CHECK POINT

EXPOSURE MANAGEMENT

Safe Remediation:

Confident Remediation in Production



Remediation carries operational risk. For CISOs and infrastructure security teams, a security change can affect production traffic, application availability, system performance, or business operations. The potential for disruption can slow remediation even when the exposure itself is well understood.

The pressure to act is increasing. Vulnerability volumes continue to grow, and advances in automation and AI are accelerating exploitation. Patching production systems can require testing, coordination, and scheduled change windows, extending the time an exposure remains available.

Safe Remediation evaluates remediation actions using evidence from the organization's environment before enforcement. Security teams can understand the expected impact of a change, apply it with greater confidence, and verify the result after execution. Existing security controls can also provide faster protection during the patching process.

1 What is Safe Remediation?

Safe Remediation is the process of reducing an identified exposure through a remediation action that is evaluated for security effectiveness and potential operational impact.

Security capabilities behave within the specific context of each organization. Enabling a protection can affect legitimate traffic, system performance, or business operations depending on the environment. Safe Remediation evaluates the behavior of the specific security capability within that environment before it progresses into enforcement.

Remediation actions are targeted to the specific exposure and protection being addressed. This focused approach allows the potential effect on business operations to be evaluated before a change is applied.

The process follows four stages: Observe, Prove, Act, and Confirm. Observe collects information from existing security and IT tools. Prove evaluates the proposed action using evidence from the environment. Act applies the approved change through the relevant control or management system. Confirm verifies that the action was implemented successfully.

