SIXMAP WHITEPAPER

SixMap Preemptive Exposure Management Platform

Bridge the gap between what the security team defends and what sophisticated threat actors find through advanced reconnaissance.

Preemptively mitigate risks before an attack takes place.

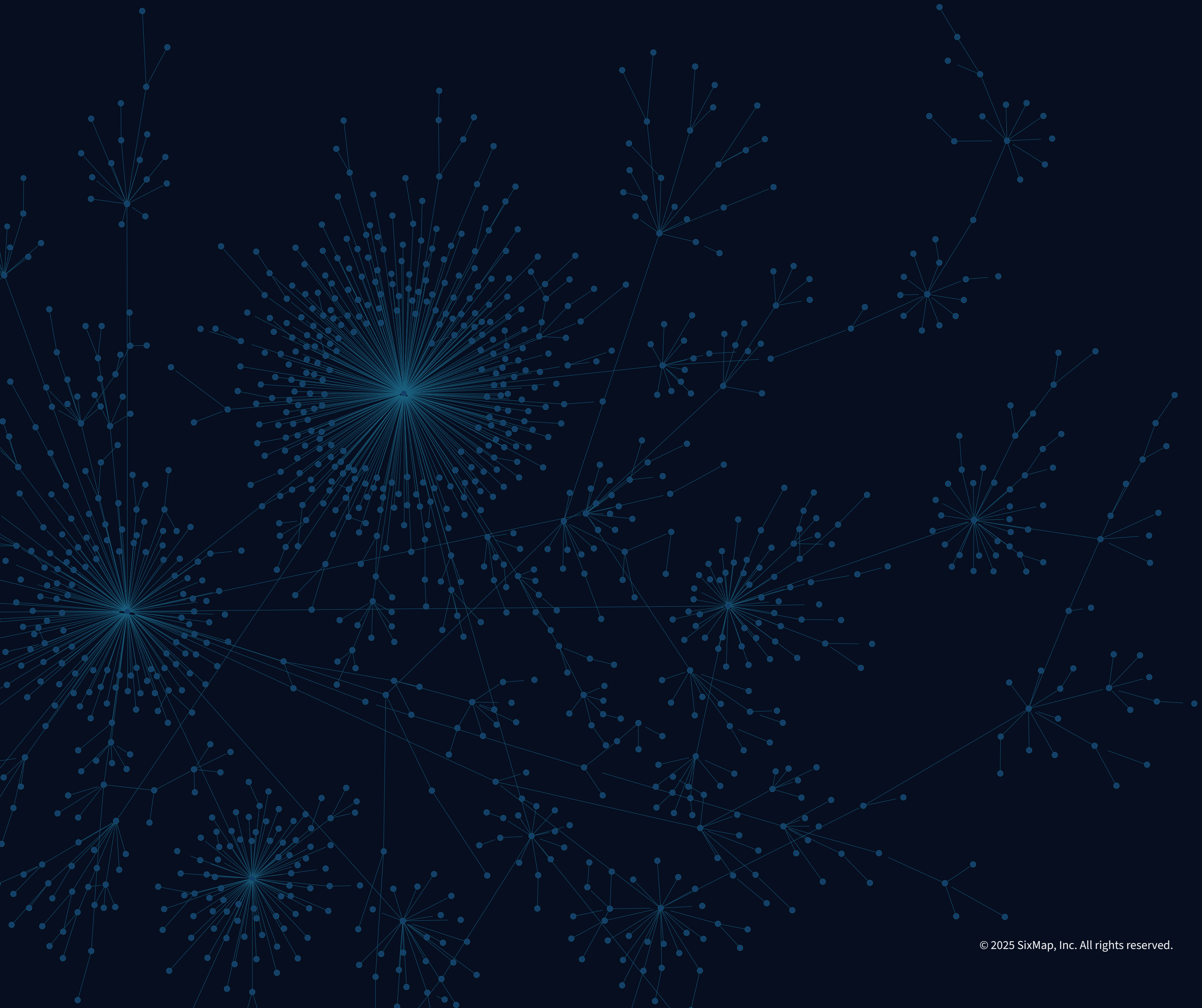

Table of Contents

Executive Summary

In cybersecurity, change has always been constant, but AI is accelerating the pace to an entirely new level. Threat actors are now using AI to increase both the frequency and velocity of their attacks, automating everything from reconnaissance to exploitation.

