Understanding the Kenna Risk Score

Prioritizing Vulnerabilities with Data Science

For users of vmware Carbon Black

KENNA Security

A part of Cisco.

When you're facing a tidal wave of vulnerabilities within your enterprise, how can you know which ones to remediate first? The most pragmatic approach is to prioritize—enabled by assigning some type of "score" to a vulnerability. There's just one (pretty big) catch: An effective, calibrated mechanism for scoring vulnerabilities is hard to find.

The Signal in the Noise

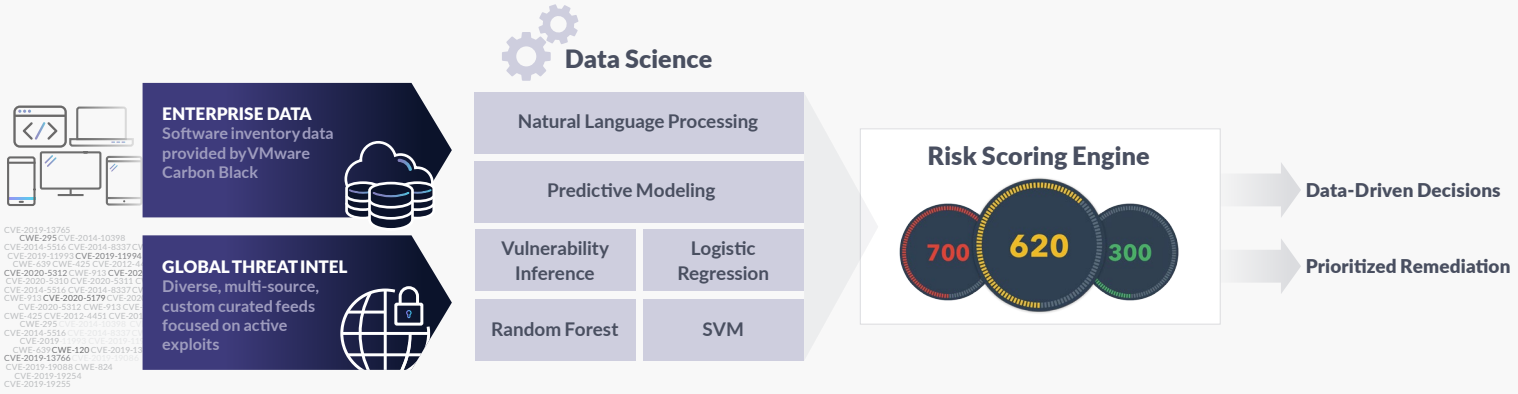
There are a number of different prioritization strategies that enterprises deploy. The most popular one is the Common Vulnerability Scoring System (CVSS), an industry standard for determining the severity of security vulnerabilities. CVSS has laid a foundation for scoring vulnerabilities, but basing your remediation on it can cause problems. For example, if your remediation strategy is CVSS 7+, you would have to remediate nearly half of your vulnerabilities in order to cover all those that are scored as critical. CVSS measures the severity of a given vulnerability, but doesn't take into account what vulnerabilities are actually being exploited in the real world. It's static and it lacks context. It can't tell you what the real risk is that the vulnerability poses. And, ultimately, it prioritizes more vulnerabilities than you'll ever be able to remediate.

Here's what we know: Any given organization, regardless of size, can address about 10% of vulnerabilities in its environment. This means that an effective scoring system has to be able to extract the signal from the noise. It has to successfully prioritize the small subset of vulnerabilities that pose a real risk (the 2-5% of observed vulnerabilities are actually exploited in the wild) and confidently deprioritize vulnerabilities that pose little risk. Instead of being faced with remediating nearly half of your vulnerabilities (like with CVSS 7+), imagine being able to focus your time on that 5% that really matters.

The Kenna Risk Score

A critical piece of the prioritization puzzle is the right context to understand the true level of risk that a vulnerability poses to an organization. Kenna Security's Risk Score—a score you'll be able to find within VMware Carbon Black—ingests and processes billions of data points from internal and external sources, including more than 18 threat and exploit intelligence feeds. Kenna then automates the analysis of this data leveraging proven data science techniques like predictive modeling and machine learning to deliver an accurate risk score for every vulnerability. (Fun fact: several of these methodologies are patented by Kenna!)

