CHECKLIST · EXPOSURE MANAGEMENT

10 POINTS

Safe Remediation Best Practices

Your essential checklist for reducing risk without disrupting operations.

Finding an exposure is only the beginning. Addressing it requires choosing the right remediation action, understanding its potential impact, and confirming that the fix works as intended. Use this 10-point checklist to make informed remediation decisions while protecting business operations.

01 Understand the Risk

Before taking action, establish what needs attention and why.

- [ ] Look beyond vulnerability severity. Consider exploitability, active threats, asset criticality, and business impact to determine which exposures require immediate attention.
- [ ] Understand what's already protected. Review existing security controls to identify protections already in place and determine where additional action is needed.
- [ ] Identify affected assets and dependencies. Understand which systems, applications, and services are exposed, including how they connect to business operations.

02 Choose the Right Response

The best remediation approach depends on the exposure, available controls, and operational requirements.

- [ ] Consider alternatives to patching. Evaluate options such as virtual patching, IPS protections, configuration changes, and security policy updates when immediate patching is impractical or too slow.
- [ ] Work with your existing security stack. Identify which deployed security controls can address the exposure and coordinate remediation through those technologies.

03 Validate Before Enforcement

Reducing risk should not introduce unnecessary operational disruption.

- [ ] Assess the potential impact. Determine how the proposed remediation could affect legitimate traffic, applications, services, and system availability.
- [ ] Verify the scope before applying changes. Confirm that the intended assets, configurations, and policies are targeted. Test or simulate changes where

supported.

- [ ] Prepare for unexpected outcomes. Establish appropriate approvals, define rollback procedures, and consider a controlled rollout for changes that could affect critical operations.

04 Confirm the Outcome

A remediation action is only successful when its effectiveness has been verified.

- [ ] Validate that the exposure was addressed. Confirm that the intended security action was applied successfully and that the relevant protection is active.
- [ ] Check for unintended disruption. Review application behavior, system health, and security telemetry to identify unexpected effects following remediation.

Fix Fast. Break Nothing.

Safe Remediation combines risk context, remediation intelligence, and operational validation to help security teams select effective actions and reduce exposure through existing security controls. With Check Point Exposure Management, organizations can connect exposure discovery, prioritization, and remediation across technologies from different vendors.

Book a Demo Ready to see Safe Remediation in action?