Yet even as attackers adopt advanced AI tooling, the underlying tactics have not changed. Most AI-driven attacks still rely on familiar, highly effective techniques, particularly the exploitation of vulnerabilities in software running on Internet-facing assets.

So, while next-generation threats like AI-driven attacks present a real risk, foundational issues such as shadow IT, misconfigurations, and unpatched vulnerabilities remain the primary weaknesses that AI agents will use to compromise a system and gain a foothold in a victim's network.

This dynamic reveals a simple truth: defenders must use new innovations in the same way attackers do. Security teams need to apply advanced technologies to automate and accelerate foundational practices such as keeping asset inventories current, managing vulnerabilities, and continuously monitoring the external attack surface. This approach allows defenders to keep pace with threat actors.

SixMap's technology provides these capabilities and ensures defenders operate on equal footing with attackers. The SixMap platform is designed to deliver continuous reconnaissance in the same way a brigade of malicious AI agents deployed by a nation-state APT would. SixMap discovers all entities, assets, exposures, and risks, multiple times per week for every customer.

By closing the gap between what adversarial AI will find through reconnaissance and what the security team is currently defending, SixMap helps organizations preemptively mitigate risks before an attack takes place.

The Challenges

Security leaders face major challenges in defending their organizations against cyber attacks. And the stakes are high: a cyber incident can have significant financial consequences, including extended disruption of operations, lawsuits, regulatory fines, and other serious repercussions.

Complex, Dynamic Organizational Structures

Large organizations, both public and private, are sprawling and complex. They're also constantly evolving through restructuring, M&A activity, expansion into new regions, new departments or business units, and other more. This evolution creates complexity and risk.

Expanding Digital Footprints & Increased Attack Surfaces

While the organization itself is changing shape, the digital footprint is steadily expanding in parallel to support growth. This means more networks, cloud resources, domains, applications, and data– all of which needs to be properly inventoried, monitored, and protected.

Huge Volume of Vulnerabilities, Limited Time & Resources

The number of vulnerabilities and misconfigurations in a typical IT environment has been skyrocketing for years. Security teams are struggling to keep up. With many teams short staffed, there simply isn't enough time to mitigate all risks and prioritization remains a challenge.

Limitations of Existing Exposure Management Products

Many cybersecurity vendors over-promise and under-deliver. This is especially true for exposure management products, many of which fail to live up to their marketing claims. In the next section, the specific limitations of different product categories will be discussed in greater detail.

Overview Of Existing Approaches & Their Limitations

Most exposure management tools are useful in limited ways but fall short of delivering a complete solution. Below is a summary of the existing product categories and their constraints.

External Attack Surface Management Tools

External attack surface management products promised to give organizations a comprehensive view of their digital estate. It's an important objective, but EASM tools didn't live up to the hype.

Incomplete Asset Discovery

EEASM tools start with a few seed domains and use Internet records to find additional assets assumed to belong to the customer. This approach misattributes assets and misses segments of the digital estate.

Limited Asset Attribution

With discovery limited to DNS records, WHOIS data, and SSL certificates, EASM tools are inequipped to untangle which domains and IP addresses belong to what organization. Ownership is often unclear.

Partial Exposure Assessments

Most EASM tools only assess the top 1,000 to top 5,000 most common ports on each host. This leaves the majority of ports unmonitored, potentially exposing critical risks to the public Internet.

Mass IPv4 Internet Scanners

Mass Internet scanners build a census of the entire IPv4 space and act as a search engine for Internet-connected devices. This is valuable data but has few use cases for security teams that are only concerned with protecting a very small fraction of all IP addresses globally.

Challenges With Attributing Assets

Because mass Internet scanners check all IP addresses in the IPv4 space, they struggle to understand which assets are owned by a given organization. They struggle to show customers their digital estate.

