EXPOSURE DATA YOU CAN TRUST WITH SIXMAP

Exposure management has a data problem. Many vendors provide data that's inaccurate, generating false positive alerts that waste time, and incomplete, allowing true positive vulnerabilities to go undetected.

SixMap provides complete and accurate data that others cannot. A proprietary technology called 6Gen enables discovery across IPv4 & IPv6, inspects all 65,535 ports on every asset during every scan, and delivers precise data on all external assets, exposures, and risks.

New Innovations To Address Familiar Challenges

The modern automated SOC demands precise, real-time data about assets, exposures, and risks. However, many security leaders simply don't trust the data they get from their current toolset. All too often, alerts turn out to be false positives because an asset belongs to a third-party organization. The vulnerability may be real but it's on somebody else's system.

At the same time, security leaders still worry about hidden risks. If their existing tools provide incomplete data, they still have "unknown unknowns." This could be due to inadequate host discovery that fails to uncover all assets. It could also be caused by partial exposure assessments that only scan the most common ports, leaving blindspots on non-standard ports.

These data limitations lead to real business challenges. Security teams waste time trying to triage alerts and determine whether an asset belongs to their organization. Unknown assets and services create invisible risks that could potentially lead to an incident. Automated workflows are bogged down with bad data that degrades the efficacy of investments in AI-powered solutions.

SixMap brings several new innovations to the market that overcome the limitations of legacy exposure management tools. SixMap's computational mapping technology enables precise asset discovery across both the IPv4 and IPv6 address spaces, plus port inspection of all 65,535 ports for each host on every scan. These capabilities result in more accurate and complete data on external assets, exposures, and vulnerabilities, which saves time, streamlines automated workflows, and focuses attention on the real risks that matter most.

SixMap: Providing Exposure Data Worth Acting On

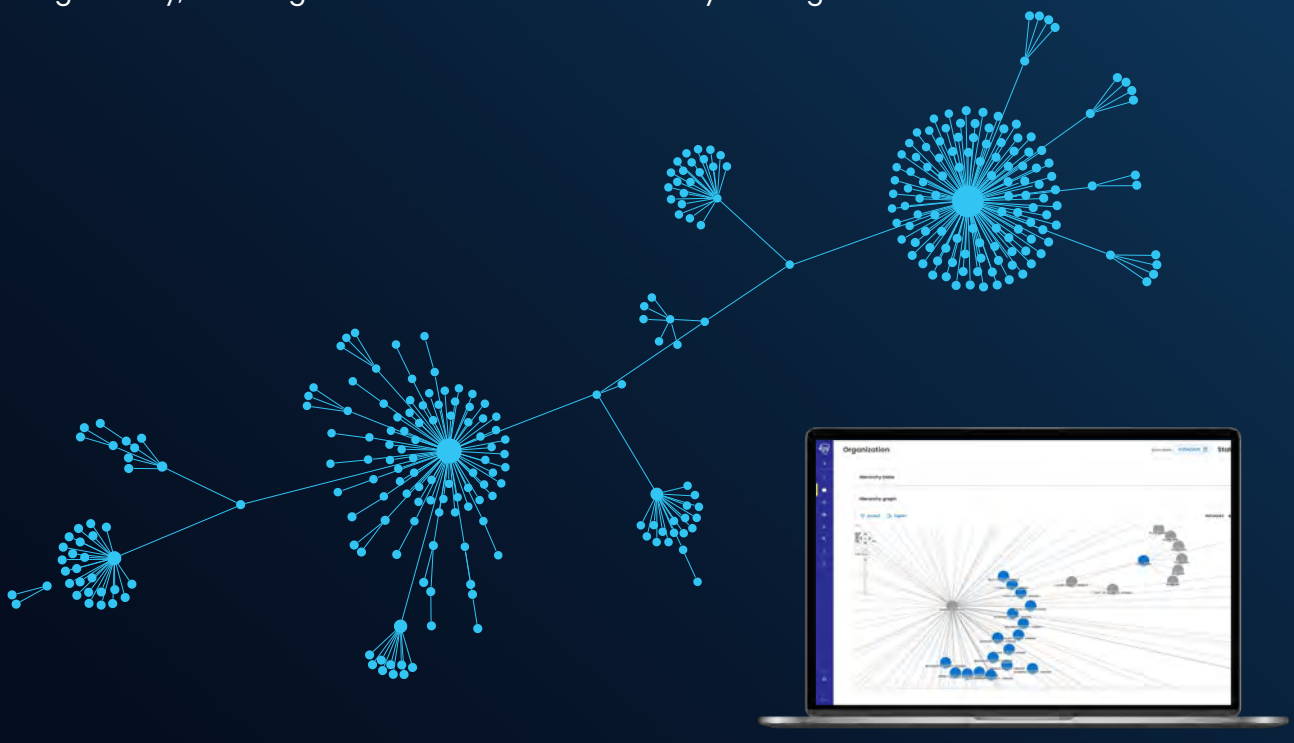
SixMap's preemptive exposure management platform provides the data security teams need to enhance automation, reduce time wasted on false positives, and increase focus on real risks.

