CHECK POINT

EXPOSURE MANAGEMENT

CHECK POINT AGENTIC EXPOSURE VALIDATION

PROVE WHAT ATTACKERS CAN EXPLOIT. ACT BEFORE THEY DO.

WE SECURE YOUR AI TRANSFORMATION

CHALLENGE

Organizations face the harsh reality of having to deal with ongoing vulnerabilities, leaked credentials, misconfigurations and control gaps. The threats grow exponentially with the rise of agentic tools and sophisticated cyber attacks.

Attackers no longer wait for security teams to triage findings, correlate tools, or schedule manual patching cycles. They use agentic capabilities to automate limitless exploit opportunities, dynamically changing attack methods until successful penetration. The time to being hacked has dramatically shrunk, leaving security teams unable to deal with the sheer volume, intensity, and complexity of attacks. The same rules no longer apply.

Security teams need the tools to match the speed of agentic attacks and act quickly and confidently while ensuring corporate processes, safe validation, and business continuity.

HOW IT WORKS:

Agentic Exposure Validation follows a safe proving loop:

1. Understand the context
The agent analyzes the relevant asset, technology, CVE, credential, service, or exposed code.

2. Enrich with intelligence
It correlates customer-specific exposure data with live threat intelligence, exploit research, patch analysis, and attacker behavior..

3. Identify the validation gap
The agent checks whether existing detections or controls already cover the exposure.

4. Build a targeted validation
It creates a focused validation path that mirrors attacker reasoning without using disruptive techniques.

5. Review for safety and accuracy
An independent AI reviewer evaluates each validation for safety, novelty, accuracy, and exploit depth.

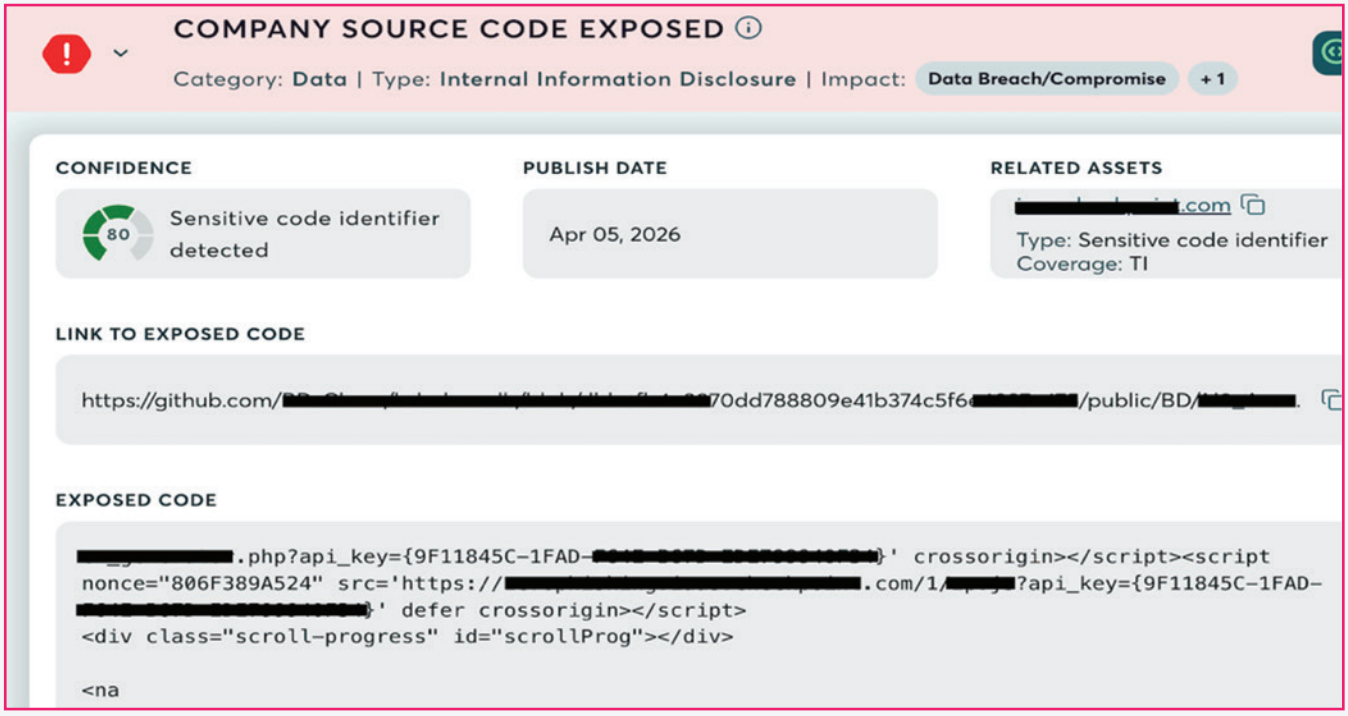
6. Prove, pivot, or delete
If the exposure is proven, it is reported. If blocked, the agent pivots to another safe path. If unproven, it is removed instead of shipped as noise.

© 2026 Check Point Software Technologies Ltd. All rights reserved.

SOLUTION

Check Point Agentic Exposure Validation uses AI agents to reason like attackers across your specific environment. By adding an agentic layer, it enhances discovery and scanning of potential exploits into a full agentic attacker model.

Agentic Exposure Validation fuses intelligence sources such as source code exposure, leaked credentials, CVE intelligence, and threat research with external discovery data such as certificates, technologies, open ports, web interfaces, services, and exposed assets. Using this combined context, the agentic attacker model can test different attack vectors within minutes and at scale. It correlates external attack surface data, asset context, live exploit research, threat intelligence, and protection coverage to validate whether an exposure is truly exploitable - safely, continuously, and with evidence security teams can act on.



In practice, this delivers continuous, effective black-box penetration testing at scale. It helps customers and prospects uncover critical exposures the way a threat actor would, making it a critical validation element within a Continuous Threat Exposure Management (CTEM) program and enabling teams to take proactive measures before attackers do.

© 2026 Check Point Software Technologies Ltd. All rights reserved.

ALERT-DRIVEN API KEY EXPLOITATION

The agent receives a leaked credential alert, reads the source, understands the API, and crafts a targeted validation.

ALERT	READ CONTEXT	RESEARCH	CRAFT EXPLOIT	VALIDATE
API key detected in public GitHub	Reads full repository to understand the API	Maps endpoint, authentication mechanism, API docs	Builds targeted requests using various techniques	Confirms if leaked key still grants access

Agentic Exposure Validation helps teams answer the questions that drive action:

- Can this exposure be used by an attacker?
- Does it affect our actual environment?
- Are there any security controls to stop the attack path?
- Is the finding proven, or just another theoretical risk?
- Which attack vectors can be tested safely based on our real attack surface and intelligence context?
- What proactive action should we take first to reduce the most attacker-usable exposure?

CONTACT US TODAY TO GET AGENTIC EXPOSURE VALIDATION ACTIVATED FOR YOUR ORGANIZATION.

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391

www.checkpoint.com

© 2026 Check Point Software Technologies Ltd. All rights reserved.