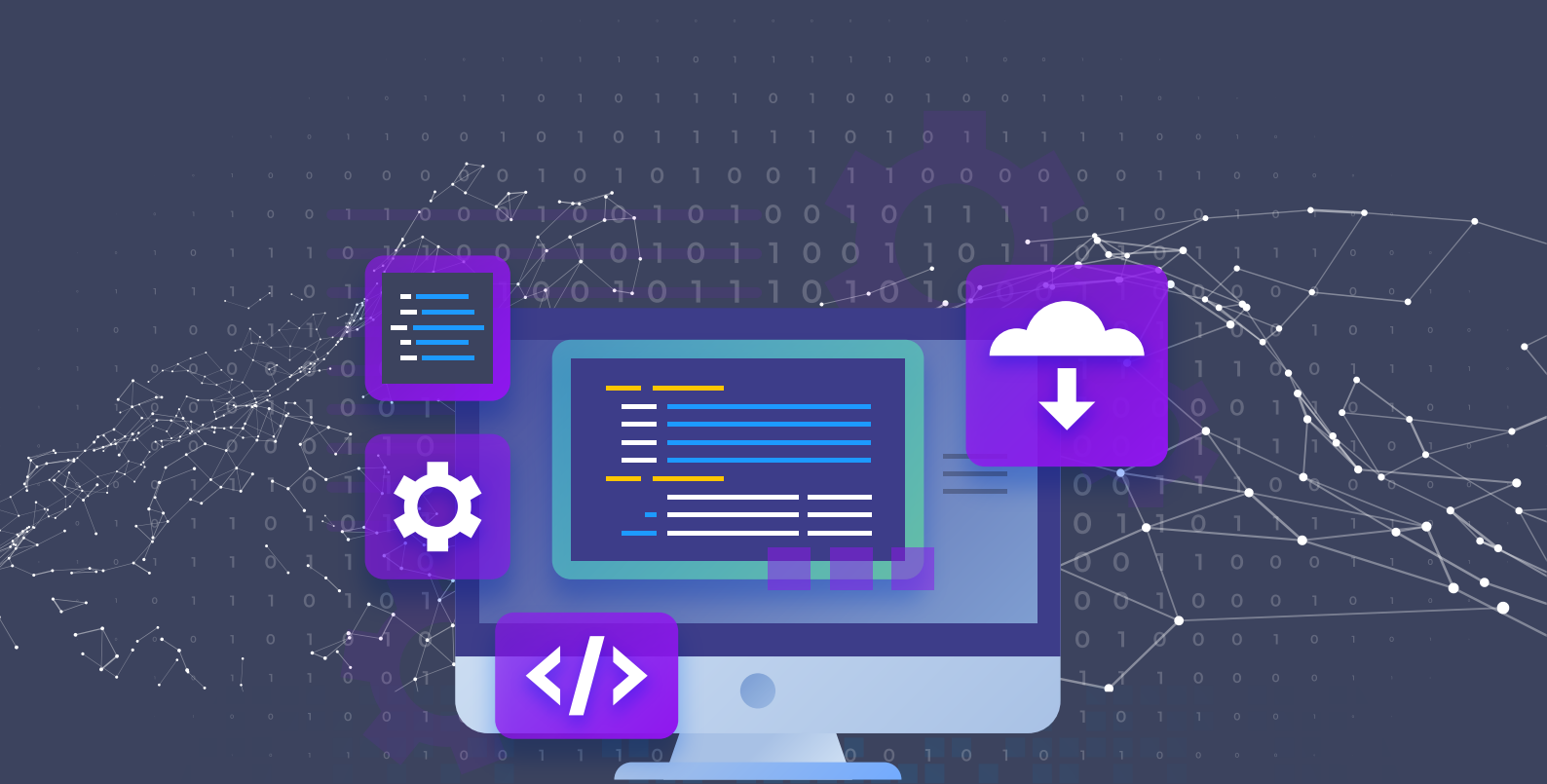


# An Award Winning IoT Security Platform

With features that will win your heart <3



# Table of Content

<b>A.</b>		
Overview.....		<a href="#">03</a>
<b>B.</b>		
Highlights.....		<a href="#">04</a>
<b>C.</b>		
Assessment Enabling Hardwares.....		<a href="#">06</a>
EXPLIoT-Box Integration Dashboard		
<b>D.</b>		
SaaS Platform.....		<a href="#">07</a>
▪ Project Dashboard.....		<a href="#">07</a>
▪ IoT Security Assessment Dashboard.....		<a href="#">08</a>
▪ Cloud Assessment Dashboard.....		<a href="#">09</a>
▪ Network Assessment Dashboard.....		<a href="#">10</a>
▪ Radio Assessment Dashboard.....		<a href="#">11</a>
▪ BLE Assessment Dashboard.....		<a href="#">12</a>
▪ Zigbee Assessment Dashboard.....		<a href="#">13</a>
▪ Firmware Assessment Dashboard.....		<a href="#">14</a>
▪ Hardware Assessment Dashboard.....		<a href="#">16</a>
▪ Compliance Dashboard.....		<a href="#">19</a>
▪ Reports.....		<a href="#">20</a>
▪ Issue Tracking.....		<a href="#">21</a>

# 1.

# Overview

## IoT Auditor Platform Comprises Two Components

- 1 Assessment Enabling Hardwares  
(EXPLIoT-Box, Zigbee Auditor, Bus Auditor)
- 2 An IoT Auditor SaaS Platform

