FirstWave



PRODUCT DATASHEET

IT asset discovery, compliance
and AI-matched vulnerability management

Open-AudIT 7

Know exactly what's on your network. Discover it without credentials, map it, benchmark it and prove compliance.

Version 7.0 · November 2026

FirstWave

Open-AudIT 7

IT asset discovery, compliance and AI-matched vulnerability management

Open-AudIT discovers, audits and records what's connected to your network. Its agentless discovery engine captures hardware, software, configuration and network detail across every device, on a schedule or on demand, and keeps a history of every change.

Version 7 rebuilds discovery so a working inventory exists before you enter a single credential. It adds network, routing and application mapping, Windows and Active Directory benchmarking against the DISA STIGs, four new compliance control sets, and registers for certificates, domains and vendors. AI-driven vulnerability detection matches your devices to global CVE intelligence and alerts you to the risks that matter.

353
device types classified, up from 98

1,304
compliance controls across five standards

30 days
full Enterprise trial with every download, unlimited devices

Discover devices without credentials

The new discovery engine identifies devices from what each open port reveals, including OT equipment such as PLCs and SCADA systems, NAS devices and server management controllers. Credentialed audits then fill in the detail.

AI-powered vulnerability detection

Automated detection of vulnerabilities mapped to CVEs. See which devices are affected and how severe the risk is, and compare against historical vulnerability baselines over time.

Security and compliance benchmarking

Benchmark Windows, Linux and Active Directory against the DISA STIGs, CIS Benchmarks, NIST 800-171 and the Essential Eight. Track controls for ISO 27001, ASD Essentials, NCA ECC, CBDDO and BDDK.

Network, routing and application mapping

See what each device connects to, how your networks link through routed links and VPN tunnels, and which discovered servers and databases each application depends on.

Directories and people

Connect Active Directory and Entra. Flag unused accounts, passwords that never expire and changes to privileged groups, and link every directory user to the devices they use.

Certificate, domain and vendor registers

Track ownership, expiry and renewal dates so certificates and domains are renewed on time, with vendors linked to the items they supply.

Configuration change management and baselines

Track and report on configuration changes, software licensing, shadow IT and hardware warranty status. Compare software, hardware, users and netstat data against your required baseline.

Scheduled reporting and role-based access

Schedule any report for delivery by email in CSV, JSON, XML or HTML. Roles carry Create, Read, Update and Delete permissions per endpoint and work with Active Directory, LDAP, Entra and Okta.

WHAT'S NEW IN VERSION 7

Discover first, then audit

FirstWave

Version 7 focuses on discovery. A rebuilt engine identifies equipment from the protocols it already speaks, so you have a working inventory as soon as a scan completes. Credentialed auditing remains for the full picture. Much of the release comes directly from customer and partner requests.

Discovery

EVERY EDITION

- A credential-free engine identifies devices from open ports and keeps the full parsed response as JSON in the discovery log.
- OT discovery over BACnet, Modbus, S7 and EtherNet/IP for PLCs and SCADA devices.
- Redfish, IPMI and Intel AMT identify management controllers. SSDP retrieves the device's own web page. TLS certificates name the vendor.
- ARP discovery feeds addresses from the server, switches, routers and audited computers into the scan queue.
- Parallel subnet scanning: large ranges are split into subnets and scanned in parallel.
- Active Directory networks as discovery targets, with collectors on Windows (Enterprise).

Directories and people

ENTERPRISE

- Directories connect to Active Directory and Entra and keep a change history.
- The summary flags accounts unused for more than 30 days, passwords set never to expire, group membership changes in the last 7 days, and membership of Administrators, Domain Admins and Enterprise Admins.
- People fills a new collection from directory users, with their directory details and the devices they use.
- Network, routing and application mapping are on page 4.

Benchmarking

ENTERPRISE

- Windows machines benchmark against the DISA STIGs during the audit with no extra setup, with severity and pass or fail per rule.
- Active Directory is benchmarked against the DISA STIGs, with results in the directory's Security view.
- Linux benchmarks carry forward on OpenSCAP profiles: CIS Benchmarks, DISA STIG, NIST 800-171 and the Essential Eight.
- Four new control sets join ISO 27001: CBDDO and BDDK (Türkiye), NCA ECC (Saudi Arabia) and ASD Essentials (Australia). Together, 1,304 controls.

Registers

ENTERPRISE

- Domains record the registrar, securing certificate, expiry date and when renewal work should start. Status: Active, Due For Renewal or Expired.
- Vendors become a register of contact, legal and payment details, linked to the items they supply.
- Certificates record issuer and fingerprint, match to web servers by serial number, and stay active while any device uses them.

