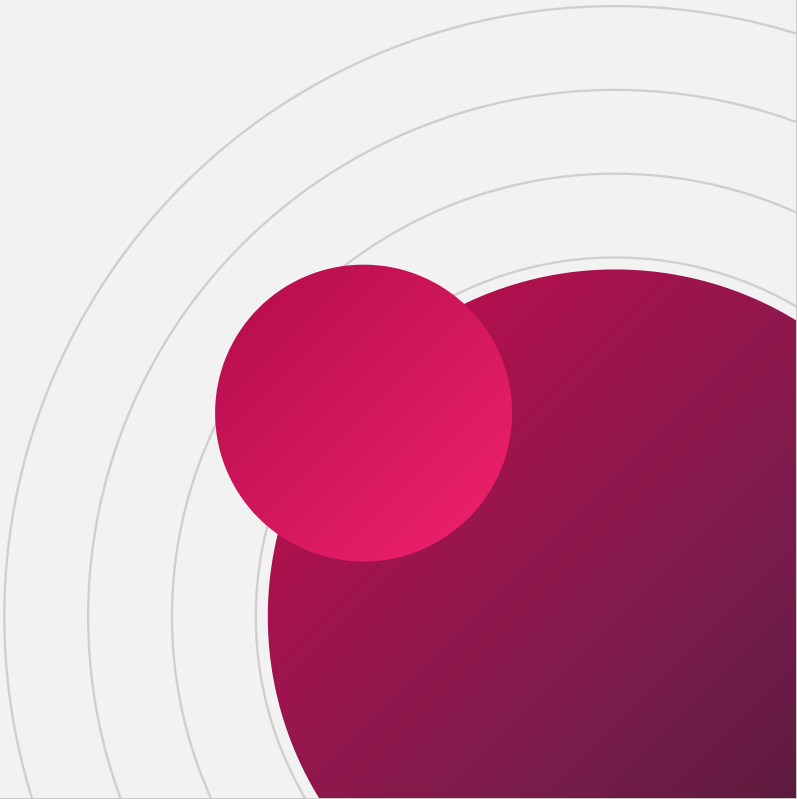
CHECK POINT

EXPOSURE MANAGEMENT

Storm — Ransomware in the Age of AI

09/23/2026

A Check Point Exposure Management intelligence brief tracking the emergence and rapid scaling of the Storm ransomware-as-a-service operation.



CONTENTS

Table of Contents

01	Executive Summary	03
02	Introduction	04
03	Key Findings	05
04	Victimology	07
05	Storm's Advanced Leak-Site Presentation	09
06	AI as a Branding Strategy	10
07	Conclusions	11
08	Contact Us	12

01 / OVERVIEW

Executive Summary

Storm emerged in August 2026 as a financially motivated ransomware operation and rapidly established itself as a high-volume extortion actor.

50+
Victims claimed within six weeks of public activity

3
Regions targeted — North America, Europe, and Oceania

90/10
Maximum affiliate revenue share advertised by the group

Within approximately six weeks of public activity, the group claimed more than 50 victims across North America, Europe, and Oceania, targeting organizations in healthcare, finance, manufacturing, government services, transportation, and critical infrastructure sectors. Victim postings indicate a particular concentration in the United States, Canada, Germany, and Australia.

Unlike many newly observed ransomware brands, Storm entered the ecosystem with a mature public identity. Prior to its first observed victim publication, a known Initial Access Broker (IAB), BigBro, advertised the creation of the ransomware operation and launched a formal affiliate recruitment campaign. The group promoted itself as the "first AI-powered, quantum-resistant ransomware" platform and publicly outlined an aggressive affiliate revenue-sharing model, indicating an intention to operate as a Ransomware-as-a-Service (RaaS) program.

Storm's infrastructure also stands out from the broader ransomware ecosystem. The group's Tor-based leak site incorporates a highly polished user interface featuring an interactive global victim map, sector tagging, searchable victim lists, integrated file-tree visualization, and custom CAPTCHA mechanisms. Such features suggest investment in branding, user experience, and operational scalability that exceeds what is commonly observed among newly established ransomware operations.

> "No evidence has been identified to indicate that AI is used in the group's ransomware deployment, victim targeting, encryption routines, or extortion processes."

Although Storm heavily emphasizes artificial intelligence in its marketing materials, no evidence has been identified to indicate that AI is used in the group's ransomware deployment, victim targeting, encryption routines, or extortion processes. However, the group's automation-focused affiliate program, centralized victim management capabilities, and sophisticated platform design may indicate an effort to reduce operational overhead and increase affiliate productivity through automation.

