Risk-Based Vulnerability Management through CMDB and ITSM Integration

NorthStar.io

Improve asset data quality for better risk management on your journey towards a comprehensive Cyber Theat Exposure Management (CTEM) program

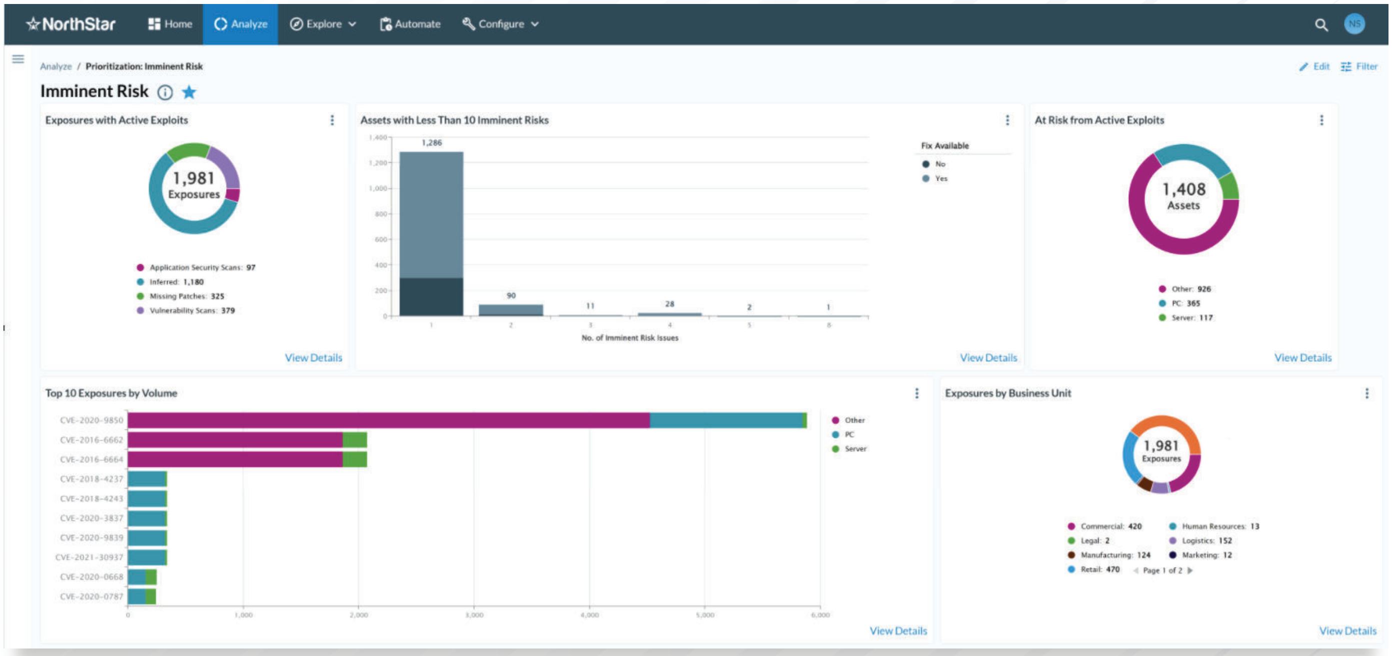
VISIBILITY IS CRITICAL

As the world of vulnerability management continues to mature, managing vulnerabilities and maintaining accurate asset data remains a persistent challenge.

Organizations still rely on IT service management (ITSM) and Configuration Management Database (CMDB) systems to keep track of assets and issues, and these systems regularly suffer from data inaccuracies, manual processes, and slow remediation times.

In fact, up to 40% of CMDB data is typically outdated or incorrect, leading to misinformed decisions and inefficient asset management. Similarly, vulnerability remediation processes are often hindered by lengthy ticketing workflows, with 60% of organizations reporting delays in addressing critical vulnerabilities due to manual effort.

That's where NorthStar shines...quickly and seamlessly integrating with any ITSM and CMDB platform and providing a bi-directional flow of data between systems. Not only automating ticket creation for high-risk vulnerabilities but also enhancing the accuracy of CMDB data. Through agentless aggregation, normalization, deduplication, and conflict resolution, NorthStar improves asset data quality and context, ensuring that the right assets are tied to the correct vulnerabilities.



