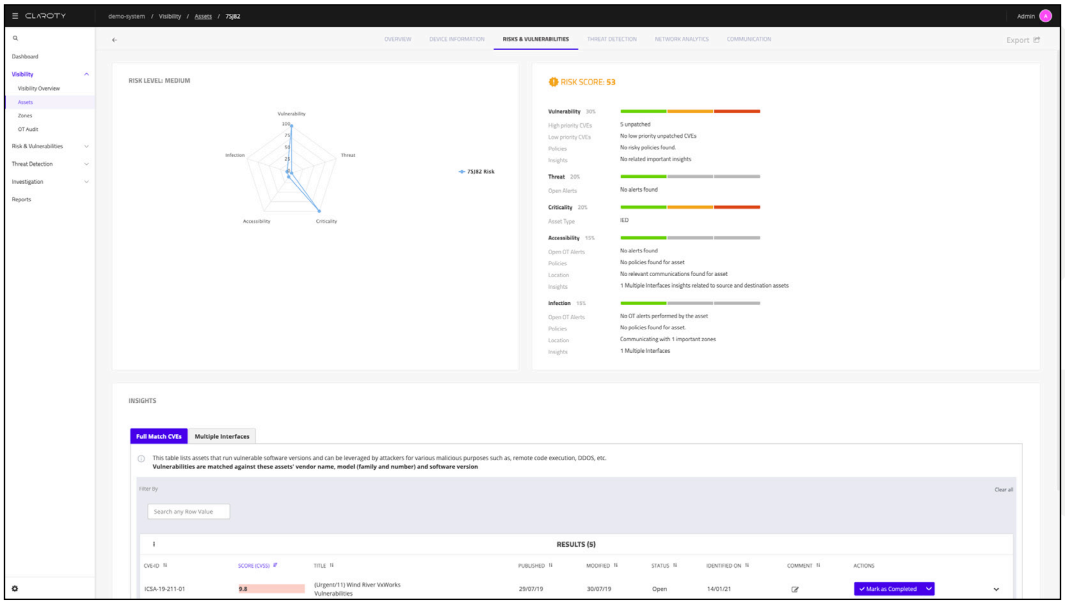
This table lists assets, running Windows operating system version, matched against known vulnerabilities published by Microsoft.
Vulnerabilities are matched against these Windows assets' version, build number and list of installed security patches

Filter By: Search any Row Value

RESULTS (281)

CVE-ID	SCORE (CVSS)	TITLE	PUBLISHED	MODIFIED	AFFECTED ASSETS	ACTIONS
CVE-2020-0796	10.0	Windows SMBv3 Client/Server Remote Code Execution Vulnerability	12/03/20	12/03/20	1 asset - click to filter	Mark All as Completed
CVE-2019-1181	9.8	Remote Desktop Services Remote Code Execution Vulnerability	12/08/19	12/08/19	1 asset - click to filter	Mark All as Completed
CVE-2018-8626	9.8	Windows DNS Server Heap Overflow Vulnerability	10/12/18	10/12/18	1 asset - click to filter	Mark All as Completed
CVE-2019-0697	9.8	Windows DHCP Client Remote Code Execution Vulnerability	11/03/19	11/03/19	1 asset - click to filter	Mark All as Completed
CVE-2019-0726	9.8	Windows DHCP Client Remote Code Execution Vulnerability	11/03/19	11/03/19	1 asset - click to filter	Mark All as Completed
CVE-2019-0736	9.8	Windows DHCP Client Remote Code Execution Vulnerability	12/08/19	12/08/19	1 asset - click to filter	Mark All as Completed
CVE-2019-0547	9.8	Windows DHCP Client Remote Code Execution Vulnerabilty	07/01/19	07/01/19	1 asset - click to filter	Mark All as Completed

Image 3: *View of the OT asset inventory within CTD, showing all full-match CVEs identified and unaddressed within the network*



RISK SCORE: 53

Vulnerability 30%	
High priority CVEs	5 unpatched
Low priority CVEs	No low priority unpatched CVEs
Policies	No risky policies found.
Insights	No related important insights
Threat 20%	
Open Alerts	No alerts found
Criticality 20%	
Asset Type	IED
Accessibility 15%	
Open OT Alerts	No alerts found
Policies	No policies found for asset
Location	No relevant communications found for asset
Insights	1 Multiple Interfaces insights related to source and destination assets
Infection 15%	
Open OT Alerts	No OT alerts performed by the asset
Policies	No policies found for asset.
Location	Communicating with 1 important zones
Insights	1 Multiple Interfaces

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

Filter By: Search any Row Value

RESULTS (5)