Confidential | Check Point Copyright © All Rights Reserved 2026

02 / BACKGROUND

Introduction

Storm first appeared publicly in August 2026 as a ransomware operator conducting financially motivated extortion through file encryption and ransom demands.

The group operates like a modern Ransomware-as-a-Service (RaaS) program, outsourcing intrusion activity to affiliates while providing infrastructure, negotiation capabilities, support services, and monetization mechanisms. Public communications indicate Storm seeks to position itself as a premium service provider within the ransomware ecosystem rather than simply a malware developer.

An early indicator of this strategy was the group's association with a darknet forum advertisement published by the Initial Access Broker BigBro. The advertisement announced the launch of the operation, outlined affiliate opportunities, and emphasized global expansion while explicitly prohibiting activity against Commonwealth of Independent States (CIS) countries, a restriction commonly observed among Russian-speaking threat actor groups.

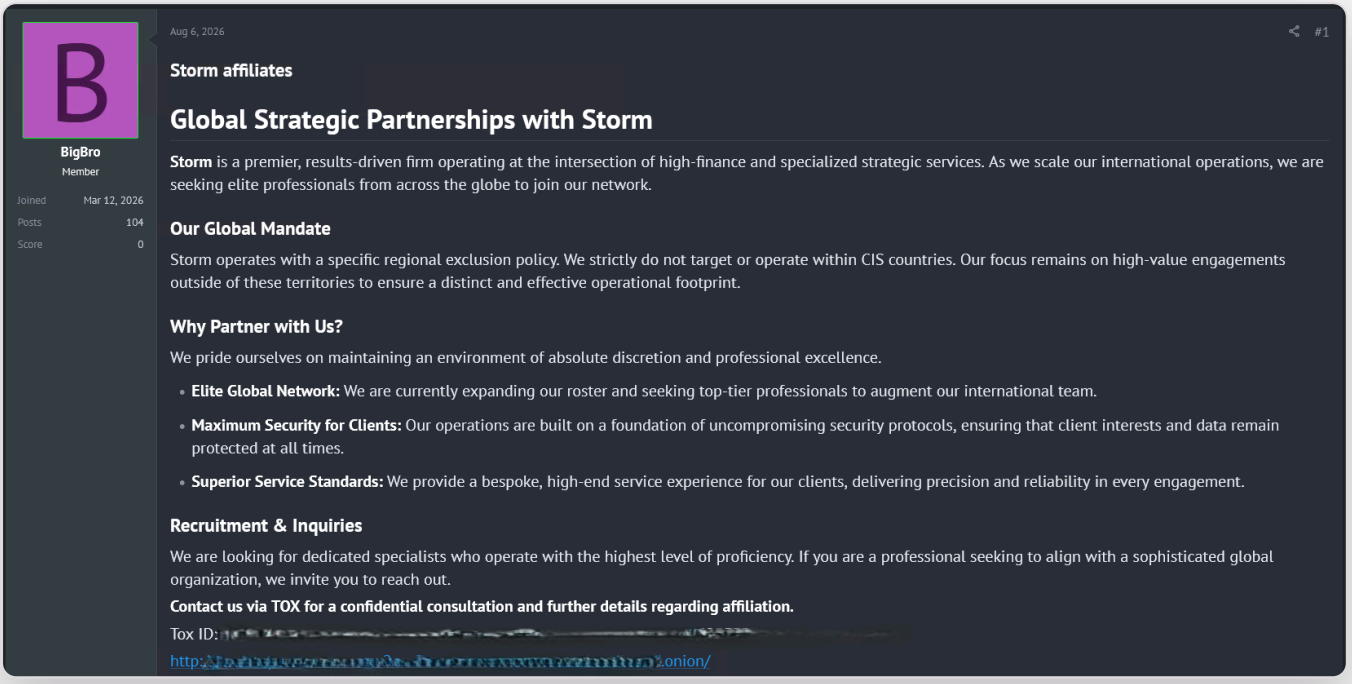


Figure 1. First affiliation post on darknet forums by BigBro.