# 2. Highlights

## Assessment Enabling Hardware



EXPLIoT Box



Zigbee Auditor

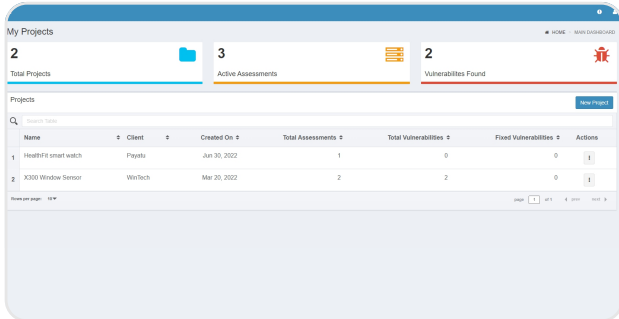


Bus Auditor

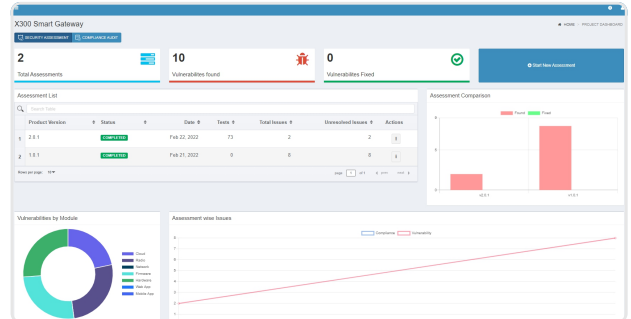


Learning Kit

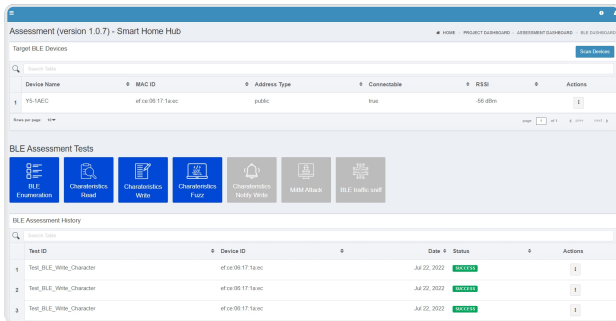
# An IoT Auditor SaaS Platform



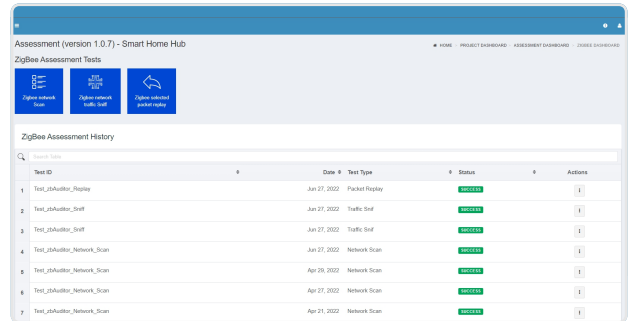
Project Dashboard



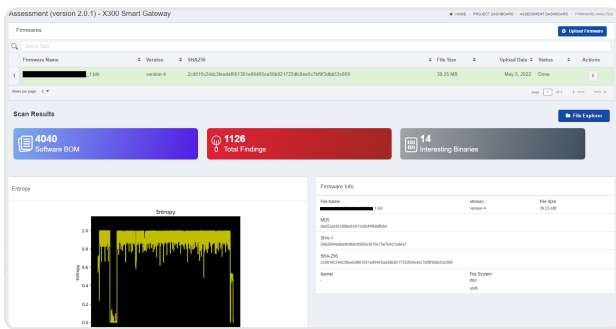
IoT Security Assessment Dashboard



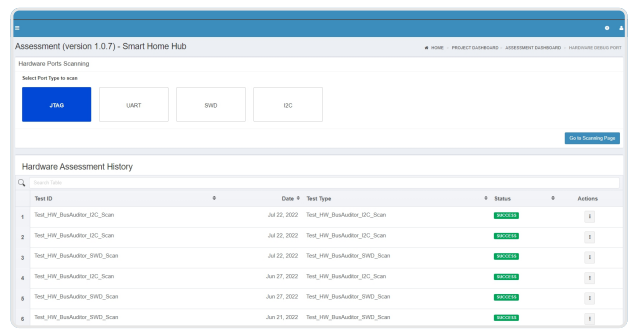
BLE Assessment Dashboard



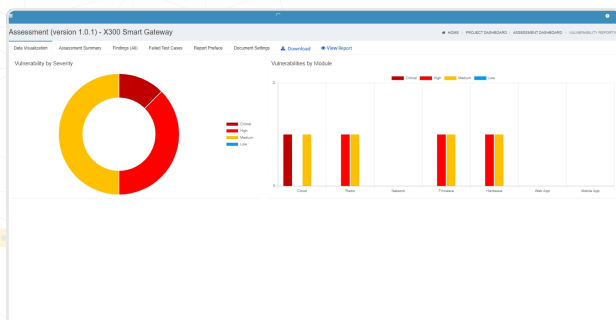
Zigbee Assessment Dashboard



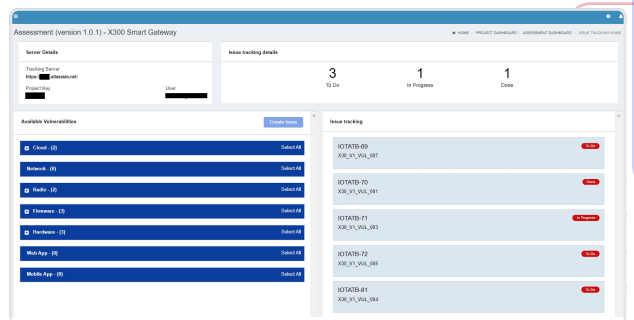
Firmware Assessment Dashboard



Hardware Assessment Dashboard



Reports



Issue Tracking

# Assessment Enabling Hardware

## EXPLIoT-Box Integration Dashboard

This hi-tech device gives engineers the unique ability to perform the product's safety checks on-site! You can now test Radio and Hardware for your target device locally with the EXPLIoT-Box.