By integrating business context - such as asset value, criticality, and operational impact - NorthStar helps organizations prioritize remediation based on risk and business impact. This ensures that critical vulnerabilities affecting high-value assets are addressed first, aligning vulnerability management with broader business objectives.

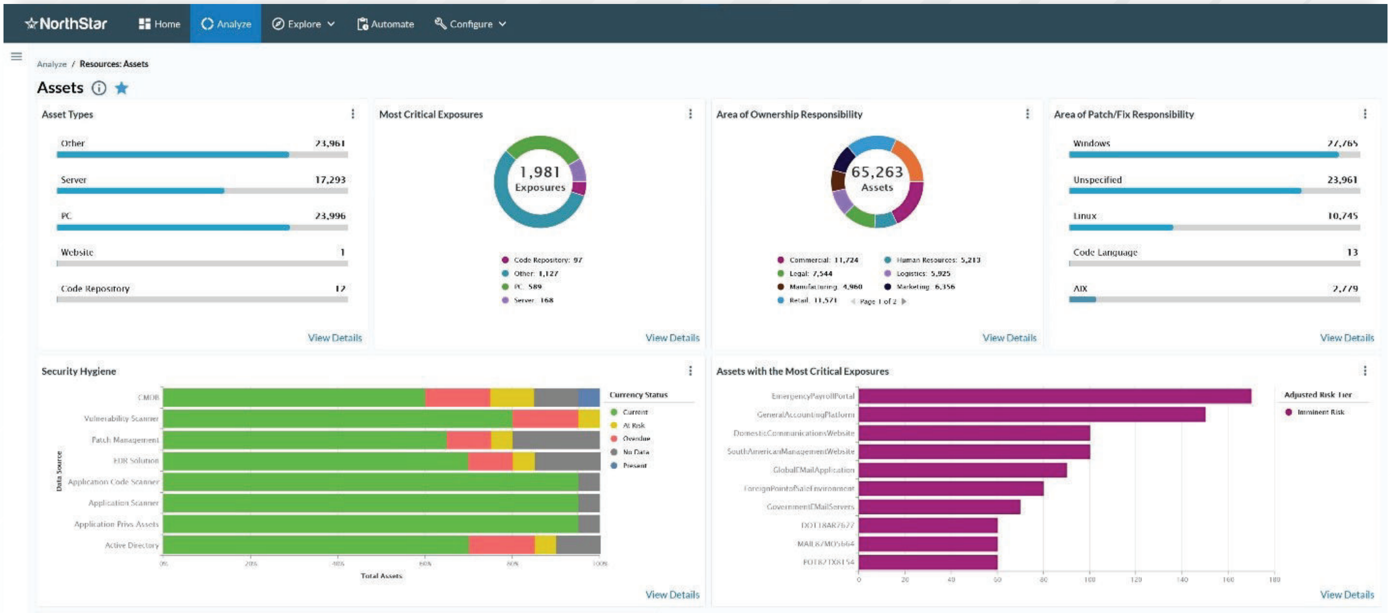
With this approach, NorthStar helps reduce remediation times by up to 60%, increases operational efficiency by 40%, and supports a more strategic and risk-informed response to security threats.

KEY FEATURES

1. **Risk-Based Vulnerability Prioritization:**
   - NorthStar provides a flexible risk-based prioritization model that integrates vulnerability and exposure data, business context and threat intelligence, enabling organizations to prioritize based on their unique standards, policies, and risk tolerance.
   - Integrated with virtually any tool in the ITSM/CMDB space, NorthStar ensures teams focus on vulnerabilities that affect critical assets, aligning remediation efforts with business objectives.
2. **Enhanced CMDB Data Accuracy:**
   - Data in many CMDB platforms can be incomplete or inaccurate due to manual processes, data drift, or inconsistent data sources. NorthStar solves these challenges through agentless aggregation, normalization, deduplication, and conflict resolution.
   - NorthStar enhances the accuracy of asset data within any CMDB system by ensuring that configuration items reflect real-world conditions, improving reliability for vulnerability management and remediation.
3. **Automated Ticket Creation:**
   - NorthStar integrates seamlessly with ITSM platforms to automate the creation of tickets for vulnerabilities or configuration issues based on prioritized risk. Each ticket is enriched with relevant asset information, details on vulnerabilities and exposures, threat intelligence, and recommended remediation actions.
4. **Ticket Information Ingestion for Enhanced Reporting:**
   - Ticketing information (e.g., ticket ID, status, and other key details) from ITSM platforms is ingested back into NorthStar, enabling organizations to track progress and manage decision-making more effectively.
   - This two-way data flow allows for comprehensive reporting on remediation timelines and operational performance.
5. **Efficient Asset and Configuration Synchronization:**
   - NorthStar's integration ensures that vulnerability data is correctly mapped to configuration items within any CMDB platform.
   - Synchronizing asset information across systems maintains up-to-date inventories, helping organizations make more informed decisions on prioritization and remediation.