NEW IN VERSION 7 · ENTERPRISE

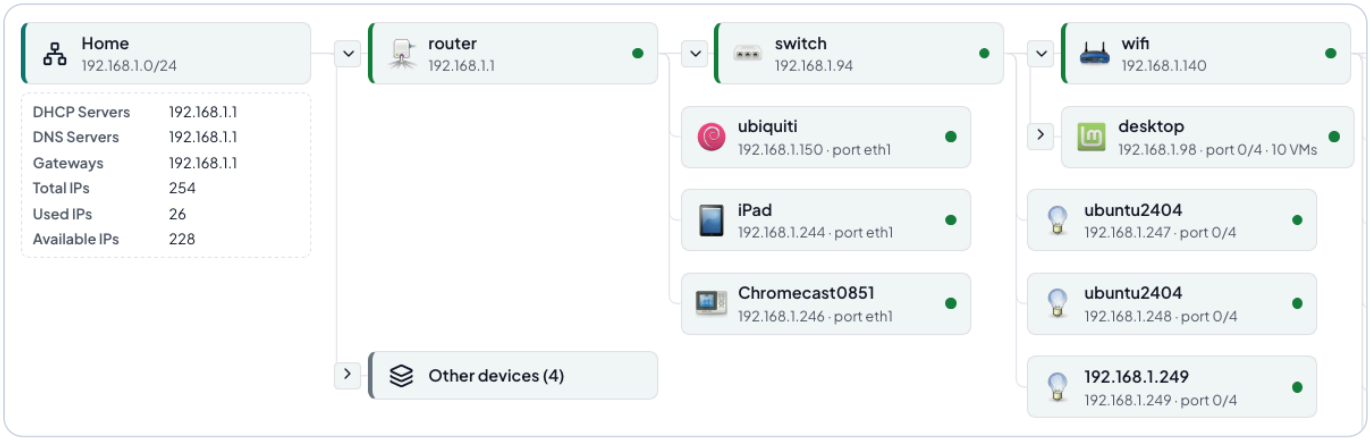
See how everything connects

FirstWave

Three new maps turn the inventory into a picture of how your environment fits together. All three draw on the same discovery and audit data, so there is nothing extra to configure, and better audit coverage of your network gear gives a more accurate map.

Network Dependency Mapping

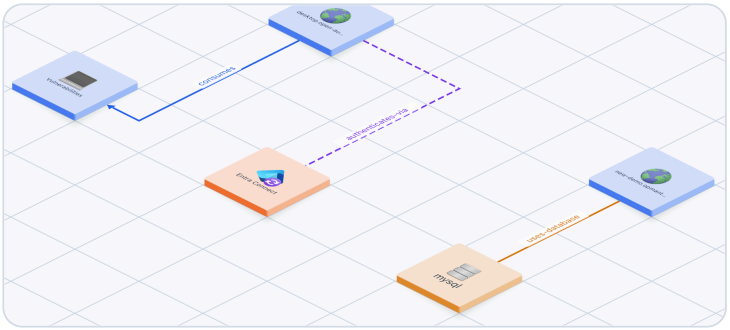
A network drawn from its router through switches and Wi-Fi to the devices on each port, with name, address, connected port and status for every device, and the network's DHCP, DNS, gateway and IP counts alongside.

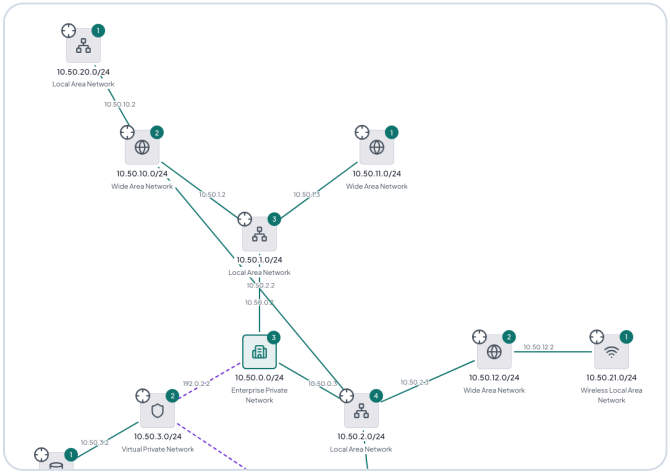


Application Relationship Mapping

Model an application as its components, such as websites, APIs, databases and cloud services, joined by plain-named relationships: consumes, authenticates-via, uses-database, uses-certificate.

You choose only from discovered, available servers and their databases, and a search across components shows which applications a server carries.





Network Routing Map

How your networks connect to each other through routed links and VPN tunnels. Each network carries its device count, and the map can be redrawn centred on any network with a chosen number of hops.

VLANs read from switch ports are listed beneath their network, each a link to its devices, and a network carrying one VLAN is ringed in that VLAN's colour.