Limited Asset Attribution

With discovery limited to DNS records, WHOIS data, and SSL certificates, EASM tools are inequipped to untangle which domains and IP addresses belong to what organization. Ownership is often unclear.

Partial Exposure Assessments

Most EASM tools only assess the top 1,000 to top 5,000 most common ports on each host. This leaves the majority of ports unmonitored, potentially exposing critical risks to the public Internet.

Legacy Vulnerability Management Products

Vulnerability management platforms offer both internal and external scanning capabilities but do not provide several key features that enterprise security teams need to defend today.

Limited Discovery

VM products require a list of target IP addresses and domains to scan. While some vendors may also provide host discovery, the functionality is rudimentary and can leave many assets undetected.

Point-In-Time Assessments

Vulnerability scans are often point-in-time processes rather than continuous assessments. This leaves risks exposed in the time that passes between scans.

Low-Fidelity Results

Many vulnerability scanners are noisy, generating a very large volume of network traffic, providing an enormous list of low-severity findings that contain many false positives.

SixMap Preemptive Exposure Management Platform

SixMap's Preemptive Exposure Management platform is designed to show you who you are, what you own, what's running in your environment, and what risks need to be mitigated first.

First incubated by the NSA to protect government and defense agencies, SixMap's technology is trusted by the cyber defenders who safeguard some of the nation's most critical networks, systems, and data. Now, these military-grade capabilities are available to private enterprises through the SixMap Platform.

The SixMap platform is an agentless SaaS solution that is very rapidly deployed without any effort. Customers are only required to provide their organization's name and they begin receiving value from day one.

There are four main stages to SixMap's continuous process.

Organizational Mapping

By mapping your organizational structure from the ground up, SixMap reveals all the distinct entities that need to be protected.

Host Discovery

6Gen, SixMap's proprietary computational mapping algorithm, provides comprehensive visibilityon every domain and IP address across IPv4 and IPv6.

Exposure Assessment

An exhaustive yet non-intrusive risk assessment inspects every asset to identify all open ports, services, exposures, and security issues.

Risk-Based Prioritization

Vulnerability detection across the attack surface, plus enrichment of every CVE with threat intelligence for simplified prioritization and faster risk mitigation.

MAP:
Organizational Mapping

SixMap's unique organization mapping capability finds all of the entities that belong to a single root organization. An entity could be a subsidiary, brand, operating company, business unit, product line, department, regional legal entity, or other distinct suborganization. A few examples will help clarify the relationship between a root organization and its entities and descendants.

Suppose the root organization is the California University System. There are 10 major campuses: Berkeley, Davis, Irvine, Los Angeles, Merced, Riverside, San Diego, San Francisco, Santa Barbara, and Santa Cruz. Each of these universities would be an entity, and each entity would then have a series of descendants beneath it. In this example, those descendants would perhaps be the admissions department, the athletics department, the financial aid office, the library system, student housing offices, on-campus dining facilities, the student bookstore, etc.

At a large technology company like Google, entities would perhaps translate to products: Google Search, Google Maps, Gmail, Google Cloud Platform, Google Pay, YouTube, Android, DeepMind, and so on. For a large retail corporation like Nestlé, entities would likely be distinct brands, e.g. Cheerios, DiGiorno, KitKat, Nescafe, Nesquick, Perrier, and more.

SixMap uses a combination of automation and AI, overseen by an internal research team for assurance purposes, to map out a given organization. A multitude of data sources, including proprietary data from partners plus OSINT data ingested from more than a dozen sources, are used in building the organization map.

Internal research shows that SixMap discovers anywhere between 5x and 10x the number of subsidiaries, entities, and descendants typically known to leading business intelligence firms. Crucially, the only thing a customer needs to provide to get started is the root organization's name.

Once all the entities are documented and the organization's structure has been fully mapped, SixMap builds a hierarchy of the organization. This provides two major benefits.