Confidential | Check Point Copyright © All Rights Reserved 2026

03 / KEY FINDINGS

Storm Launched With a Structured Affiliate Program

Storm did not emerge as a single-actor ransomware campaign. Evidence suggests the operation was designed from inception as a scalable affiliate ecosystem. The group's public recruitment materials advertised:

- Windows, Linux, ESXi, and NAS lockers
- Automated victim chat management
- Call-center services for victim pressure
- Legal advisory services
- Technical support for bypassing AV/EDR solutions
- DDoS capabilities
- Media and journalist outreach services

The affiliate compensation structure is aggressive

REVENUE GENERATED	AFFILIATE SHARE
Up to $500K	75%
Up to $750K	80%
Above $750K	90%

Storm also openly solicits Initial Access Brokers, Data brokers, and Network access providers. This model mirrors mature RaaS operations rather than newly formed ransomware groups.

Confidential | Check Point Copyright © All Rights Reserved 2026

03 / KEY FINDINGS — CONTINUED

Storm's Own Pinned Recruitment Post

Shortly after BigBro's advertisement, Storm published its own pinned introduction on darknet forums, restating the affiliate offer directly in the group's voice and formalizing the RaaS pitch shown in Figure 1.

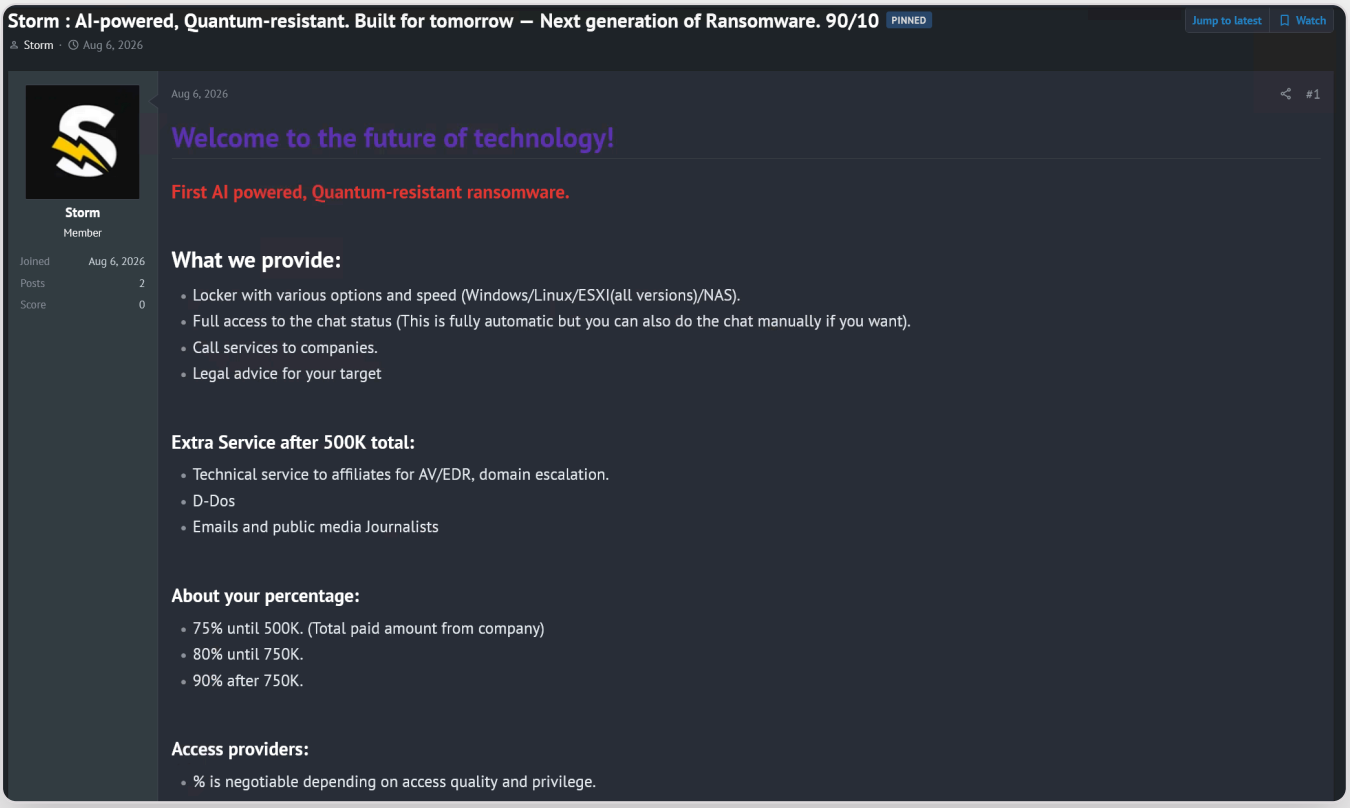


Figure 2. First group post on darknet forums.

