REDINENT IoT THREAT SCANNER

Redinent IoT Threat Scanner ™ automatically discovers IoT and embedded devices, finds vulnerabilities and common weaknesses at scale. After the assessment, Redinent users receives a detailed report of the findings that includes an overview of the IoT devices, vulnerabilities, weaknesses, risks and threats the platform found while running in the user's environment.

IoT ASSET INVENTORY AND CLASSIFICATION

The Redinent platform discovers and classifies every IoT and Unmanaged device in user's environment that includes but not limited to Smart IP Cameras, Smart Solar Panels, Smart HVAC Systems, Wifi Routers, Smart Motion
Sensors, Smart Water Meters, Smart TV, Smart Speakers,
Wifi Printers, Smart Smoke Detectors/Smart Fire Alarms,
Smart Conferencing, Smart EV Charging Stations,, Smart
Lights, Smart Access Card/Control, Smart Gas/Utility
Sensors, Smart Elevator Control, Smart Thermostat, Smart Meter, Smart Switch, Smart Home and many more.
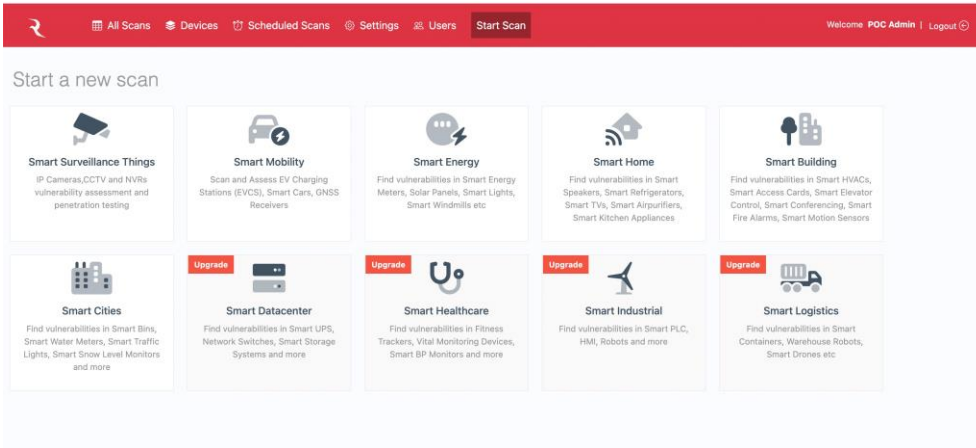
RISK AND THREAT ASSESSMENT

After identifying a device, the Redinent platform calculates the asset's risk score based on factors, including: **::** Risks originating from unpatched firmware versions or known hardware exploits.
:: Risks originating from human error and configurational weaknesses.
:: Risks originating from OEM themselves including obscure white-labelling and underlying firmware detections.

DEEP & EXHAUSTIVE

:: Scan IoT Devices to provide security teams with visibility into vulnerabilities

:: Monitor trends across various scans through customisable dashboards

:: Minimise network impact, optimise security and compliance assessments, and unify reporting through a single assessment for vulnerabilities, configurations, controls, and policy checks.

:: Receive in-house step-by step instructions from Redinent experts to remediate risks.

:: Eliminate a traditional blind spot for security teams and stay compliant with privacy regulations.

Redinent - IoT Threat Assessment Modules

Redinent - Exploit Driven Testing with Evidence

Redinent benefits compared to modern IoT security platforms

	Modern IoT Security Platforms	Redinent
SCAN TYPE	Tests are run on network traffic generated from the IoT device	Tests are **run directly** on IoT Device
COVERAGE	Tests are run only for the white labeled company	Tests are run for the **original OEM detected** by Redinent
ACCURACY	Prone to false positives	**Zero False Positives** , Exploit and Intrusion based
ANALYSIS	Traditional Analysis	**Innovative IoT Vulnerability**
RESEARCH	Zero Days not a priority	**Highest Number of Zero Days** for IP Cameras

Zero Days are integral part of Redinent

Proven in various infrastructures Redinent® delivers the following core capabilities

:: Fast unified secure compliance

Minimise network impact, optimise security and compliance assessments, and unify reporting through a single assessment for vulnerabilities, configurations, controls, and policy checks.