**EXPLIoT Box**

[Redacted Key] Copy Generate Key Delete Key

**My Boxes**

+ Add New EXPLIoT Box

10000000 [Redacted]	
Serial No 1000000 [Redacted]	Assigned to [Redacted] e
Device Status <b>Active</b>	Connection Status <b>Connected</b>

# 3.

# SaaS Platform

## Project Dashboard

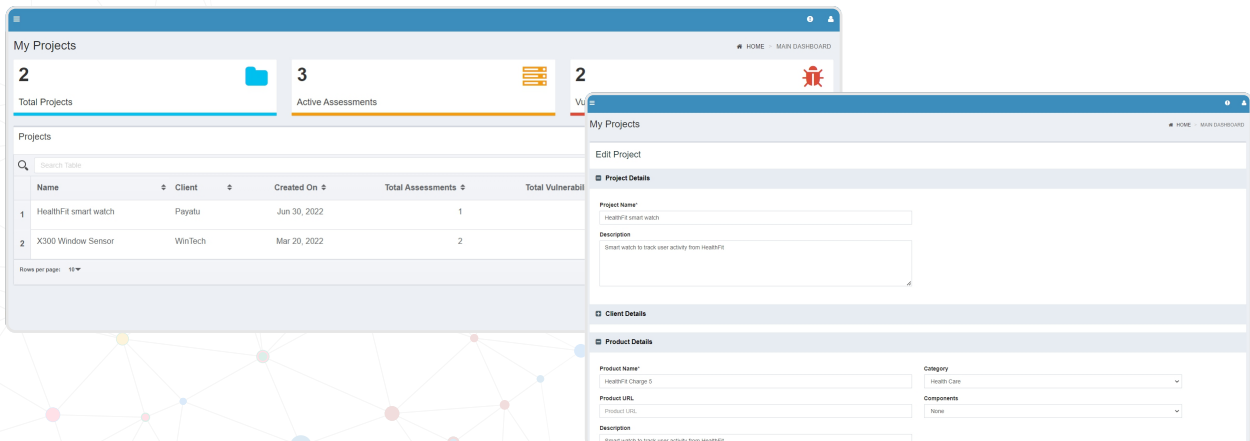
The Project Dashboard keeps you updated by displaying what needs to be done right now and the level of risk involved so you can make the right decisions.

You can efficiently attend to all your product security & compliance-related assessments under a single project. Having this information all in one place, you can easily get a high-level overview of the product's security posture and understand exactly the areas of improvements while completing the audit.

### Example: Active Projects, Assessments and Vulnerabilities

- 1 Manage all your products individually
- 2 Create/manage all projects related to a product under same dashboard
- 3 Get assessment status of all your products in one go
- 4 Select compliance standards for products\*

**Note:** Features marked with asterisk (\*) are under development



# IoT Security Assessment Dashboard

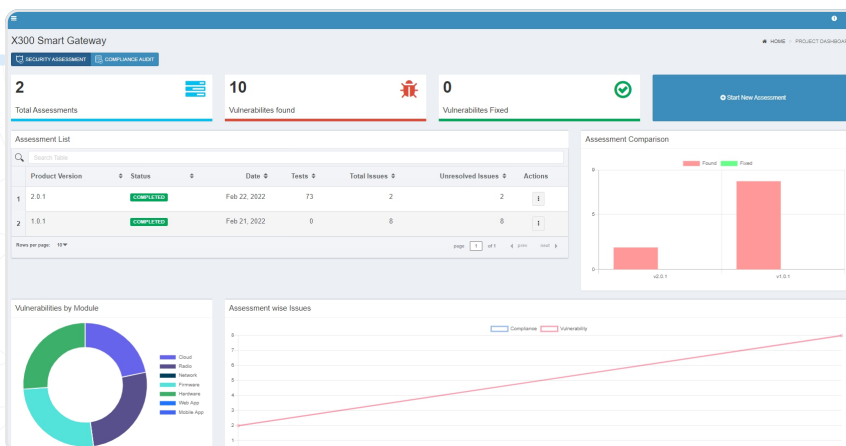
**An innovative feature designed to manage the security of your smart products, smartly!**

It helps you test and audit your products' security and summarizes the security posture with graphs that are easy to grasp.

With the help of this feature, you can now automate security assessment of new and old versions, scan vulnerabilities & measure the quality of the product security over time.

On top of that, you can compare results with previous assessments to check for progress and regression. By doing this, you can ensure that your product remains as secure as possible while keeping track of any potential regressions so you can quickly fix them before they have a chance to affect your product adversely.

- 1 Create/edit/delete product assessments
- 2 Add modules (Cloud, Network, Radio, Firmware, Hardware)
- 3 Select compliance standards for the assessment (IoXt security pledge, IoTSE compliance framework release 2, ISA 62443)
- 4 Compare & analyze security assessment's quality & progress





# Cloud Assessment Dashboard

## Infrastructure as a Code

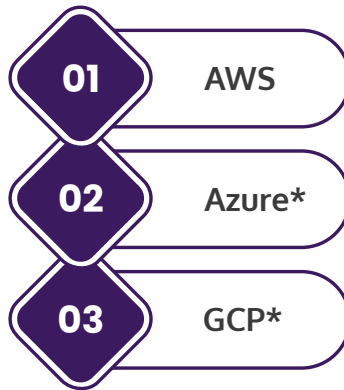
### Is your cloud configured correctly?

Are you using Azure or AWS cloud? Are you following cloud best practices?

Are you confident that your cloud IaaS has been configured correctly?

Make sure you are doing it right! Get your Terraform & Cloud Formation files automatically scanned for potential vulnerabilities. Identify where best practices may be lacking and what scenarios you must avoid when creating infrastructure as code - the fastest, most efficient way to audit your IaaS.

### Supported Cloud Provider



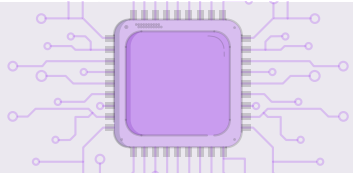
**Note:** Features marked with asterisk (\*) are under development

The screenshot displays the 'Assessment (version 2.0.1) - X300 Smart Gateway' dashboard. The left sidebar shows 'Infrastructure as code' with 'IaaS Provider' set to 'Terraform'. Below it, 'Cloud Service' is set to 'Amazon Web Services', and 'Steps to generate input file' is 'Input File (post)'. A 'Drag and drop file here' area is visible. The 'Tests' section shows a table with two entries:

Test ID	IaaS Type	File Name
1	IAC_Terraform_Audit	aws_s3_e_plan_out_1.json
2	IAC_Terraform_Audit	aws_terraform_ec2_s3_planout.json

The main content area shows 'Scan Results' for 'IAC\_Terraform\_Audit'. It contains a table with columns: Resource Identifier, Resource Name, Vulnerability, Severity, and Action.