First, every single entity and descendant acts as an initial starting point for the host discovery process, which provides a much more comprehensive asset inventory than would otherwise be possible. Many competing exposure management tools only begin the discovery process from the root organization, which may fail to detect large portions of the organization's digital estate. Because SixMap takes an entity-first approach, the results are more accurate and complete.

Second, every asset is automatically assigned to the entity that owns and controls it. This solves the problem of asset attribution, which is a challenge for many legacy exposure management tools. SixMap customers receive asset and exposure data that's automatically structured and easily managed, without any effort or administration.

DISCOVER:
Host Discovery Across IPv4 and IPv6

With the organization map established, SixMap uses every entity and descendant as a starting point for the discovery procedure. The objective is to find all of the network assets– networks, IP addresses, and domains– that the root organization must protect.

This process begins with identifying all of the autonomous systems and BGP prefix announcements associated with a given organization by fuzzy matching on the global BGP routing table, from the perspective of Tier 1 ISPs.

SixMap actively measures and models the Internet using bi-coastal high performance computing (HPC) data centers. Our HPC infrastructure is connected directly to the Internet backbone with an independently owned and operated in-house network using Tier-1 ISP grade technology. (i.e.~ 1 Tbps of switching capacity, designed with numerous 100 Gbps switching components and 10 Gbps 1510 nm single mode fiber lines for redundancy and reliability.)

In addition, the SixMap platform identifies network blocks that have been sub-allocated to the customer’s organization from ISPs and other organizations—again using contextual analysis on the blocks. SixMap also leverages near-real-time global passive DNS data and global active mapping data to identify all the domains and subdomains associated with the customer’s organization.

6Gen, SixMap’s proprietary technology, was initially developed to discover and inventory all live hosts in the vast IPv6 space– a project once thought to be impossible. Simply stated, 6Gen works by reducing the difficulty of the problem using real-time modeling and advanced computation. It determines where hosts are likely to exist and looks there, rather than blindly guessing or using exhaustive scanning techniques that attempt to check each possible address.

The SixMap Platform now uses 6Gen to find hosts with extremely high precision across both the IPv4 and IPv6 spaces. While many security leaders are convinced they do not use IPv6, SixMap routinely finds IPv6 assets in use for almost all organizations evaluated. Internal data indicates that 6% to 9% of the externally facing IP addresses in use by large enterprises in the USA are in the IPv6 space.

Research from industry giants like Cisco and Google show that more than 50% of all Internet traffic in the USA is on IPv6, leaving IPv4 with less than half of all Internet traffic today, so we expect to see a higher percentage of enterprise assets shifting over to IPv6 in the near future.

The end result of the Host Discovery procedure is a complete and accurate asset inventory that is continuously updated and delivered to customers. Every netblock, IP address, domain, and subdomain is assigned to the entity that owns it so the data is structured and easy to manage.

ASSESS:
Comprehensive Exposure Assessment

Once all hosts have been discovered and the asset inventory is complete, the exposure assessment process begins. SixMap continuously inspects all 65,535 ports on each asset.

As with the Host Discovery procedure, SixMap's Exposure Assessment process uses 6Gen's computational mapping technology to reduce the difficulty of the problem. Ultimately, this technique reduces the search space from billions of IP/port tuples down to just thousands. The concept is simple but hard to execute: learn about the network using as few measurements as possible, use the model to predict what the network looks like, and then validate the model with active probing.

It may sound like this approach would yield inferior results to traditional exposure management tools that implement exhaustive probing to discover IPs and ports. In practice, SixMap's technology achieves something that is counterintuitive; it finds more hosts and open ports while sending fewer probes. This is true because traditional exhaustive probing leads to difficult tradeoffs; you can either inspect fewer ports, reduce the frequency of the assessments, or overload the network with traffic (which may trigger automatic security mechanisms that block the scan, leading to incomplete results).

Generally speaking, the tradeoff that legacy exposure management tools chose is inspection of fewer ports. These products typically only check the top 1,000 to 5,000 most common ports and thus fail to detect services running on non-standard ports. Research consistently shows that 7% to 10% of services run on non-standard ports that fall outside of the top 5,000. Products that do not inspect all ports are simply overlooking potential risks and creating blind spots.