The Safe Remediation Process

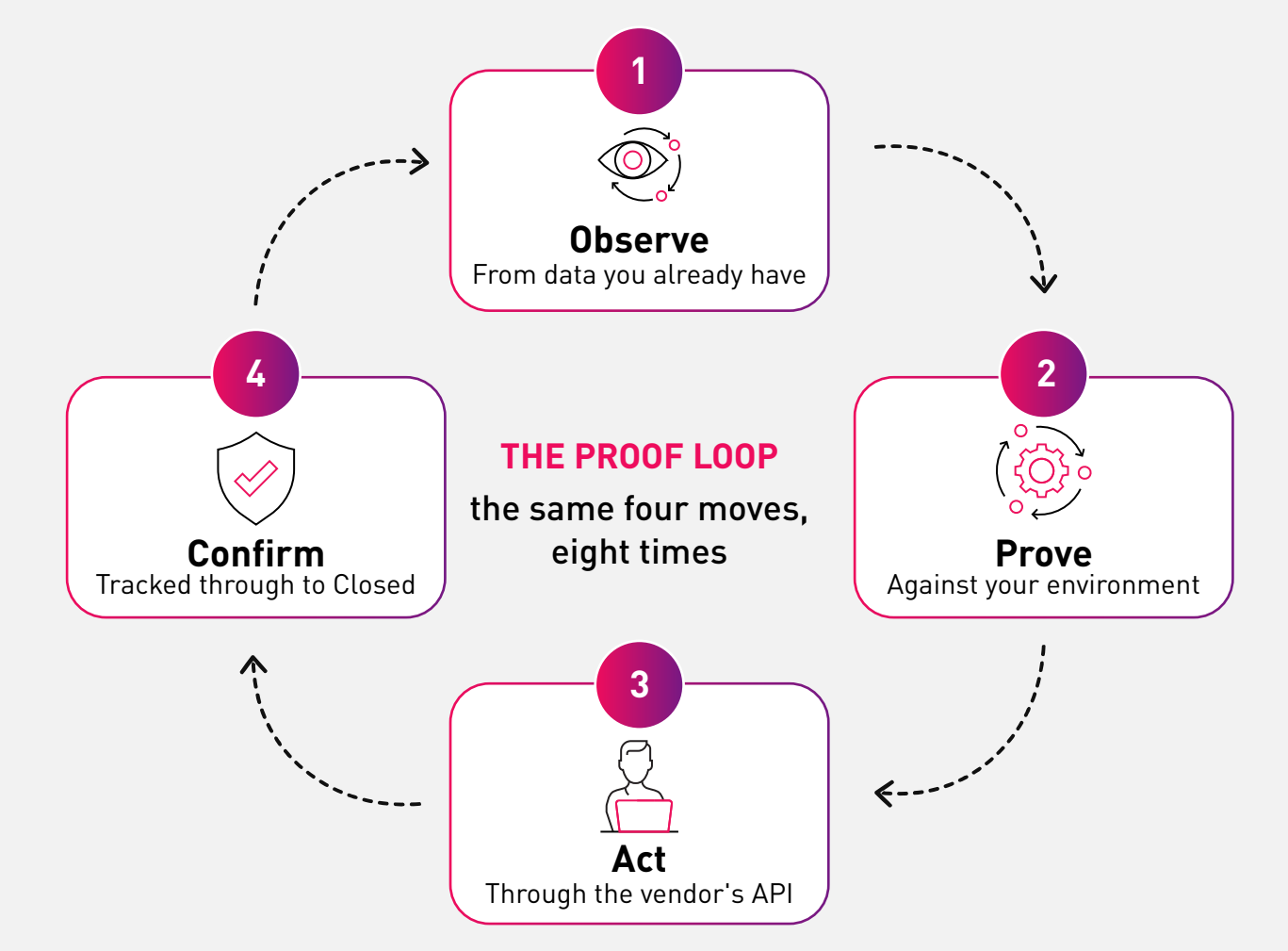


Figure 1. The Safe Remediation process moves from environmental observation through validation, execution, and confirmation.

2 Why Safe Remediation Is Needed

The time between identifying an exposure and reducing it creates an opportunity for exploitation. Operational concerns can extend that window when teams need evidence about how a proposed change will affect production.

Existing protections may remain inactive or in Detect mode as teams evaluate performance, false positives, and business continuity. Security configurations also change over time as applications, network segments, traffic patterns, and exceptions evolve.

Across measured organizations, 47% had less than 50% protection enablement. This highlights opportunities to identify security capabilities already available in the environment that can be activated or adjusted as part of remediation.

These conditions create a remediation challenge. Security teams need enough evidence to act quickly with confidence that the proposed change will preserve production stability. Safe Remediation evaluates current environmental evidence to support that decision.

