NorthStar

THE NEXT STEP

FACTORING BUSINESS RISK INTO VULNERABILITY MANAGEMENT

Traditional Vulnerability Management tools have long relied on industry recognized severity ratings to help classify and prioritize vulnerabilities.

By focusing on technical severity, organizations were prioritizing their remediation efforts by eliminating the most severe issues first. While this provided a rudimentary framework for vulnerability remediation, numerous issues emerged as asset counts and data volumes dramatically increased. The NorthStar Exposure Risk and Vulnerability Navigator was designed to improve current Vulnerability Management and remediation processes in two key areas:

The focus on CVE identified vulnerabilities is too narrow to adequately express and in turn, respond to the current threat landscape. Vulnerability teams and products should broaden their focus to address *all* exposures: vulnerabilities, missing patches, and misconfigurations on assets and business services.

Understanding the business value and potential consequence associated with an asset or business service cannot be adequately measured on the same scale as vulnerabilities. Measured on its own and independently calculated, business importance can more accurately express both the value and risk associated with an organization's assets and services.

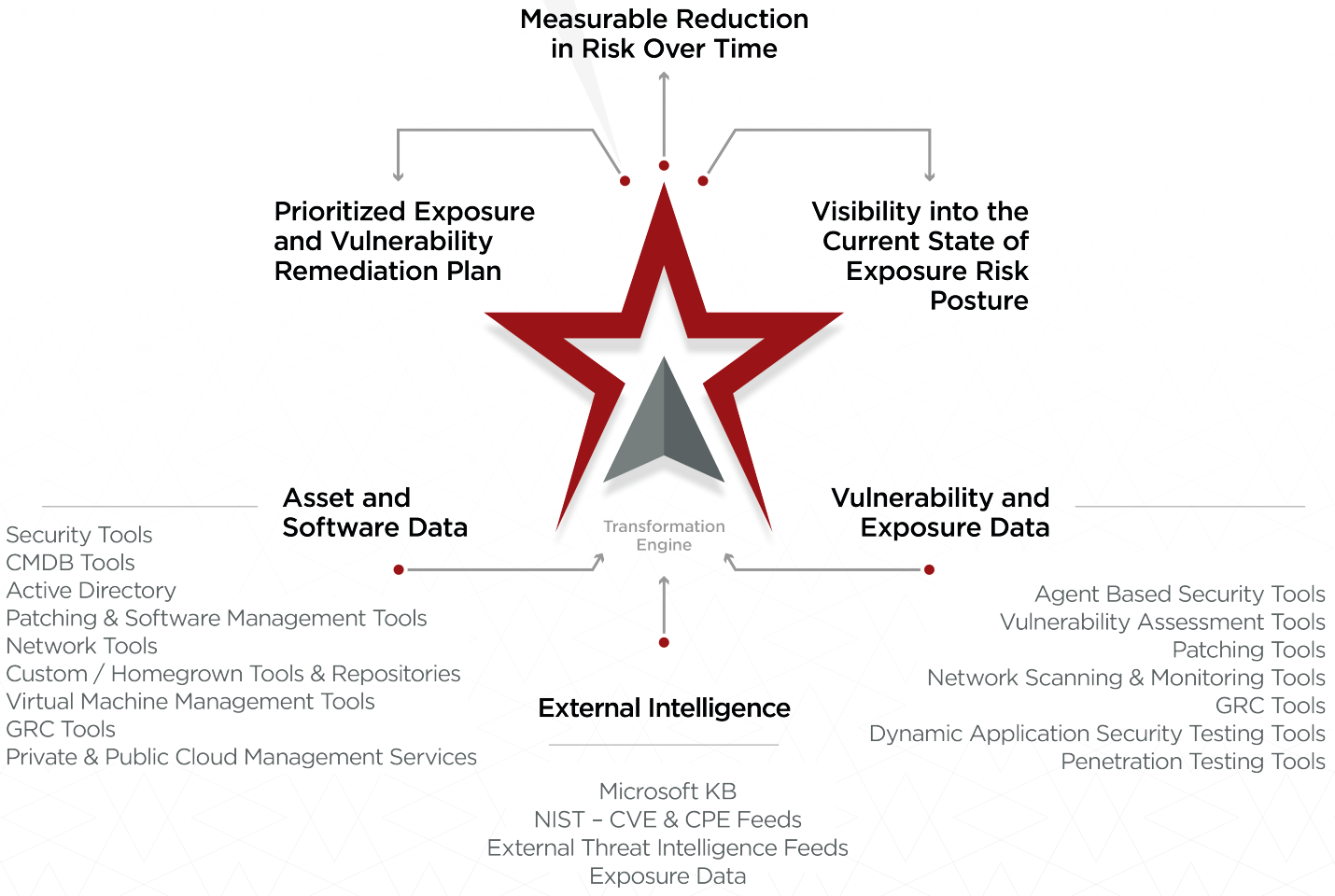
ADDRESSING EXPOSURES
BROADENING THE FOCUS BEYOND VULNERABILITIES

As Vulnerability Management has matured as a process, a standardized taxonomy and language has evolved to satisfy the need for security professionals to formalize the way they describe and talk about vulnerabilities. Growing out of this effort, CVE IDs and CVSS scores soon became the standard for classifying, managing, and remediating vulnerabilities.

As a result, security tools have heavily focused on technical severity ratings and external threat intelligence to enrich vulnerability data enabling organizations to begin basic prioritization of remediation efforts. This focus on technical severity has dominated the Vulnerability Management market and thought leadership for many years.