Using the lessons learned from 6Gen's computational mapping approach, SixMap developed technology that conducts exposure assessments in a manner that is orders of magnitude more efficient than traditional approaches. All 65,535 ports are inspected on each asset during each exposure assessment. The assessments run continuously– meaning, a new process begins the moment the previous one ends. For smaller customers, this means daily assessments. For very large customers, it means two to three assessments per week.

A key capability in the SixMap platform is quickly viewing the differences between any two assessments. If the two most recent assessments are selected, customers can quickly see all the changes that have occurred in their environment over the past 24 to 72 hours: new assets that have been deployed, new domains, newly opened ports with a service exposure, etc. This allows security teams to quickly spot and address new risks almost immediately after they appear. It also simplified reporting by revealing the delta over any desired period of time.

Once SixMap has built the asset inventory, assessed each host, and captured all IP/port tuples to understand which ports are open on which hosts, we run service version number (SVN) detection modules. This fingerprints the exact network service, software, and version in use, giving customers a comprehensive view of all exposures visible from the Internet.

PRIORITIZE:
Risk-Based Prioritization Of Vulnerabilities

After the Exposure Assessment is complete, SixMap provides customers with a comprehensive view of all netblocks, IP addresses, domains, subdomains, open ports, and services across their organization's attack surface.

The next step is converting identified services and version numbers into precise CPE entries detailing vendor, product, and exact version information. With accurate CPE data established, the SixMap platform checks CVE databases to determine whether documented vulnerabilities exist for the specific products in use. When relevant CVEs are found, they are recorded, enriched with threat intelligence, and prioritized by risk to streamline remediation efforts.

Because SixMap's host discovery and exposure assessment procedures are more accurate and comprehensive than legacy tools, so too are the vulnerability detection and prioritization processes. The SixMap platform uncovers entire segments of network assets that may be overlooked and finds exposed services running on non-standard and ephemeral ports, thus detecting vulnerabilities and misconfigurations that other tools would not be able to detect. At the same time, the accuracy of SixMap's data ensures that all vulnerabilities are present on assets that belong to the customer, and not on assets that in fact belong to a third-party.

Every CVE detected is enriched with threat intelligence data. These enrichments include: the severity of the vulnerability, the level of access needed to exploit it, whether or not it has been exploited in the wild, the probability it will be exploited within the next 30 days, and which threat actors are known to exploit it. Both financially-motivated ransomware gangs as well as state-sponsored APTs are included.

By providing all of these data points, 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.

It's important to emphasize yet again that all of the discovered assets and exposures are automatically assigned to the entity that owns and is responsible for managing them. When a vulnerability or high-risk misconfiguration is detected, it's easy for customers to see which asset is at risk and what entity is responsible for securing that asset. This reduces Mean Time To Remediate (MTTR), since security teams don't need to spend time validating the asset, trying to understand who owns it, or tracking down who to contact in order to have the risk mitigated.

Primary Use Cases

Customers use SixMap's data in a variety of ways.

Preemptive Exposure Management

Preemptively detecting, responding to, and remediating risks before attackers can target them.

EXAMPLE: A new CVE is published and the security team knows they have the vulnerable software deployed in their environment. They need to know all instances of this CVE and the exact systems that are exposed. The team uses SixMap to quickly pull the data and start remediation.

IPv6 Adoption Preparedness

Continuously discovering, assessing, and monitoring all IPv6 assets visible from the Internet.

EXAMPLE: An organization has many resources and workloads deployed with public CSPs. Many of these platforms enable IPv6 by default, and the security team needs to understand which assets are dual-stack. SixMap provides this data immediately, giving a complete list of assets running IPv6.

Auditing & Compliance

Maintaining audit-ready inventories of entities, network assets, service exposures, and vulnerabilities.

EXAMPLE: A security leader at a large enterprise is preparing for a cyber audit. Aggregating and verifying all of the data from dozens of subsidiaries and operating companies globally is almost impossible. SixMap continuously provides automatically-structured data on assets, exposures, and risks to streamline audits and compliance checks.

