NORTHSTAR EXPOSURE RISK AND VULNERABILITY NAVIGATOR

NorthStar

The NorthStar Exposure Risk and Vulnerability Navigator is an automated, integrated, data-driven platform that helps you prioritize and remediate the cyber risks that matter most to your business.

IT’S A MATTER OF PRIORITIES

Regardless of size, organizations are struggling with the daunting task of vulnerability risk management. According to Gartner, the average time to exploit from time of disclosure has dropped from 25 days to roughly 8 days in the last two years. In addition, the OWASP Top 10 Vulnerabilities, which are often ranked medium, made up about 40% of all vulnerabilities in the last decade.

Organizations don’t have enough time or people power to address every issue that gets identified,and remediation efforts are being held back by manual processes and a disconnected vulnerability response process that compromises their ability to protect the organizations in a timely manner. But how do you decide which issues need to be addressed first?

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 that the most important things are remediated first?

How do you ensure your limited resources are focused on the right areas?

How are you addressing the gaps and discrepancies that exist between vulnerability assessment and patch management?

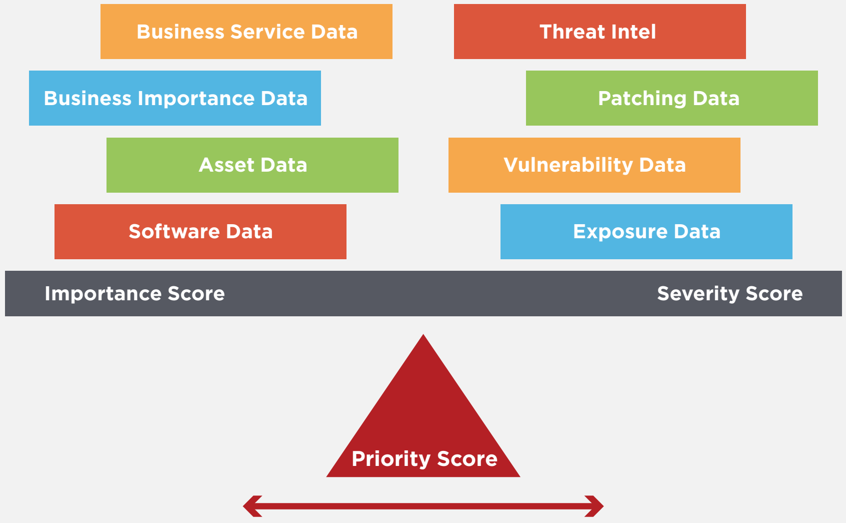
How do you ensure you have accurate and complete data you can trust?

DISRUPTING LEGACY VULNERABILITY MANAGEMENT PRACTICES

The concept of remediating based on consequence is not entirely new, but NorthStar’s approach is - we score business importance separate from technical severity to help you understand and prioritize your exposure risk based on overall business impact.

We understand no organization is the same. So, in addition to out-of-the-box attributes, NorthStar allows you to determine custom attributes and their weight toward the overall score, so you get a custom-tailored view of risk to your business. Leveraging metrics and data the business has already established, NorthStar consumes existing business data into a bespoke scoring model that reflects what matters most to your business and creates the foundation for prioritizing exposure remediation.

Additionally, NorthStar allows for high level adjustment of the scoring model based on your tolerance for technical or business risk. We believe that in order for you to trust a risk score...you should not only have transparency into how it was calculated but have the control to adjust the model to fit your unique environment and requirements.



The risk calculator allows you to customize how different factors affect the risk and priority scores of assets. How do you want to drive prioritization – more by the technical severity of the vulnerabilities or more by the importance of the asset? How much should each of your importance weights count towards the overall importance of an asset? You define the importance categories, you define the weights – all from easy to manipulate sliders:

IT’S NOT ROCKET SCIENCE

Accurate decisions require accurate data. NorthStar intelligently pulls data from your existing sources and cleans/correlates/ranks the accuracy of each source based on confidence and aging. That information is then pulled into SuperLists, providing an accurate and comprehensive view of every asset and business application.

With the complete asset inventory delivered through NorthStar’s SuperLists, the vulnerability management “problem” can be solved! Since NorthStar consolidates all IT-related data under one roof, the days of console-hopping and Excel-aggregation are over. Vulnerabilities, missing patches, device misconfiguration data, and security tool data layered with separate technical severity and business importance scores can now be viewed in a single platform.

As your environment changes, NorthStar remains constant and tracks those changes. You don’t have to set it at the individual asset level. NorthStar has application grouping so you can set it once and the rules are applied to any new device or application.

BRIDGING THE GAP BETWEEN IT SECURITY AND IT OPERATIONS

The visibility gap between IT Security and IT Operations has historically been a challenge for both teams. IT Security is tasked with the responsibility of creating a strategic vision for mitigating risk to the business through the creation and enforcement of standards and policies. However, IT Operations sometimes struggles to get their hands on the relevant information and context required for proper and timely remediation.