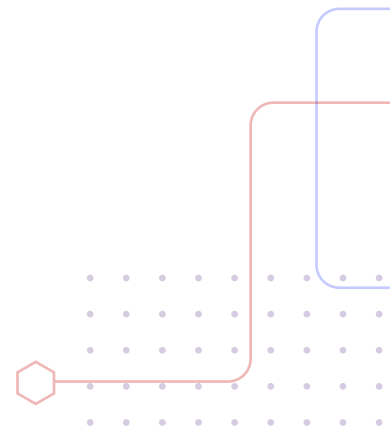
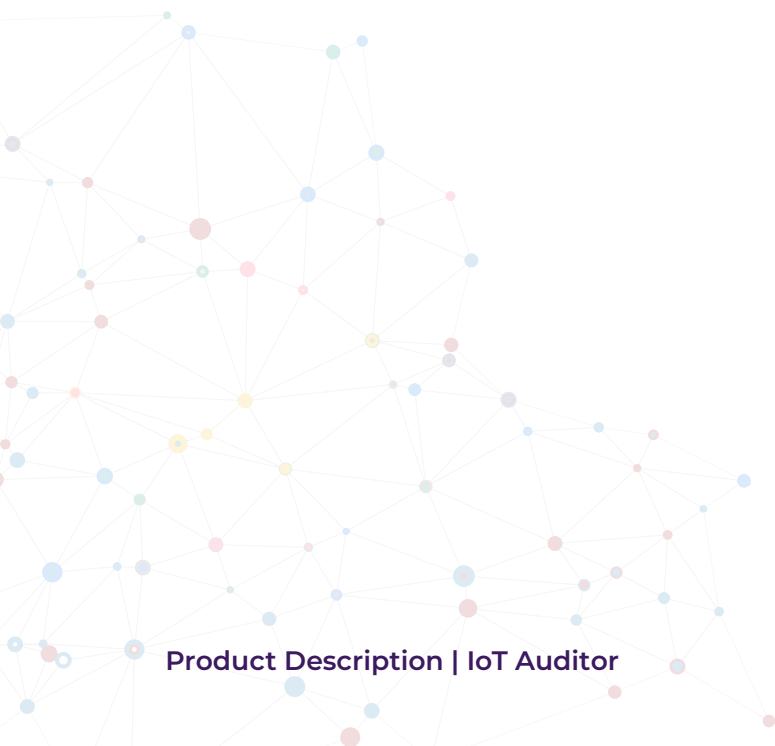
Resource Identifier	Resource Name	Vulnerability	Severity	Action
iam				
aws_iam_role_policy	test_policy	Wildcard used while defining Action ["*"] in test_policy	Medium	▲
aws_iam_role_policy	test_policy	Wildcard used while defining Resource "*" in test_policy	Medium	▲
ec2				
aws_instance	role-test	All volumes for instance role-test are not encrypted	Medium	▲
s3				
aws_s3_bucket_policy	s3test	Bucket aws:arn:aws:s3:::terraform-getting-started-bucket: open to world. Danger	High	▲
aws_s3_bucket_policy	s3test	Bucket aws:arn:aws:s3:::terraform-getting-started-bucket: Wildcard "*" access	Medium	▲
aws_s3_bucket_policy	s3test	Bucket aws:arn:aws:s3:::terraform-getting-started-bucket: open to world. Danger	High	▲
aws_s3_bucket_policy	s3test	Bucket aws:arn:aws:s3:::terraform-getting-started-bucket: has delete access	Medium	▲
s3				
aws_s3_bucket_policy	s3test	Bucket aws:arn:aws:s3:::terraform-getting-started-bucket: open to world. Danger	High	▲
aws_s3_bucket_policy	s3test	Bucket aws:arn:aws:s3:::terraform-getting-started-bucket: Wildcard "*" access	Medium	▲
aws_s3_bucket_policy	s3test	Bucket aws:arn:aws:s3:::terraform-getting-started-bucket: open to world. Danger	High	▲
aws_s3_bucket_policy	s3test	Bucket aws:arn:aws:s3:::terraform-getting-started-bucket: has delete access	Medium	▲



# Cloud Security\*

**Note:** Features marked with asterisk (\*) are under development

Take the stress out of auditing your cloud infrastructure with an advanced Cloud Security Audit Feature. The Cloud Security Audit feature scans your cloud infrastructure assets and maps them against the industry's best practices.





# Radio Assessment Dashboard

What makes your IoT smart? The radio protocols like BLE, Zigbee & Wi-Fi Technologies! But with this great connectivity comes a greater chance of vulnerabilities and security risks.

## Radio Assessment Dashboard comes to the rescue!

It helps you scan and identify the potential security gaps in your radio protocols with graphs and charts- so you can quickly understand, analyse and patch them, keeping your IoT product secure.

### Supported Radio Protocols

- 01 Bluetooth low energy
- 02 Zigbee
- 03 Wi-Fi\*

**Note:** Features marked with asterisk (\*) are under development

# BLE Assessment Dashboard

## Supported BLE Test

- 1 BLE device scan
- 2 BLE service and characteristics enumeration
- 3 BLE characteristics: read, write & fuzz

Assessment (version 1.0.7) - Smart Home Hub

Target BLE Devices

Device Name	MAC ID	Address Type	Connectable	RSSI	Actions
Y5-1AEC	ef:ce:06:17:1a:ec	public	true	-56 dBm	[Info]

BLE Assessment Tests

- BLE Enumeration
- Characteristics Read
- Characteristics Write
- Characteristics Fuzz
- Characteristics Notify Write
- MIM Attack
- BLE traffic sniff

