NORTHSTAR
ATTACK SURFACE MANAGEMENT

★ NorthStar

NorthStar is an automated, data-driven platform that helps you gain visibility into your attack surface, identify security hygiene issues, and prioritize remediation of the cyber risks that matter most to your business.

VISIBILITY IS CRITICAL

Technology is an investment — a large one at that. You want to protect your investment while receiving the most value from it. We get it. However, you can't secure what you can't see, and many asset tracking tools on the market today only give you a glimpse of your entire IT asset landscape.

NorthStar creates the foundation for an aggregated, ground-up view of all the assets in your IT environment and how they relate to key business functions. Instead of relying on a single, potentially incomplete or stale source of information, NorthStar intelligently pulls data from across multiple platforms to assemble all the information you need to make informed and actionable decisions.

That's where NorthStar comes in - we're prioritizing exposure remediation by analyzing the severity of the vulnerabilities in the environment and the importance of the business functions they impact. This, in turn, gives a prioritized and actionable remediation plan that will have the greatest influence on protecting your business.

Answering Key Business Questions: ???

How do you ensure visibility across your entire cyber landscape?

How do you ensure that security controls are in place on the right assets?

How are you identifying the most important cyber assets to the business?

How are you integrating asset and business context into your remediation prioritization process?
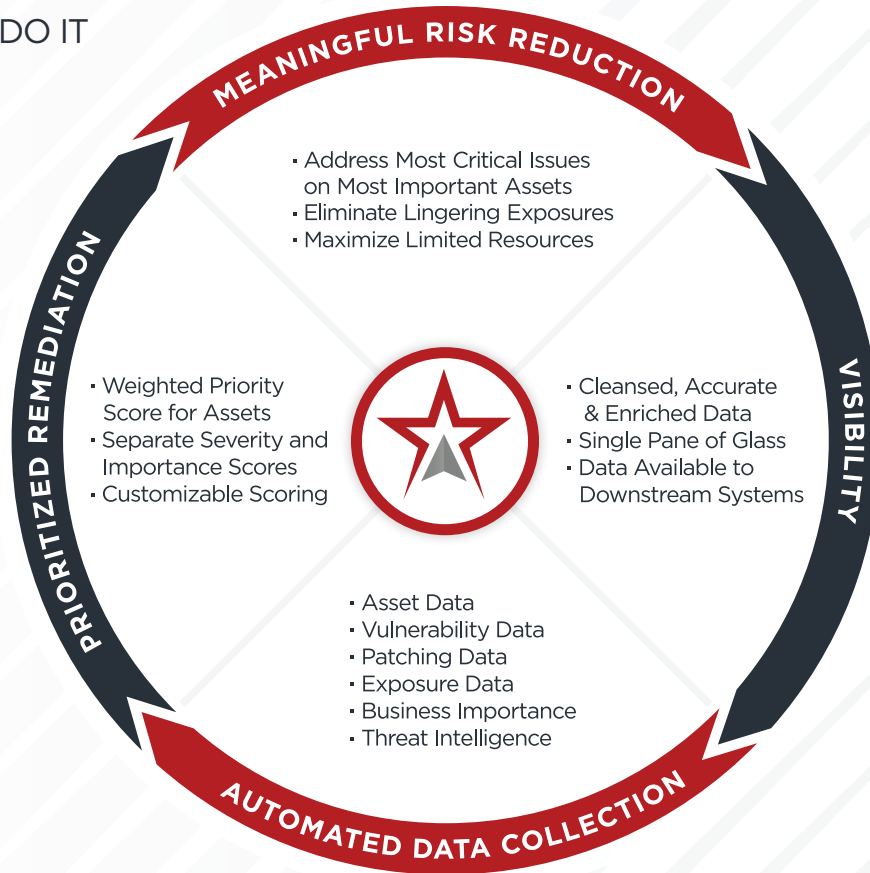
YOUR ASSET UNIVERSE AT YOUR FINGERTIPS

Visualizations and risk metrics are only as good as the data driving them. If the underlying data is incomplete or suspect, the resulting reporting can only be trusted to a limited extent. NorthStar approaches this problem differently by collecting asset information from a wide variety of data sources and ranking the accuracy of each source based on confidence and aging. That information is then compiled into SuperLists, which provide an accurate and comprehensive view of every IT asset - physical, virtual, cloud, software, or container.

After the data is automatically collected, it is then normalized, correlated, and de-duplicated, ensuring that your view of the attack surface is complete, accurate, and timely. NorthStar not only makes the data available for immediate consumption, but can also automatically feed data into other existing solutions to enable automation and overall data hygiene of other solutions like your CMDB or SIEM.

WHAT WE DO
AND HOW WE DO IT

MEANINGFUL RISK REDUCTION
- Address Most Critical Issues on Most Important Assets
- Eliminate Lingering Exposures
- Maximize Limited Resources

VISIBILITY
- Cleansed, Accurate & Enriched Data
- Single Pane of Glass
- Data Available to Downstream Systems

PRIORITIZED REMEDIATION
- Weighted Priority Score for Assets
- Separate Severity and Importance Scores
- Customizable Scoring

AUTOMATED DATA COLLECTION
- Asset Data
- Vulnerability Data
- Patching Data
- Exposure Data
- Business Importance
- Threat Intelligence

GO AGENTLESS

The prospect of adding yet another security agent creates friction, not only with IT, but with asset owners. By pulling directly from existing data sources via API, database queries, or flat files, NorthStar avoids disrupting your business operations. NorthStar's data ingestion capabilities were designed with flexibility as a core capability, ensuring that we can make the most of your existing data resources on day one - without waiting for a vendor to build a new plug-in.

KNOW WHAT YOU DON'T KNOW

Since NorthStar collects and analyzes data from many sources, it automatically tells you where you are missing security tools or key configurations. The ability to quickly define the characteristics of in-scope devices ensures that you are not chasing 'false flags' while enabling speedy identification of basic issues that are unnecessarily increasing your attack surface. The absence of multiple security tools will often indicate the presence of shadow-IT, which NorthStar will optionally identify based on the criteria that you specify. Not all problems are equal and NorthStar enables you to decide which ones represent the greatest risk to your business.