SOLUTION BRIEF

Kenna.VM

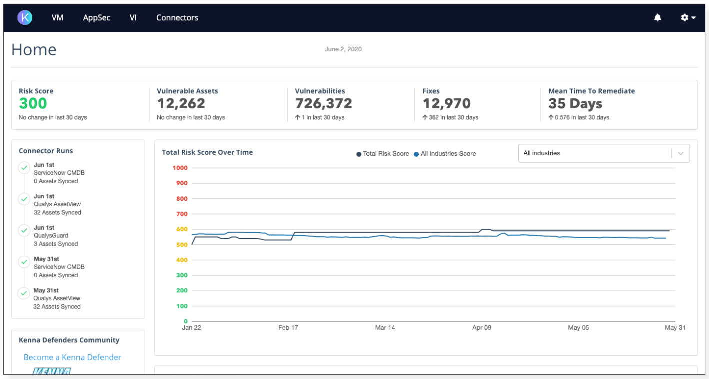
KENNA Security

Kenna.VM

Take a risk-based approach to vulnerability management

No one wants their organization to be the subject of the next data breach headline because a vulnerability was left unpatched. No one. But in order to prevent a breach—high profile or otherwise—you need to fix vulnerabilities before they get exploited. Easier said than done given that the average large enterprise has thousands of assets and millions of vulnerabilities, with dozens of new ones discovered each day. The good news is that two percent of vulnerabilities are ever actively exploited in the wild. But even two percent of millions of vulnerabilities is still more than security and IT teams can handle. What you need is a solution that takes all of your internal security data, analyzes it along with billions of pieces of external data, and then tells you which vulnerabilities pose the most risk. A solution like Kenna.VM.

With Kenna, you can get more from your security data and stop manually managing vulnerabilities in Excel spreadsheets. Your security professionals will no longer have to waste valuable time researching each and every vulnerability in order to assess their severity, nor will you expend resources needlessly remediating based on insufficient methods such as using Common Vulnerability Scoring System (CVSS) scores. You'll finally be able to evaluate and prioritize based on true risk.



Home

June 2, 2020

Risk Score	Vulnerable Assets	Vulnerabilities	Fixes	Mean Time To Remediate
300	12,262	726,372	12,970	35 Days
No change in last 30 days	No change in last 30 days	↑ 1 in last 30 days	↑ 362 in last 30 days	↑ 0.576 in last 30 days

Connector Runs

- Jun 1st ServiceNow CMDB 0 Assets Synced
- Jun 1st Qualys AssetView 32 Assets Synced
- Jun 1st QualysGuard 3 Assets Synced
- May 31st ServiceNow CMDB 0 Assets Synced
- May 31st Qualys AssetView 32 Assets Synced

