The Kenna Application Risk Module

Helping Security and DevOps teams, Developers, and Executives team up to proactively remediate risk
The application attack surface continues to grow in size and complexity. This brings with it correspondingly elevated levels of risk, with nearly 30 percent of successful breaches analyzed in the 2017 Verizon DBIR involving an application layer attack.

To combat these ever increasing threats, a risk-based approach is now required to measure and manage application layer vulnerabilities. The Kenna Application Risk Module makes this possible.

Finding and prioritizing application vulnerabilities is an extremely time consuming, manual process that is rarely undertaken comprehensively. Application security teams know there is risk, but they simply don’t have the time, expertise, or context to find and remediate the relatively small percentage of application vulnerabilities that expose them to the most risk. As a result, all too often the wrong vulnerabilities are fixed while dangerous applications continue to run. Or worse, nothing is done at all until the application is compromised and the team is forced into reaction mode.

The Kenna Application Risk Module overcomes these challenges by empowering security teams, DevOps, and developers to continuously, effectively, and proactively remediate the high-risk application vulnerabilities that are most important.

The Kenna Application Risk Module can determine an application’s importance to the business by assessing the business criticality of the application, as well as various application attributes. This is achieved by extending the capabilities of the Kenna Security Platform to process and normalize all application security data, including static and dynamic scanners, penetration test results, bug bounty data, and open source scanners. To help compute the relative risk score for each vulnerability, it also gathers near real-time telemetry from existing Web Application Firewall (WAF) deployments to determine which vulnerabilities are being attacked.

All remediation efforts are then prioritized, enabling DevOps teams and developers to focus on the vulnerabilities that will have the maximum impact on risk reduction.
### Key Benefits

**Automated**
Analyzes and prioritizes application vulnerabilities to focus scarce security, DevOps, and development resources on what matters most.

**Proactive**
Enables security and DevOps teams to proactively incorporate business criticality of applications and prioritize vulnerabilities by risk score.

**Prescriptive**
Directs findings and remediation guidance to cross-functional teams to help them work toward a common set of goals.

**Comprehensive**
Ingests and normalizes the industry’s most comprehensive list of SAST, DAST, pen test and bug bounty data, and open source scanners.

---

**The Kenna Application Risk Module**

---

<table>
<thead>
<tr>
<th>Assets</th>
<th>Vulnerabilities</th>
<th>Fixes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2,004</td>
<td>2,046</td>
<td>4,248</td>
</tr>
</tbody>
</table>

---

**Windows Servers**

<table>
<thead>
<tr>
<th>Top Priority</th>
<th>Active Breaches</th>
<th>Easy Exploits</th>
<th>Predicted Exploits</th>
<th>Malware Exploits</th>
<th>Popular Targets</th>
<th>Zero-Day Valns</th>
</tr>
</thead>
<tbody>
<tr>
<td>37,882</td>
<td>235,116.9</td>
<td>8,575</td>
<td>34,575</td>
<td>2,153</td>
<td>56,043</td>
<td>204</td>
</tr>
</tbody>
</table>

---

**Connector Names**

- Sonatype: 863
- QualysGuard: 451
- WhiteHat Sentinel: 704
- Tripwire: 982

**Classification**

- CVE: 12,302
- CWE: 18,755
- WASC: 7,093

---

**Connector Filter**

- Group:
  - Save Group
  - Reset Filter

- Asset Filters:
  - Score: 30-60
  - Severity: 1
  - Threat: 1

---

**Vulnerability Filters**

- Score: 30-60
- Severity: 1
- Threat: 1

---

**Windows Servers**

- CVE: 2009-3762
  - Windows XP SP3 and SP2, Windows Server 2003 SP1, and Windows Vista SP1.
  - CVE: 2010-1823
    - PHP 5.1.12 and 5.4.x before 5.4.2.
    - Fixed in PHP 5.1.12 and 5.4.2.

---

**Kenna Security**

---
The Kenna Security Platform is a scalable, cloud-based solution that gives organizations of any size a centralized platform for collaboration and remediation against cyber risk.

The Kenna Application Risk Module extends the capabilities of this proven platform by applying the same data science to vulnerabilities at the application layer. By discovering and prioritizing application vulnerabilities and communicating the results to all application stakeholders, the Kenna Application Risk Module focuses the organization's limited DevOps and development resources to reduce the most risk.

Kenna Connectors pull application assets and vulnerabilities from all connected application information sources.
Reports Risk at Scale

Enterprises have a portfolio of hundreds of developing, in-service, and legacy applications.

Kenna assesses, manages, and tracks risk across this entire application landscape. As the threat landscape changes, the Kenna Security Platform immediately reassesses the current and forecasted threat environment, enabling risk and executive teams to quickly understand overall risk to the organization's application portfolio. Using this intelligence they can determine, for example, which applications might be worth remediating or retiring. This also helps CISOs and other decision makers to confidently report the current risk environment, as well as improvements in the organization's risk posture, to upper management and the board.

Because the Application Risk Module is an extension of the Kenna Security Platform, organizations can now measure and track business risk across their full stack of networks, systems, and applications.

Integrates With Any Existing Application Security Tool

Kenna seamlessly integrates with all application vulnerability security tools and normalizes the data across disparate tools.

The platform also integrates with content and asset management systems and GRC platforms to provide the context required to determine application criticality.

The Kenna Application Risk Module continuously distills findings from throughout your existing security infrastructure to calculate risk scores of application vulnerabilities. Kenna accepts real-time telemetry from dozens of data sources, including:

- Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)
- Web Application Firewall (WAF) Telemetry
- Open Source
- Bug Bounty Programs
- Application metadata
How it Works

The Kenna Application Risk Module leverages all available context to proactively prioritize application vulnerabilities:

1. Kenna Connectors pull application assets and vulnerabilities from all connected application information sources

2. Enterprise application “context” metadata is leveraged to tailor the results of the risk analysis to the organization’s specific environment, including which assets are most important or contain the most sensitive data

3. Application context is determined including a base application vulnerability score, application location, and whether or not the application requires authentication

4. Attack telemetry is analyzed from local WAF’s to help further provide near real-time context on what is being exploited

5. An overall risk score is calculated for each vulnerability and each application

6. Remediation is prioritized, and remediation guidance is delivered, based on the most optimal risk score reduction

7. For organizations that use an Imperva WAF, Kenna can generate rules that further automate application protection

Supported Input Sources

- Micro Focus
  - Formerly Hewlett-Packard Fortify
  - Formerly Hewlett-Packard Fortify on Demand

- IBM
  - IBM AppScan

- Checkmarx
  - Checkmarx

- Bugcrowd

- WhiteHat Security
  - WhiteHat Sentinel
  - WhiteHat Source

- Veracode
  - Veracode
  - Veracode XML

- Black Duck
  - Black Duck

- Imperva
  - Imperva WAF
About Kenna Security

Kenna Security empowers companies to manage cyber risk. The Kenna Security platform, powered by Cyber Risk Context Technology, leverages data science to track, measure, and predict real-world exploitations, and provides organizations with a centralized platform for collaborating on vulnerability remediation. Kenna counts amongst its customers many Fortune 100 companies, and serves nearly every major vertical. Kenna Security is headquartered in San Francisco.