WhiteHat ATTACK SURFACE MANAGEMENT

POWERED BY BIT DISCOVERY

The average enterprise has tens or even hundreds of thousands of internet-accessible assets. These assets include websites, DNS servers, VPN's, databases, and IoT devices, to name a few. Additionally, these assets reside on-prem, in the cloud, across geographically distributed data centers, and are connected through dozens of non-contiguous IP-ranges. Unfortunately, most organizations lack a comprehensive inventory of these assets, which makes securing them a challenge.

After all, an organization can't ensure the security of an asset if it doesn't know it exists.

Staying Ahead of Threat Actors

The past decade has seen exponential growth in internet-exposed assets. Coupled with the accelerated shift to a remote workforce, many IT teams are overwhelmed as they try to defend not only their internal network, but also their digital presence across the internet and cloud. That's not good news when one considers that today's highly organized threat actors deploy targeted attack surface mapping tools before they attack.

Today's organizations need a smarter way to discover and manage their global external attack surface, so they can successfully protect their business.

Complete Attack Surface Visibility

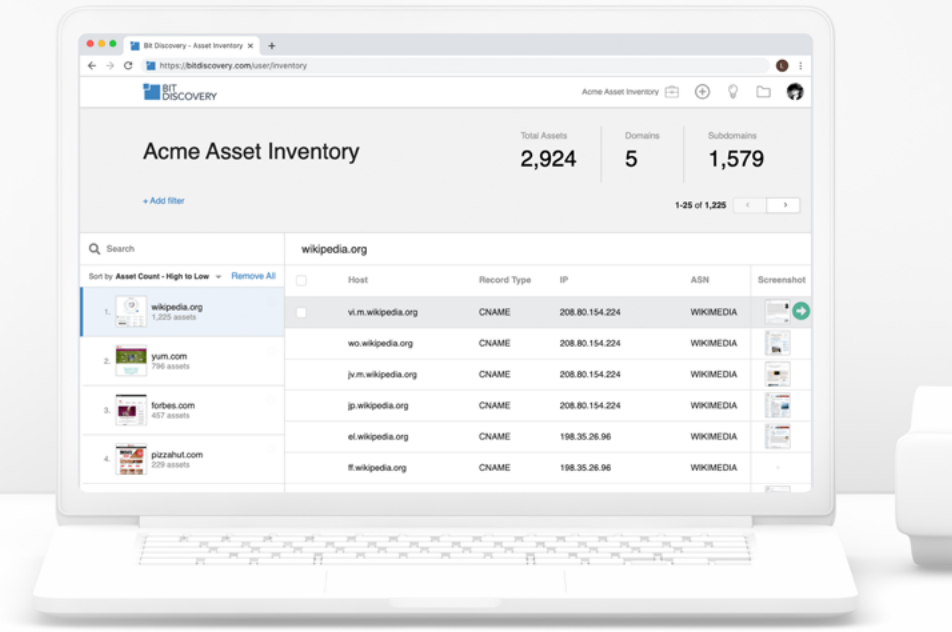
WhiteHat Security's Attack Surface Management powered by Bit Discovery delivers a fast, simple, and automated way for organizations to create a comprehensive inventory of their complete attack surface. Leveraging an innovative database of nearly 4.5 billion Internet-connected assets, Attack Surface Management discovers, learns, and provides a complete inventory of an organization's internet exposed assets, details about where in the tech stack exposure exists, and alerts when the attack surface changes. Using this information, organizations can more quickly identify and prioritize their security resources.

Simplify AppSec Security at Scale

With Attack Surface Management, organizations will now have an instant and comprehensive view of their assets, with applications mapped to those assets and ranked by priority. This will enable IT teams to adopt a holistic view of their attack surface and adopt a strategic approach to securing their most at-risk applications. Once identified, IT teams can easily port a prioritized list of assets into WhiteHat's Sentinel platform by leveraging a purpose-built API integration, thereby identifying vulnerabilities in web applications before they can be compromised by threat actors.

Attack Surface Management: Automated, Simplified Visibility Across Your Organization

Attack Surface Management empowers organizations with unparalleled visibility and control of their web facing assets Together with WhiteHat's Sentinel platform, organizations are empowered with unparalleled visibility and control of their web facing assets.



ATTACK SURFACE MANAGEMENT BENEFITS:

Complete Attack-Surface Visibility

Achieve an accurate inventory of your entire *internet-accessible* assets, no matter where they reside - on-prem or in the cloud

Reduce Risk

Identify and prioritizing at-risk assets – before threat actors have an opportunity to exploit them

Part of an Holistic AppSec Solution

Easy-to-use integrations with WhiteHat's Sentinel platform allows organizations to discover, learn, and secure their attack surface - faster

Simplify Security

Intuitive, easy-to-use dashboards reduce manual processes and improve efficiencies

WHITEHAT SECURITY, INC. 1741 Technology Dr. #300, San Jose, CA 95110 • 1.408.343.8300 • www.whitehatsec.com