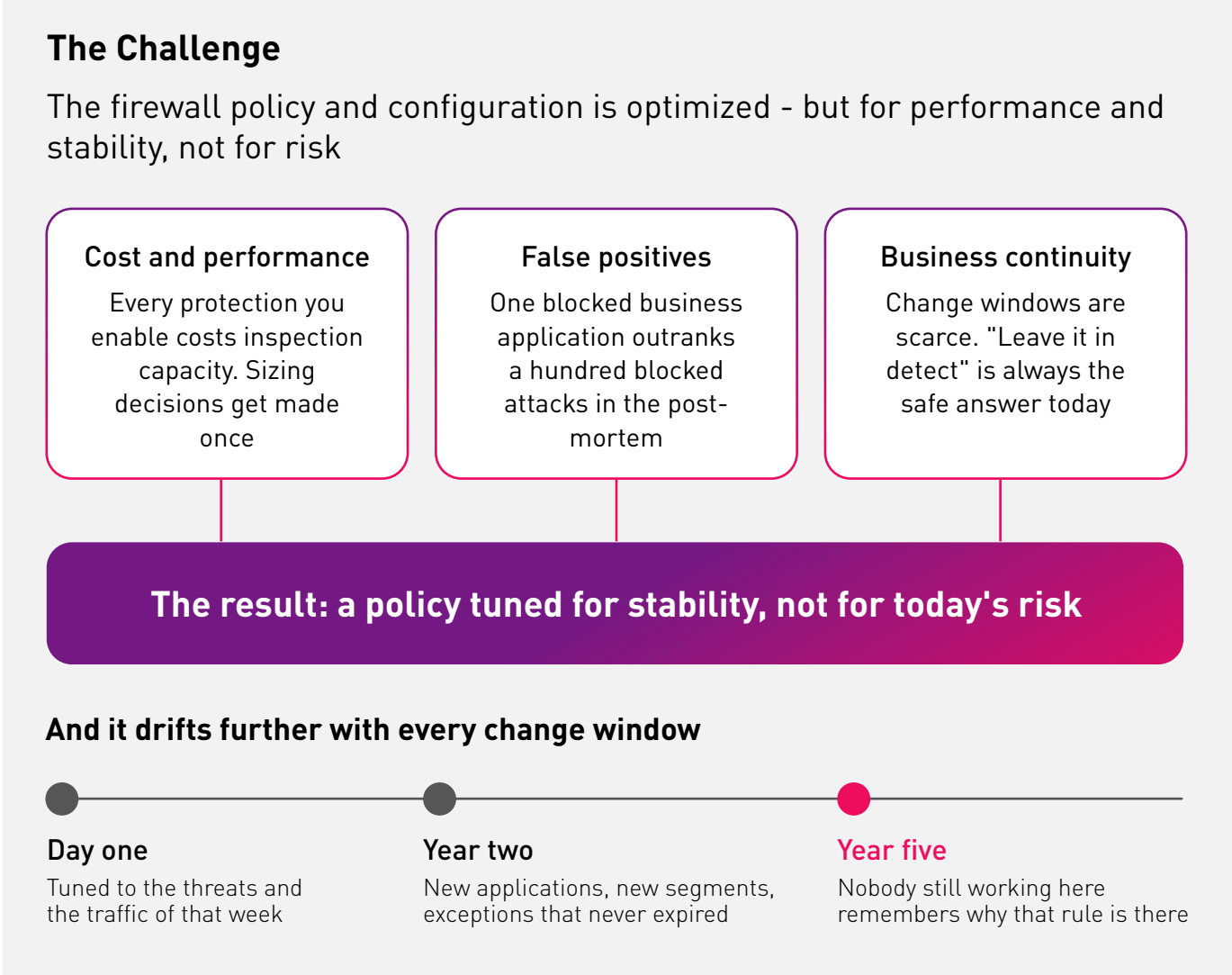


Figure 2. Performance requirements, false positives, business continuity, and configuration drift can influence how security protections are configured over time.

3 What Needs to Happen Before Safe Remediation?

Safe Remediation begins with an exposure that has already been identified and prioritized for action. Exploitability, asset context, existing security coverage, and available controls help determine the appropriate remediation path.

The example below shows how additional context can narrow a large vulnerability queue into a much smaller set of exposures requiring action. In one sample environment, 338 findings were identified. Of these, 283 had a CVSS score of seven or higher, 89 had a confirmed public exploit, 63 were identified by a cybersecurity agency as actively exploited, and one had no compensating control in place.

