ACDS
ADVANCED CYBER DEFENCE SYSTEMS

Attack Surface Management

Discover, prioritise and remediate vulnerabilities in your attack surface. Identify your vulnerable assets before they are exploited. Harness the most extensive data sources across the internet.

With the rapid proliferation of cloud providers, software, web properties, remote devices, and more, it is becoming incredibly challenging for security teams to identify risks and take action.

As an organisation's attack surface is constantly evolving, its security team needs access to a comprehensive and highly contextualised data feed for security analysis at scale.

External Attack Surface Management (EASM) is the process of continuously discovering, monitoring, evaluating, prioritising and remediating possible entry points within an organisation's IT infrastructure that could be susceptible to an attack.

75% of employees will acquire, modify, or create tech outside of IT teams' visibility by 2027. (Gartner)

30% of assets are unknown and unmanaged because of fast digital transformation. (Forrester)

A market-leading attack surface management solution giving full-internet visibility into your external attack surface.

ACDS combines multiple massive data sources to feed its powerful anomaly detection engine, picking up configuration errors and vulnerabilities that often go undetected by others. Regular monitoring of an organisation's external attack surfaces for changes and new assets will alert of any weakness or vulnerability that might be exploited.

Our advanced detection model helps to discover, identify and monitor the entirety of your attack surface. Combining the power of data science and analytics we deliver a highly vetted list of vulnerabilities and their critical risk factor to ensure prompt action and tracking. Organisations can see results instantly after deploying ACDS' Attack Surface Management tool.

Key Features:

- Comprehensive Asset Discovery using massive, historic data sources and scanning to keep your asset inventory always up-to-date.
- Full visibility into your external attack surface, with vulnerability detection across all of your internet-facing IPs and domains.
- Custom anomaly detection engine using deep experience and expert-trained machine-learning algorithms.
- Monitor and flag certificate misconfiguration and expiry.
- Risk scoring of vulnerabilities, weaknesses, and anomalies for rapid triage, combining industry-standard scoring with new predictive scoring methods (CVSS, EPSS).
- Advanced software and device fingerprinting for accurate and reliable system identification that is resistant to data spoofing (including JARM, JA4, recog, and proprietary detection fingerprints).

CONVENTIONAL ASM APPROACH:

Limited view only finds one additional asset

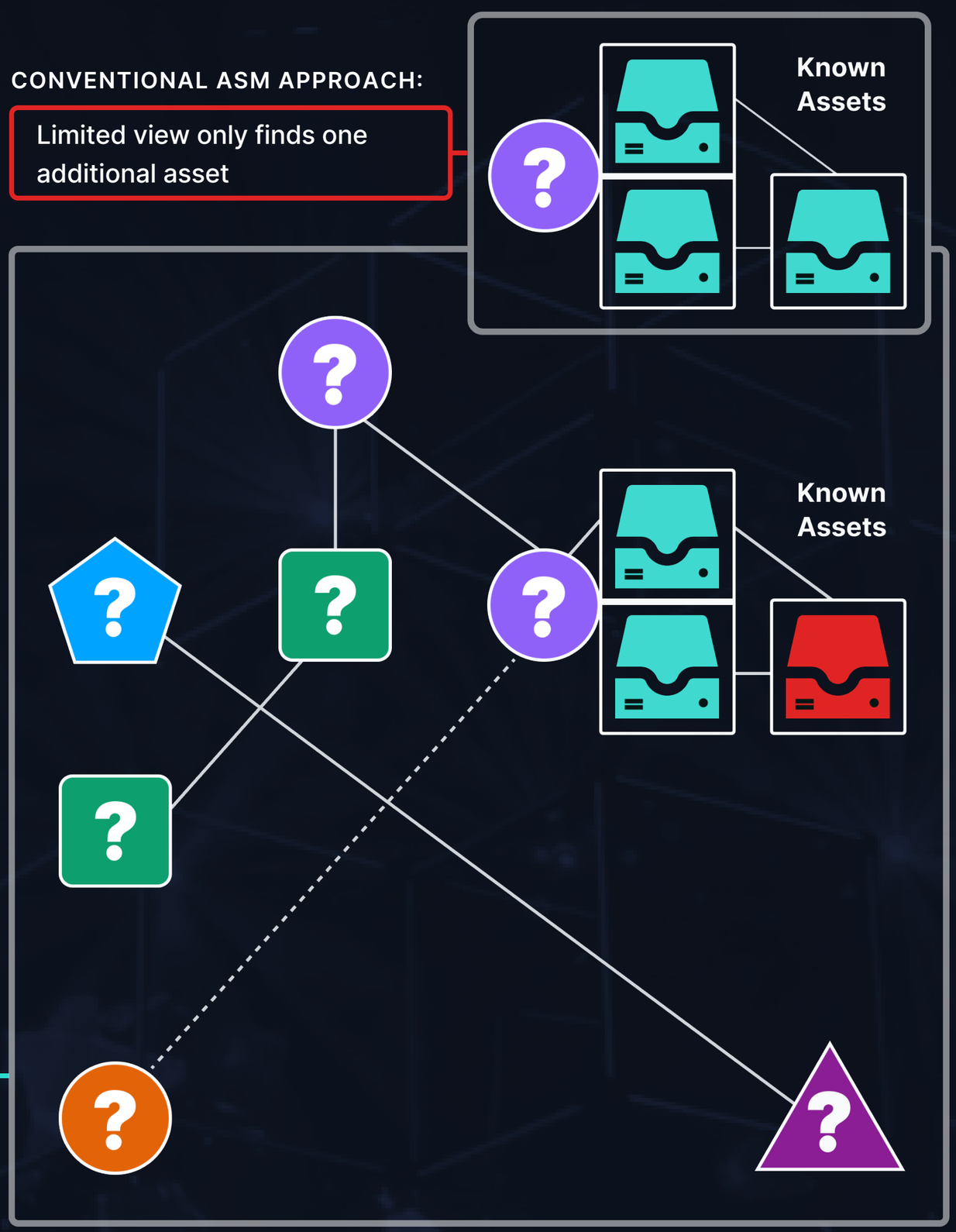
ACDS ASSET DISCOVERY:

Adds seven assets to your baseline:

- 2 Domains • 1 IOT Device
- 1 Subdomain • 2 IP Addresses
- 1 Mail Server

We also found:

- 1 Vulnerable Service



Benefits:

- We access the most extensive data sources across the internet daily, monitoring full IPv4 coverage and targeted IPv6 exploration.
- Discover all of your internet-facing devices and assets including IT (on-prem, cloud, hybrid); Operational Technology; IoT; Shadow IT and unapproved personal devices enabling you to take immediate action on critical vulnerabilities via our proprietary risk identification prioritisation algorithm.
- Proven to flag the most critical vulnerabilities that other enterprise solutions can not, with better data coverage and fewer false positives.
- Nice and clean business reporting via an easy-to-use user interface.

ACDS
ADVANCED CYBER DEFENCE SYSTEMS