:: Discover vulnerabilities like an attacker

Redinent® expert scanning system emulates techniques used by human hackers to build upon knowledge from prior exploits and identify additional vulnerabilities, resulting in a more complete risk assessment.

:: Vulnerability Validation with Evidence

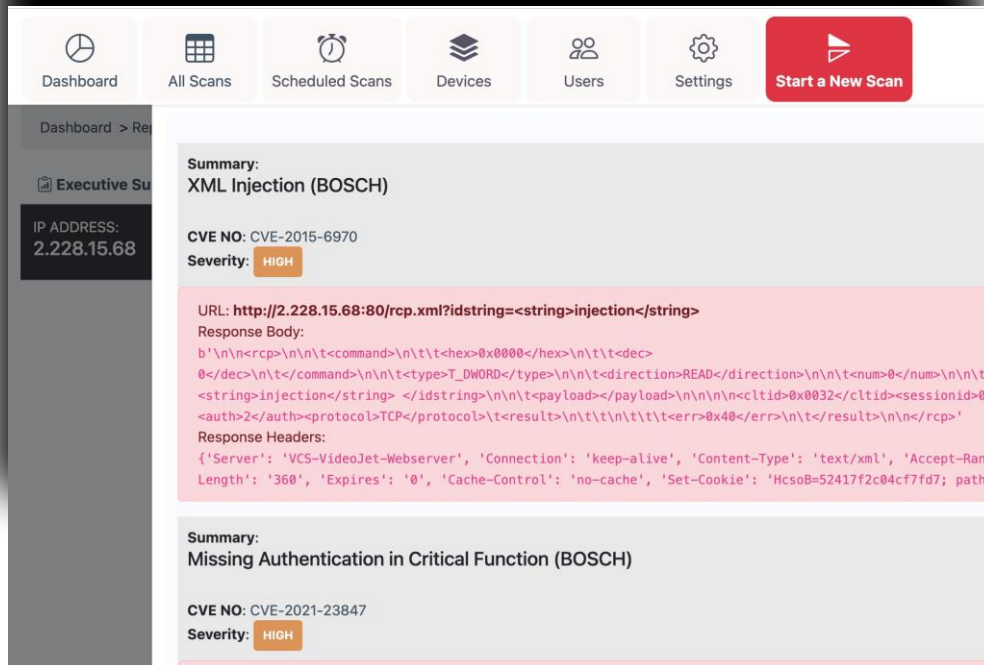Redinent® not only finds vulnerabilities but captures and records evidence to validate risk

:: Powerful Risk and Data Analytics

Redinent® provides built-in and fully customisable report templates to create reports for everyone.

