Next Generation Vulnerability Discovery and Protection Platform

Key Advantages

Find Hidden Vulnerabilities

Locate 50 to 200% more vulnerabilities, the one missed during typical DAST and vulnerability testing cycles

OWASP Top 10

Recognizes sophisticated attacks on web applications including the risks in the OWASP Top 10

Easy Deployment and Zero Tuning

Simple deployment, no changes to the testing methodology, and easy setup in less than an hour

Zero Day Attacks

Deterministic technology to detect zero-day and unpatched vulnerabilities

Complete Visibility

Detailed telemetry on every discovered vulnerability including line of code visibility

Enhanced Vulnerability Detection for Web Applications and Application Workloads

Even with an increased focus on security during development, web applications are still making it to production with vulnerabilities that are exploitable by cyber criminals and vulnerabilities that are found during testing often take longer to remediate due to limited information on the discovered vulnerabilities.

K2 Cyber Security enhances the visibility and information provided by DAST (Dynamic Application Scanning Testing) and penetration testing tools by monitoring the application execution directly on the application server, while the testing tools launch their scans and attacks. By residing directly on the application server, K2 has visibility into application execution and application server activity that does not make it back to the testing tool.

K2 has developed an innovative technology to detect “hidden” vulnerabilities, including Remote Code Execution, SQL Injection, Cross Site Scripting and other OWASP Top 10 web applications risks during DAST testing. K2 supplements testing tools by providing additional detail on discovered vulnerabilities, including exact filename and line of code where the vulnerability exists to help organizations locate the vulnerability and remediate the issue.

K2’s unique technology along with the visibility available by residing on the application server, lets K2 discover additional hidden vulnerabilities that are missed by DAST and penetration testing tools.

By adding K2 to the web application testing process, organizations benefit by discovering additional hidden vulnerabilities, reducing the remediation time needed to fix discovered vulnerabilities, and releasing the web applications to production more quickly.

With K2 organizations will be able to:

- Get web applications to production in less time
- Remediate discovered vulnerabilities quickly
- Pinpoint location of discovered vulnerabilities immediately
- Reduce the amount of vulnerabilities that make it to production in web applications
- Discover and remediate more vulnerabilities during development testing
- Help quickly identify possible false positives

Use Cases

01 Vulnerability Detection

Security teams have a short window to find and fix vulnerabilities in applications. Current penetration testing and scanning tools create too many false alerts and provide limited intelligence on the location of vulnerabilities. K2's Agent is deployed in tandem with penetration testing/scanning tools and provides the exact location of vulnerable code for every attack.

- Increases the number of vulnerabilities that can be remediated
- Provides exact location of vulnerable code
- K2's agent does not interfere with security testing methodology

02 Web Application Protection

Vulnerabilities in web applications are the leading cause of high-profile breaches. The increasing sophistication of attacks on web applications can evade detection from signature and pattern matching based solutions like EDR and WAF. K2's unique patent pending technology protects against the OWASP Top 10 and other sophisticated attacks in real-time without generating false alerts.

- Comprehensive web application language and platform support
- Unique high-performance architecture
- Detailed attack telemetry lowers remediation cost

03 Memory Based Attack Protection

Sophisticated attackers are increasingly using memory-based attack techniques like return oriented programming which cannot be detected by EDR and other security solutions. The K2 Platform uses a deterministic technique of Optimized Control Flow Integrity (OCFI) that creates a unique "DNA" map of the application. The "DNA" map is used at runtime to expose deviations caused by memory based and file-less attacks

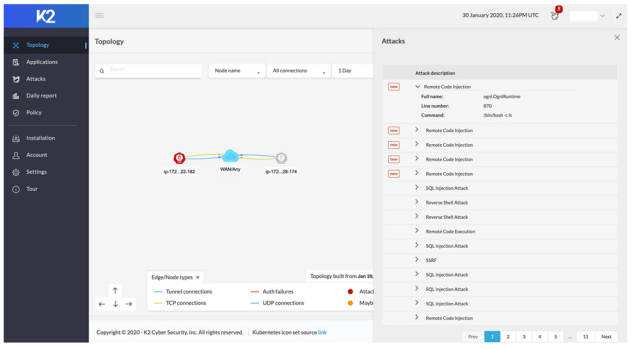
- Protect against file-less and buffer overflow attacks
- Unique "DNA" map of applications eliminates false alerts
- Last line of defense for business-critical applications

Ready to Redefine the Security for Web Applications and Cloud Workloads?

If increasing the efficiency and productivity of your application testing requirements, strengthening your security posture, and adding a last line of defense for a comprehensive application security strategy are a priority, then the Next Generation Application Workload Protection Platform from K2 Cyber Security will help get you there.

To schedule a demo or just to learn more about K2, send us an email at

info@k2io.com



K2 Cyber Security, Inc

2580 N. First Street, #130,
San Jose, CA 95131 USA

Phone: 1 (669) 284 9992

Email: info@k2io.com
Sales: sales@k2io.com

About K2 Cyber Security

K2 Cyber Security delivers the Next Generation Application Workload Protection Platform to secure web applications and container workloads against sophisticated attacks including OWASP Top 10 and memory-based attacks. K2's Platform is deployed on production servers for runtime protection of applications and on pen-testing / pre-production servers to identify the location of the vulnerable code in real-time. K2's solution generates the least false alerts, eliminates breaches due to zero-day attacks and dramatically reduces security cost.