M&A Due Diligence

Comprehensively evaluating the cyber risk of a company before, during, and after M&A activity.

EXAMPLE: A large corporation is conducting due diligence ahead of an acquisition, with one major aspect being the cyber risk assessment. The security team uses SixMap to evaluate the company's cyber risk and report the findings to leadership, then continues to monitor after the acquisition.

Advanced Red Teaming

Performing nation-state level reconnaissance to conduct red team exercises for an organization.

EXAMPLE: A sophisticated offensive security company is contracted to run red team exercises for a large, multi-national organization. The offensive security company must fully map out the organization's digital estate. SixMap provides all of the data they need, with almost no input or effort.

Proactive Threat Hunting

Proactively finding anomalies that may indicate a threat, such as data exfiltration or a backdoor.

EXAMPLE: A remote access service (e.g. SSH or RDP) is detected on a non-standard port, which is unusual and out of compliance with company policy. Threat Hunters investigate to determine whether it's an employee breaking rules or an attacker establishing persistent network access.

SixMap's Key Differentiators

The Exposure Management space is crowded, with cybersecurity vendors offering similar products that are often hard to distinguish from one another. SixMap stands out by offering several key competitive advantages that differentiate us in a noisy market.

Mission-Oriented Philosophy

SixMap's roots in national defense have bestowed the company with a mission-oriented view of cybersecurity. We're not just focused on conducting basic attack surface reconnaissance. Rather, our objective is to preemptively protect customers against cyber attacks, safeguard all assets across the organization, and ensure continuity of operations.

Strategic Entity-First Approach

Every other solution on the market begins with network discovery. They take a few domains or IP addresses as seed assets and immediately turn to internet records, such as DNS, WHOIS, and SSL certificates, to try to map out your organization's attack surface. SixMap is the only vendor that starts by mapping out your organization and all its entities before beginning network discovery. This entity-first approach produces far more complete visibility on assets and exposures, plus every asset is automatically structured and assigned to the entity that owns it.

Advanced Core Technology

Whereas many exposure management tools are limited to Internet records to conduct host discovery, SixMap provides a real innovation: the 6Map computational mapping technology. First developed to map out the vast IPv6 space, the computational mapping techniques employed by 6Gen enable SixMap to find hosts with extremely high precision across both the IPv4 and IPv6 address spaces, in an extremely efficient manner.

Conclusion

For large enterprises, cybersecurity is no longer a minor technical problem to be solved with a few new tools. Cybersecurity is now a major business challenge that requires the right combination of people, processes, and technologies to properly address the challenges at hand. SixMap is the best-of-breed solution for helping security teams preemptively mitigate risks before they lead to a costly security incident.

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

Zero-Touch Deployment, Fast Time To Value

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

Complete and Accurate Data, Continuously Delivered

Continuously receive complete, accurate data on your assets and exposures.

Significant Time Savings, Reallocation Of Resources

Save time & redeploy your team to focus on other important projects.

Optimize Security Automation & Agentic AI SOC Platforms

Send higher-quality data to your security stack, improving automated workflows.

Enhanced ROI On Other Security Tools & Processes

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

Stronger Security Posture, Reduced Cyber Risk

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

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 at 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 1 Evaluation

"We used to spend days compiling internal and external scans before releasing a new product. Now we just launch and know SixMap will alert us immediately if there's real risk. That gives me high confidence to move faster."

-Douglas Gernat, CISO for the City of Richmond, VA

About SIXMAP

SixMap delivers the most complete and accurate external view of any public or private organization, showing security teams who they are, what they own, and what they must protect. By closing the gap between what security teams monitor and what adversaries find through reconnaissance, SixMap helps customers mitigate risks before attacks occur. Its strategic mapping ensures no assets are overlooked, while advanced technology pinpoints hosts, exposures, and risks with precision. Born out of national defense and deployed to protect some of the nation's most sensitive networks, SixMap now brings military-grade capabilities to public and private organizations to preemptively stop cyberattacks.

| 6731 Columbia Gateway Dr Suite 100 Columbia, MD 21046 | sixmap.io | in SIXMAP