CHECK POINT™

Infinity

Threat Exposure Management

# Essential License Package

Check Point Infinity Threat Exposure Management is an AI-driven exposure assessment and remediation platform that continuously identifies vulnerabilities, misconfigurations, and exploitability across the entire security stack. By leveraging compensating controls and layered defense strategies, Check Point ensures potential and active threats are proactively managed and remediated - all without disrupting business continuity.

With the ability to unify exposure data across cloud, hybrid, and on-prem environments, the platform ensures that no critical risks are missed. Unlike point solutions limited to siloed views, Check Point offers full-stack unified exposure visibility, deployment is frictionless, agentless and supports over 70 native integrations so organizations can achieve immediate value without operational overhead.

Beyond visibility, the platform enables safe remediation through continuous control assessments that validate security effectiveness and business impact before offering any fix. Whether it's hardening configurations, eliminating false positives, or prioritizing vulnerabilities, remediation actions can be executed via direct APIs, existing workflows, or ITSM tools for maximum flexibility and risk reduction.

The Check Point Threat Exposure Management Vulnerability Remediation Package is comprised of the following capabilities.

| Capability | Description | Vulnerability Remediation License Package |
|---|---|---|
| **Network Security Controls Included By Default (firewalls; WAF; etc.)** | Threat Exposure Management supports a variety of Security Controls, including NGFW and WAFs. Network Security Controls are the main pillar for pricing. | 5 |
| **Network Security Control integrations allowed** | Network Security Controls supported in selected package | Check Point Only |
| **External Vulnerability Source (i.e. VA/VM scanners; Wiz; CAASM; EDR; ASM; BAS; MDM/UEM)** | Which external vulnerability scanners can be integrated with Threat Exposure Management | Wiz / Harmony Endpoint / Infinity External Risk Management |

| Capability | Description | Vulnerability Remediation License Package |
|---|---|---|
| **Number of Assets (i.e. seats; servers; users; workloads; endpoints) Included By Default** | Threat Exposure Management supports a variety of Security Controls, including but not limited to: EDR, UEM, CNAPP. Assets are the second pillar for pricing. | 500 |
| **Network Security control assessment and hardening** | Assess and harden your security controls – harden protections from Inactive to Prevent | Network Only |
| **Identify False Positives** | Proactively identify False Positives in network traffic | ✓ |
| **Vulnerability Prioritization and Remediation** | Prioritize, deduplicate and remediate vulnerabilities detected by your vulnerability scanners (Including Actual Patching and Virtual Patching) | - |
| **Custom Protections** | Custom protections provided by Threat Exposure Management; helps you elevate your security posture | - |
| **IoC Mgmt. – Manual operations** | Manually Add, Update and Delete IoCs from your security controls; including bulk upload | ✓ |
| **IoC Mgmt. – Cross-Platform Enforcement** | Disseminate IoCs detected on one of your security controls to all your integrated Security Controls | - |
| **IoC Mgmt. - Feed Ingestion (i.e. Adaptive; Attack Surface Threats; Torrent; Shodan.io)** | Automatically ingest and disseminate IoCs from various feeds (commercial, open source, government, proprietary) | - |
| **Private Exposure Map** | A private exposure map that helps you visually view and filter the different exposures of your organization | - |
| **Endpoint and Operating SysThreat Exposure Management Security Control Assessment and Hardening** | Assess and harden your Endpoint and Operating SysThreat Exposure Management security controls | - |

# Licensing Details

The licensing instructions are related to all Threat Exposure Management packages: Vulnerability Remediation, IoC Management, Vulnerability Remediation, Complete.

| | Licensing Instructions |
|---|---|
| **Vulnerability Remediation Package** | Installation and Integration - Customers will receive up to 8 hours of Professional Services as part of the license for Vulnerability Remediation and Management tiers. The Complete tier will include up to 12 hours. |
| | CSM Onboarding - Customers will receive up to 8 one-hour onboarding sessions to help them get trained and start using Veriti effectively (included in Vulnerability Remediation and IoC Management). The Complete tier will include up to 12 hours. |
| | Network Security Controls (First pillar for pricing)<br>• Any NGFW or WAF is included<br>• Cloud deployments like Cloudflare are considered as a single asset<br>• Virtual/Physical appliances are counted based on their count |
| | Network Security Control integrations allowed<br>• Which Network Security Controls are allowed in the package<br>• For Vulnerability Remediation only CP is allowed |
| | External Vulnerability Source<br>• Vulnerability scanner that can be integrated with Threat Exposure Management<br>• For Vulnerability Remediation only CP and Wiz are allowed |
| | Maximum number of Assets (seats, servers, users...) (Second pillar for pricing)<br>• We license against two pillars: Network Controls (Firewalls and WAFs) and Assets (anything that isn't a Network Security Control), such as workloads, endpoints (servers, desktops, and pcs), etc. |

**The following table displays the number of default network security controls and assets per pricing tier for the Vulnerability Remediation Package**

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **# of Network Controls** | 5 | 10 | 20 | 50 | 100 | 200 | 500 | 1,000 |
| **# of Assets/Users** | 500 | 1,000 | 2,000 | 5,000 | 10,000 | 20,000 | 50,000 | 100,000 |

When counting network security controls and assets, we use the maximum number of the two to determine the amount needed.

## Examples

**Question:** What differentiates a Network Security Control (default limit: 5) from an Asset (default limit: 500)? Are Network Security Controls defined as a subset of assets? E.g., an environment of 2 firewalls, 2 servers, and 10 users equals 14 assets with 2 NETWORK SECURITY CONTROLSs (firewalls)?

**Answer**: We license against two pillars: Network Controls (Firewalls and WAFs) and Assets (anything that isn't an NETWORK SECURITY CONTROLS), such as workloads, endpoints (servers and PCs), etc. In your example 10, you should use the MAX of all assets.

---

**Question**: If a customer has 30 VM workloads and 500 endpoints, should we count 500 assets or 530?

**Answer**: 500 Assets

---

**Question**: The max amount of Network Security Controls is 5, but what if you need more than 5?

**Answer**: If you need more than the maximum 5 network security controls, you can select the add-ons to increase the amount or choose a different package.

---

**Question**: How do you calculate clusters/HA security gateways

**Answer**: Each security gateway is considered as a Network Security Control.

## Additional Services

**Services plan:** Choose a subscription term from 1 to 5 years. The default selection is 1 year. If desired, you can extend the service period to 2, 3, 4, or 5 years.

**Assets and Users:** For additional Network Security Controls and Assets, two add-ons are available to expand coverage. Additional Threat Exposure Management Network Security Controls and Additional Threat Exposure Management Assets.

## Support

Support services are included with each subscription. The standard support term is one year and matches the solution period. Support is delivered as Direct Enterprise Support, expert assistance from Check Point engineers to help you get the most from your deployment. The recommended Premium level provides 24x7 coverage every day with a committed 4-hour response time. An optional Elite level also offers 24x7 coverage, adding on-site expert care, committed response times, and priority handling for critical service requests.

Each package includes comprehensive onboarding and ongoing support to ensure you get the most value from Threat Exposure Management:

**Threat Exposure Management Installatio**n – Full setup and deployment (for customers without prior Proof of Concept).

**Integration Assistance** – Support for integrating Threat Exposure Management with all supported security products in your environment (existing or future).

**Initial Training** – Six one-hour Customer Success Manager (CSM) sessions covering configuration, usage, and best practices.

**Ongoing Enablement** – Quarterly CSM meetings for continued training, feature updates, and system health checks.

**Worldwide Headquarters**
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

**U.S. Headquarters**
100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391

**www.checkpoint.com**