BENEFITS

- **Enhanced CMDB Data Integrity:** NorthStar's data aggregation, normalization, and deduplication processes improve the accuracy of asset data within any CMDB platform, ensuring a more reliable foundation for managing vulnerabilities and configuration changes.



- **Holistic Reporting and Decision Making:** By ingesting ticketing information from multiple ITSM platforms, NorthStar delivers end-to-end visibility into remediation workflows. This comprehensive view of ticket statuses and progress helps teams make more informed decisions and optimize operational performance.

- **Focused Remediation Efforts:** NorthStar's risk-based vulnerability prioritization ensures that the most critical vulnerabilities are addressed first, minimizing the impact on essential business systems and reducing overall risk.

- **Streamlined Operations:** Automating ticket creation across ITSM platforms reduces manual processes, freeing resources for higher-priority tasks and speeding up vulnerability remediation.

- **Improved Visibility:** The integration with any ITSM and CMDB platform provides a centralized view of IT assets, vulnerabilities, and ticketing information, making it easier to track remediation efforts and align them with business and security objectives.

- **Enhanced Compliance and Governance:** NorthStar's integration with ITSM and CMDB sytems ensures compliance with internal governance policies and regulatory frameworks, as remediation is prioritized and tracked based on risk.

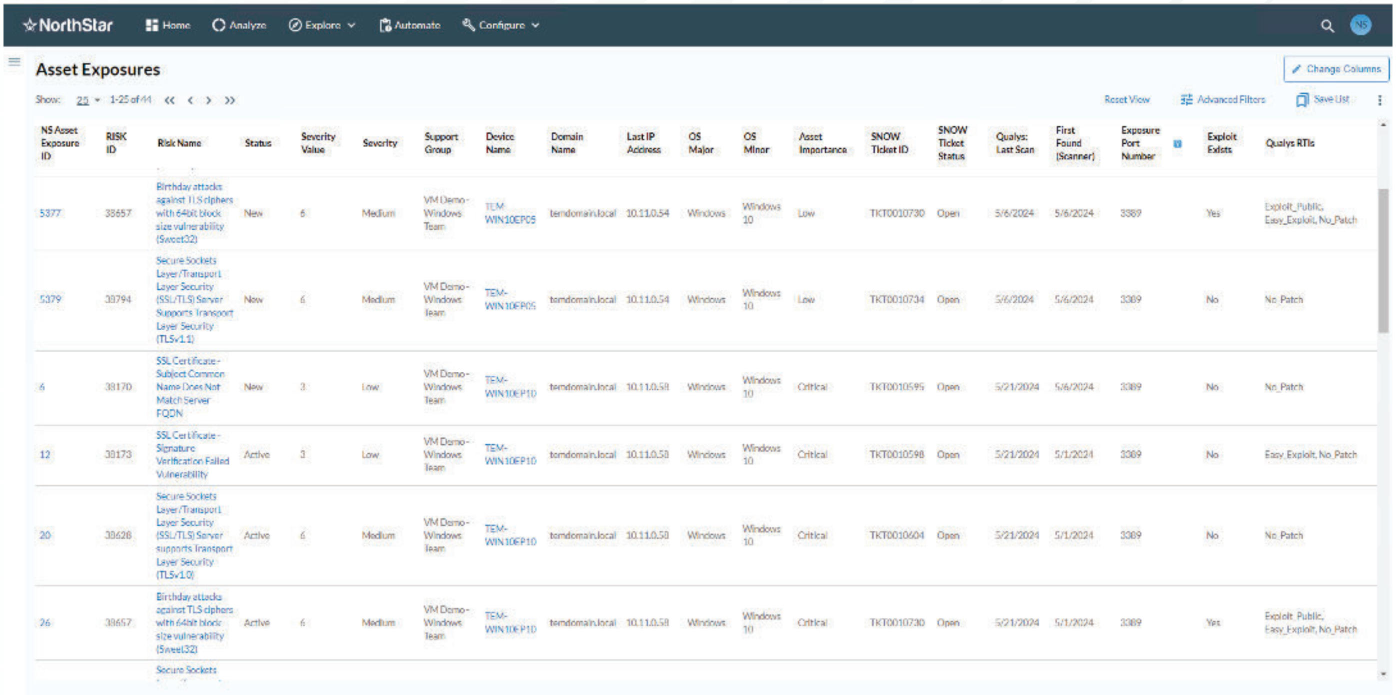
NorthStar | KNOW WHAT YOU'RE PROTECTING

USE CASES

1. **Automated Vulnerability Ticketing:** When NorthStar identifies a high-risk vulnerability, it automatically creates a ticket in any integrated ITSM system. The ticket includes comprehensive details about the vulnerability, affected assets, and recommended remediation actions.

2. **Ingesting Ticket Data for Better Tracking:** As ITSM tickets are created and updated, NorthStar ingests critical ticketing information such as ticket ID and status, providing security teams with visibility into the remediation process and helping track progress across all consolidated vulnerabilities and exposures.

