dot™

dot

Technical Features

awencollective.com

awen by SAPPHIRE

Oct 2023

version 2.1

Contact

awen@sapphire.net

0845 58 27001

dot™ BY AWEN

Discover what's on your Industrial Control System network with Dot. Dot is a software system which performs Asset & Vulnerability Discovery on Operational Technology (OT), including ICS, SCADA and IIoT systems. Built using security-by-design and safety-critical scanning technology to support modern and legacy networks. Dot uses deep packet inspection and exclusive active scanning software to build a full picture of your network.

The first step in establishing an effective OT cyber security programme

Gather in-depth information about your OT assets

Accurate information on vulnerabilities, and informed risk scoring

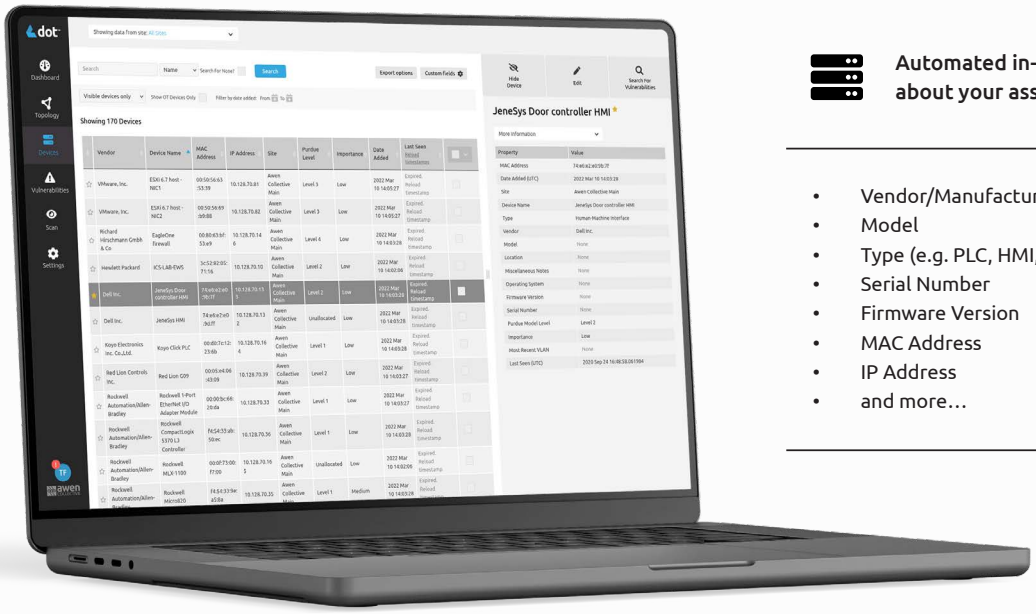
Flexible and scalable to meet the constraints of your OT environment

Easy to deploy, reach 100% visibility of your OT assets

Gain a total understanding of your OT architecture

Book a demo

ASSET DISCOVERY



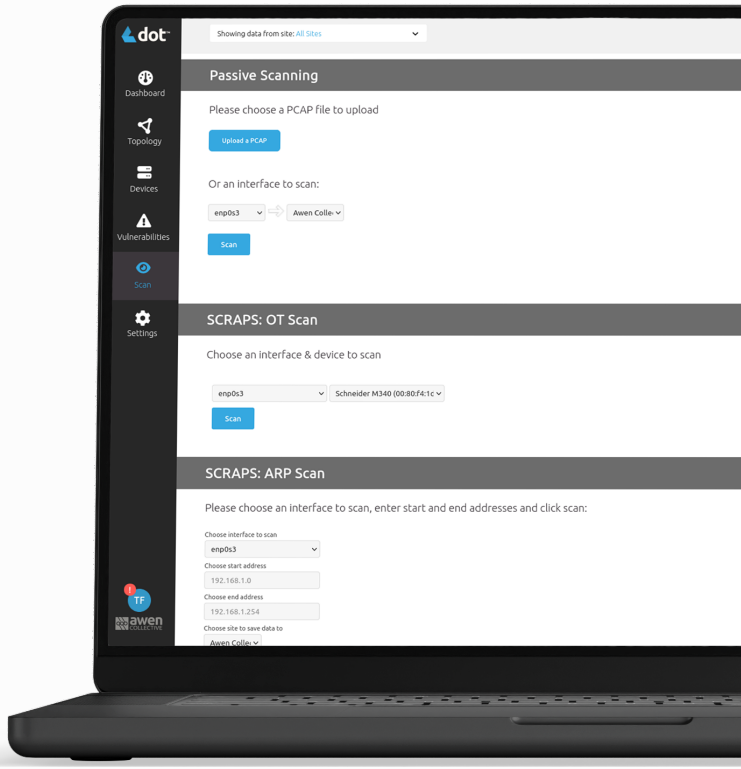
Automated in-depth metadata discovery about your assets including;