BLE Assessment History

Test ID	Device ID	Date	Status	Actions
1 Test_BLE_Write_Character	ef:ce:06:17:1a:ec	Jul 22, 2022	SUCCESS	[Info]
2 Test_BLE_Write_Character	ef:ce:06:17:1a:ec	Jul 22, 2022	SUCCESS	[Info]
3 Test_BLE_Write_Character	ef:ce:06:17:1a:ec	Jul 22, 2022	SUCCESS	[Info]
4 Test_BLE_Enumeration	ef:ce:06:17:1a:ec	Jul 22, 2022	SUCCESS	[Info]

# Zigbee Assessment Dashboard

## Supported Zigbee Test

- 1 Zigbee network scan
- 2 Zigbee traffic sniffing
- 3 Zigbee traffic replay

Assessment (version 1.0.7) - Smart Home Hub

ZigBee Assessment Tests

- Zigbee network Scan
- Zigbee network traffic Sniff
- Zigbee selected packet replay

ZigBee Assessment History

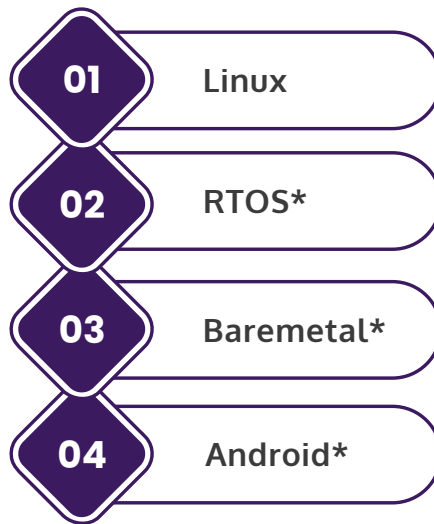
Test ID	Date	Test Type	Status	Actions
1 Test_zbAuditor_Replay	Jun 27, 2022	Packet Replay	SUCCESS	[i]
2 Test_zbAuditor_Sniff	Jun 27, 2022	Traffic Snif	SUCCESS	[i]
3 Test_zbAuditor_Sniff	Jun 27, 2022	Traffic Snif	SUCCESS	[i]
Test_zbAuditor_Network_Scan	Jun 27, 2022	Network Scan	SUCCESS	[i]
Test_zbAuditor_Network_Scan	Apr 29, 2022	Network Scan	SUCCESS	[i]
Test_zbAuditor_Network_Scan	Apr 27, 2022	Network Scan	SUCCESS	[i]
Test_zbAuditor_Network_Scan	Apr 21, 2022	Network Scan	SUCCESS	[i]

# Firmware Assessment Dashboard

The firmware assessment dashboard quickly scans & reverse engineers the Linux Firmware for known and potential vulnerabilities of installed packages, application binaries and other files.

This feature will help you reduce the overhead by analyzing the security posture of the firmware.

## Types of Firmware Supported

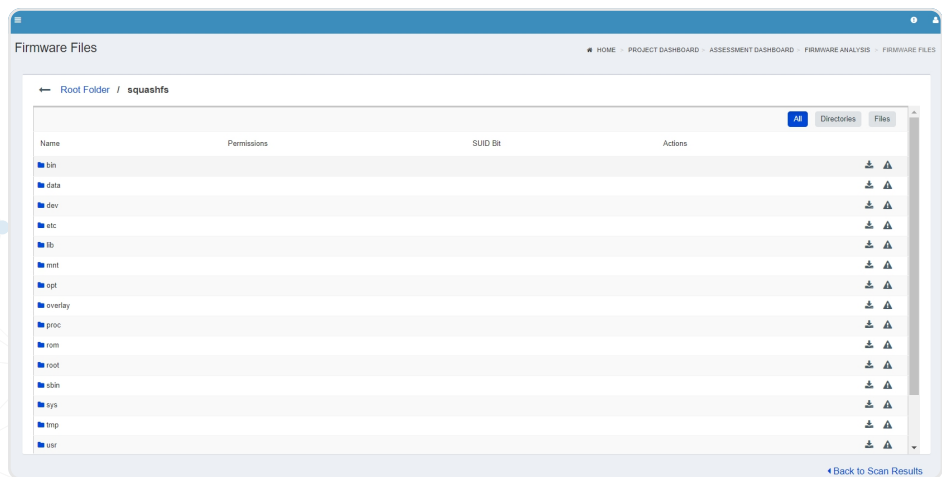
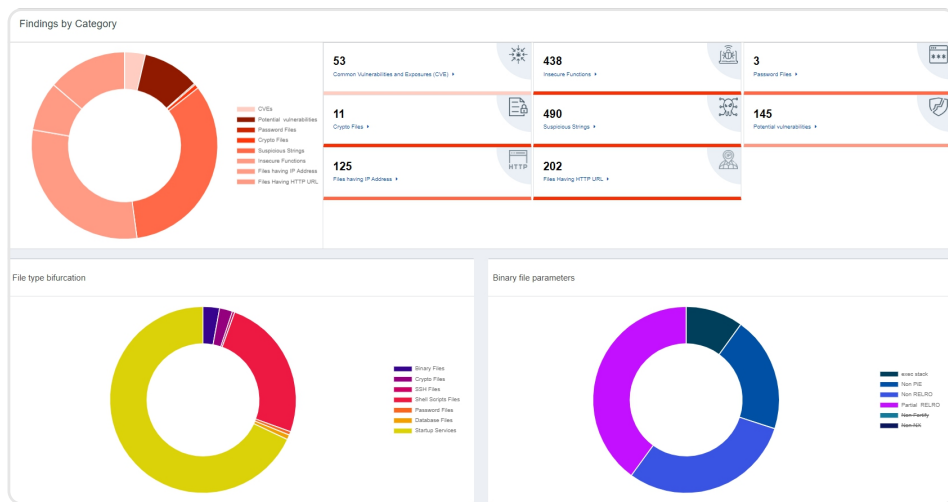


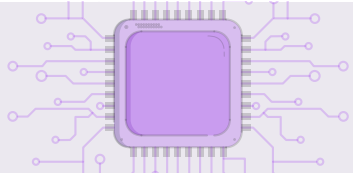
**Note:** Features marked with asterisk (\*) are under development

The screenshot displays the 'Assessment (version 2.0.1) - X300 Smart Gateway' interface. At the top, there's a 'Firmwares' section with a search bar and an 'Upload Firmware' button. Below is a table with columns for Firmware Name, Version, SHA256, File Size, Upload Date, Status, and Actions. One entry is visible: a file named '...\_1.bin' with version 'version-4', a long SHA256 hash, a size of 39.25 MB, and an upload date of May 5, 2022. The 'Scan Results' section features three summary cards: '4040 Software BOM', '1126 Total Findings', and '14 Interesting Binaries'. Below this is an 'Entropy' graph showing a fluctuating yellow line on a black background. To the right, the 'Firmware Info' section provides details for the selected file, including MD5, SHA-1, SHA-256, Kernel, and File System (JFS2, ubifs).

