How Kenna Security Works

A Peek "Under the Hood" of Modern Vulnerability Management

When the first vulnerability scanner appeared on the market, organizations were provided with tangible evidence of security holes in their networks. Since then, many vendors followed suit, and soon organizations would have access to data on weaknesses or flaws within their infrastructure, applications, and eventually, connected devices. It's immensely valuable data, but complications arose as the volume of the data spiraled out of control. Suddenly, an organization might have thousands of vulnerabilities but not nearly enough resources to patch every single one. The question becomes, "How can I possibly patch everything?"

The reality is that you can't patch everything. Most organizations simply do not have the manpower or time to patch every vulnerability identified by their scanner. And even if they had the time, trying to patch everything wouldn't be an efficient use of that time. Why not? Because every vulnerability doesn't result in a breach.

Kenna Security was founded to address this exact problem—to extract the signal from the noise of security data and identify the vulnerabilities that pose real risk to an organization so that it can focus their limited resources. Most security companies create new security data, but Kenna Security helps you make sense of that deluge of data.

Which Vulnerabilities Really Matter?

- 2%-5% of published vulnerabilities have observed exploits in the wild

- 23% of published vulnerabilities have associated exploit code

- The chance of a vulnerability being exploited in the wild is 7 times higher when exploit code exists

- 50% half of exploits are released within two weeks of the CVE publication date

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

Kenna Security and the Cyentia Institute, Prioritization to Prediction - Volume 3: Winning the Remediation Race
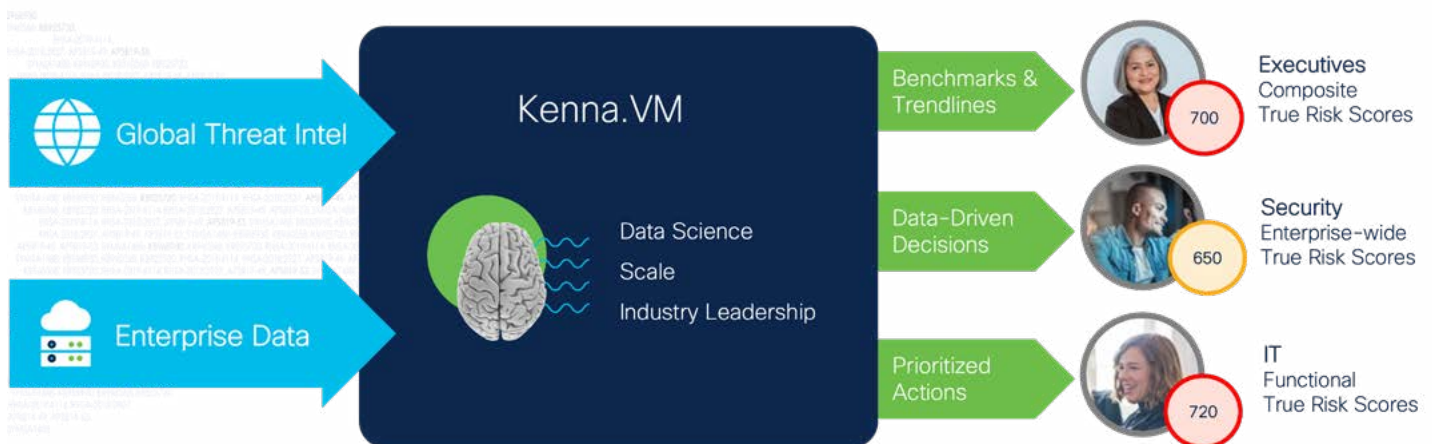
The Right Data Provides the Right Context

The best place to start this conversation is the data that Kenna Security uses to help organizations prioritize their vulnerability remediation efforts. There are two datasets that provide the framework for decision making: 1) enterprise data from every available source across the customer's infrastructure, applications, and the Internet of Things (IoT), and 2) global threat intelligence, which includes custom-curated exploit and threat intelligence feeds. This data is analyzed by 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, Kenna Security analyzes the following internal and external data sources:

Ground Truth Telemetry		Internal Security Data Sources
15+ exploit and threat intelligence feeds 15+ billion security events 7+ billion managed vulnerabilities		• 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:	**Threat Intelligence:**	
• Metasploit • Exploit DB • ReversingLabs • Proofpoint • Secureworks CTU • D2 Elliot • Contagio • Black Hat Kits on rotation (AlphaPack, Blackhole, Phoenix, more)	• 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, 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 intelligence feeds to determine the volume and velocity with which attackers are exploiting vulnerabilities in the wild.

Easily Exploitable

• We analyze data from 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 and determine the prevalence of that malware.

Zero Day

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

Using Data Science to Understand Risk

As we said before, not every vulnerability will result in a breach. The wide range of internal and external data can help us to understand which vulnerabilities are most likely to result in a breach–that is, which vulnerabilities pose a real risk. Kenna Security uses proven data science techniques, including machine learning, natural language processing, and predictive modeling to assess, prioritize, and even predict risk. These approaches allow us to dynamically calculate the risk of every vulnerability to enable security and IT teams to embrace risk-based vulnerability management.

Using predictive modeling, Kenna can calculate the risk of a vulnerability as soon as it is revealed. 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–a branch of artificial intelligence aimed at making sense of "natural" human language–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 keywords and phrases that are shown to be high indicators of risk.