- Vendor/Manufacturer
- Model
- Type (e.g. PLC, HMI, Firewall, Switch, etc.)
- Serial Number
- Firmware Version
- MAC Address
- IP Address
- and more…

Easy to deploy. 100% visibility.

Data is discovered using passive network scanning and SCRAPS™

- Data input can be real-time or from PCAP files
- Initial discovery can be completed without any direct connectivity to your OT network, ensuring no impact to operations
- The depth of data discovered can be increased through the use of SCRAPS™ (Safety CRitical Active Protocol Scanning)
    - Targeted and validated active scanning to ensure the retrieval of valuable asset metadata without impacting the operations of a live OT environment
    - SCRAPS™ can also be used to validate whether the data feed provided to Dot is capturing all network traffic, or if it's missing data from devices on the network



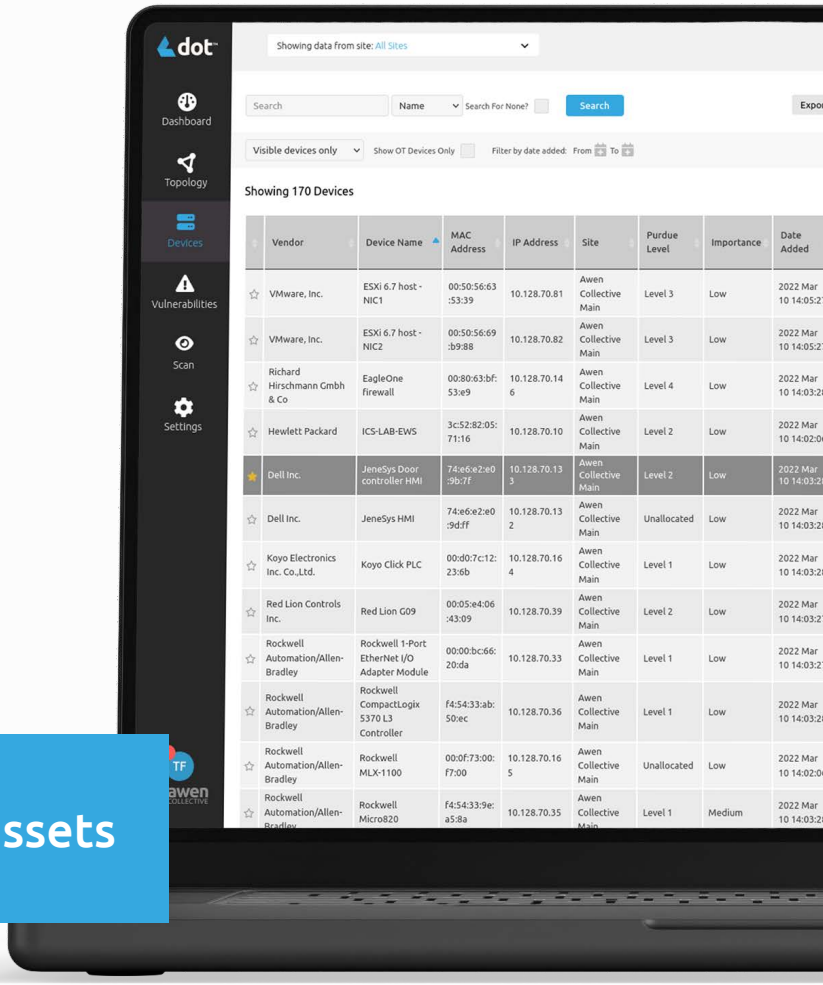