# Supported Test Cases

- 1 Firmware architecture information
- 2 Entropy graph
- 3 File system enumeration
- 4 Binary file analysis
- 5 File system analysis



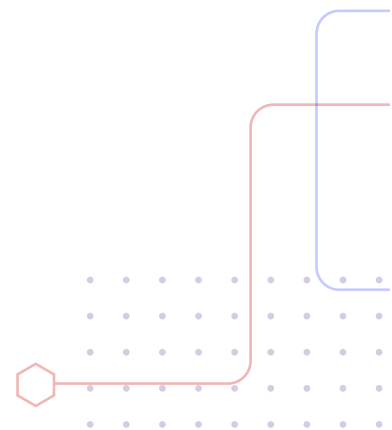
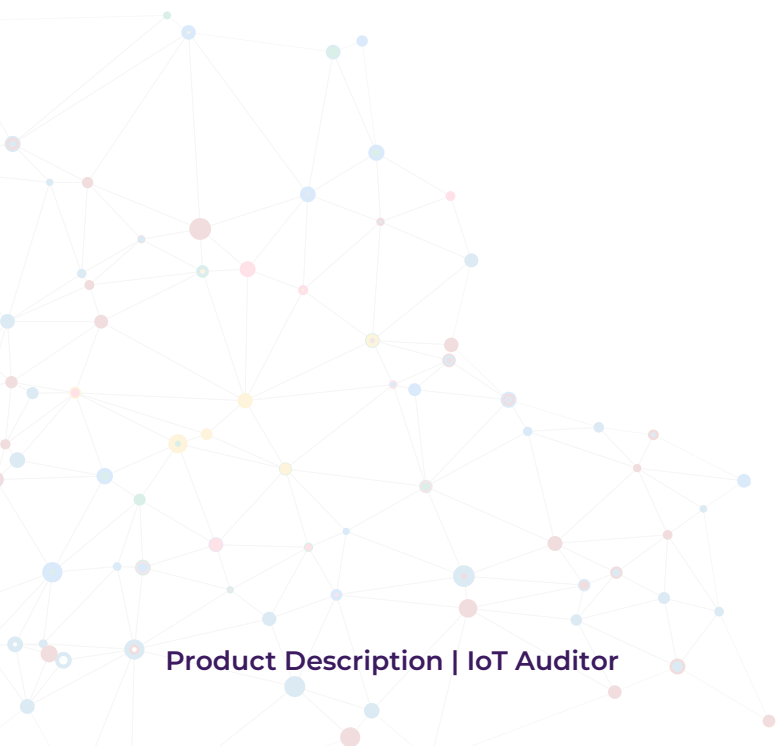


# Hardware Assessment Dashboard

Inspecting target hardware for open debug ports has never been easier.

## Supported Hardware Protocols

- 1 JTAG
- 2 SWD
- 3 UART
- 4 I2C

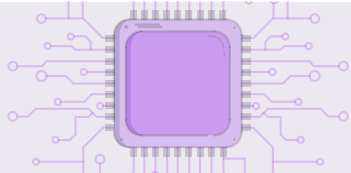




# Hardware Debug Port Dashboard

The dashboard is divided into two main sections. The top section, titled 'Assessment (version 1.0.7) - Smart Home Hub', features a 'Hardware Ports Scanning' area with a 'Select Port Type to scan' section. It contains four buttons: 'JTAG' (highlighted in blue), 'UART', 'SWD', and 'I2C'. Below this is a 'Hardware Assessment History' sidebar with a search bar and a list of six test entries, each with a 'Test ID' and a description like 'Test\_HW\_BusAuditor\_I2C\_Scan'. The bottom section, titled 'Assessment (version 2.0.1) - X300 Smart Gateway', displays 'Hardware Test Scan Results' in a table format. The table has columns for 'JTAG ID', 'TCK pin', 'TMS pin', 'TDO pin', 'TDI pin', and 'TRST pin'. It shows two rows of data. Below the table is a 'Rows per page' dropdown set to '10', a pagination control showing 'page 1 of 1', and a 'Back to Dashboard' link.

JTAG ID	TCK pin	TMS pin	TDO pin	TDI pin	TRST pin
1 0x4ba00477	4	3	1	2	
2 0x06431041	4	3	1	2	



