Cyberint
A Check Point Company

Infinity External Risk Management Services

ACTIVE VULNERABILITY SCANNING DATASHEET

YOU DESERVE THE BEST SECURITY

Cyberint's Active Vulnerability Scanning (AVS) uses advanced automation to validate your organization's exposures, determine which can be exploited, and issue real-time alerts. Continuously and actively test your external digital assets so you can quickly identify and remediate exploitable issues before they lead to a major incident.

CHALLENGE

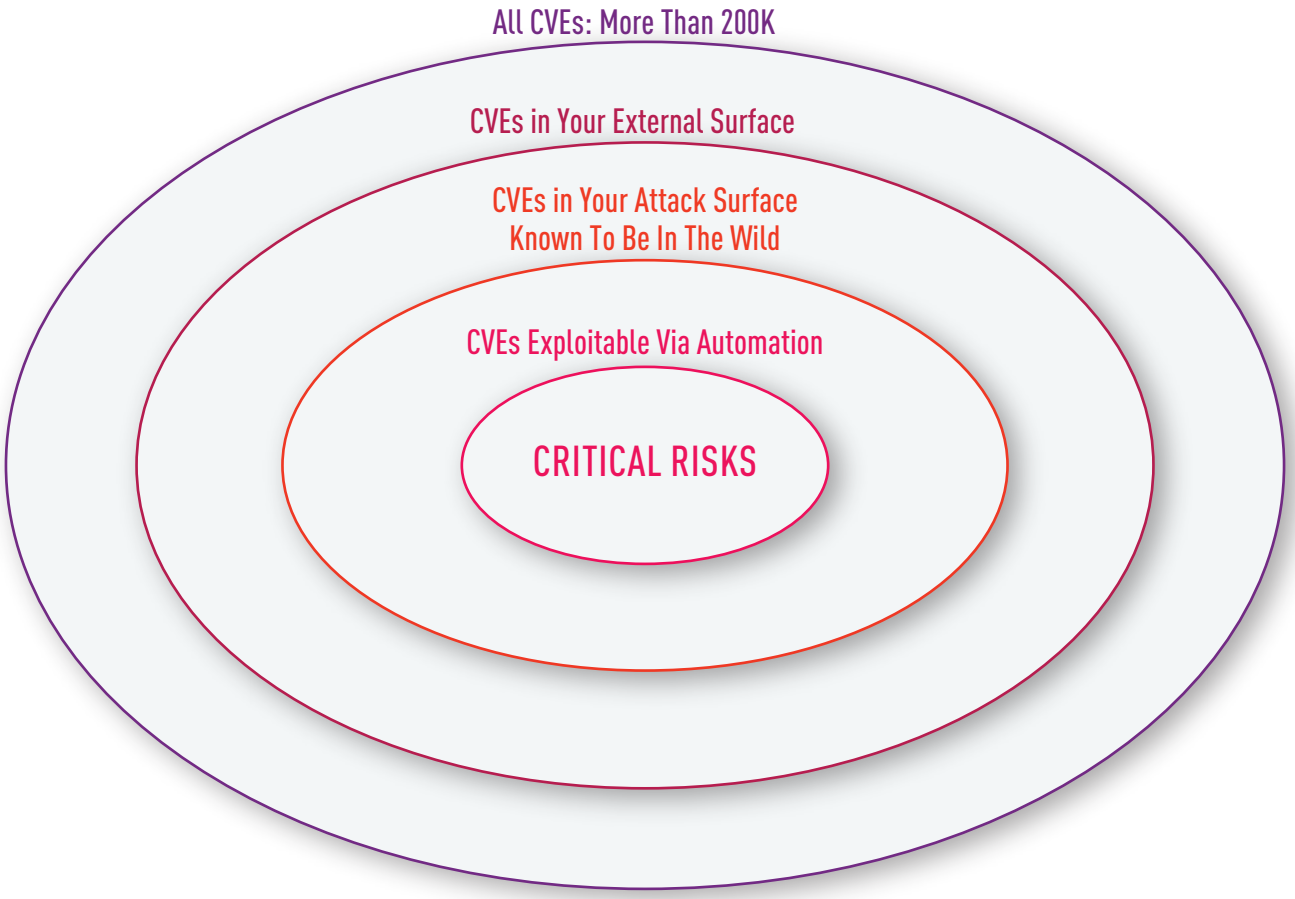
Standard CVE detection relies on fingerprinting software and version numbers, then checking those technologies in a CVE database. This approach is useful but it stops short of attempting exploitation so the findings are unvalidated. It also limits detection to the vulnerabilities that have been documented and assigned a CVE number. Other common security issues cannot be discovered through this typical approach.