NorthStar is the next evolution of Vulnerability Management. It widens visibility beyond traditional vulnerabilities to include additional critical aspects of risk management and remediation. NorthStar enables vulnerabilities to be categorized as a subset of the larger family of exposures.

Common exposure categories may include traditional vulnerabilities, missing OS and application patches, missing or misconfigured common tooling, and misconfigurations of system and security settings. Each of these categories represent a uniquely important and measurable impact on the attack surface and subsequent risk related to an asset that cannot be adequately expressed in the current lexicon of Vulnerability Management.



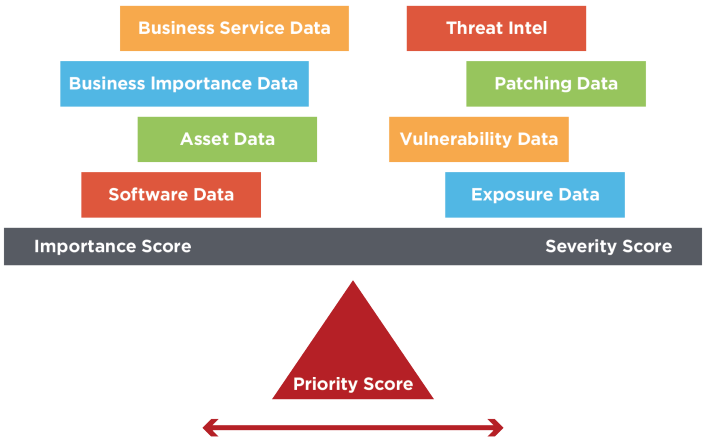
UNDERSTANDING BUSINESS IMPORTANCE OF DEVICES AS AN INDEPENDENT COMPONENT OF RISK

The second challenge with the current state of Vulnerability Management is the encapsulation of business importance into the technical severity model. NorthStar was built on the premise that the technical severity of exposures present on any given asset and the business importance of that asset are fundamentally different in a few distinct ways.

Vulnerabilities		Business Importance
Vulnerabilities have inherent qualities that are present irrespective to the specific asset or organization in which that asset is operating. The language and scales used to measure technical severity were developed precisely for common understanding and classification.	VS	**The business importance of an asset is unique** with respect to its purpose and context to the organization. The idea of importance classification is, at its core, subjective and based on the needs and goals of the organization.
IT Operations and Security teams can have an identifiable and measurable impact on the aggregate technical severity ratings of assets. Through remediation efforts and the deployment of compensating controls, these teams impact the aggregate technical severity ratings by simply eliminating or reducing risks associated with known exposures.	VS	**Business importance typically cannot be adjusted** or remedied by IT Operations or Security. Both the business function of assets and services and their associated risks are typically driven or controlled by application and business leadership and are independent of technical controls and/or adjustments.

Because of these distinctions, **NorthStar was designed to address business importance as a separate calculated score to better reflect the risk landscape and the dynamic relationship that exists between technical severity and business importance.**

By leveraging these interrelated concepts and scoring, NorthStar can provide the necessary context for asset and service level risk identification and, more importantly, the prioritization of remediation on the most critical assets and business services.



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

NorthStar

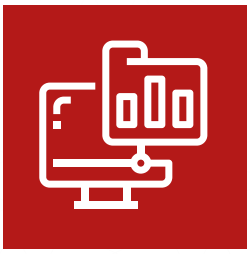
EMPOWERING REMEDIATION THROUGH CONTEXT

With NorthStar, remediation efforts can be driven in ways that best reflect the available resources and risk appetite of the organization. NorthStar uses the Severity scores and Importance scores to calculate a weighted average called a Priority score.

Priority scores allow an organization to create a list of the most vulnerable AND the most important assets. Therefore limited resources can be prioritized effectively during their remediation efforts. A key differentiator is how NorthStar empowers organizations to decide what business and technical factors are most important to them when deciding on the final Priority calculations and weightings.

NORTHSTAR DELIVERS
A SINGLE SOURCE OF TRUTH

NorthStar's automated and agentless data aggregation enables correlation, normalization, and consolidation of asset state data without any additional scanning. This collected data is cleansed, enriched, and consolidated through our Transformation Engine and can be leveraged by many different aspects of the organization because of its superior accuracy, context, and comprehensiveness.



NORTHSTAR DELIVERS
SIMPLIFIED AND FASTER DATA INTEGRATIONS

Simplifying the process of integrating data sources was a key design focus of NorthStar. Engineered completely vendor agnostic, NorthStar simplifies the integration process by pushing the configuration entirely to the front-end web UI. Whether the data exists in a simple spreadsheet, database, or through an API, NorthStar facilitates data connector configuration without the need for a developer's skill set or lengthy enhancement requests through a vendor.

NORTHSTAR DELIVERS
COMPLETELY CUSTOMIZABLE SCORING

Designed to adapt to every customer's risk landscape, NorthStar's Priority Scoring is completely customizable and flexible enough to ensure that only the most important factors for each customer affect the overall scoring.

NorthStar's data model allows for the addition of organization-specific exposures and the adjustment of attributes that contribute individually to the Severity and Importance scores as well as the resultant Priority scores for assets and services. The freedom and transparency of NorthStar's flexible scoring model allows organizations to adjust the overall scoring to better reflect their business needs and risk appetite.

Customers leverage NorthStar to:

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

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 betweeen assets and business services

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.
- **Delivers out of the box dashboards,** and easily customizable dashboards configured through the front-end UI
- **Enforce robust role** based access control and dataset security

NorthStar | NAVIGATOR

NorthStar
516 N. Ogden Ave Suite 115
Chicago, IL 60642
Give us a call
312.421.3270
Send us an email:
connect@northstar.io
For more info, visit us at:
www.northstar.io