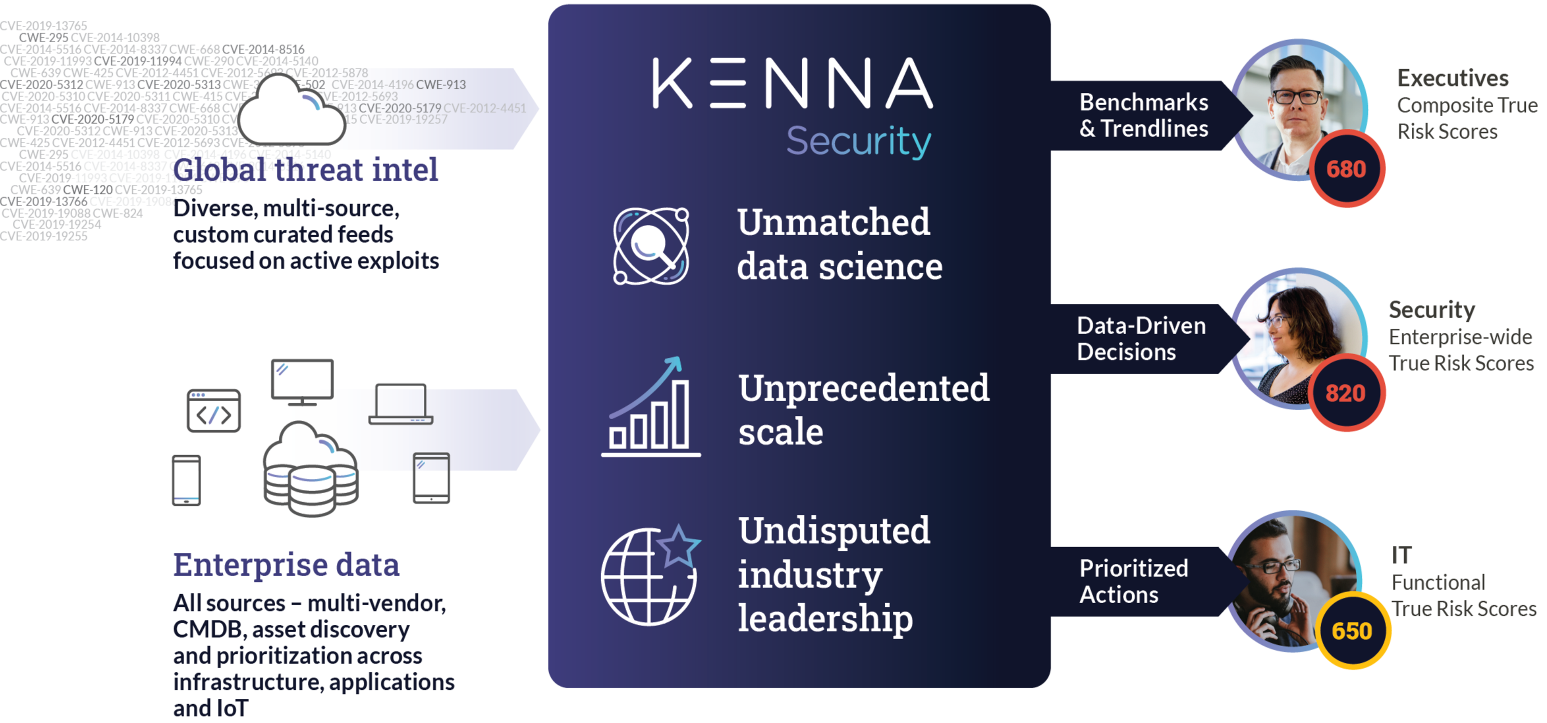
Total Risk Score Over Time

Kenna Defenders Community

Kenna.VM is a scalable, software-as-a-service (SaaS) solution that delivers the most informed and accurate risk prioritization available, enabling security and IT operations teams to take a risk-based approach to vulnerability management by prioritizing and proactively managing the vulnerabilities that matter most. The solution combines 18+ threat and exploit intelligence feeds, 12.7+ billion managed vulnerabilities, global attack telemetry, and remediation intelligence to accurately track and measure real-world exploit activity across the enterprise's global attack surface. Using predictive modeling technology, Kenna.VM can also accurately forecast the future risk of vulnerabilities the instant they're discovered, allowing organizations to proactively manage risk.

Kenna Predictive Model vs. CVSS

TWICE THE EFFICIENCY	HALF THE EFFORT	ONE-THIRD THE FALSE POSITIVES	BETTER COVERAGE
61% vs. 31%	19K vs. 37K CVEs	7K vs. 25K CVEs	62% vs. 52%



Global threat intel

Diverse, multi-source, custom curated feeds focused on active exploits

Enterprise data

All sources – multi-vendor, CMDB, asset discovery and prioritization across infrastructure, applications and IoT

KENNA Security

Unmatched data science

Unprecedented scale

Undisputed industry leadership

Benchmarks & Trendlines

Data-Driven Decisions

Prioritized Actions

Executives
Composite True Risk Scores

Security
Enterprise-wide True Risk Scores

IT
Functional True Risk Scores

The Science Behind Kenna

Kenna.VM is the only solution designed to look outside the organization to analyze and understand the volume and velocity of attacker activity and combine that data with extensive internal data sources to provide the context required to determine which vulnerabilities to remediate first. Employing machine learning and data science, the solution ingests, aggregates, and processes tens of billions of pieces of data, from more than 55 sources, including more than 18+ threat and exploit intelligence feeds, and then automates the analysis of this data using our proven data science algorithm to deliver an accurate, quantifiable risk score for every vulnerability within seconds.