ASSET DISCOVERY

Easily filter and focus on the assets that matter most

- Arrange your assets by site - view one or all sites at any time
- Search your assets by Name, MAC Address, IP Address, Vendor, Type, and many more criteria
- Limit your search by when traffic was last seen from a device

Export asset data

- Your data belongs to you - all asset metadata and network connectivity information stored in Dot is exportable via CSV



In depth information on assets

Compatibility with many OT protocols and vendors including

- Siemens S5 and S7
- Ethernet/IP
- CIP
- Modbus
- Bacnet
- DNP3
- IEC 61850
- LLDP
- MQTT
- OPCUA
- Profinet
- SSDP
- Schneider Foxboro IA
- and more…

Plus many IT protocols often found within OT environments including

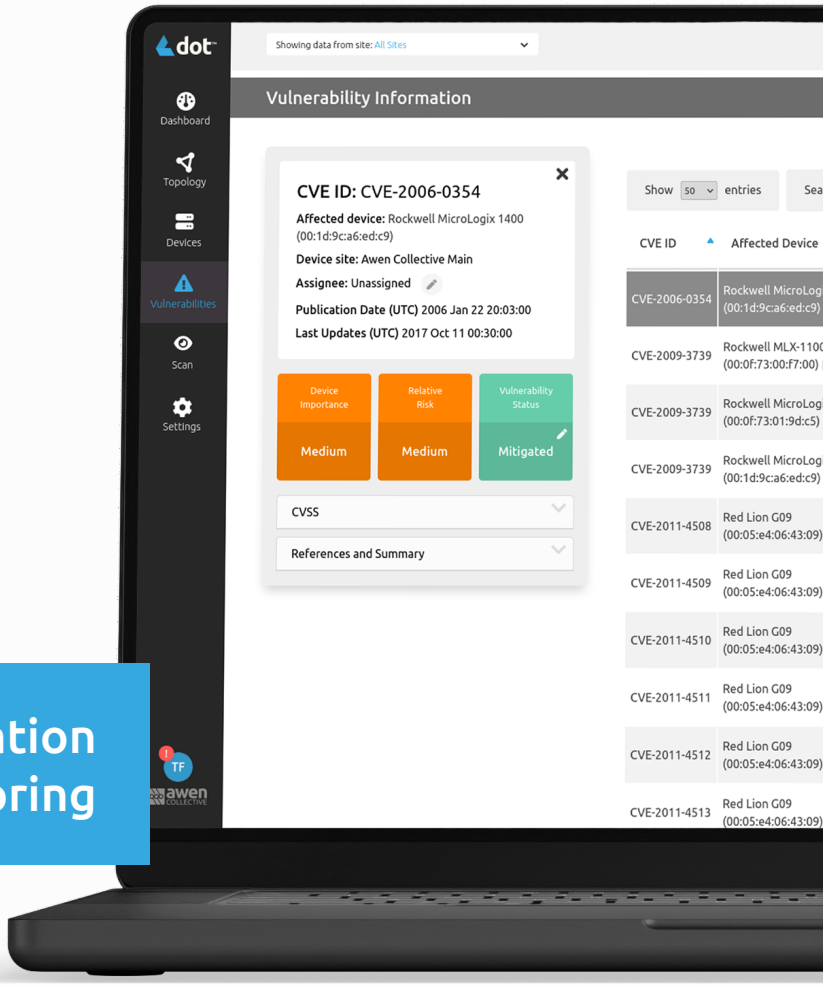
- DNS
- FTP
- HTTP
- ICMP
- IMAP
- POP3
- RDP
- SMB
- SMTP
- SNMP
- SSH
- and more…