We then analyze the data using a number of predictive technologies, including support-vector machines (SVM), 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.
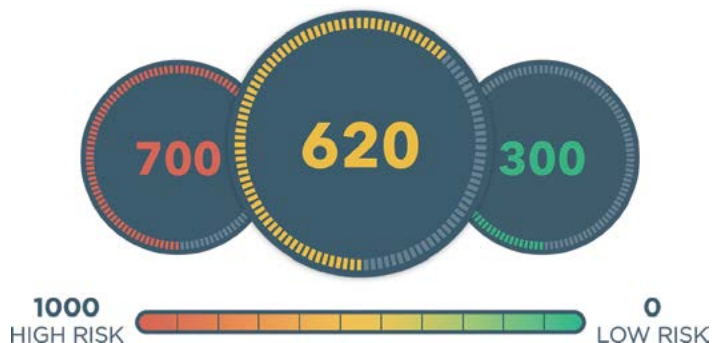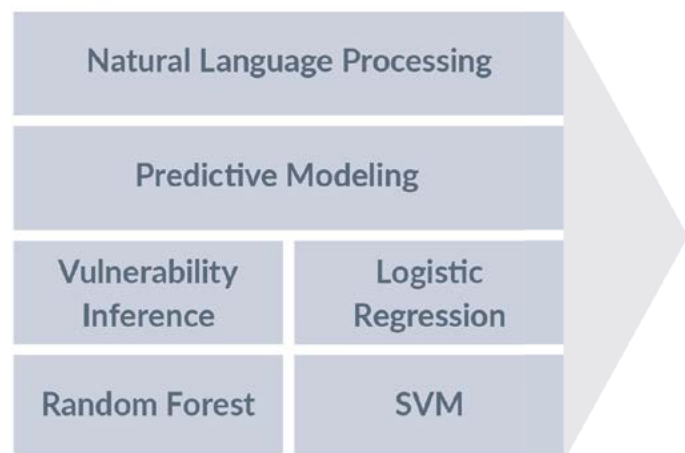
Actionable Risk Scoring

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, you will understand your organizations' current risk posture and identify the actions you can take to reduce the greatest amount of risk.

Data Science

Natural Language Processing	
Predictive Modeling	
Vulnerability Inference	Logistic Regression
Random Forest	SVM

700 620 300

1000
HIGH RISK

0
LOW RISK

Remediation Intelligence to Guide the Reduction of 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.

Thanks to Kenna Security's integration with popular ticketing systems like Remedy, Jira, ServiceNow, and Cherwell, Security and IT teams have the same level of actionable intelligence, and 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.

Top Fix Groups

530

530 → 406 | 530 → 505 | 530 → 526 | 530 → 526 | 530 → 528

Group 1
Risk Score Reduction of 124, 3 Fixes

Remedy incident | ServiceNow Ticket | JIRA issue | Send via email | Export CSV

VNC remote control service installed
271 Vulns Affected

Diagnosis | Solution | CVEs Addressed 0 | Assets Affected 271 | Scanner IDs 1

AT&T Virtual Network Computing (VNC) provides remote users with access to the system it is installed on. If this service is compromised, the user can gain complete control of the system.

Kenna Fix ID: 147830

X.509 Server Certificate Is Invalid/Expired
172 Vulns Affected

Diagnosis | Solution | CVEs Addressed 0 | Assets Affected 172 | Scanner IDs 1

The TLS/SSL server's X.509 certificate either contains a start date in the future or is expired. Please refer to the proof for more details.

Kenna Fix ID: 972028

Weak Cryptographic Key
259 Vulns Affected

Diagnosis | Solution | CVEs Addressed 0 | Assets Affected 259 | Scanner IDs 1

The key length used by a cryptographic algorithm determines the highest security it can offer. Newly discovered theoretical attacks and hardware advances constantly erode this security level over time. Taking this into account, as of 2011, governmental, academic, and private organizations providing guidance on cryptographic security, such as the National Institute of Standards and Technology (NIST), the European Network of Excellence in Cryptology II (ECRYPT II), make the following general recommendations to provide short to medium term security against even the most well-funded attackers (eg. intelligence agencies):

- Symmetric key lengths of at least 80-112 bits.
- Elliptic curve key lengths of at least 160-224 bits.
- RSA key lengths of at least 1248-2048 bits. In particular, the CA/Browser Forum Extended Validation (EV) Guidelines require a minimum key length of 2048 bits. Also, current research shows that factoring a 1024-bit RSA modulus is within practical reach.
- DSA key lengths of at least 2048 bits.

Additionally, starting in 2014, the Certificate Authority/Browser Forum has mandated that 1024-bit RSA keys no longer be supported for SSL certificates or code signing.

Kenna Fix ID: 974713

The Bottom Line

When the rubber meets the road, Kenna Security's approach not only helps reduce and manage risk, but it does so while saving money, resources, and time. Vulnerability management is a notoriously resource-heavy and friction-filled task. Security teams face a tidal wave of data on known vulnerabilities, while IT teams are being crushed by the demand to patch everything. Kenna Security shifts away from this unproductive and taxing status quo to embrace a risk-based approach to vulnerability management that is more appropriate for modern organizations. This approach helps organizations focus on the vulnerabilities that matter, remediate faster, and align the entire business around a common objective. Ultimately, Kenna Security allows you to do more with less.

To learn more about Kenna Security, visit

kennasecurity.com/the-science-behind-kenna