To understand what attackers are doing in real time and evaluate which vulnerabilities are most likely to pose a threat to the organization's specific environment, Kenna.VM analyzes a variety of external and internal data sources, which are listed to the right.

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.

Ground Truth Telemetry

- 18+ exploit intelligence feeds
- 12.7+ billion managed vulnerabilities
- 1+ billion security events processed monthlyy
- 29+ billion successful exploitation events
- Global attack telemetry
- Remediation intelligence

Internal Security Data Sources

- Vulnerability scanners
- Endpoint, Container and Cloud Workload Security Solutions
- 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

Kenna Security's Solution

1. Ground Truth Telemetry

Kenna analyzes billions of pieces of information to understand attacker activity in real-time. We understand what attackers are doing, how they're doing it, and the tools they're using to exploit vulnerabilities in the wild. Kenna analyzes Ground Truth Telemetry to determine:

VOLUME AND VELOCITY

We process and analyze threat data from 18+ feeds* to determine the volume and velocity with which attackers are exploiting vulnerabilities in the wild

EASILY EXPLOITABLE

We analyze data from all available 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

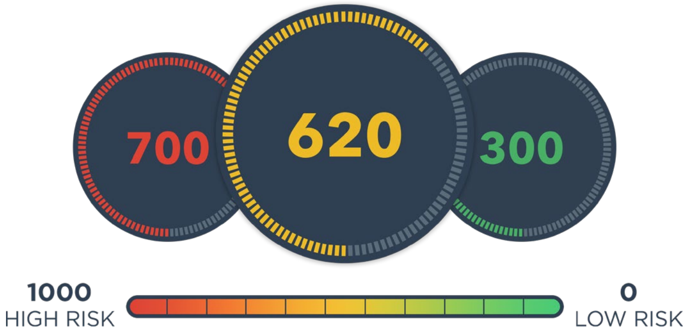
*Kenna Intelligence Feeds

EXPLOIT INTELLIGENCE

- Metasploit
- Canvas Exploitation Framework
- Github Exploit Feed - Cyentia Institute
- Exploit DB
- ReversingLabs
- Proofpoint
- Secureworks CTU
- D2 Elliot
- Contagio
- Continually Updated Black Hat Kits

THREAT INTELLIGENCE

- AlienVault OTX
- AlienVault Reputation
- Silobreaker Threat Intelligence
- Secureworks CTU
- Emerging Threats
- ReversingLabs
- Exodus Intelligence
- SANS Internet Storm Center
- X-Force Exchange



2. Risk Scoring Engine

Leveraging Ground Truth Telemetry and your internal security data, the Kenna Risk Scoring Engine algorithmically determines the risk scores of each unique vulnerability and group of assets. The risk score takes into account the number of instances of each vulnerability in your environment, the potential severity, and the assets that are threatened as a result of each vulnerability. Your organization will understand, in real time, your current risk posture and—more importantly—the actions you can take to affect the greatest impact on risk reduction.

3. Predictive Modeling

By harnessing machine learning, predictive modeling, and other data science techniques, Kenna enables security and IT teams to finally embrace predictive vulnerability management by calculating 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.

4. Remediation Intelligence Engine

Kenna prioritizes remediation efforts based on what will reduce your risk score the most. The vulnerabilities that pose the greatest risk to the organization and whose remediation will have the maximum impact on risk score reduction are entered into a ticketing system. Because vulnerabilities are prioritized based on the risk score and not solely on how many assets will be impacted, these recommendations generate an increase in efficacy across all vulnerabilities.

Why Kenna?