Confidential | Check Point Copyright © All Rights Reserved 2026

04 / KEY FINDINGS

Victimology

Storm accumulated over 50 publicly listed victims within its first six weeks of operation, representing a significant initial growth rate for a newly established ransomware brand.

Observed victims are based in the United States, Germany, Canada, and Australia. Affected sectors include Business Services, Finance, Manufacturing, Healthcare, Retail, and Automotive, among others. The victim list suggests a preference for organizations where operational disruption can create strong incentives to pay, particularly healthcare providers, financial institutions, municipalities, and manufacturers.

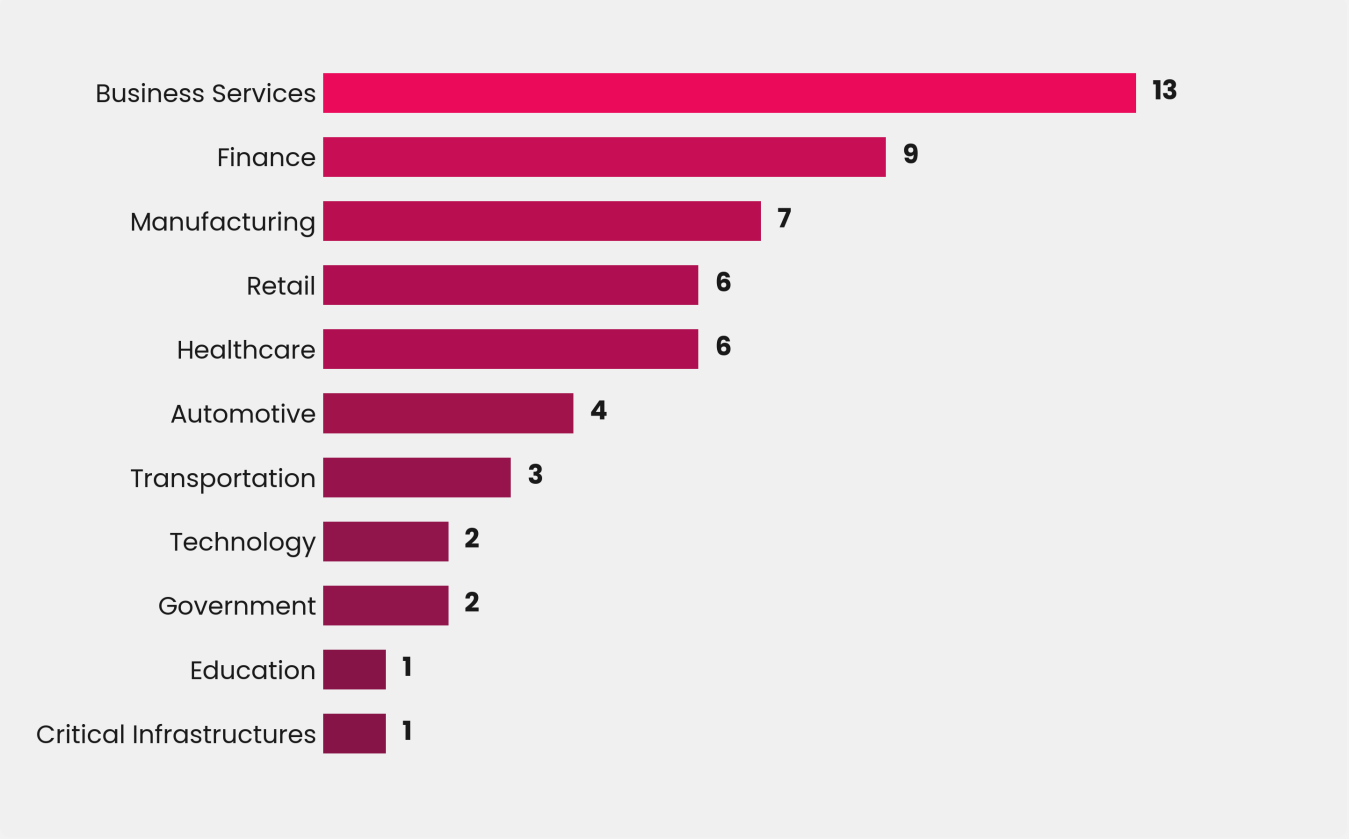


Figure 3. Storm's sector targeting distribution — incident count by sector.

