UltraHeals

# ATTACK SURFACE MANAGEMENT

## Problem

In the current digital era, cyberattacks pose a persistent and evolving threat. Organizations with expansive attack surfaces – the totality of their internet-facing digital assets – are particularlyvul-nerable to exploitation by determined adversaries.

- **Limited Visibility**

Undiscovered assets, such as misconfigured cloud resources or forgotten public servers, can become gateways for attackers.

- **Unmitigated Vulnerabilities**

Unidentified and unpatched vulnerabilities represent critical weaknesses in an organization's security posture. Some of these vulnerabilities persist undetected for extended periods.

- **Reactive Security**

Security efforts become a desperate attempt to address breaches after they have already occurred. This reactive approach is analogous to securing a perimeter after a break-in has transpired.

- **Risk of Regulatory Non-Compliance**

Numerous regulations mandate the implementation of robust security practices. Non-compliance can incur significant financial penalties and reputational damage.

## The Need

To combat these threats, we need a multi-pronged approach that prioritizes proactive measures and continuous vigilance. Ultra-Heals' Attack Surface Management (ASM) platform offers a robust suite of features designed to empower organizations with proactive security measures.

**Here's a breakdown of its key functionalities:**

### Attack Surface Identification and Management

- **Attack Surface Management**

Automates vulnerability identification in external infrastructure, empowering organizations to proactively mitigate potential threats and enhance their overall security posture.

- **Discover Unknown External Assets**

Utilizes public internet scanning, advanced port scanning, and subdomain enumeration to detect hidden external assets and pinpoint critical exposed ports and active hosts.

- **Cloud Security Protection**

Detects and addresses cloud security misconfigurations on AWS, Azure, GCP, and Digital Ocean, protecting organizations from risks and data breaches.

## Vulnerability Assessment and Intelligence

- **Vulnerability Intelligence Module (VIM)**

Engages in continuous, internet-wide scanning to uncover active and passive vulnerabilities with an advanced scanning engine, ensuring robust web application and web server security. It comes with 10,000+ Payloads for automated Black Box and Grey Box Testing.

- **Prioritized Vulnerability Remediation**

Correlates exploit existing vulnerabilities, offering insights into actively targeted vulnerabilities to prioritize defense strategies effectively.

- **Vulnerability Operation Center (VOC)**

Provides a centralized view of vulnerabilities, synchronized patch management, continuous monitoring, and facilitates cross-functional collaboration to ensure timely and effective remediation.

## Risk Evaluation and Centralized Management

- **Risk Score**

Provides a comprehensive assessment of an organization's security posture by analyzing vulnerabilities and exposed risks, prioritizing areas that need immediate attention.

- **SSL Certificate Vigilance**

Tracks SSL/TLS certificates' statuses, alerting on active, expiring, or expired certificates to enhance web security and maintain user trust.

- **Compliance-Centric Vulnerability Management**

Seamlessly maps identified vulnerabilities to critical compliance standards, ensuring security efforts align with regulatory needs and providing actionable compliance risk insights.

## Benefits

The Ultra-Heals platform delivers unparalleled security advantages, empowering organizationsto fortify their defenses and streamline their cybersecurity operations ensuring that businesses can operate with confidence, knowing their digital assets are protected against evolving threats.

### Enhanced Security Posture

By proactively identifying and mitigating vulnerabilities, organizations can significantly reduce their risk exposure and safeguard critical assets from potential cyber threats.

### Regulatory Compliance

Streamlined vulnerability management ensures alignment with key compliance standards, reducing the risk of regulatory penalties and enhancing overall governance.

### Operational Efficiency

Centralized oversight and automated vulnerability assessments enable faster, more effective remediation processes, minimizing downtime and resource expenditure.

### Improved Risk Management

Comprehensive risk scoring and prioritized remediation efforts allow organizations to focus on the most critical threats, optimizing their security investments.

