Cyber Risk Context Technology™

The Data Science Behind Kenna Security's Risk-Based Vulnerability Management Platform

Top Vulnerability and Exploit Statistics

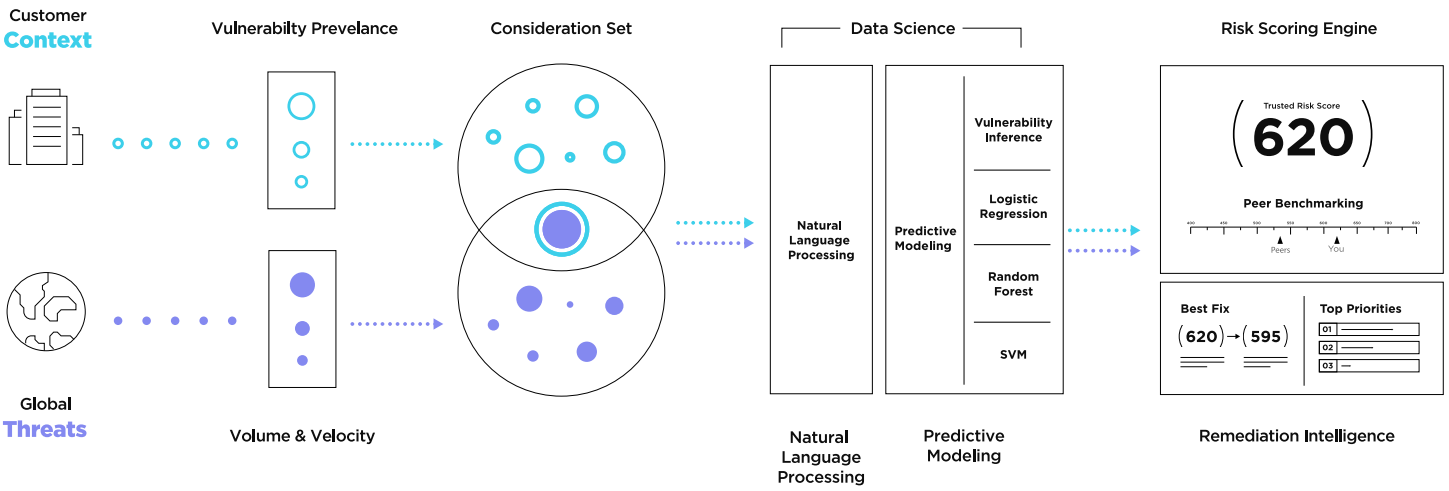
- 23% of published vulnerabilities have associated exploit code
- 2% of published vulnerabilities have observed exploits in the wild
- The chance of a vulnerability being exploited in the wild is 7 times higher when exploit code exists
- 50% of exploits publish within two weeks surrounding new vulnerabilities
- 13% of exploits emerge a month or more after vulnerabilities are published. Only 1% emerge beyond 1 year
- The volume of exploitation detections jumps five-fold upon release of exploit code

"Kenna Security and the Cyentia Institute, Prioritization to Prediction, Volume 1: Analyzing Vulnerability Remediation Strategies"

Imagine a set of technologies built from the ground up on a data science foundation that is designed to look outside the organization to analyze and understand the volume and velocity of attacker activity, combine that data with extensive internal data sources, employ predictive modeling and other data science techniques to generate actionable risk scores, and efficiently guide the user in reducing their organization's vulnerability risk.

We call this overarching set of technologies Cyber Risk Context Technology™, and it's at the heart of the Kenna Security Platform.

How it works



Cyber Risk Context Technology can be broken down into four major, highly coupled areas that work closely together to provide the user with an optimized risk reduction process. These four areas are: Data Analysis, Data Science, Risk Scoring, and Remediation Intelligence.

Comprehensive Data Analysis

The Kenna Security Platform ingests, aggregates, and processes tens of billions of pieces of data, from more than 55 sources, including more than 15 threat and exploit intelligence feeds, and then automates the analysis of this data using our proven data science algorithms to deliver an accurate, granular, and quantifiable risk score for every vulnerability within seconds.

To understand what attackers are doing in real time and evaluate which vulnerabilities are likely to pose a threat to the organization's specific environment, we analyze the following internal and external data sources:

Ground Truth Telemetry

- 15+ sources of exploit intelligence
- 15+ billion security events
- Global attack telemetry
- Remediation intelligence
- 3+ billion managed vulnerabilities

Internal Security Data Sources

- Any vulnerability scanner
- Asset- and network-specific data from configuration management database (CMDB) tools
- Penetration testing
- Bug bounty programs
- Static application testing
- Dynamic application testing
- Open source tools
- Custom data sources in JSON format

Exploit Intelligence:

- Metasploit
- Exploit DB
- ReversingLabs
- Secureworks CTU
- Black Hat Kits on rotation (AlphaPack, Blackhole, Phoenix, more)
- Proofpoint
- Exploit DB
- Proofpoint
- Secureworks CTU

Threat Intelligence:

- AlienVault OTX
- AlienVault Reputation
- Secureworks CTU
- Emerging Threats
- ReversingLabs
- Exodus Intelligence
- Sans Internet Storm Centre
- X-Force Exchange

Kenna uses all of this data to get a full view into the potential impact of each vulnerability, including the volume and velocity of attacker activity, as well as how critical each threat could be given your specific environment, and then translates that context into actionable security intelligence to guide remediation efforts and resource allocation.