Confidential | Check Point Copyright © All Rights Reserved 2026

04 / KEY FINDINGS — CONTINUED

Healthcare Was Targeted Heavily During the Group's Early Campaign

Several of Storm's earliest and most impactful victim claims involved healthcare organizations, including:

- Southern Indiana Radiological Associates
- Pinnacle Hospital
- WindRose Health Network
- Our Hospice of South Central Indiana
- OVP Health
- Rood & Riddle Equine Hospital

Healthcare environments remain attractive ransomware targets due to operational sensitivity, time-critical services, and high costs associated with downtime. The concentration of healthcare victims during Storm's first month suggests a deliberate targeting preference rather than random victim selection.

Storm Targets Increasingly Larger Organizations

Although many victims appear to be mid-sized organizations, several claimed victims indicate a willingness to pursue larger enterprises, including:

ORGANIZATION	ESTIMATED REVENUE
Pinnacle Treatment Centers	~$440M
United Group of Companies	~$307M
McCarthy Tire Service	~$297M

The progression from mid-market organizations toward larger enterprises may indicate increasing affiliate confidence, improved access acquisition, or expanding operational capabilities.

Confidential | Check Point Copyright © All Rights Reserved 2026

05 / KEY FINDINGS

Storm's Advanced Leak-Site Presentation

One of Storm's most distinguishing characteristics is the sophistication of its leak-site infrastructure. Observed features include:

- Interactive world map displaying victim locations
- Industry-based filtering
- Victim timelines and status tracking
- Search functionality
- Integrated document tree previews
- Custom graphical CAPTCHA

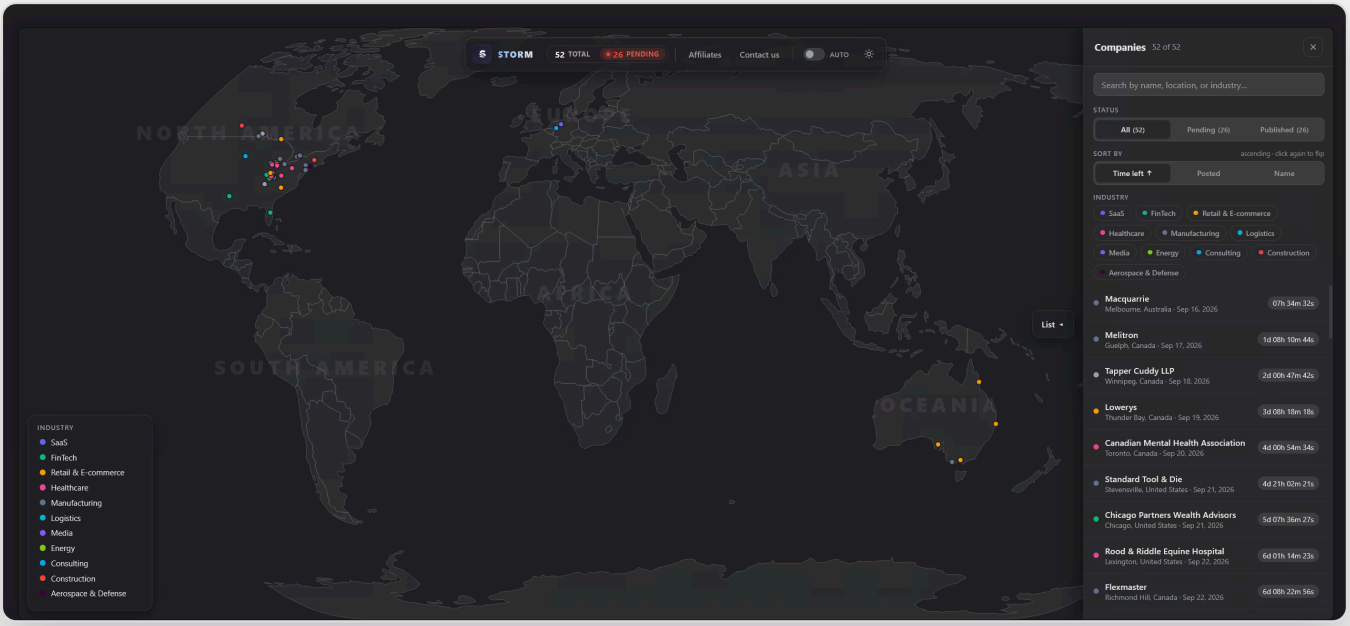


Figure 4. Storm's advanced data leak site.