Accurately Measure Your Organization’s Risk

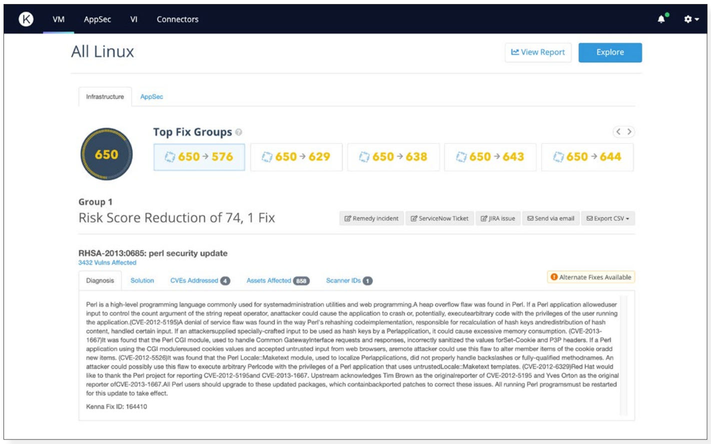
Get the most informed and accurate risk assessment available by combining your vulnerability data, asset information, and real-time threat intelligence. The solution has flexibility that takes into account the asset criticality you define, in addition to real-time threat intelligence from 15+ exploit feeds, 7+ billion managed vulnerabilities, global attack telemetry, and remediation intelligence.

Prioritize High-Risk Vulnerabilities

Not all vulnerabilities are created equal, and many of them pose little to no risk. The solution automatically prioritizes the vulnerabilities that pose the most risk to the organization, so your teams can focus on remediating those first, making the best use of your limited resources.

Predict Future Exploits

With Kenna’s predictive modeling technology, you can, for the first time, accurately forecast which vulnerabilities will become weaponized the moment they are discovered. This type of technology enables you to achieve better coverage with twice the efficiency for half the effort of common remediation strategies such as fixing vulnerabilities with a CVSS score of 7 and above.



All Linux

Group 1

Risk Score Reduction of 74, 1 Fix

RHSA-2013:0685: perl security update

3432 Vulns Affected

Perl is a high-level programming language commonly used for systemadministration utilities and web programming.A heap overflow flaw was found in Perl. If a Perl application alloweduser input to control the count argument of the string repeat operator, anattacker could cause the application to crash or, potentially, executearbitrary code with the privileges of the user running the application.(CVE-2012-5195)A denial of service flaw was found in the way Perl's rehashing codeimplementation, responsible for recalculation of hash keys andredistribution of hash content, handled certain input. If an attackersupplied specially-crafted input to be used as hash keys by a Perlapplication, it could cause excessive memory consumption. (CVE-2013-1667)It was found that the Perl CGI module, used to handle Common GatewayInterface requests and responses, incorrectly sanitized the values forSet-Cookie and P3P headers. If a Perl application using the CGI modulereused cookies values and accepted untrusted input from web browsers, aremote attacker could use this flaw to alter member items of the cookie oradd new items. (CVE-2012-5526)It was found that the Perl Locale::Maketext module, used to localize Perlapplications, did not properly handle backslashes or fully-qualified methodnames. An attacker could possibly use this flaw to execute arbitrary Perlcode with the privileges of a Perl application that uses untrustedLocale::Maketext templates. (CVE-2012-6329)Red Hat would like to thank the Perl project for reporting CVE-2012-5195and CVE-2013-1667. Upstream acknowledges Tim Brown as the originalreporter of CVE-2012-5195 and Yves Orton as the original reporter ofCVE-2013-1667.All Perl users should upgrade to these updated packages, which containbackported patches to correct these issues. All running Perl programsmust be restarted for this update to take effect.

Kenna Fix ID: 164410

Align IT and Security Efforts with Business Objectives

Objective risk scoring improves collaboration between departments by giving them one common language, and helps security and IT communicate clearly and succinctly with management, so they can make data-driven investment decisions. In addition, dissemination of information between departments is automated, so security and IT share the same intelligence on the vulnerabilities and how to fix them.

Leverage Existing Investments

The solution easily integrates with your existing vulnerability scanners, ticketing systems, and other security infrastructure components to maximize efficiency across the organization. Kenna.VM is completely data agnostic, so you can leverage the volumetric data you already have from the investments you’ve already made.

> “Kenna’s important if you want to mature your technology usage and spend your time managing vulnerabilities, not managing spreadsheets.”
>
> Jasper Ossentjuk
> CISO, TransUnion

Find out more about the robust threat intelligence of Kenna.VM at **www.kennasecurity.com**

KENNA Security
A part of Cisco.