Book a demo

See our latest protocol support list for more information

VULNERABILITY MANAGEMENT

- Accurate and verifiable vulnerability information can be discovered using your in-depth asset data
- Vulnerabilities published by vendors are identified and attributed to assets
- Vulnerabilities can be assigned to a member of your team to triage and action as appropriate
- Relative vulnerability severity scores via CVSS can be interrogated and re-calculated based on individual system knowledge
- Overall risk to your organisation is deduced based on the severity of the vulnerability and the importance of the asset (or group of assets) to your operations
- Prioritise vulnerabilities via risk to your organisation
- Links to further information and remediation advice
- Export vulnerability data via CSV
- Works in an offline environment - cache vulnerability definitions for use when Dot is deployed in an offline or airgapped environment



Accurate vulnerability information and informed risk scoring

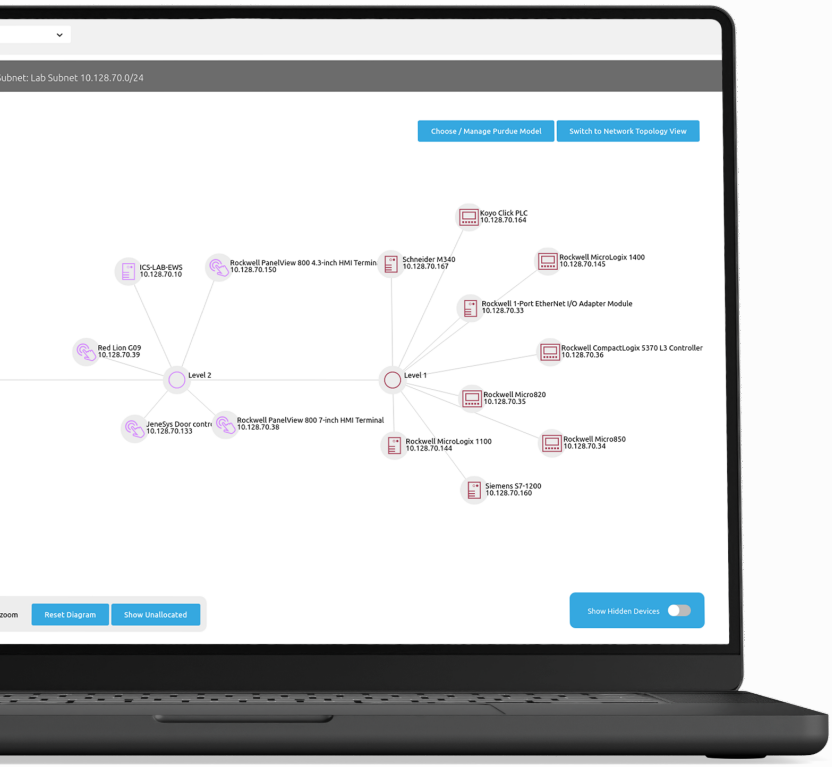
DASHBOARD

See vital statistics about your assets and vulnerabilities at a glance

PDF REPORTS

Generate PDF reports for print, directly from the dashboard.