SOLUTION

The Cyberint Active Vulnerability Scanning (AVS) capability tests your organization's exposures for exploitability. This includes using automated attempts to exploit known CVEs as well as automated attacks—credential stuffing, SQL injection, path traversal, cross-site scripting, and more—to detect unknown vulnerabilities in your organization's digital assets and applications.

KEY BENEFITS

- Continuously validate your exposures to understand which are exploitable.
- Go beyond ordinary CVE detection with automated exploitation tests.
- Detect common security issues not documented in CVE databases.
- Run dynamic application security testing (DAST) on your web apps.
- Quickly remediate your most urgent risks before they lead to a breach.



Validate Exposures To Determine Which Are Exploitable

Run thousands of automated security tests to attempt exploitation of known CVEs, test your digital assets for security issues without assigned CVE numbers, and actively test web applications.

Automated CVE Exploitation

Attempt exploitation of CVEs with templated exploit code to know whether a vulnerability poses a serious risk.

Continuous Exposure Validation

Check exposed web interfaces and open ports for exploitability through credential stuffing and other techniques.

Dynamic Web App Testing

Test your web applications for issues like SQL injections, cross-site scripting, path traversal, and more.

Leverage Automation To Reveal Your Greatest Risks

Use automated, continuous testing to identify your organization's most critical attack surface risks—the ones that can be easily exploited by threat actors.

24x7 Security Testing

Continuous exposure validation and security testing that runs around the clock to uncover major risks.

Better-Informed Risk Scoring

Use automation to know exposures which can be exploited, leading to more precise and accurate risk scoring.

Attack Surface Reduction

Active discovery and testing of your Internet-facing assets helps you eliminate risks and minimize your attack surface.

Accelerate Remediation & Reduce External Cyber Risk

Gain visibility on exploitable vulnerabilities and misconfigurations in your external attack surface. Prioritize these critical risks so you can quickly remediate them before they lead to an incident.

Real-Time Alerting

Alerts are issued in real time when an exploitable risk is detected. Consume alerts in your SOC tools or ticketing system.

Simplified Prioritization

Comprehensive assessment and risk scoring makes it easy to understand which risks are most critical.

Quantified Risk Reduction

Track your security posture score over time, as well as other metrics like mean time to acknowledge and remediate.

> **Because we're a small team, the Check Point analysts are like an extension of us, which really helps from a risk management standpoint.**
>
> Evans Duvall, Cyber Security Engineer, Terex

> **We realized that Check Point was much more than an EASM solution, it delivered much value with highly relevant intelligence from the deep and dark web.**
>
> Benjamin Bachmann, Head of Group Information Security, Ströer

> **Once we identified the need to address the risk of fraudulent websites and social profiles, I quickly realized we needed to handle this in a scalable manner. Our solution is to use Check Point to help us automatically detect and takedown these threats.**
>
> Ken Lee, IT Risk and Governance Manager at Webull Technologies

SCHEDULE A DEMO

Recognition As An Industry Leader From Trusted Analysts

Gartner FROST & SULLIVAN G2 IDC

ABOUT CYBERINT

Cyberint, now a Check Point company, reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Check Point External Risk Management solution provides superior visibility through continuous discovery of the evolving attack surface, combined with the automated collection and analysis of vast quantities of intelligence from across the open, deep and dark web. A team of global military-grade cybersecurity experts work alongside customers to rapidly detect, investigate, and disrupt relevant threats – before they have the chance to develop into major incidents. Global customers, including Fortune 500 leaders across all major market verticals, rely on Check Point External Risk Management to protect themselves from an array of external risks, including vulnerabilities, misconfigurations, phishing, impersonation attacks, malware infections, exposed credentials, data leaks, fraud, and 3rd party risks.

For more information visit: https://cyberint.com / checkpoint.com/erm