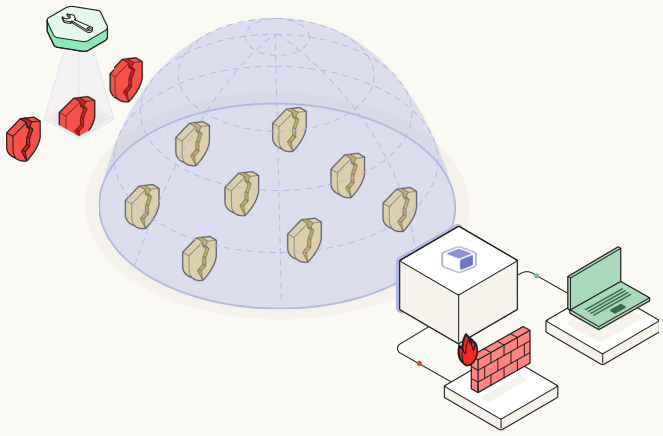
Keep Exploits Out Until Patches Go In

Mitigate vulnerabilities with compensating security controls



THE CHALLENGE

Patching can’t keep pace with vulnerability discovery

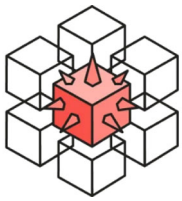
Security teams have always had more vulnerabilities than they can patch at once. AI-powered attacks are making that imbalance significantly worse. With the help of AI, attackers can begin exploiting new vulnerabilities in days. But patch cycles can take weeks. AI-powered vulnerability research is widening that gap by finding vulnerabilities faster than organizations can validate, prioritize, and remediate them.

The result is a growing backlog. Security teams are asking themselves: What needs to be patched first?

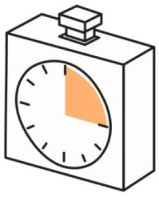
Traditional vulnerability prioritization helps teams rank risk based on severity, exploitability, and asset importance. What it often cannot tell them is whether existing security controls are actively preventing a vulnerability from being exploited.

The same critical vulnerability can represent very different levels of immediate risk depending on whether an endpoint control is enforcing, a prevention signature is in the traffic path, a firewall policy can inspect the exploit, an exception bypasses protection, or a control is running in alert-only mode. Reach identifies these conditions directly from control configuration rather than assuming that the presence of a security product equals protection.

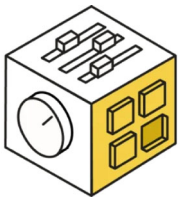
Security teams still need to patch vulnerabilities. But they need a better way to mitigate what they can in the short term, and the ability to quickly determine which ones require their attention first.



Security teams have more vulnerabilities than they can patch at once. AI-powered discovery is making the backlog grow even faster.



Attackers exploit new vulnerabilities in days, while patch cycles often take weeks. Teams need protection before the patch is ready.



Traditional prioritization ranks vulnerabilities by risk, but misses if existing security controls can mitigate the exploit.

Two equally critical vulnerabilities can pose different risks. Teams must know what’s already protected and what needs attention first.

THE SOLUTION

Mitigate vulnerabilities with compensating controls until patches go in

Reach connects vulnerability intelligence with the real-world state of the security controls protecting each affected asset. Reach's compensating controls architecture combines three layers of intelligence:

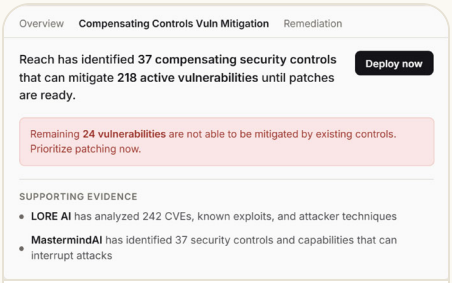
- LORE agents analyze CVEs, known exploits, proof-of-concept code, and attacker techniques to understand how a vulnerability can be exploited.
- MastermindAI identifies the security controls and capabilities that can interrupt the attack.
- Reach then evaluates your deployed controls to determine whether that protection is actively present and effective.

Security teams can now decipher if a vulnerability can be exploited right now given the compensating controls available.

Reach classifies each vulnerability and asset combination as mitigated, partially mitigated, not mitigated, or unknown, with evidence behind every determination.

In an illustrative environment with 1000 vulnerabilities, if compensating controls are effectively mitigating 950, teams can focus immediate remediation on the 50 that remain exposed while normal patching continues across the rest.

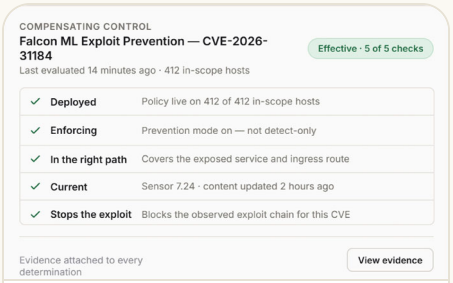
Reach helps keep exploits out until patches go in, verifies that compensating controls are deployed, enforcing, current, and capable of stopping the attack, and continuously monitors those protections for change. If a control drifts or weakens, Reach alerts you and provides recommendations on how to activate the right controls to reinforce protection and mitigate the vulnerability.



01

Keep exploits out until patches go in

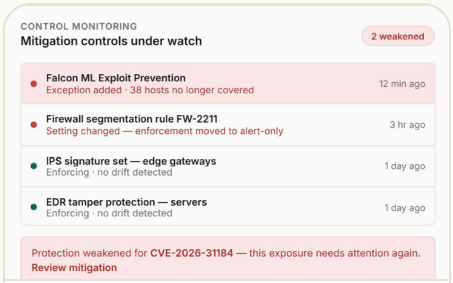
Put compensating controls to work to close security gaps until patches are ready. Separate vulnerabilities mitigated by existing controls from those that remain exposed. Focus remediation on the vulnerabilities that need attention first while normal patching continues across the rest.



02

Prove the control really protects

Go beyond whether a compensating control exists. Reach evaluates whether it is deployed, enforcing, in the right path, current, and capable of stopping the exploit, with evidence behind every determination.



03

Know when protection changes and how to fix it

Controls drift, settings change, and exceptions get added. Reach continuously monitors the controls behind mitigation decisions so teams can identify when protection weakens and activate the correct configuration to reinforce protection and mitigate the vulnerability.

Mitigate vulnerabilities with compensating security controls

LEARN MORE AT

reach.security/connect