Volume and Velocity
We process and analyze threat and exploit data from more than 15 sources to determine the volume and velocity with which attackers are exploiting vulnerabilities in the wild.

Easily Exploitable
We analyze data from all available exploit toolkits in the commercial space and dark web to determine which ones have weaponized capabilities.

Malware Exploitability
We determine which malware strains exploit vulnerabilities as one of the steps in their process and determine the prevalence of that malware.

Zero Day
We analyze all available zero-day information and determine whether a customer is susceptible.

Custom Data Sources
Threat and vulnerability data from sources internal to the organization, like penetration testing and bug bounty program data can be ingested, aggregated, and correlated to augment the extensive set of external threat and vulnerability data we collect.

Vulnerability Prevalence
We analyze Kenna's managed vulnerability database to identify the top 5% of all vulnerabilities that have been exploited over the past six months, and compare it with your vulnerabilities to determine which are most likely to be exploited.

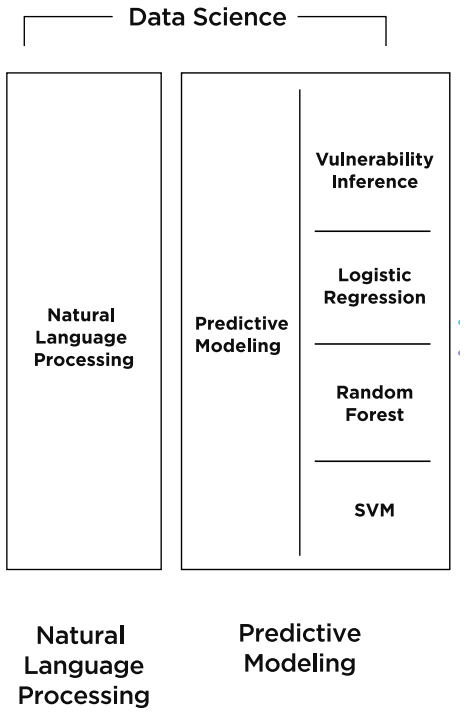
Data Science for Risk-Based Vulnerability Management

Kenna uses proven data science techniques, including machine learning, natural language processing, and predictive modeling to assess, prioritize, and even predict risk. By harnessing the power of data science, Kenna dynamically calculates the risk of each vulnerability to enable security and IT teams to finally embrace predictive vulnerability management.

Using predictive modeling, Kenna can calculate the risk of a vulnerability as soon as it is revealed—and long before an exploit can be built. Our predictive modeling forecasts the weaponization of new vulnerabilities with a confirmed 94 percent accuracy rate, and then prioritizes remediation based on the risk of exploitation. This gives your organization the foresight needed to remediate high-risk vulnerabilities before attackers can mount an attack.

Natural language processing investigates social media sites, the dark web, and other places where vulnerabilities are discussed, and extracts the language associated with vulnerabilities to assist in risk assessment. Natural language processing is also used to help score vulnerabilities that do not have a Common Vulnerability Scoring System (CVSS) score by analyzing various text key words and phrases that are shown to be high indicators of risk.

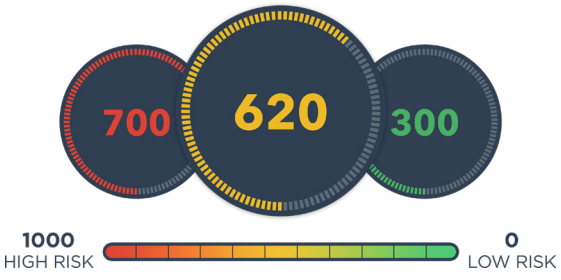
We then analyze the data using a number of predictive technologies, including SVM (support-vector machines), random forest, logistic regression, and vulnerability inference. The data from our predictive models is then used by our risk scoring engine to produce an actionable risk score for every vulnerability.



Actionable Risk Scoring

Leveraging Ground Truth Telemetry and an extensive amount of internal security data, the Kenna Risk Scoring Engine ties into Kenna's predictive model to algorithmically determine risk scores for each unique vulnerability and in concert with asset criticality scores, determines an actionable risk score for each asset and group of assets that ranges from zero (no risk) to 1000 (highest risk).