The SixMap solution has four primary capabilities: organization mapping, host discovery, exposure assessment, and risk-based prioritization using threat intelligence data.

MAP - Organizational Mapping

SixMap's unique organization mapping capability finds all of the subsidiaries and legal entities that belong to a single parent organization. Internal research shows that SixMap discovers anywhere between 5x and 18x the number of subsidiaries typically known to major business intel firms. The only thing a customer needs to provide to get started is the organization's name.

Once all the entities are documented, SixMap creates a map of the organizational hierarchy. This provides two major benefits. First, it acts as a starting point for the asset discovery process, setting the stage for a more complete inventory. Second, all assets are automatically categorized by their parent legal entity, resulting in structured data that's easily managed.



DISCOVER - IPv4 & IPv6 Host Discovery

With the organization map established, SixMap uses every subsidiary and legal entity as a starting point for the discovery procedure. This broader perspective identifies many assets that would otherwise be missed, enabling SixMap to provide a comprehensive asset inventory.

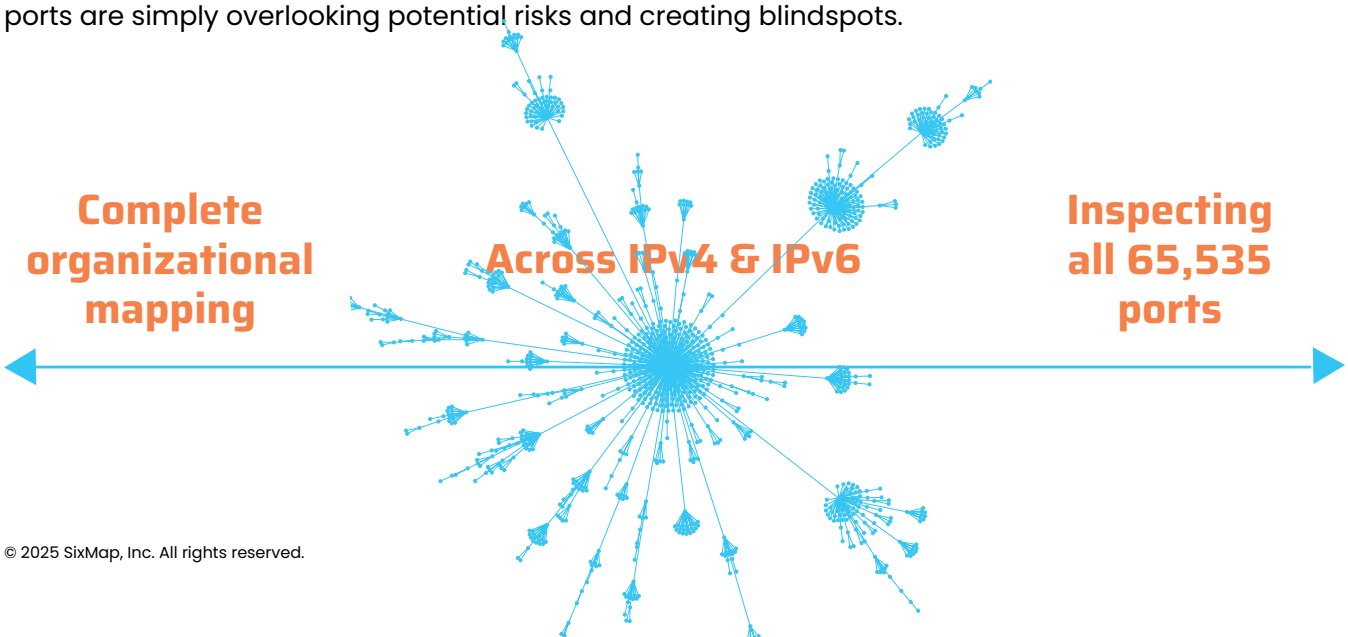
SixMap's discovery process uses a proprietary innovation called 6Gen, which discovers hosts across the IPv4 and IPv6 spaces. 6Gen is a computational mapping algorithm that implements statistical modeling techniques to find hosts with extremely high precision, uncovering many more domains and IP addresses than legacy tools that rely exclusively on WHOIS data and DNS records.