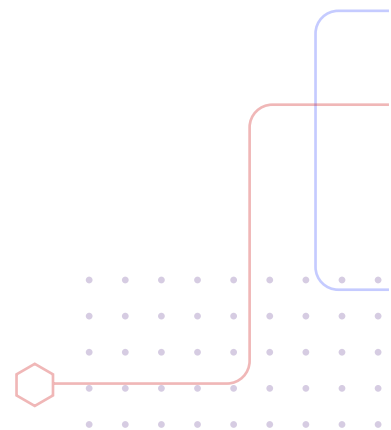
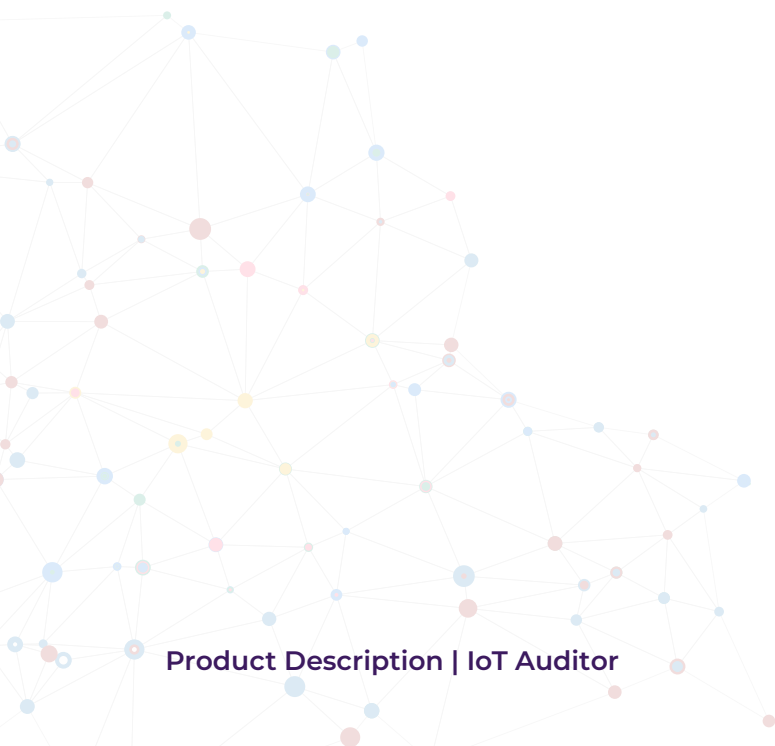
## Memory Extraction\*

**Soon you can** extract memory contents from your hardware much faster in a unified dashboard.

### Supported Protocols

- 1 SPI memory read/write
- 2 I2C memory read/write

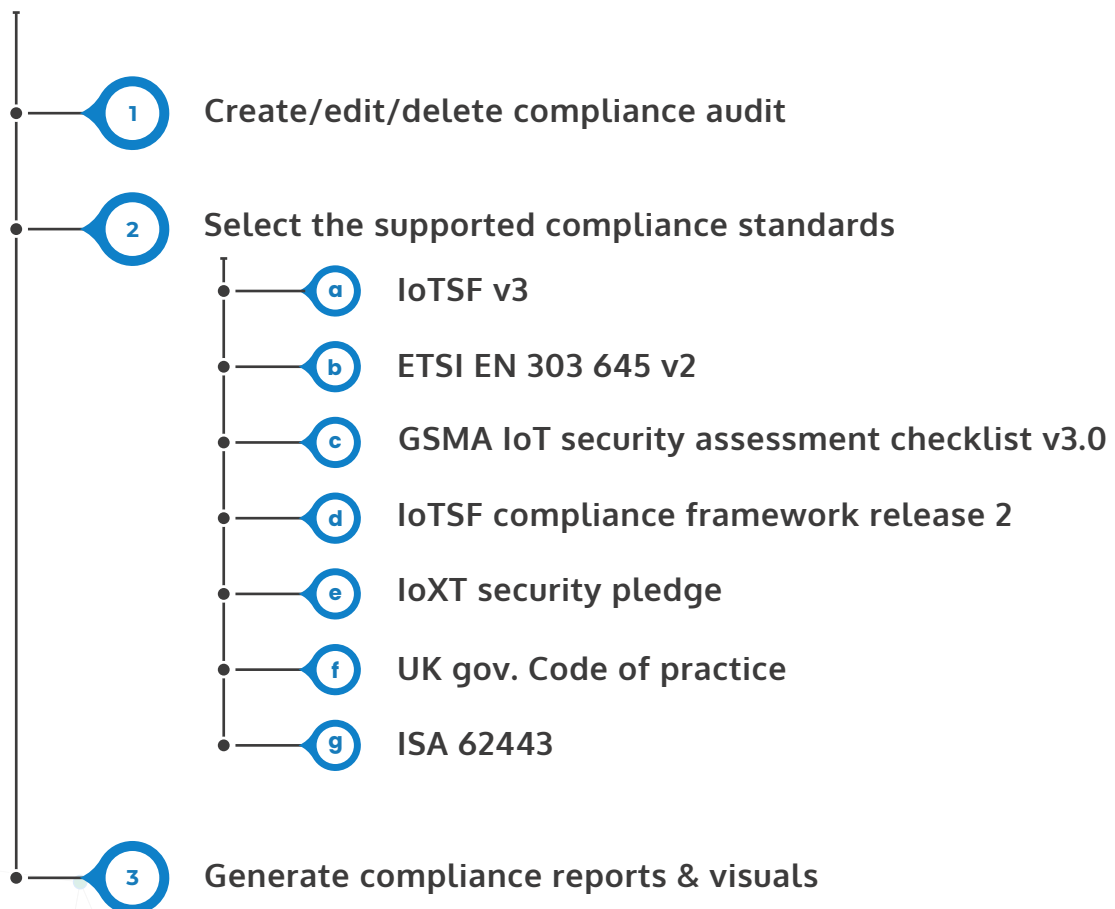
**Note:** Features marked with asterisk (\*) are under development



# Compliance Dashboard\*

Enforcing regulatory compliance guidelines is vital to the sustained growth of your business. With the Compliance Audit feature, you can create a compliance audit and easily generate reports after the audit is complete.

This feature makes it easy to take care of compliance audits because it nestles the audit processes into your workflow to streamline the compliance process for everyone involved!