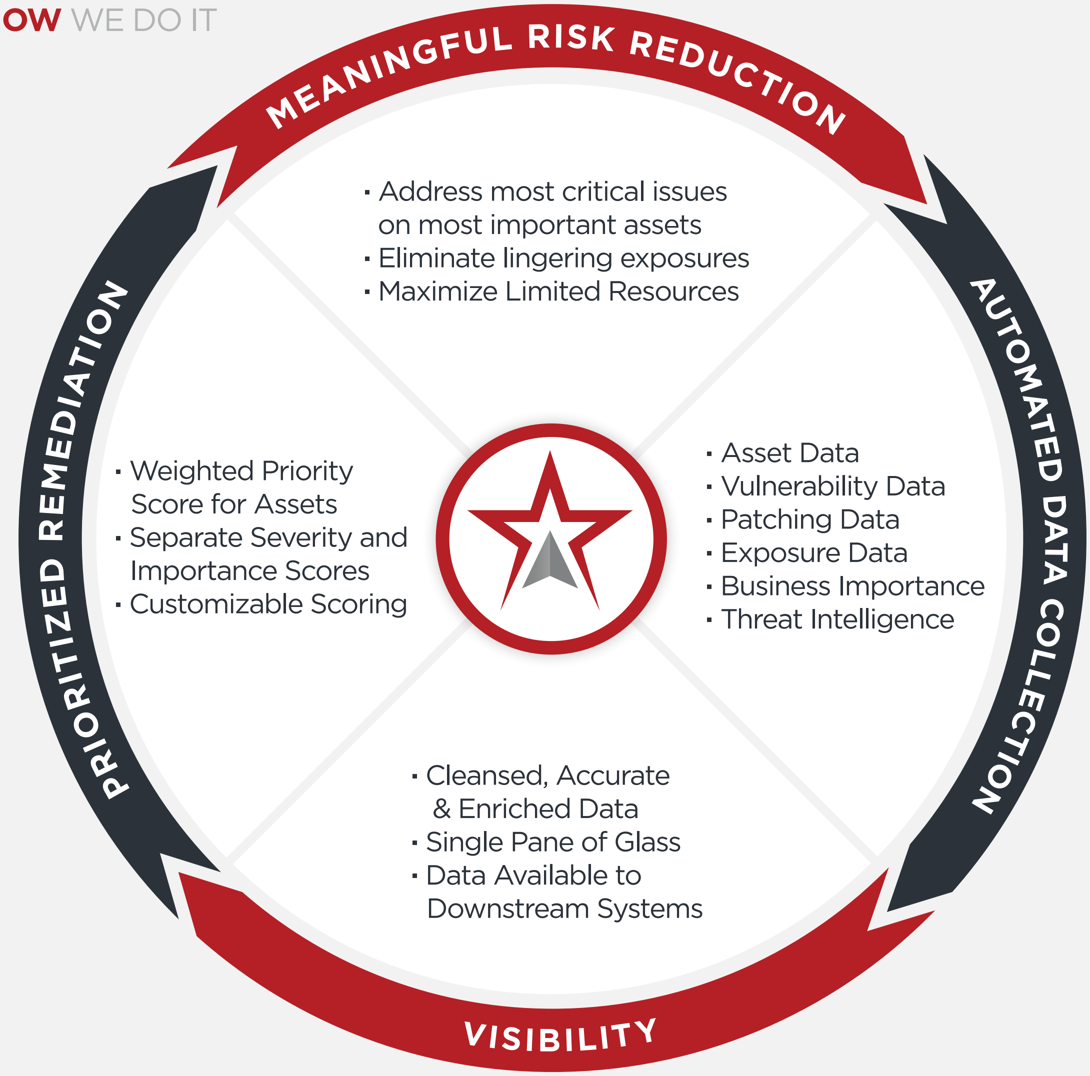
NorthStar helps break down these silos and empowers both teams to effectively work together towards the common goal of protecting the business. Through the aggregation of data from all IT security and relevant IT tools, NorthStar automatically normalizes, applies context, and intelligently handles conflicts in data. By associating CVE ID with patch ID and other remediation options, NorthStar reduces the visibility gap by translating risk into a common language for both the vulnerability management and patch management teams, effectively streamlining the remediation process.

NAVIGATE YOUR OWN CYBER (RISK) SPACE

Different things are important to different people. No one outside of your organization, third-party intelligence feed, AI, or machine-learning algorithm is ever going to be able to accurately define what's most important to your business.

NorthStar does not force you into a scoring model that you don't understand; it is built on a data-driven approach that offers the flexibility required to ensure that organizations are able to prioritize what matters the most to their business. Organizations need to understand the underlying data that is driving any all scores and dashboards. NorthStar's commitment to 'showing our work' offers visibility and transparency into the scoring model thereby fostering trust in leadership, management, and technical teams that they're operating on a common model towards a common goal.

WHAT WE DO
AND **HOW** WE DO IT



- Address most critical issues on most important assets
- Eliminate lingering exposures
- Maximize Limited Resources

- Asset Data
- Vulnerability Data
- Patching Data
- Exposure Data
- Business Importance
- Threat Intelligence

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

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

KEY BENEFITS

Prioritize vulnerability and exposure remediation based off of risk to YOUR business

- Gain key insight into the business importance of individual assets and business services
- Leverage the flexibility to decide what business and technical factors are most important to your organization
- Provide visibility into exposures beyond vulnerabilities, such as coverage gaps and misconfigurations across security tooling and compensating controls

Address the visibility gap that inherently exists between IT Security and IT Operations

- Provide automated correlation of vulnerability and patch information
- Accelerate remediation efforts by integrating with IT Management and Service Desk systems
- Provide valuable insights to IT incident response teams before, during, and after IT-related security events

Provide simple, powerful, and dynamic reporting

- Validate that the most important issues have been remediated
- Slice and dice dashboards and reports that fit the needs of your organization by line of business, location, business services, etc.
- Deliver out of the box dashboards, and easily customizable dashboards configured through the front-end UI
- Enforce robust role-based access control and dataset security

Provide a complete and accurate inventory of all devices and all exposures

- Gain visibility into the variety, severity, and age of exposures existing in their environments
- Enrich existing asset inventory and management systems with relevant business and data classifications
- Assist in data hygiene efforts to accurately map the complex relationships between assets and business services

NorthStar | KNOW WHAT YOU'RE PROTECTING