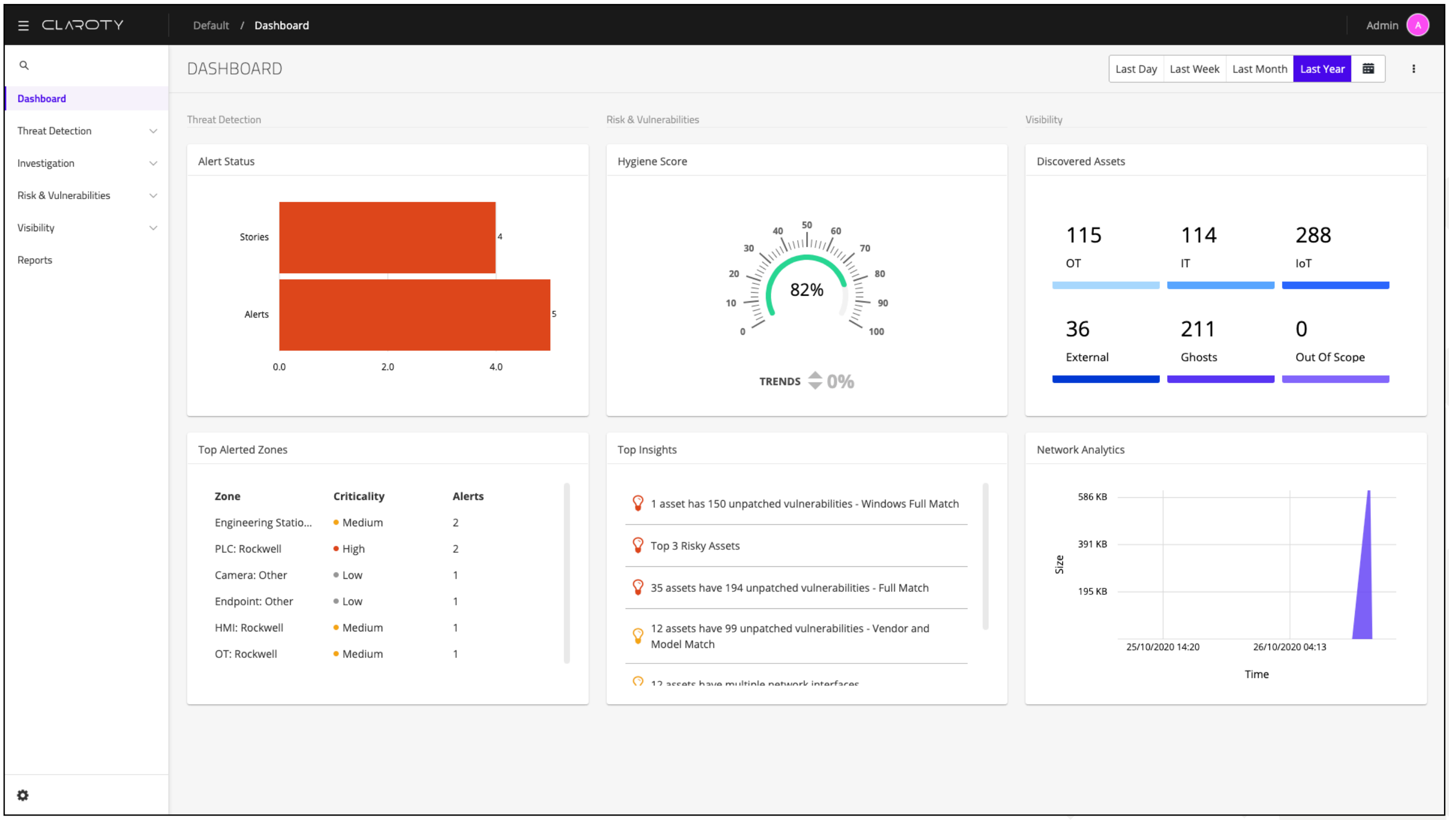
CVE-ID	SCORE (CVSS)	TITLE	PUBLISHED	MODIFIED	STATUS	IDENTIFIED ON	COMMENT	ACTIONS
ICSA-19-211-01	9.8	(Urgent/11) Wind River VxWorks Vulnerabilities	29/07/19	30/07/19	Open	14/01/21		Mark as Completed

Image 4: *View within CTD of the breakdown of the Asset Risk Score, automatically assigned to and continuously updated for each asset in the inventory*

Expanded Disaster Recovery Coverage

The comprehensive OT visibility provided by the CTD Connector for AssetCentre extends to all assets spanning your entire OT environment – even assets that are not yet backed up in AssetCentre and thus not yet accounted for in your disaster recovery plan. Whenever CTD identifies such an asset in your OT environment, the asset will automatically populate in a dashboard showing it does not currently exist in AssetCentre.

This capability makes it easy to pinpoint and address gaps in your disaster recovery plan. Once you've added all previously missing critical assets to AssetCentre, your inventory within CTD will enable you to confidently validate that they are now backed up. As a result, you'll gain expanded disaster recovery coverage and peace of mind that the integrity and availability of your most critical assets will face significantly reduced exposure to risk in the event of an incident.



115	114	288
OT	IT	IoT
36	211	0
External	Ghosts	Out Of Scope

Zone	Criticality	Alerts
Engineering Statio...	● Medium	2
PLC: Rockwell	● High	2
Camera: Other	● Low	1
Endpoint: Other	● Low	1
HMI: Rockwell	● Medium	1
OT: Rockwell	● Medium	1

1 asset has 150 unpatched vulnerabilities - Windows Full Match

Top 3 Risky Assets

35 assets have 194 unpatched vulnerabilities - Full Match

12 assets have 99 unpatched vulnerabilities - Vendor and Model Match

12 assets have multiple network interfaces

***Image 5:** View of CTD's home-page dashboard outlining overall network hygiene score, discovered assets, vulnerability insights, and more.*

CLAROTY

About Rockwell Automation

Rockwell Automation, Inc. (NYSE: ROK), is a global leader in industrial automation and digital transformation. We connect the imaginations of people with the potential of technology to expand what is humanly possible, making the world more productive and more sustainable. Headquartered in Milwaukee, Wisconsin, Rockwell Automation employs approximately 24,000 problem solvers dedicated to our customers in more than 100 countries.

To learn more, visit www.rockwellautomation.com.

About Claroty

Claroty empowers organizations to secure cyber-physical systems across industrial (OT), healthcare (IoMT), and enterprise (IoT) environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, threat detection, and secure remote access. Backed by the world's largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.

To learn more, visit **www.claroty.com**.

CONTACT US
contact@claroty.com