While many security leaders are convinced they do not use IPv6, SixMap routinely finds IPv6 assets in use for almost all organizations evaluated. Internal research indicates that 6% to 9% of the IP addresses in use by large enterprises are in the IPv6 space, with the vast majority of IPv6 addresses running in public cloud environments.

ASSESS - Exposure Assessment

Once all hosts have been discovered and the asset inventory is complete, the exposure assessment can begin. SixMap inspects all 65,535 ports on each asset, every single scan. This stands in sharp contrast to legacy exposure management tools, which typically scan only the top 1,000 to 5,000 most common ports and fail to detect services on non-standard ports.

Research consistently shows that around 7% of services run on non-standard ports that fall outside of the top 5,000. It's essential to assess each and every port to fully understand what services are in use, what versions are running, and where known vulnerabilities exist. Products that do not inspect all ports are simply overlooking potential risks and creating blindspots.



PRIORITIZE - Risk-Based Prioritization

Because SixMap's discovery technology finds far more hosts, and because the exposure assessment inspects all ports rather than just a small subset, a greater number of vulnerabilities are uncovered as compared to traditional exposure management tooling. The data is also more accurate, giving security teams confidence that they can trust and act on the data received.

The CVEs that SixMap detects are all enriched with threat intelligence data, including the severity of the vulnerability, whether or not it's known to be exploited in the wild, the probability it will be exploited within the next 30 days, and which threat groups are known to exploit it.

By providing all of these enrichments, SixMap reduces friction in security operations and vulnerability management. Security teams can focus efforts on the real risks that matter most, ensuring time is used efficiently and critical risks are mitigated before an attack occurs.

Summary: Key Benefits & Business Value

In short, SixMap provides exposure data you can trust. With more complete and accurate data related to your assets, exposures, and risks, your organization receives immense business value that can be seen along a number of important dimensions.

GAIN VALUE INSTANTLY

Get results and value immediately after an initial zero-touch deployment.

ENABLE AUTOMATION

Send better data to your security stack, improving automated workflows.

ACCESS DATA YOU CAN TRUST

Get complete, accurate data about your assets and exposures.

ENHANCE SECURITY ROI

Improve returns on other tools that depend on accurate asset data.

SAVE TIME & RESOURCES

Save time & redeploy your team to other important projects.

REDUCE CYBER RISK

Accelerate vulnerability remediation cycles, reduce risk, and stay secure.

SIXMAP: TRUSTED BY SECURITY LEADERS AT THE WORLD'S LARGEST ORGANIZATIONS.

"Out of thousands of Internet-facing assets, SixMap was able to automatically pinpoint the most pressing vulnerabilities that required immediate action based on quantifying the risk by correlating the threat actors and exploitable vulnerabilities. We're glad they have partnered with AWS to deliver value to their customers."

Elwin Wong, CISO of Ross Stores

"One of the most powerful cybersecurity capabilities required to operate and defend computer networks … SixMap Computational Mapping provides public and private sector teams automation for network management and defense so that they can efficiently and effectively operate and defend IPv4-only, dual-stack, and IPv6-only networks."

United States Army, SBIR I Evaluation

SixMap provides the most accurate and complete external view of your organization—no input required, just the company name. Our preemptive exposure management platform interrogates all 65,535 ports as standard operating procedure—across IPv4 and IPv6—continuously hunting unknown assets, misconfigurations, and blindspots other tools miss. Built for security teams tired of tools that assume too much and miss even more, SixMap replaces guesswork with precision. So you can act faster, reduce exposure, and see what attackers see.

BOOK DEMO

SixMap, Inc.
6731 Columbia Gateway Dr Suite 100, Columbia, MD 21046

SIXMAP.IO