Features

FirstWave

DISCOVERY AND AUDIT

DEVICE DISCOVERY

- Networked devices, servers and virtual machines, with or without credentials.
- OT devices, NAS, printers, UPS units, cameras, IoT and management controllers.
- Cloud instances on AWS, Azure and Google Cloud.
- 353 device types classified and filterable.

DEVICE AUDITING

- Hardware: motherboards, processors, disks and memory.
- Software: installed packages, services, executables and files.
- Network: cards, IP addresses, open ports and routes.
- Users and groups, via SNMP, SSH, WinRM, WMI or agents.

MAPPING

- Network Dependency Mapping of device connections.
- Network Routing Map across routed links and VPN tunnels.
- Application Relationship Mapping to servers and databases.
- Locations on OpenStreetMap and racks visualised with space-use reports.

SECURITY AND COMPLIANCE

VULNERABILITIES

- AI matches installed software to CVEs and alerts on new risks.
- Affected devices and severity at a glance.
- Compare against historical vulnerability baselines.

BENCHMARKS AND STANDARDS

- Windows and Active Directory against the DISA STIGs.
- Linux on OpenSCAP: CIS, DISA STIG, NIST 800-171, Essential Eight.
- ISO 27001, ASD Essentials, NCA ECC, CBDDO and BDDK control sets.

DIRECTORIES AND REGISTERS

- Active Directory and Entra with change history and privileged-group alerts.
- Certificates, domains and vendors with ownership, expiry and renewal dates.
- Antivirus and firewall status from Windows clients.

BUSINESS MANAGEMENT

IT ASSET MANAGEMENT

- Detailed inventory of hardware, software and network assets.
- Every change, addition or removal recorded over time.
- Who has each device, where it is and its warranty status.

SOFTWARE LICENSING

- Match installed software with purchased licences.
- Find shadow IT and approve or ban software packages.
- Report on over-subscription before the bill arrives.

REPORTING AND NOTIFICATIONS

- Schedule any report by email, filtered by organisation.
- CSV, JSON, HTML and XML output.
- Weekly hardware, software, new-device and unseen-device reports.

EASE OF USE AND PURCHASING

ACCESS AND INTEGRATION

- Role-based access control with Active Directory and LDAP, and Entra or Okta sign-in.
- Fully documented RESTful JSON API for CMDB integration.
- Rules: if this, then that, on any device attribute.

EASY IMPLEMENTATION

- Simple install with dependencies handled for you.
- Ready-to-go dashboard, custom widgets, any browser.
- In-application documentation for every feature.
- Collectors scale discovery across sites and servers.

LICENSING

- Licensed by device count, not by the number of discoveries or audits.
- Subscription, pay-as-you-grow and MSP scale options.
- Unlimited user accounts. Support portal and wiki included.

Editions

Every install starts with a 30-day Enterprise trial on unlimited devices. Afterwards, buy a licence, ask us for an extension, or move to Free on up to 100 devices.

FirstWave

CAPABILITY	FREE	PROFESSIONAL	ENTERPRISE
Discovery: credential-free engine, OT, ARP, 353 device types	✓	✓	✓
Auditing, change detection and device management	✓	✓	✓
Custom fields and attribute values	✓	✓	✓
Data export (CSV, XML, JSON) and the JSON API	✓	✓	✓
Software licence reporting and in-app documentation	✓	✓	✓
Commercial support		✓	✓
Dashboards, summaries and reporting over time		✓	✓
Scheduling of discoveries, baselines, reports and queries		✓	✓
Vulnerabilities: AI-matched CVE reporting		✓	✓
Geographical maps, clusters and custom audit scripts		✓	✓
Network, routing and application mapping			✓
Directories (AD, Entra), People, AD as a discovery target			✓
Benchmarks: DISA STIGs for Windows and AD, OpenSCAP for Linux			✓
Standards: ISO 27001, ASD Essentials, NCA ECC, CBDDO, BDDK			✓
Registers for certificates, domains and vendors			✓
Baselines, rules, software packages, file change detection			✓
Agents, collectors and cloud audits (AWS, Azure, Google)			✓
Role-based access control, Entra or Okta sign-in, racks, widgets			✓

Find out what answers on your network.

Download Open-AudIT 7 and run the full Enterprise product for 30 days, or talk to us about licensing, an extended trial or a guided demo for your environment.

Download Open-AudIT | **Book a Demo →**

EMAIL
connect@firstwave.com

WEB
firstwave.com · open-audit.com

PHONE
Asia Pacific: 1300 174 419 · +61 2 9409 7000
USA & Canada: +1 (833) 823-8810
Mexico & Latin America: +52 55 5993 4830
United Kingdom: +44 808 164 1268

© 2026 FirstWave Cloud Technology Ltd (ASX: FCT)