3. **Enhanced CMDB Data:** NorthStar aggregates data from multiple sources, resolving inconsistencies and normalizing information to improve the accuracy of any integrated CMDB platform. This ensures IT remediation and IT security teams have a current, reliable asset inventory for managing vulnerability remediation.



Asset Exposures

Show: 25 1-25 of 44

NS Asset Exposure ID	RISK ID	Risk Name	Status	Severity Value	Severity	Support Group	Device Name	Domain Name	Last IP Address	OS Major	OS Minor	Asset Importance	SNOW Ticket ID	SNOW Ticket Status	Qualys: Last Scan	First Found (Scanner)	Exposure Port Number	Exploit Exists	Qualys RTIs
5377	38657	Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)	New	6	Medium	VM Demo-Windows Team	TEM-WIN10EP05	temdomain.local	10.11.0.54	Windows	Windows 10	Low	TKT0010730	Open	5/6/2024	5/6/2024	3389	Yes	Exploit_Public, Easy_Exploit, No_Patch
5379	38794	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1)	New	6	Medium	VM Demo-Windows Team	TEM-WIN10EP05	temdomain.local	10.11.0.54	Windows	Windows 10	Low	TKT0010734	Open	5/6/2024	5/6/2024	3389	No	No_Patch
6	38170	SSL Certificate - Subject Common Name Does Not Match Server FQDN	New	3	Low	VM Demo-Windows Team	TEM-WIN10EP10	temdomain.local	10.11.0.58	Windows	Windows 10	Critical	TKT0010595	Open	5/21/2024	5/6/2024	3389	No	No_Patch
12	38173	SSL Certificate - Signature Verification Failed Vulnerability	Active	3	Low	VM Demo-Windows Team	TEM-WIN10EP10	temdomain.local	10.11.0.58	Windows	Windows 10	Critical	TKT0010598	Open	5/21/2024	5/1/2024	3389	No	Easy_Exploit, No_Patch
20	38628	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)	Active	6	Medium	VM Demo-Windows Team	TEM-WIN10EP10	temdomain.local	10.11.0.58	Windows	Windows 10	Critical	TKT0010604	Open	5/21/2024	5/1/2024	3389	No	No_Patch
26	38657	Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)	Active	6	Medium	VM Demo-Windows Team	TEM-WIN10EP10	temdomain.local	10.11.0.58	Windows	Windows 10	Critical	TKT0010730	Open	5/21/2024	5/1/2024	3389	Yes	Exploit_Public, Easy_Exploit, No_Patch
		Secure Sockets																	

TECHNICAL SPECIFICATIONS

- **Integration Method:** Configuration based mapping through API, Database Import, and/or flat file ingestion.
- **Supported Platforms:** Cloud and On-Premise
- **Data Flow:** Two-way synchronization of vulnerability data, ticketing information, and asset updates between NorthStar and ITSM/CMDB platforms
- **Scalability:** Supports Large Enterprise environments