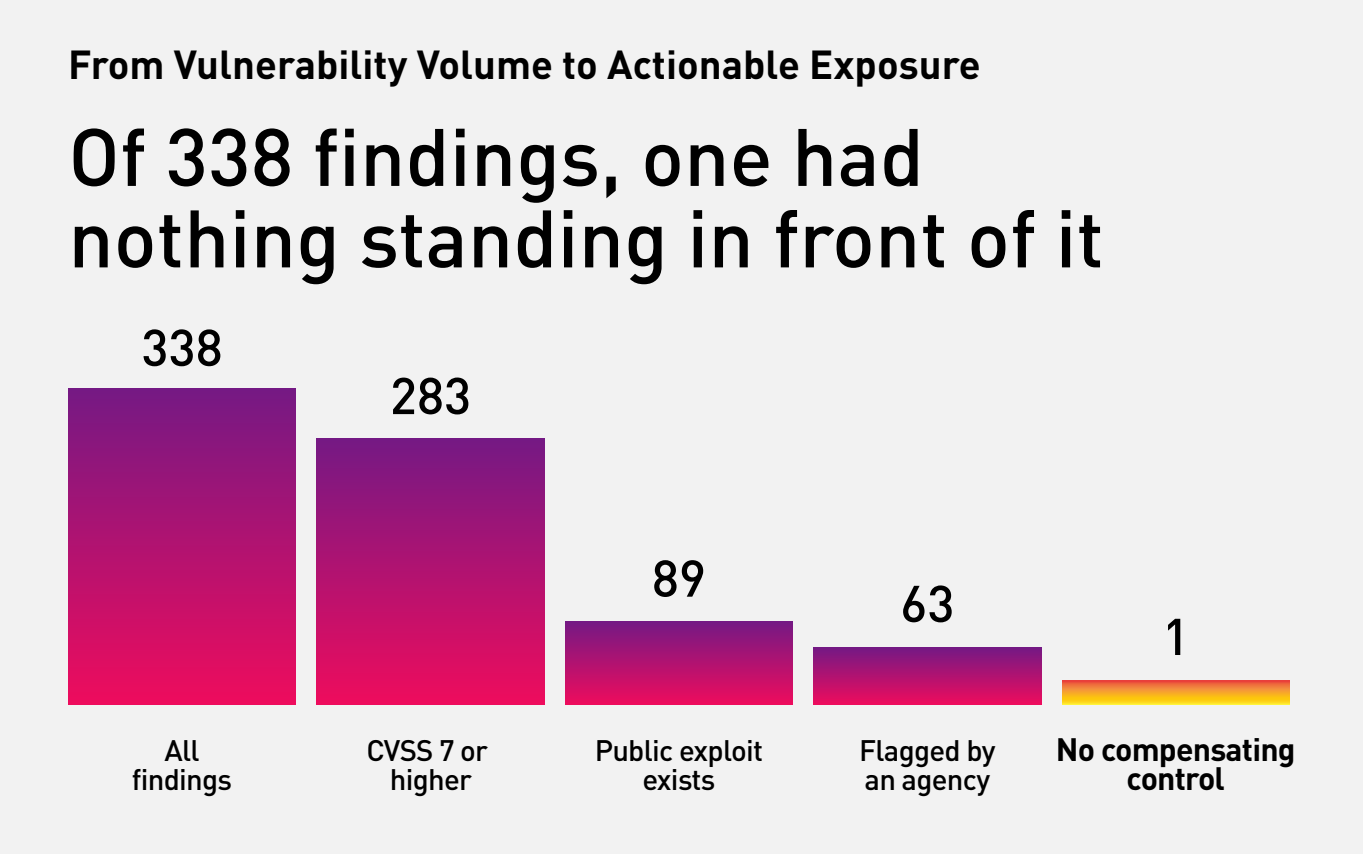


Figure 3. Example exposure prioritization in a sample environment.

Improving Exposure Confidence

Before an exposure moves into remediation, security teams need sufficient visibility and confidence in the underlying findings. Unscanned assets and potential false positives can affect that picture by creating gaps in coverage or introducing findings that may not require action.

Unscanned assets can leave security teams without the information needed to identify vulnerabilities and assess exposure. Surfacing these assets helps identify coverage gaps and bring them into the exposure management process.

False positive detection helps identify findings that require further evaluation. Reviewing these findings helps improve the accuracy of the exposure data used to prioritize remediation activity.

4 Types of Safe Remediation

Every remediation action introduces a production consideration. Enabling an IPS protection can affect legitimate traffic. A configuration change can affect an application or endpoint. A hardening action can influence system behavior. Security teams need confidence that the selected action will reduce exposure and preserve the systems that depend on it.

Safe Remediation can use security capabilities across the operating system, endpoint, network, web application, SASE, cloud, and other security layers. The remediation types described below represent examples of the actions and conditions Safe Remediation can address across these environments. Additional remediation types can be supported based on the exposure, affected asset, available controls, and operational requirements.

Direct Patching and Virtual Patching

When a patch is available and ready for deployment, patching addresses the underlying vulnerability. Asset criticality, exploitability, exposure, and existing protection can help determine patch priority.

Patching production systems can require testing and coordination before deployment. During that period, an existing security control can serve as a compensating control by blocking the relevant exploit path. This virtual patch can reduce immediate exposure during the patching process.

Safe Remediation can correlate vulnerability data with existing IPS coverage to identify whether a relevant signature exists and determine its current enforcement state. A protection operating in Detect can become a candidate for hardening. An exposure without an available compensating control can be directed toward patching or another remediation action.