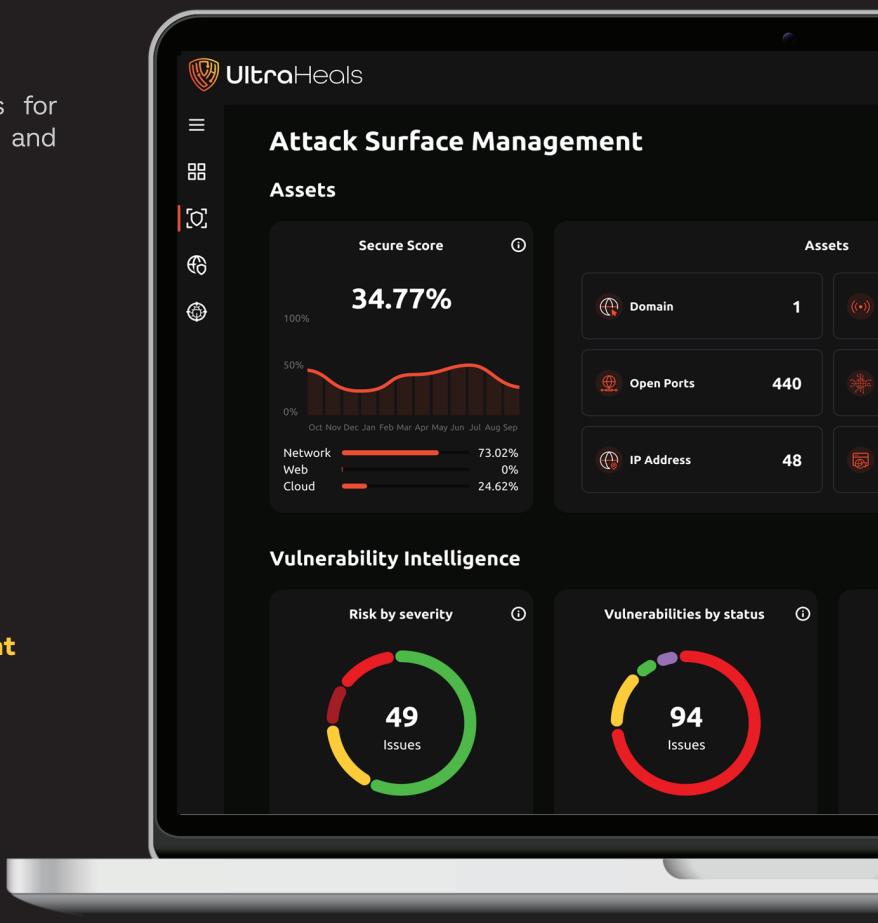
### Increased Cloud Security

Robust detection and correction of cloud misconfigurations protect against data breaches, ensuring the integrity and confidentiality of cloud-stored information.

### Continuous Protection

Ongoing monitoring of SSL certificates and real-time vulnerability intelligence keep organizations ahead of emerging threats, maintaining continuous security vigilance.

## Competitive Edge




### Prioritization Based on Active Exploits

- Correlates active exploits with vulnerabilities for targeted remediation for both known exploits and those not yet discovered by security vendors.
- Ensures resources are allocated effectively to address the most critical threats.

### Cloud-Agnostic Misconfiguration Detection

- Provides comprehensive coverage across multiple cloud platforms.
- Ensures consistent and effective security for organizations with hybrid or multi-cloud deployments.

### Compliance-Centric Vulnerability Management

- Seamlessly maps vulnerabilities to critical compliance standards.
- Simplifies compliance efforts by translating vulnerabilities into actionable compliance insights.

## Case Studies

### Attack Surface Management for a Malaysian E -Commerce Giant

- Revenue: $1.5 Billion  Employees: 5,000+
- Ultra Heals' Attack Surface Management identified an environment variable which contains production database credentials that was exposed to public internet without any authentication.

### Automated Penetration Testing for UAE Government Facility

- Revenue: $8 Million Employees: 150
- In the semi-government sports facility sector in UAE, the Automated Pentesting tool successfully identified a Remote Code Execution vulnerability in their Mail Server, showcasing the platform's capability in detecting critical security threat efficiently

## Our Customers

35+ Clients

10+ Countries

## Testimonials

**Nabil S.**
Senior Product Manager, Sixth Force Solutions

Currently, we're closely engaged with the Cyber-heals team on two other products. It's a pleasure to have a reliable security partner to address critical challenges. Their new tool, Ultra heals, enhances capabilities, contributing to the identification of vulnerabilities in our attack surface promptly.

**Hasan Ahamed**
Head, IT Infrastructure, Abdullah Al Othaim Co., KSA

Excited to share that we just experienced a remarkable demo of the cyber Heals - Ultra Security Platform! With its cutting-edge capabilities. ASM brings a whole new level of protection to our organization, helping us stay one step ahead of emerging cyber threats.

## About Cyber Heals

Cyber Heals is the global cybersecurity firm behind the Ultra-Heals platform. Founded on the belief that defense is more than reaction, we combine cutting-edge AI with the expertise of our seasoned cybersecurity professionals. Headquartered in the UK with a global presence, Cyber Heals is dedicated to safeguarding your digital infrastructure, wherever you operate. We are compliant with **ISO 27001, ISO 9001, GDPR** and **SOC2**.

Ready to fortify your defenses?

Get a complimentary scan of your organization's attack surface today and take the first step towards enhanced security.
Click here to schedule your free scan now!"

**Contact us**

sales@cyberheals.com

www.cyberheals.com