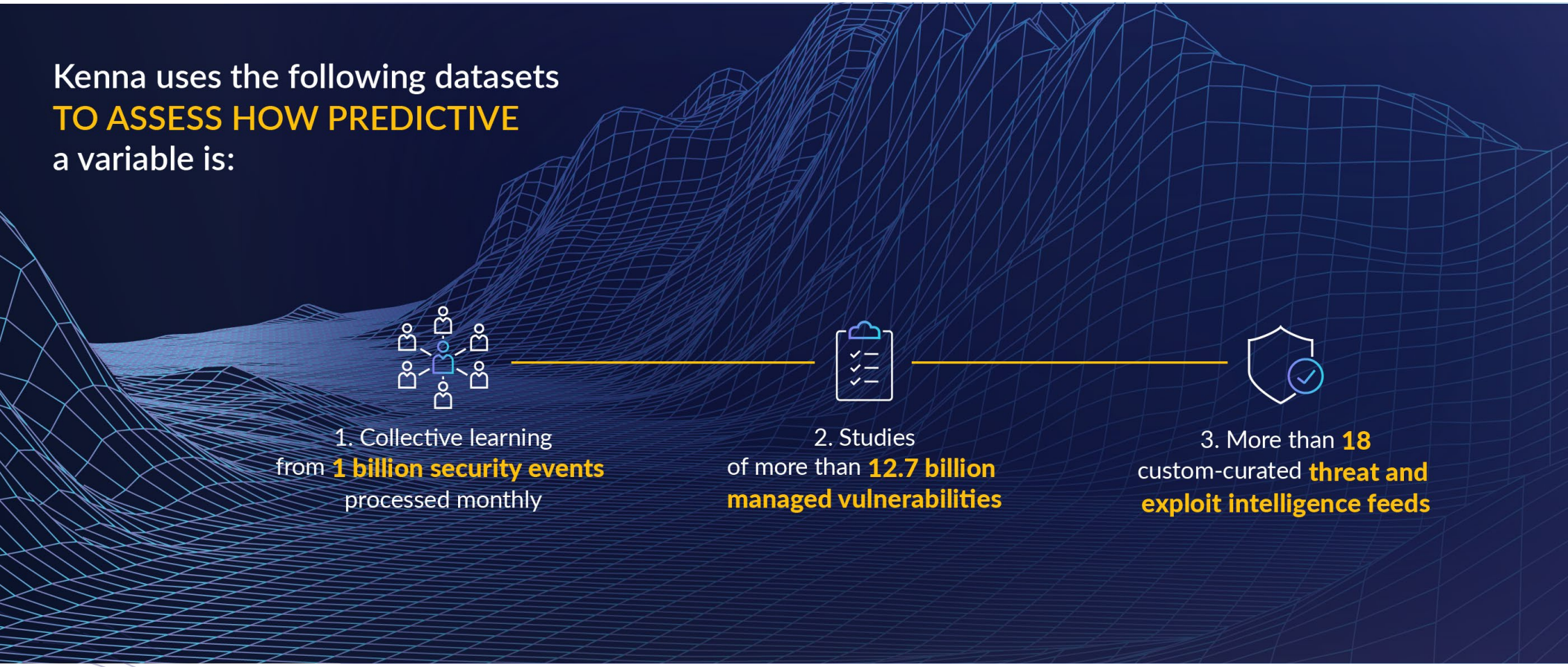
The result is a dynamic scoring method that takes into account the real-world threat landscape and ultimately enables security analysts to understand the real level of risk in their environment and effectively prioritize which vulnerabilities to remediate first.



Kenna uses advanced data science techniques to analyze data from within your organization and external threat and vulnerability data sources and accurately score each vulnerability.

What's Behind Kenna's Model?

The selection of scoring variables is a key component of the modeling process. The Kenna Risk Score takes into account what is happening in real-time, in the wild, for each vulnerability. The score then provides an estimate of the likelihood of exploitation to deliver a rank ordering of the probability of exploitation using that particular attack vector.



Every vuln within VMware Carbon Black Cloud Vulnerability Management is assigned a risk score of between 0.0 (no risk) and 10.0 (maximum risk).