IPS Activation and Hardening

Safe Remediation can identify IPS protections that are inactive or operating in Detect mode and evaluate whether they are ready for enforcement.

IPS logs provide evidence about false positives and traffic behavior. CPU utilization provides information about the operational capacity of the underlying device. Protections mapped to exploitable vulnerabilities can receive higher priority.

Activation moves an inactive protection into Detect, where it can inspect traffic and generate telemetry. After validation, an eligible protection can progress from Detect to Prevent.

Once the policy installation completes, the associated insight closes and the protection is confirmed as enforced.

Check Point Exposure Management data found that IPS and WAF protections blocked an average of 2,032 attacks per organization in the analyzed environments.

Indicator Enforcement

Threat indicators can be collected from subscribed intelligence feeds and internal sources, deduplicated, and matched with the security controls capable of enforcing them.

Each indicator is evaluated against the indicator types supported by the target control. An unsupported indicator type is skipped for that control and remains available to compatible controls. Once distributed, the installed state shows which enforcement points received the indicator.

Indicators that have been deliberately deleted or excluded remain excluded, preventing a subscribed feed from introducing them again.

Over one month, 11.27 million IoCs were deployed in response to attacks observed across the measured environments. IoCs are enforced for six hours before removal to limit false positive risk.

Adaptive block lists provide another form of indicator enforcement. Gateway access logs identify malicious indicators that should be blocked. Addresses that have not been observed for more than a week are removed, allowing the list to adjust as activity changes.

Operating System Hardening

Operating system hardening begins with detection scripts that identify targeted configuration states without modifying the host.

When remediation is selected, a corresponding hardening script can be applied through existing patch management infrastructure to a selected test group. Each host is checked again after execution, providing a before and after view of whether the targeted configuration is still detected.

The results from the test group can then inform broader deployment of the configuration change.

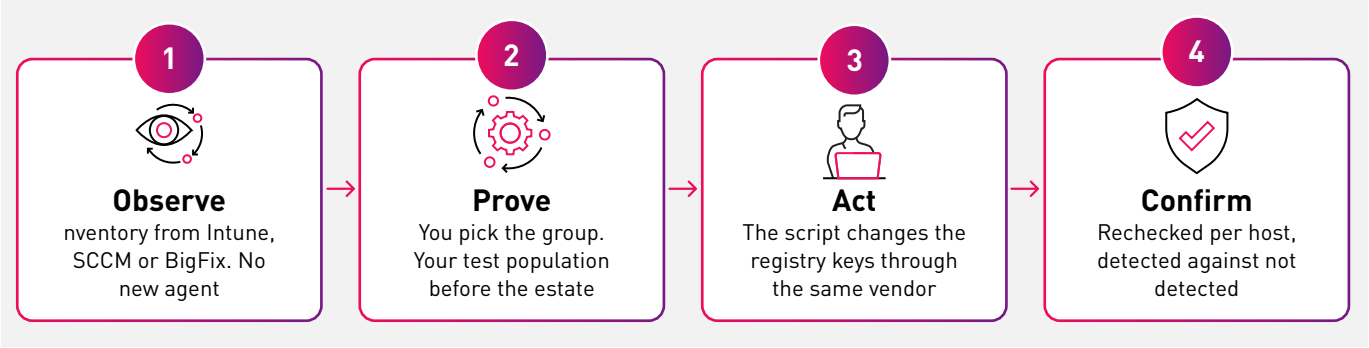


Figure 4. Operating system remediation can be validated through a selected test population before broader deployment, with affected hosts rechecked following execution.

Endpoint Hardening

Safe Remediation can also evaluate the active configuration of endpoint security products. Policy and module states are collected through the vendor API and compared with the vendor's hardening baseline.

Where the vendor API supports remediation, configuration changes can be written directly into the existing endpoint console. Settings that cannot be changed through the available API remain visible as recommendations for manual action.

System Health

Safe Remediation can identify system health conditions that may affect the availability or operation of security products. Examples include an expired license, an available software update, an available product update, or a product that has been disabled.