:: Compliance

Redinent enables organisations to stay compliant with ISO 27001 and COBIT standards for risk, vulnerability, and configuration management requirements.
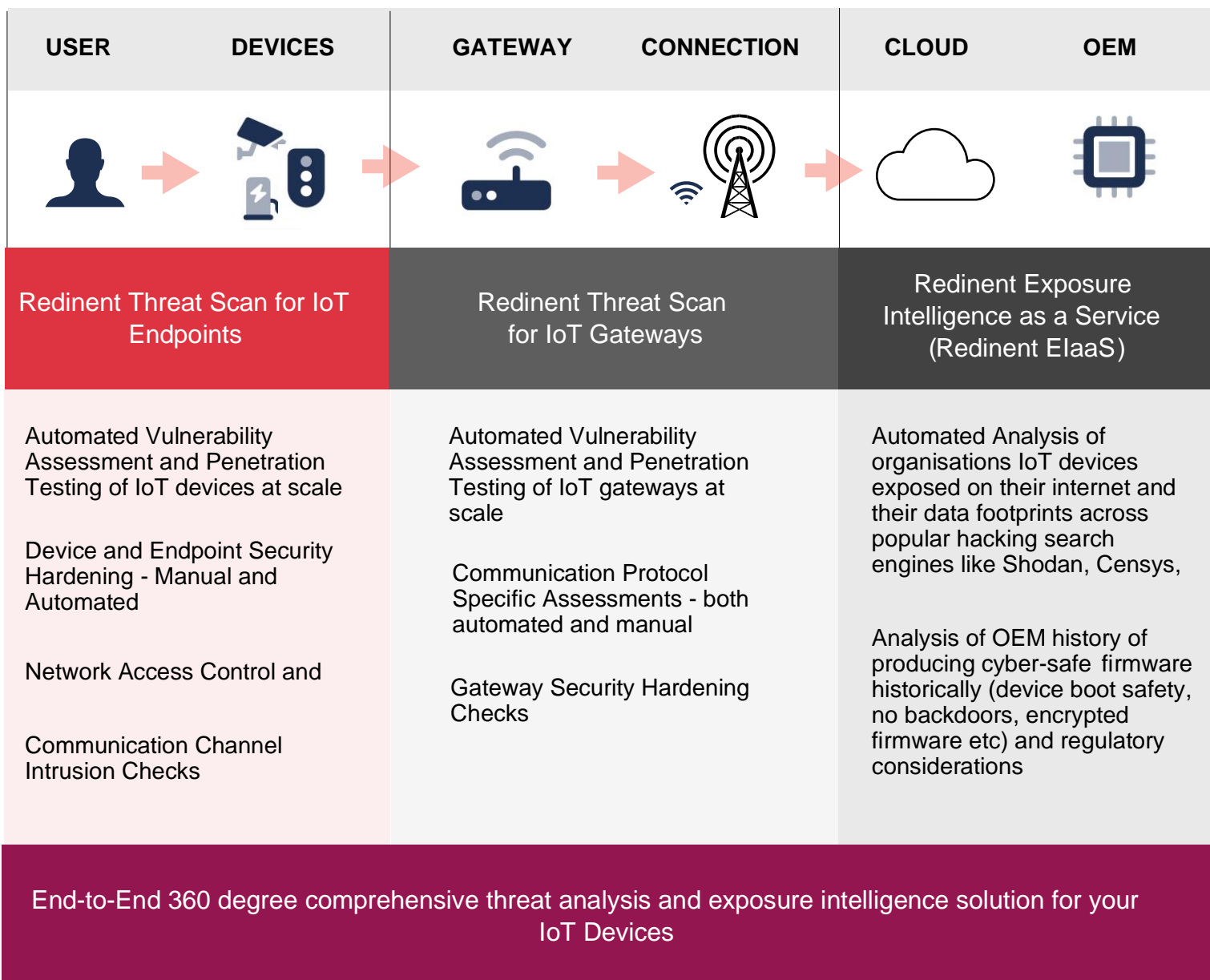
IoT Threat Mitigation Solution across the entire stack

USER DEVICES	GATEWAY CONNECTION	CLOUD OEM

Redinent Threat Scan for IoT Endpoints	Redinent Threat Scan for IoT Gateways	Redinent Exposure Intelligence as a Service (Redinent EIaaS)
Automated Vulnerability Assessment and Penetration Testing of IoT devices at scale Device and Endpoint Security Hardening - Manual and Automated Network Access Control and Communication Channel Intrusion Checks	Automated Vulnerability Assessment and Penetration Testing of IoT gateways at scale Communication Protocol Specific Assessments - both automated and manual Gateway Security Hardening Checks	Automated Analysis of organisations IoT devices exposed on their internet and their data footprints across popular hacking search engines like Shodan, Censys, Analysis of OEM history of producing cyber-safe firmware historically (device boot safety, no backdoors, encrypted firmware etc) and regulatory considerations

End-to-End 360 degree comprehensive threat analysis and exposure intelligence solution for your IoT Devices

About Redinent

Redinent Innovations, based out of Bangalore, India is an IoT cybersecurity player, has redefined modern IoT Security with world's most advanced enterprise grade IoT threat scanner for protecting IoT assets and data. Redinent provides hyper-accurate vulnerability reports backed with penetration evidence with periodic protection from threats and immediate time-to-value to businesses.

Learn More
www.redinent.com

Follow Us:
Twitter | Linkedin