



Uptime v3 Agreement - Special Conditions for Checkpoint, Blue Coat- Crossbeam and EMC-RSA Products

1 Definitions and Interpretation

- 1.1 “**Best Effort Commitment**” means NTT will endeavour to resolve Incidents within a timeframe with no guarantee and taking into account any external factors that are out of its control such as international cross - border customs clearing.
- 1.2 “**Blue Coat-Crossbeam**” means Blue Coat Systems, Inc. headquartered in Sunnyvale, California, United States and Crossbeam Systems which was acquired and absorbed by Blue Coat Systems in 2012.
- 1.3 “**Check Point**” means Check Point® Software Technologies Ltd headquartered in Tel Aviv, Israel.
- 1.4 “**EM C-RSA**” means **EM C Corporation (stylised as EM C²)** headquartered in Hopkinton, Massachusetts, United States and RSA Security, Inc. which was acquired by EMC Corporation in 2006 and operates as a division within EMC.
- 1.5 “**Next Business Day (NBD) Commitment**” means the Commitment Level where the identification of hardware failure is confirmed before 15:00 on a Business Day, NTT will dispatch Parts to Site before 18:00 on the Next Business Day.

2 Application

- 2.1 For the purposes of these special conditions “**Security Configuration Items**” means the products listed in clause 2.2.
- 2.2 These special conditions apply to:
- (a) Checkpoint:
 - (i) secure gateway hardware appliances:
 - A. NG Firewall;
 - B. NG Threat Prevention;
 - C. NG Secure Gateway; and
 - D. NG Data Protection;
 - (ii) software:
 - A. Software Secure Gateway;
 - B. Virtual Systems; and
 - C. Software Blades;
 - (b) Blue Coat-Crossbeam:
 - (i) hardware appliances:
 - A. X20, X30 and X50;
 - B. X60 and X80; and
 - C. NPM, APM and CPM blades;
 - (ii) Software f or X-series:
 - A. Check Point Secure Gateway;
 - (c) EMC-RSA;
 - (i) hardware appliances:
 - A. RSA SecurID Appliance 130 and 150; and
 - (ii) Software:
 - A. RSA Authentication Manager.
- 2.3 These special conditions do not apply to Security Configuration Items that have been classified as End-of-Life by Check Point, Blue Coat-Crossbeam or EMC-RSA.

3 Subscription Services

- 3.1 Subscription Services only provides Software support as described in clauses 4 to 9 inclusive.

4 Subscription Service options

NTT's obligations

- 4.1 NTT must provide the Client with the following Subscription Service options, the Service Elements of which are described in clauses 5 to 9 inclusive:
- (a) Service Level: Subscription Services:
 - (i) Access to SecureKnowledge Advanced™;
 - (ii) Patches;

- (iii) Upgrades; and
- (b) Service Level: Remote Support and Subscription Service:
 - (i) Access to SecureKnowledge Advanced™;
 - (ii) Patches;
 - (iii) Upgrades; and
 - (iv) Remote Support Response;
- (c) Service Level: Remote Support, Subscription Services and Software Engineer:
 - (i) Access to SecureKnowledge Advanced™;
 - (ii) Patches;
 - (iii) Upgrades;
 - (iv) Remote Support Response; and
 - (v) Onsite Technical Support

4.2 NTT must provide the Subscription Service options on the Software listed in clause 2.2

5 Access to SecureKnowledge Advanced™

NTT's obligations

- 5.1 This clause 5 applies to Check Point Security Configuration Items only.
- 5.2 NTT must provide the Client with advanced level access to SecureKnowledge Advanced™, the online, self-service knowledge base to answer technical installation, configuration and Upgrade needs in relation to Check Point Software, which includes expanded access to more detailed solutions, tips, resource guides, and in-depth diagnostic and troubleshooting tools to reduce solutions times and costs via the SecureKnowledge Advanced™.

6 Patches

NTT's obligations

- 6.1 NTT must provide the Client with access to all Patches as and when supplied by the manufacturer during the Term of this Agreement.

7 Upgrades

NTT's obligations

- 7.1 NTT must make Upgrades available to the Client during the Term of the Agreement upon receipt of a Service Request.
- 7.2 Availability of Upgrades is subject to the release of the Upgrade by the manufacturer.

Exclusion

- 7.3 NTT does not install the Upgrade.

8 Remote Support response

NTT's obligations

- 8.1 NTT must provide the Remote Support Business Continuity Level that:
 - (a) is available with a Response Commitment only (indicating the time within which an engineer will have commenced the Remote Support session); and
 - (b) provides for an engineer giving support through any combination of telephone, email or secure connection to the security Configuration Item.

9 On-site technical support

NTT's obligations

- 9.1 NTT must:
 - (a) if any Incident with a security Configuration Item cannot be resolved by telephone, dispatch a security Software engineer to the Client's Site within the Service Calendar and within the Response Time and if the Client's Site is within 50km of a mainland Australian capital city CBD;
 - (b) have a security Software engineer remain at the Site until one of the following Events occurs:
 - (i) the Incident is resolved;
 - (ii) resolution of the Incident requires escalation to the Software manufacturer and a suitable Workaround has been put in place;
 - (iii) resolution of the Incident requires escalation to the Software manufacturer and no suitable Workaround is available;

- (iv) a suitable Workaround has been put in place and there is a requirement to replicate the Incident in NTT's security lab to assist in finding a Permanent Resolution to the Incident;
 - (v) the Incident is determined to have been caused by a hardware failure; and
 - (vi) the Incident is determined to have been caused by an error or defect excluded in the Agreement;
- (c) f or all Incidents escalated to the Software manufacturer, have a security Software engineer return to the Site within the Response Time after receipt of a possible Workaround or Permanent Resolution from the Software manufacturer;
- (d) if the Permanent Resolution provided by the Software manufacturer is not successful, a security Software engineer will remain at the Site during Business Hours until one of the items listed in clause 9.1.b is reached;
- (e) f or all Incidents requiring replication within the NTT security lab, have a security Software engine er return to the Site within the Response Time after a Permanent Resolution to the Incident has been found;
- (f) if required, escalate any Incidents that cannot be resolved locally to the Software manufacturer, manage the Incident on the Client's behalf and provide regular updates on the Incident status;
- (g) if requested, assist the Client to resolve hardware issues and Restore the Security Configuration Item to its last know n working configuration by:
- (i) coordinating the resolution of hardware issues through the Inc ident management process if the hardware is covered by a NTT Uptime v3 Agreement; or
 - (ii) performing the required work at an Additional Charge.

The Client's obligations

- 9.2 In the event of hardware failure, the Client must resolve the hardware issue and Restore the Security Configuration Item to its last known working configuration.

10 Incident Management

- 10.1 Engineer to Site only provides hardware support as described in clause 10.

11 Engineer to Site

- 11.1 The Engineer to Site option applies to hardware appliances listed in clause 2.2.

NTT's obligations

- 11.2 NTT must, when the Site is within 50km of a mainland Australian capital city CBD dispatch an engineer to the Client's Site when an Incident on a Security Configuration Item that is a hardware appliance as specified in clause 2.2 is unable to be resolved remotely to:
- (a) provide a replacement hardware appliance; and
 - (b) perform the basic installation of the replacement hardware which includes racking, mounting and cabling of replacement hardware and initial Security Configuration Item setup to the point of configuration of a management interface that can be used to connect to the Security Configuration Item.
- 11.3 NTT may provide assistance to reload a configuration file backup at an Additional Charge if requested.