These conditions can leave security capabilities unavailable, outdated, or inactive. They can be surfaced as remediation opportunities so security teams can restore or update the affected product and maintain the security capabilities available in the environment.

Infrastructure Takedown

External exposures can require action against malicious infrastructure, phishing sites, impersonating profiles, or malicious applications.

Check Point Exposure Management data shows a 99%+ overall takedown success rate, with an average MTTR of 12 hours. 78% of takedowns were completed within 12 hours.

Compensating Controls

Compensating controls extend beyond virtual patching. Safe Remediation can identify security capabilities already present across the environment that can reduce exposure during the remediation process. These can include IPS protections, endpoint controls, network protections, and other available enforcement mechanisms.

Using existing security capabilities can shorten the time between exposure identification and protection, particularly when a permanent fix requires additional testing or deployment time.

These examples represent a selection of the remediation types Safe Remediation can support. Additional remediation actions can address other security conditions across the technologies and controls available in the environment.



5 Validating the Remediation

Validation gives security teams the confidence to remediate in production. Before a proposed action is enforced, Safe Remediation evaluates how that action is expected to behave in the organization's environment. The goal is to identify potential operational impact early and establish evidence that the remediation can proceed safely.

Validation continues through execution and confirmation. The evidence used depends on the remediation type. Vulnerability remediation incorporates exploitability, exposure, asset context, and existing protection. IPS validation uses production traffic and device performance. Indicator enforcement checks compatibility with each target control. Operating system changes use staged deployment and host verification. Endpoint hardening uses the security vendor's baseline.

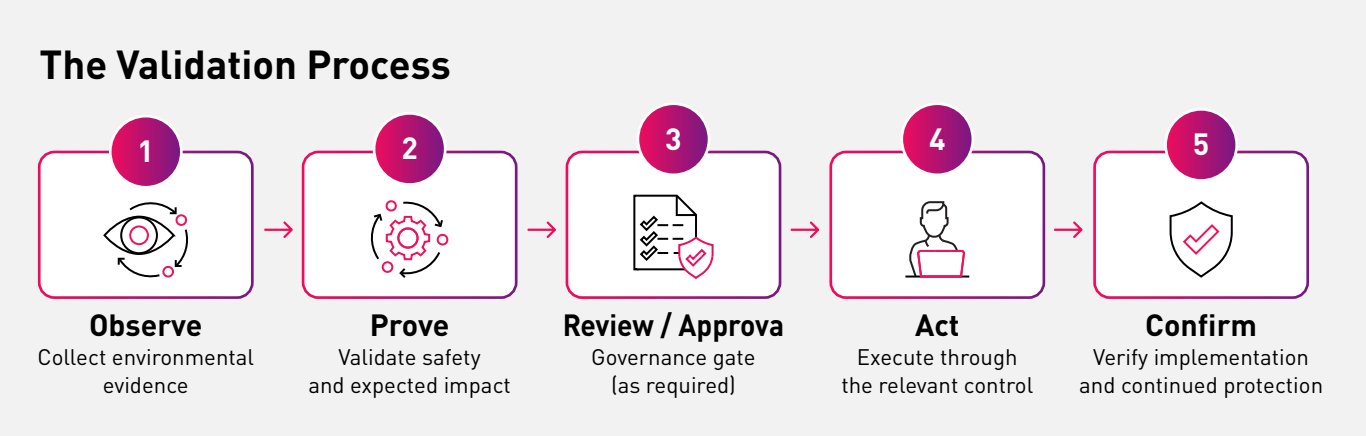


Figure 5. Safe Remediation validation from evidence through execution and confirmation.

Observe

Safe Remediation collects data already generated by security and IT systems. Depending on the remediation, this can include access logs, vulnerability findings, IPS traffic, endpoint policies, patch management information, and configuration states.

Safe Remediation uses an agentless model, relying on telemetry and APIs from existing systems to evaluate and execute remediation actions.

Prove

The proposed action is evaluated using evidence from the organization's environment. The telemetry used during validation depends on the security capability being evaluated.