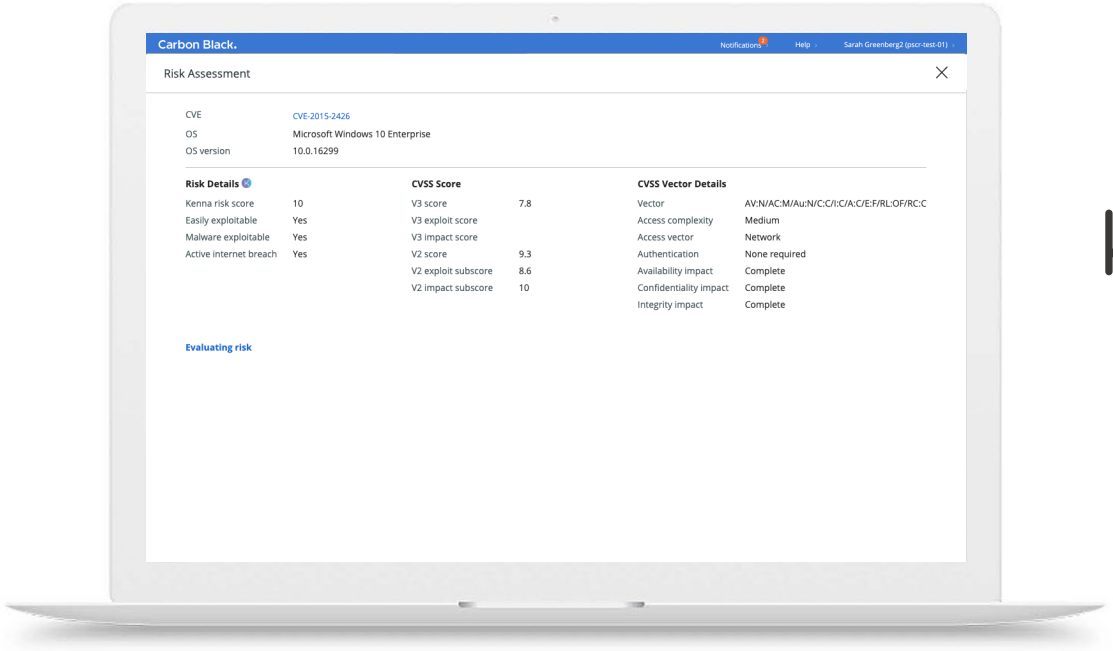
Kenna then uses a combination of vulnerability and threat factors to determine a specific risk score for each vulnerability:

- Predictive (Boolean) classification by a machine learning classifier trained on historical exploit and exploitation data (confirmed 94 percent accuracy rate)
- Availability of an exploit module in a weaponized exploit kit
- Pervasiveness of a vulnerability across disparate client environments
- Presence of a near-real-time exploitation in one or more of the above data sources
- Availability of a recorded exploit in exploit sources
- CVSS points above average
- ...and more.

Risk Scores in VMware Carbon Black

You can find the Kenna Risk Score within VMware Carbon Black Cloud Vulnerability Management for endpoints and workloads. Every vulnerability within these tools—whether they are vulnerabilities in your workload, VM, or endpoint—is assigned a risk score of between 0.0 (no risk) and 10.0 (maximum risk). Note: For those of you who are familiar with the Kenna Risk Score, please note that our typical 0-100 scale is divided by 10 within the VMware Carbon Black Cloud (e.g., a Kenna risk score of 98 will appear in the Carbon Black Cloud console as a score of 9.8).

Not only will you get the Kenna Risk Score, you'll get information to back it up, including whether or not the vulnerability is easily exploitable (Is it included in exploit kits or other public exploit sources?), malware exploitable (Is it actively exploited by malware including worms, trojan horses, and ransomware?), or involved in an active internet breach (Is it being successfully exploited in the wild right now?)



The Kenna Risk Score and details within VMware Carbon Black Cloud Vulnerability Management. A similar view is available for endpoints and workloads within the Carbon Black Cloud console.

KENNA Security
A part of Cisco.

Maximizing the Efficiency and Effectiveness of Your Limited Resources

The Kenna Risk Score helps security, IT, and infrastructure teams efficiently prioritize and proactively manage the vulnerabilities that pose the most risk to the organization. This, in turn, helps maximize the effectiveness of a vulnerability management program while making the most efficient use of limited resources. The integration of the Kenna Risk Score into VMware Carbon Black's platform enables users to determine the most critical vulnerabilities and take action, freeing up resources across the board to focus on more critical projects.

Remember: If everything is a priority, nothing is!

Want to dig deeper into Kenna's approach to vulnerability prioritization? Check out the Prioritization to Prediction research series by the Cyentia Institute and Kenna Security!

To learn more about aligning your organization around risk, visit
www.kennasecurity.com

KENNA Security
A part of Cisco.