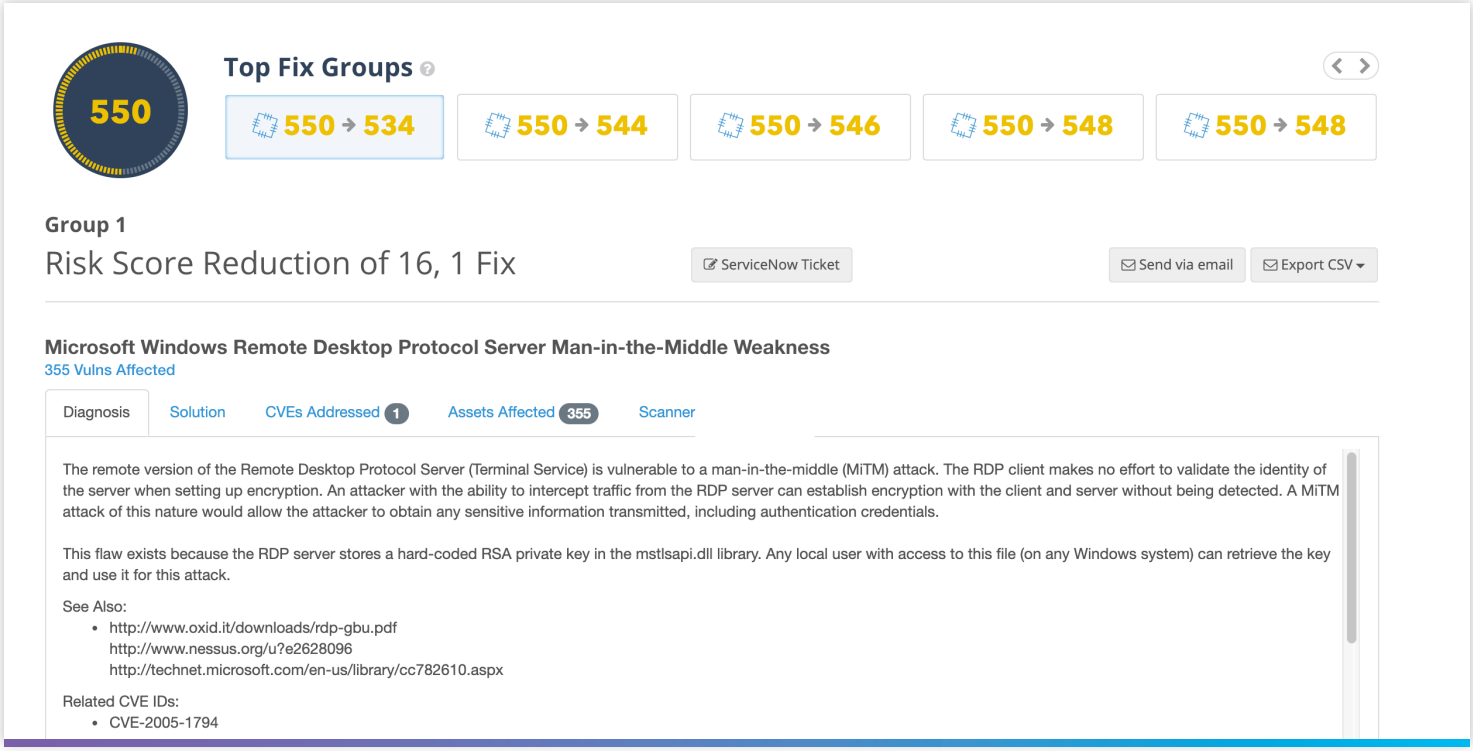
The risk score takes into account all of the internal and external variables that we use in our predictive model that are high indicators of risk. Internal risk calculations factor in the number of instances of each vulnerability in your environment, their potential severity, and the criticality of the assets that are threatened as a result of each vulnerability. External risk calculations factor in the CVSS score of the vulnerability, threat intelligence information such as whether or not an exploit kit is available for the vulnerability, the volume and velocity of exploits that take advantage of the vulnerability, and the prevalence of the vulnerability we are seeing throughout our customer environments. With accurate and quantifiable risk scores, your organization will understand your current risk posture and—more importantly—the actions you can take to reduce the greatest amount of risk.



Remediation Intelligence to Guide the Reduction of Vulnerability Risk

The Kenna Remediation Intelligence Engine prioritizes the vulnerabilities that, if remediated, will have the greatest impact on risk score reduction. The Remediation Intelligence Engine clearly identifies which vulnerabilities should be remediated first and articulates the specific impact each action will have on your organization's risk posture using a mechanism we call "Top Fix Groups". Top Fix Groups are ranked collections of fixes that, when implemented, make the highest impact on reducing the organization's risk posture with the least amount of effort. Top Fix Groups can be used with a ticketing system as part of an optimal workflow process that optimizes vulnerability risk reduction for the organization.

Integration with popular ticketing systems like Remedy, Jira, ServiceNow, and Cherwell ensures that Security and IT teams have the same level of actionable intelligence, and that IT knows what to fix, how to fix it, and why the fix is a priority. The ticketing system integrations are bi-directional in nature, and automated tracking keeps security teams informed and synchronized regarding the progress against all tickets. This tight coupling with ticketing systems saves the IT teams valuable time by promoting close collaboration with security teams, with the common mission of optimizing the organization's risk reduction - as quickly and efficiently as possible.



To learn more about the science behind Kenna visit: www.kennasecurity.com/the-science-behind-kenna

KENNA Security