For security controls, validation can incorporate logs, threat prevention logs, device CPU utilization, and metadata associated with observed attacks. This evidence is used to evaluate how the specific security capability behaves within the production environment and assess potential operational impact before the action proceeds.

IPS provides one example. A protection can operate in Detect mode, inspecting live traffic and generating telemetry with enforcement disabled. For IPS protections, validation can observe production traffic over time to evaluate false positives, traffic behavior, and device performance. Protections that complete validation can become eligible to progress from Detect to Prevent.

Depending on the remediation and available environmental evidence, validation can continue for up to seven days to evaluate behavior under production conditions.

Other remediation types use evidence appropriate to the technology involved. Operating system remediation can use a test population. Endpoint hardening can evaluate configuration against the vendor's baseline. Indicator enforcement can determine whether the target control supports the relevant indicator type.

Review and Approval

Review and approval can serve as a governance gate between validation and execution. The analysis used to evaluate remediation safety is automated. Organizations can require approval of the proposed action and its scope before execution or enable automated execution according to their configured workflows.

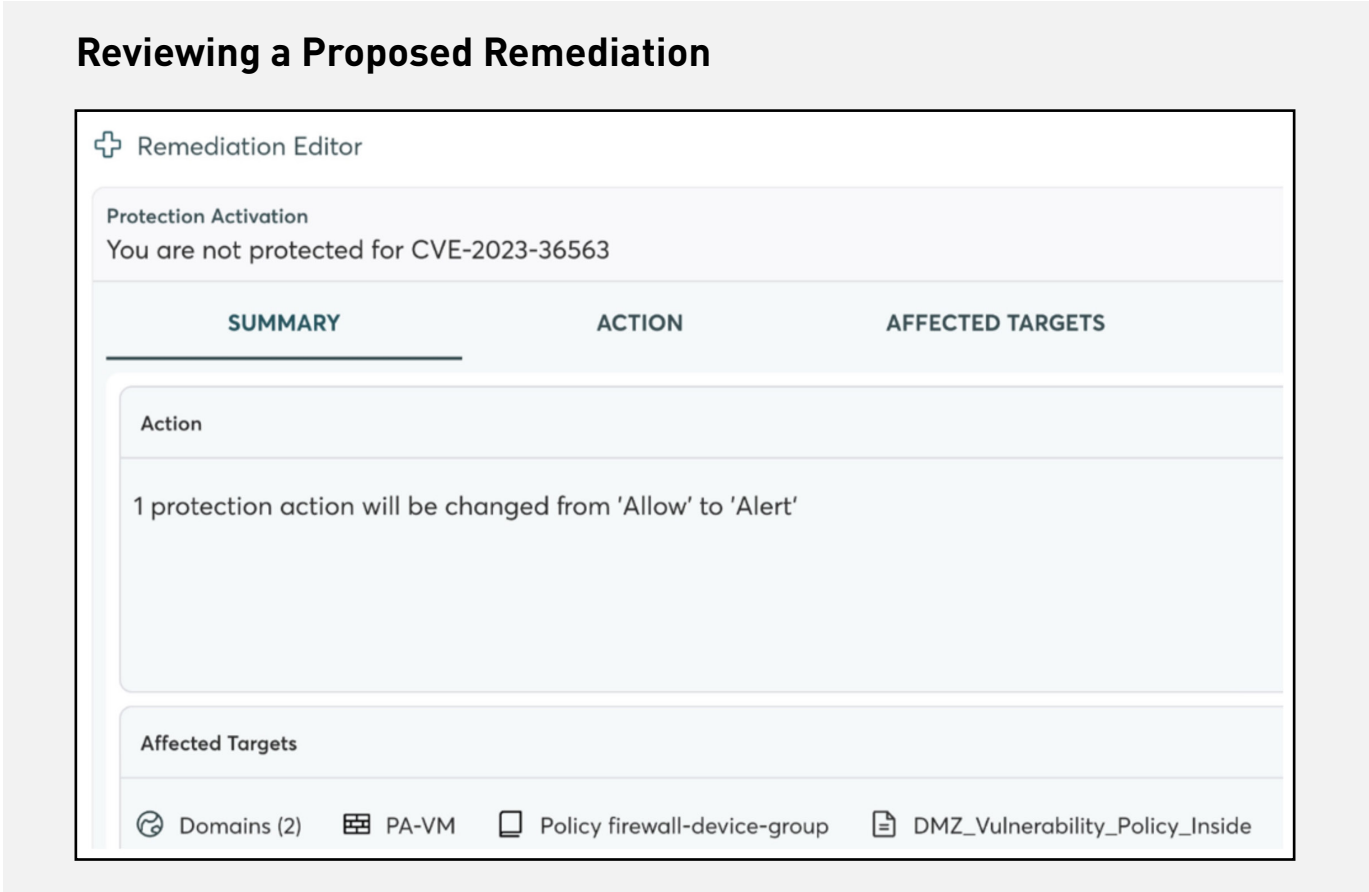


Figure 6. The Remediation Editor presents the proposed action and affected targets for review before approval.

Confirmed actions are recorded in a tamper evident audit trail with the user, timestamp, and associated insight. This creates a record of the action and its approval.

Act

Once the remediation is cleared for execution, it is applied through the system responsible for the affected control.

IPS changes are distributed through the management server. Operating system hardening uses existing patch management infrastructure. Endpoint configuration changes are written through the endpoint vendor API.

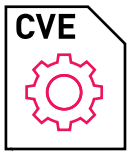
One month of remediation activity included 2.6 million IP IoC actions, approximately 1 million CVE protection actions, and 540,000 file protection actions.

Remediation Volume in a Sample Environment:



2.6M

IP IoC actions



~1.1M

CVE protection actions



540K

file protection actions

Confirm

Confirmation establishes that the remediation reached its intended state and provides evidence that the resulting protection remains in place. This gives security teams evidence that the change persists after execution.

Execution is tracked through lifecycle states including Queued, Remediating, Pending, Installing, Closed, and Failed.

