APPLIED SECURITY INTELLIGENCE

Continuous cyber-risk visibility with StarSentry

Hardware-based Deployment or Subscription Managed Service for Organisations of All Sizes

StarSentry is a cyber-risk visibility and vulnerability management solution designed for organisations of all sizes. Available as a hardware-based solution or subscription managed service, it helps organisations discover assets, identify vulnerabilities, monitor exposures and strengthen their cyber security posture **through actionable insights and ongoing oversight.**

Move Beyond Point-in-Time Assessments

As digital environments become increasingly complex, organisations may struggle to maintain continuous visibility over their assets, vulnerabilities and changing risk exposure. Periodic assessments alone can leave gaps between review cycles.

StarSentry provides ongoing visibility through automated vulnerability assessments, centralised reporting, alerts and remediation guidance—helping security and IT teams identify and address risks more effectively.

Our expert team is dedicated to guiding you through **StarSentry's** robust capabilities. Reach out to know more or schedule a demo to see how **StarSentry** can enhance your cybersecurity posture.

Key Advantages

Automated Vulnerability Assessment (VA) Scan: Seamlessly integrates into your network to automatically scan all connected devices for vulnerabilities.

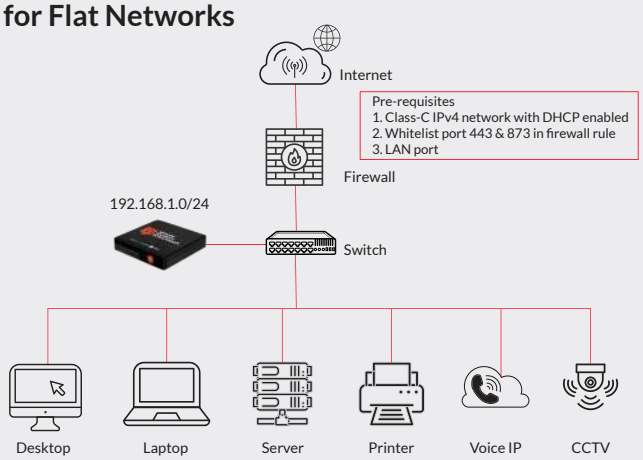
Optimize Security: Efficiently schedule and manage scans, access and download reports for review, and address vulnerabilities with StarSentry recommended solutions.

User-Friendly Interface: Provides an intuitive web portal for accessing reports, monitoring scan statuses, receiving alerts and managing the device.

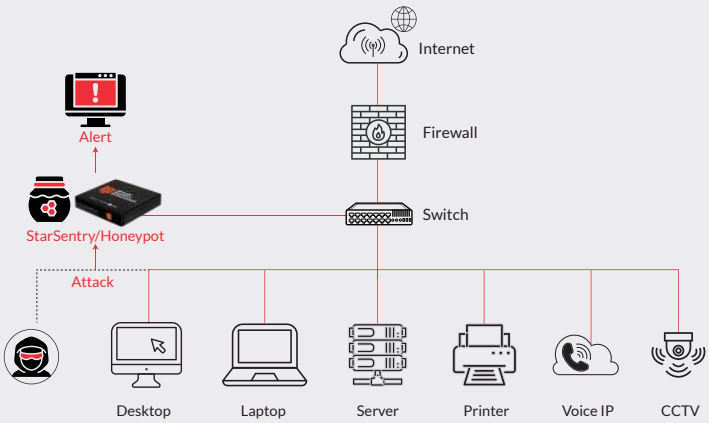
Built-in Honeypot: Acts as a decoy to attract and alert security teams to malicious activity, providing an additional layer of defence for self protection.

Network Diagram

StarSentry Hardware-Based Deployment for Flat Networks



StarSentry Built-in Honeypot



StarSentry Target Areas

Network Vulnerabilities:

- **Open Ports:** Secures open ports.
- **Weak Services:** Detects vulnerabilities in FTP, SSH, HTTP.
- **Network Protocols:** Analyzes TCP/IP, UDP, ICMP.

Host-Based Vulnerabilities:

- **Operating Systems:** Scans Windows, macOS, Linux.
- **Software:** Assesses applications, databases, custom software.
- **Misconfigurations:** Identifies risky settings.

IoT Vulnerabilities:

- **Passwords:** Detects weak passwords.
- **Protocols:** Mitigates insecure protocols.
- **Firmware:** Addresses firmware vulnerabilities.

StarSentry Minimum System Requirements

- Network: 100 Mbps or higher
- Web Browser: Compatible with Google Chrome, Microsoft Edge, Firefox, and other modern browsers.

These requirements ensure optimal performance for vulnerability scanning when using **StarSentry**.

StarSentry Awards

MALAYSIA CYBER SECURITY AWARDS

2024 - Cyber Security Innovation (Product) of the year

2023 - Cyber Security Innovation (Product) of the year

Contact us for more information about **StarSentry**:

Tel: +(60)3 - 6416 7234

Customer Care: +(60)19 - 7677 234 *(9.00am to 6.00pm (Daily)*

Enquiry: sales@appsecintel.com

APPLIED SECURITY INTELLIGENCE

MALAYSIA DIGITAL COMPANY

Applied Security Intelligence Sdn Bhd
202001035047 (1391368-M)
Unit 03, Level 3, Tower B, Vertical Business Suite, Avenue 3, Bangsar South,
No. 8, Jalan Kerinchi, 59200 Kuala Lumpur, Malaysia.
Tel: +(60)3 - 6416 7234 Enquiry: sales@appsecintel.com

Stay in touch!