GREYNOISE

CROWDSTRIKE

SOLUTION BRIEF

ILLUMINATE THE INVISIBLE ATTACK SURFACE

40%

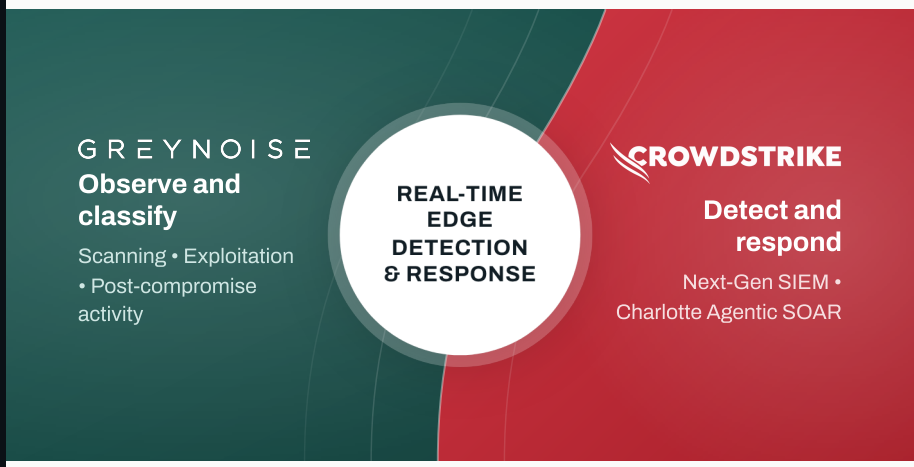
of China-nexus vulnerability exploitation cases in 2025 targeted edge devices

CrowdStrike 2026
Global Threat Report

THE VISIBILITY GAP

Attackers are targeting where visibility is weakest.

Routers, firewalls, VPN gateways, and other edge systems sit entirely outside EDR coverage and lack the telemetry needed for real-time observability and alerting. CrowdStrike calls this the **invisible attack surface**: a dangerous blind spot that can allow adversaries to gain access and establish control before defenders detect them.



GreyNoise sees attackers hitting the edge first, so analysts can:

PRIORITIZE
Active and emerging CVE exploitation

DETECT
Malicious connections and signs of compromise

RESPOND
Faster triage, investigation, and automated action

HUNT
Advanced adversaries hiding in the noise

500M
sessions observed daily

5,500+
sensors in 80+ countries

<1 min
collection to action

GREYNOISE

CROWDSTRIKE

USE CASES

FROM EDGE SIGNAL TO ACTION

Operationalize real-time attacker intelligence across detection, investigation, and response.

GET STARTED

GREYNOISE FOUNDRY APP

GREYNOISE CHARLOTTE AGENTIC SOAR APP

Both available now in the CrowdStrike Marketplace.

GREYNOISE INTELLIGENCE ACROSS THE FALCON PLATFORM

Four ways to act on threats targeting the edge

Turn observed attacker activity into decisions analysts can make inside the workflows they already use.

01

Detect What Breached the Edge

FALCON NEXT-GEN SIEM

Correlate allowed inbound firewall and WAF events with GreyNoise-classified malicious infrastructure. Surface the connections that crossed the perimeter and start investigating ASAP.

Find malicious inbound activity faster.

02

Catch Compromised Edge Devices Early

FALCON NEXT-GEN SIEM

Identify allowed outbound connections to GreyNoise-classified malicious and command-and-control infrastructure.

Surface your compromised edge devices and reduce attacker dwell time.

03

Reduce Alert Noise. Keep the Signal.

FALCON NEXT-GEN SIEM

Filter known opportunistic mass scanning from your perimeter telemetry. Prioritize what remains to give analysts a higher-fidelity alert queue of events more likely to represent targeted reconnaissance or attack activity.

Cut through alert noise and surface potentially targeted threats faster.

04

Automate Triage and Response

CHARLOTTE AGENTIC SOAR

Use GreyNoise context to recategorize severity, create cases, launch investigations, and drive containment through Charlotte Agentic SOAR workflows.

Move from signal to action faster.

THE MOST IMPACTFUL OUTCOMES FOR SECURING YOUR EDGE

- See active exploitation
- Investigate malicious connections
- Respond to signs of compromise
- Hunt advanced adversaries