**Note:** Features marked with asterisk (\*) are under development

# Reports

1

## Automated Reporting

Easy, automated & integrated reporting

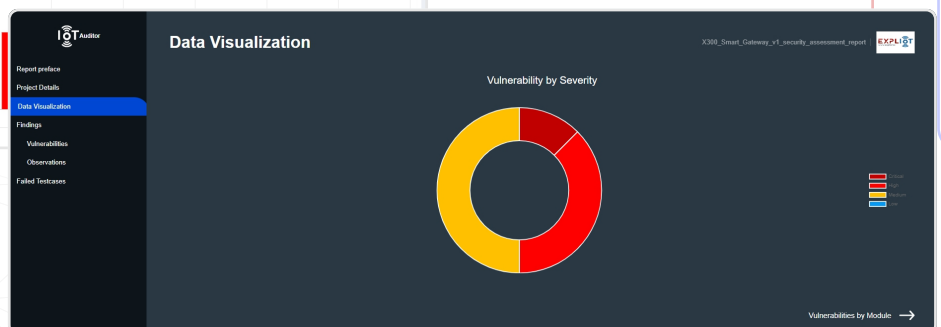
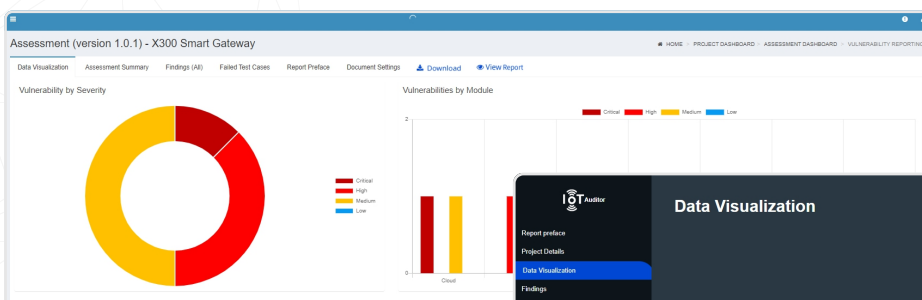
- a Automatically & easily generate reports with one click
- b Go to the report dashboard after the assessment
- c Click on create a report and download your report in just one click

2

## Manual Reporting

Record and organize vulnerabilities in report format

- a Manually add/edit/delete vulnerabilities, observations and other findings from executed tests
- b Add/edit/delete findings logged by test suite
- c Give CVSS score for vulnerabilities
- d Add reproduction steps
- e Add CWE for the discovered vulnerabilities
- f Generate HTML view of report
- g Download report in PDF format



# Issue Tracking

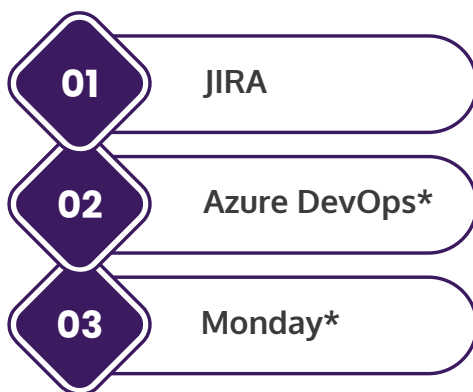
## Inbuilt Issue Tracking Feature

IoT Auditor also provides high-tech, in-built issue tracking capabilities to help you perform **vulnerability management** of the identified issues. With the help of this feature, you will be able to visualize vulnerabilities by severity and seamlessly take an informed decision to prioritize and fix them!

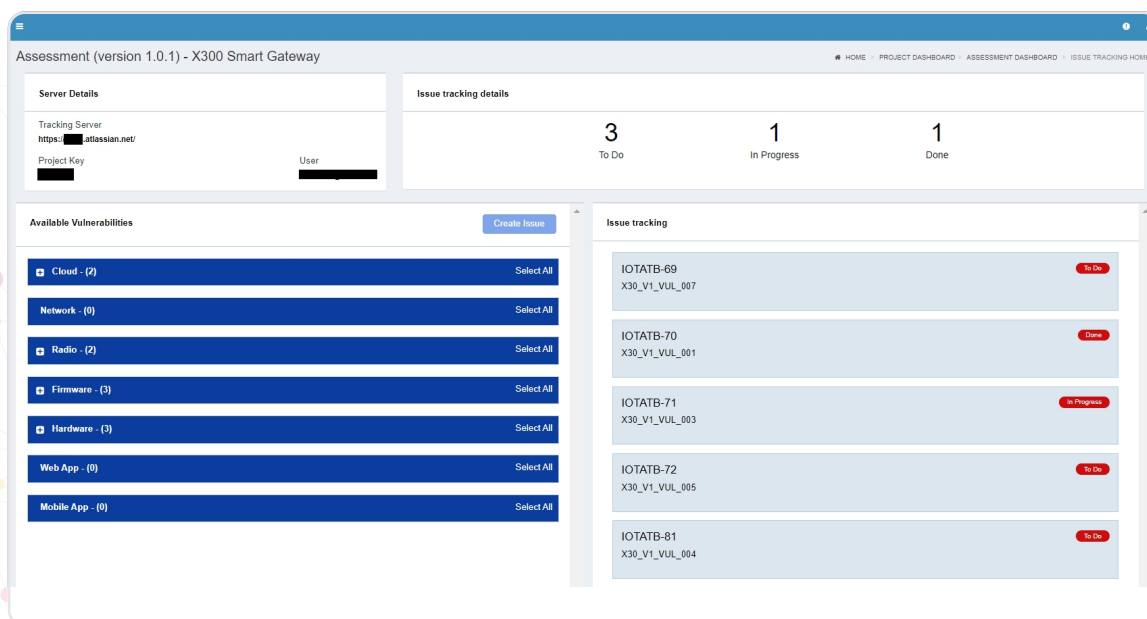
## Integrated Enterprise Issue Tracking Solution

Are you currently using enterprise issue tracking in your organization? IoT Auditor can sync with it! The new IoT Auditor can log and update the identified vulnerabilities into your existing enterprise issue tracking solution via API integration.

### Supported Tools



**Note:** Features marked with asterisk (\*) are under development



# About Us

40 Billion+ connected devices projected in 2025 could be in danger if not properly and comprehensively security-tested. We are on a mission to help solve this problem by innovating new ways to safeguard IoT Products and Things.

# The Team

Some call us hackers, and others, geeks. But when it comes to solving security problems, our thrill, passion, and determination are directly proportional to the complexity of the problem. As a team of hackers working with connected devices, we understand the importance of hacking securely and discovering the juncture of safety and security between humans and the new technology.

# The Leadership Team



**Aseem Jakhar**

Co-Founder



**Murtuja Bharmal**

Co-Founder



**Antriksh Shah**

Co-Founder