While leak-site appearance alone does not indicate technical superiority, it demonstrates a substantial investment in operational presentation and brand identity. In contrast to many ransomware portals that rely on simple listing pages, Storm appears designed to maximize victim pressure, affiliate attraction, media visibility, and brand recognition. This approach resembles commercial software platforms more than traditional cybercriminal infrastructure.

Confidential | Check Point Copyright © All Rights Reserved 2026

06 / ANALYSIS

AI as a Branding Strategy

One of Storm's most notable characteristics is its explicit branding around artificial intelligence. In recruitment material directed at affiliates, the group advertises itself as the **"First AI powered, quantum-resistant ransomware"** operation and repeatedly uses technology-focused messaging to differentiate itself from competing ransomware-as-a-service (RaaS) programs.

However, despite the prominence of AI-related claims in Storm's public messaging, currently available evidence does not conclusively demonstrate that artificial intelligence is being used in the group's intrusion, encryption, extortion, or affiliate-support workflows.

Instead, available evidence suggests the AI narrative serves three practical purposes:

Recruitment

The AI label differentiates Storm in a crowded ransomware market and appeals to prospective affiliates.

Automation Signaling

References to automated victim management and automated negotiations may indicate workflow automation rather than genuine AI-enhanced offensive capability.

Marketing

Storm presents itself as a technologically advanced platform, positioning its services as more sophisticated than competing RaaS programs.

Confidential | Check Point Copyright © All Rights Reserved 2026

07 / CLOSING

Conclusions

Storm represents an emerging generation of ransomware operations that places equal emphasis on branding, automation, and affiliate enablement alongside traditional extortion activities.

What distinguishes Storm from many newly established ransomware groups is not a demonstrated technical breakthrough, but the **maturity of its operational presentation**. Before publishing victims, the group launched a structured affiliate program, publicly recruited partners, and deployed a highly polished leak site with functionality more commonly associated with commercial software platforms than traditional ransomware portals. These investments suggest a deliberate effort to lower barriers for affiliates, streamline operations, and establish a recognizable brand within an **increasingly crowded ransomware ecosystem**.

Storm's rapid accumulation of victims across multiple sectors and geographies demonstrates its ability to attract affiliates and maintain operational momentum shortly after launch. While the group follows conventions commonly associated with Russian-speaking ransomware ecosystems, including a prohibition on targeting CIS countries, its broader significance lies elsewhere.

> "Storm offers a glimpse into how ransomware groups may evolve in the age of AI, regardless of how extensively they actually use the technology."

Rather than demonstrating a new form of AI-enabled ransomware, Storm illustrates how modern ransomware operations are increasingly adopting the marketing, automation, and scalability principles of software-as-a-service businesses.

Confidential | Check Point Copyright © All Rights Reserved 2026

CHECK POINT

GET IN TOUCH

Contact Us

ISRAEL

Tel: +972-73-226-4555
5 Shlomo Kaplan Street
6789159

USA

Tel: 1-800-429-4391
100 Oracle Parkway, Suite 800
Redwood City, CA 94065

SINGAPORE

Tel: +65-6435-1318
78 Shenton Way, #09-01 Tower 1
Singapore 079120

PHILIPPINES

Tel: +63-2-8465-9200
Unit 2005, 20th Floor, Zuellig Building,
Makati Avenue, corner Paseo de Roxas, Metro Manila

UK AND IRELAND

Tel: +44-20-7628-4211
85 London Wall, 4th Floor
London, EC2M 7AD

JAPAN

Tel: +81-3-6205-8340
Toranomon Kotohira Tower 25F, 1-2-8
Toranomon, Minato-ku, Tokyo 105-0001

ABOUT

About Check Point Exposure Management

Check Point's exposure management changes the game.

We combine billions of internal telemetry points with billions of external signals from the open, deep, and dark web to deliver a unified intelligence fabric. This provides clear visibility across the full attack surface, including brand risk.

The industry is moving from fragmented feeds to real context and real priorities. We support that shift through active threat validation, confirmation of compensating controls, and deduplication across tools, so teams can focus on what actually matters.

With safe-by-design remediation, fixes aren't just assigned, they're implemented. Every fix is validated before enforcement, enabling measurable risk reduction without downtime.

Gartner predicts organizations adopting continuous threat exposure management with mobilization will see 50% fewer successful attacks by 2028. We're leading that shift with action, not just tickets, and Fortune 500 organizations across major industries already rely on Check Point Exposure Management.

For more information visit: checkpoint.com/exposure-management