CHECK POINT SERVICES

Managed Services
Managed XDR/XPR



Infinity XDR/XPR consolidates and correlates threat data across the security estate using native correlation algorithms, Threat Cloud AI and third-party intelligence to identify threats that would otherwise remain undetected. It enables security teams to prevent, detect, investigate and respond to advanced cyber threats across on-prem and cloud environments. The platform uses machine learning, predefined and custom detection rules, and deep visibility for rapid incident detection. Automated remediation helps organizations quickly and accurately contain threats.

Infinity Playblocks automated response playbooks activate immediately upon threat detection, containing threats, preventing damage, mitigating lateral movement and reducing operational effort.

The MXDR service scope includes platform and data source management, analytics and detection tuning, Playblocks configuration, incident investigations, threat hunting and guided response.

Service Description Details

Infinity XDR/XPR correlates threat data across the environment and applies AI-driven analytics to expose critical threats. Automatic playbooks prevent spread, and clear forensics provide fast context for analysts.

Supported data connectors include:

- Check Point Quantum Security Gateway
- Smart-1 Cloud
- CloudGuard Network
- Harmony Endpoint
- Harmony Email and Collaboration
- Microsoft 365 Defender for Endpoint
- Fortinet FortiGate
- Palo Alto Networks Firewall
- CrowdStrike Falcon
- SentinelOne Singularity
- Trend Vision One
- Cisco Firepower

Service categories:

- **24/7 Infinity XDR/XPR platform management**: configuration management for data sources, daily policy tuning, incident handling and Playblock optimization.
- **24/7 managed detection and response**: investigation and response across all connected data sources.
- **SLA and incident handling**: continuous alert and incident management.
- **Ongoing collaboration and reporting**: customized runbooks, communication plans, ticketing integrations, bi-weekly meetings.
- **Onboarding project**: review, configuration and enablement of the solution.

CHECK POINT SERVICES

Our managed services team co-manages Infinity XDR/XPR threat data to help customer SOC teams detect stealthy multi-vector attacks. The team also co-manages automated Playblocks for immediate containment and mitigation.

Infinity AI Copilot augments both customer and managed services teams with generative AI for enhanced analysis and response. Analytics apply to supported connectors listed in the administration guide.

Managed Detection and Response Services

Check Point MXDR provides continuous monitoring and investigation of incidents generated by the Infinity XDR/XPR platform. This prevention-focused service provides access to experienced analysts, researchers and incident responders. Every alert or incident is reviewed and acted upon.

SLA and Incident Handling

All customer-reported or system-generated incidents are reviewed, prioritized and communicated.

Managed Services SLA

Priority	Description	Response time
Critical Infinity MDR or threat hunting incident	Notification upon confirmation of malicious activity	24x7 / 30 minutes
Critical or emergency	System down or critical alerts requiring emergency response	24x7 / 2 hours
High	High severity items with same-day priority	4 hours / same business day
Medium	Medium severity items with next business day priority	12 hours / next business day
Low	Low priority items	Best effort

MDR SLA: upon confirmation of malicious activity, an incident is published and notification sent within 30 minutes, 24/7.

Ongoing Collaboration and Reporting

- Bi-weekly standups and reporting
- Dedicated Microsoft Team for communication and document sharing
- Check Point ticketing portal
- Optional ticketing system integration via API

CHECK POINT
SERVICES

Solution Onboarding Project

1. Planning
Solution review; co-managed access review; communications and escalation planning; ticketing onboarding; scheduling of standups and reporting cadence.

2. Solution setup and initial configurations
Infinity Portal tenant setup including connectors, IoC administration, policies, reports, exclusions and notifications.

3. Advanced configurations
Exploration and configuration of Playblocks automation.

4. Monitoring, runbooks and collaboration
Runbook creation for ticket levels 1 to 3, communication and escalation planning, and optional Microsoft Team setup and integrations.

Project Completion

Final report, review meeting, confirmation of schedules and agreement on production start date

Learn More:

To learn more, contact us today at services@checkpoint.com