NETWORK TOPOLOGY



- See all your assets and how they're communicating across your OT network
- Align your OT network to the Purdue Model - understand how well-segregated your network currently is, and how you could improve it using the guidance of current standards

SETTINGS AND SECURITY

- Two Factor Authentication
- Granular user access controls
- User behaviour and audit logging capability

INTEGRATIONS

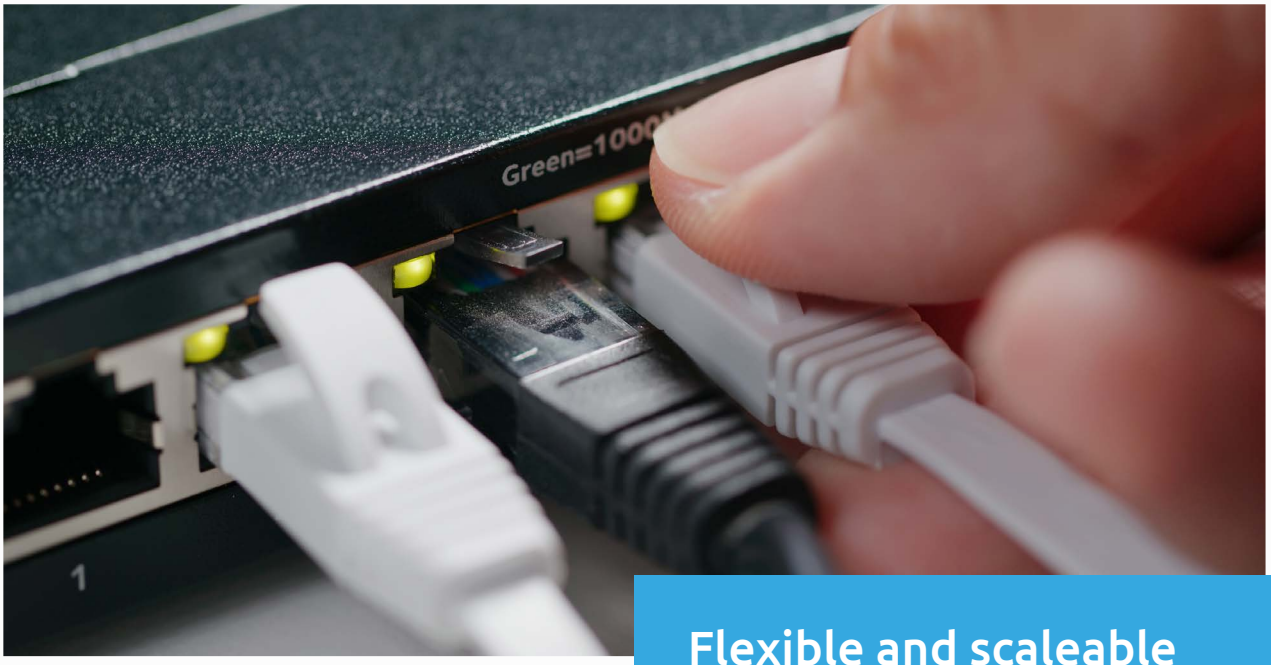
- SIEM/SOC centralised alerting via CEF/LEEF/Syslog
- Alerts via email
- More coming soon…

SIMPLE DEPLOYMENT

- Dot can be run in the cloud, on premise or on portable hardware
- Can be supplied as SaaS, a Virtual Machine or custom installed on hardware
- Dot has a small footprint and limited hardware requirements, ensuring cost-effective deployment on affordable hardware to meet all scaling requirements

Minimum 1 core, 4GB RAM, 25GB storage; subject to bandwidth of network traffic analysed and real-time data requirements

All of this means we can design the right deployment architecture for your organisation, to get you to 100% visibility across your OT estate, no matter the complexity of your OT networks, the geographical distribution of your sites, the limited network connectivity between them, or the prevalence of legacy OT equipment.



Flexible and scaleable

Book a demo

WITH SUPPORT FROM

SAPPHIRE™

National Digital Exploitation Centre
Canolfan Ecsbloetio Ddigidol Genedlaethol

Defence and Security Accelerator

Raytheon

SIEMENS

GET IN TOUCH

Dot has been developed with the support of these organisations and many more. We are continuously improving our solutions capabilities, and would be more than happy to discuss your individual requirements with you. Our collaborative and consultative approach to OT cyber security will ensure 100% visibility of your assets, working around any constraints of your OT environment.

Book a demo