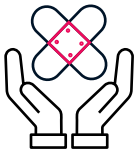
Confirmation is specific to the remediation action. For IPS, the associated insight closes after policy installation completes, confirming that the protection reached enforcement. For operating system hardening, affected hosts are rechecked after execution to determine whether the targeted configuration remains detected. Endpoint changes are written through the vendor API and reflected in the endpoint environment.

Across all measured organizations, remediation actions recorded a 99.5% success rate.

Subsequent security events can also demonstrate the value of the remediation. When an attack attempt is blocked by a protection enabled through Safe Remediation, security telemetry can show that the enforced protection prevented activity associated with the exposure.

Over the same one month period, protections applied through remediation subsequently blocked 703.56 million attacks. Of those, 21 million attacks were blocked within 24 hours of remediation. This provides measurable evidence of protection following execution.

Remediation Outcomes:



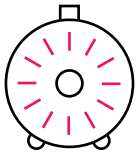
99.5%

remediation success rate across all measured organizations



703.56M

attacks blocked following remediation over one month



21M

attacks blocked within 24 hours

6 From Remediation Confidence to Scale

Safe Remediation creates a repeatable process for evaluating remediation actions before they reach production. When security teams have evidence that a proposed action has been validated against their environment, they can move from exposure identification to remediation with greater confidence.

Environments averaged 381.2 remediations per environment per month. The average time from finding an exposure to taking a remediation action was nine hours.

That confidence supports remediation at scale. Validated actions can be executed quickly through existing security controls and management systems. Workflows can support multiple approved remediation actions and maintain visibility into the status and outcome of each change.

Production telemetry, environmental context, and validation results give security teams evidence about the expected impact of a proposed change. This evidence supports faster approval and execution across larger volumes of exposures.

Check Point Exposure Management connects exposure prioritization, validation, execution, and confirmation in a single remediation process. Environmental evidence informs the action. Validation evaluates its expected impact. Execution applies the change. Confirmation verifies the resulting state. Security teams gain a consistent path from identified exposure to validated risk reduction.

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

© Check Point, 2026. All Rights Reserved.