1.0 Definitions

Alert: A log received from the Device/Asset, parsed by VisionLink, and sent to ProVision

Client or Customer: The company procuring the managed service

Device/Asset: A combination of hardware, software and licensing that is to be monitored/managed as part of the Service. This is typically the Check Point FW

Event: An activity that has been identified by ProVision to represent a potential threat that warrants additional triage by the SOC analysts to determine the nature of the activity

Incident: An activity positively identified as a breach in progress and warrants immediate engagement of Client incident handling and response personnel

Log: A record of activity written by a security device, network element, computing platform, etc. for such purposes as recording events, errors, status messages, or other operating details

OBQ: OnBoarding Questionnaire. A document or online tool to gather all the required information to set up the Service.

OnBoarding: The activities and process to bring the Client in to live Service.

POC: Client point of contact for managed service

ProVision/Portal: Foresite's next-generation cloud-based managed services platform

Service Level: Basic, Essential, Advanced (see table in Section 2)

Security Management Portal (SMP): This is the Check Point centralized Management Station hosted by Foresite. Client does not have access to the SMP

SOC: Security Operation Center from where Foresite deliver the Managed Security Services.

Ticket: Comes in various forms such as, but not limited to;

- ***Support Ticket*** – Used to log and progress Tickets of a support nature (e.g. creation of a new user)
- ***Security Incident Ticket*** - An activity positively identified for further investigation that warrants follow up (e.g. Suspected Security Issue)
- ***Change Request Ticket*** – Used for creating requests for workload to be implemented (e.g. updating a set of Rules).

VisionLink: Foresite premise appliance responsible for log and security stream aggregation and processing data from SMP.

2.0 Solution Overview

There are 3 levels of service as described in the table below;

DESCRIPTION	Basic	Essential	Advanced
Check Point HW/Licensing	Y	Y	Y
Installation & Config	Y	Y	Y
Monitoring & Analysis	24/7/365	24/7/365	24/7/365
Notification	Portal/Email	Portal/Email	Portal/Email/Phone
Escalation	Portal/Email	Portal/Email	Portal/Email Phone/Triage
Online Log Retention	30 Days	30 Days	90 Days
Business Rules Package	P1	P1 & P2	Full Suite
Change Requests per year	2	4	6
Portal, Dashboards, & Reporting	Y	Y	Y
Advance Reporting	Chargeable	Chargeable	Quarterly
Patching & Hotfix	Y	Y	Y
System Upgrades	Y	Y	Y

*System Upgrades are included for minor upgrades that can be performed remotely. If onsite work is recommended and required, this may incur additional cost.

3.0 Service Scope

Hours of Operation: Foresite's Global Security Operations Centers (SOCs) operate 24 hours per day, 7 days per week, and 365/6 days per year.

Language Support: All Services, Portal and communications are provided in English language only.

Monitoring: Foresite will monitor the Device/Asset and push and Policies via the centrally hosted SMPand analyze the log stream from the Device/Asset under Service.

Management: In addition to the monitoring, Foresite will provide management services for the Device/Asset that include policy updates, rulebase changes and any configuration changes as required for the operation of the service.

All Foresite activities will be implemented remotely. In the event of issues that require physical or local access to the Device/Asset, Client may at times be required for assistance to trouble shoot (e.g. system rebuild, power-cycle, reboot or console access).

Alerting & Escalation: Log streams collected by VisionLink are parsed, normalized, and sent to the ProVision threat engine for additional analysis. The business rules in the threat engine raise any suspicious logs or patterns of behavior to an Event. Event conditions that are deemed of interest or worthy of follow up will be brought to the attention of the Client's designated POC(s) by the creation of a Ticket within ProVision. Events are classified in to 4 severities;

- ***Emergency*** – Existence of conditions which indicate a potential security incident has occurred
- ***Critical*** – Existence of conditions which indicate the presence of a potential security threat requiring attention
- ***Warning*** – Potential Incidents that may have been averted but warrant investigation and confirmation
- ***Informational*** – System and vendor information to bring additional context to higher priority Events

All progress of Incidents will be tracked within the ProVision Ticket. The SOC may also call the Client depending on the severity of the Incident.

Ticketing: Ticket types include but are not limited to the following; Security Incident, Support Ticket and Change Request. The assignee of a Ticket will always be a Foresite SOC representative and if the status of the Ticket is set to "Waiting for Customer', then the progress of the Ticket is the responsibility of the Client's designated POC(s).

Tickets have 4 severity levels as below;

- ***P1 Emergency*** – System down or potential security Incident that warrants urgent attention
- ***P2 Critical*** – Significant impact that could lead in to a security Incident or system outage if not addressed
- ***P3 Warning*** – Moderate loss of functionality or security that should be addressed
- ***P4 Informational*** – Supporting information and notification of behavior

The SOC Analyst will work to address all Tickets although in some circumstances, the Client's designated POC(s) may need to be involved to progress and resolve the Ticket. If the Client doesn't respond to the Ticket in a timely manner, Foresite reserves the right to close the Ticket and tune out the logs to stop it reoccurring.

Tickets can be updated/progressed within the ProVision Portal or via email by responding to the Ticket update email that will get sent to all those set as a 'Follower' within the Ticket. 'Followers' can be automatically assigned for all Client Tickets or individually depending on the actual Ticket. 'Followers' are confirmed during OnBoarding and can be adapted throughout the lifetime of the Service.

Log Retention: Foresite stores ProVision security stream data consisting of processed log information (Alerts) for the period detailed in the Service Overview table. Aggregated data used for the Reporting is available throughout the lifetime of the Service.

4.0 ProVision Portal

Foresite provides the ProVision Portal for access to the Service. The Portal is the interaction between the SOC Analysts and the Client. Through the ProVision Portal, Clients can;

- View Dashboards for summary of Service
- Manage Devices/Assets and system inventory
- View and search Alert logs and Events
- Access Reports

- Search, update and manage all types of Tickets

5.0 Reporting

Foresite provides a multitude of preconfigured reports that are all available in the ProVision Portal. Reporting is very flexible, including custom and quick date ranges, Device/Asset or Account information, tabular or graphical view in a variety of different formats including bar graphs, line graphs, heat maps and more.

With the aim of continuous improvement, Foresite reserves the right to add/remove/change the reporting in the ProVision Portal.

6.0 OnBoarding

Foresite will work with the partner or client to connect the Devices/Assets to SMP and complete the OnBoarding information. The client is required to complete a small document called the OnBoarding Questionnaire to help with information about the key assets and contacts for the Service. This document will be share with client during the OnBoarding.

7.0 Service Level Agreement (SLA)

Availability of the ProVision Portal: Foresite's ProVision Portal is guaranteed available 99% of the time over a one-year period and measured annually.

8.0 Client Pre-requisites

The following requirements must be confirmed by the Client for the operation of the Service;

- Client must have purchased valid Hardware/Software/Subscriptions for the Service.
- ***Security Operation*** – All Devices/Assets that are brought in to the Service must contain a valid Rulebase or configuration to protect the security of the Service. Foresite can apply the base configuration for the service and reserves the right to audit any configurations to assess if remedial work may be required to address any issues
- ***Connectivity*** - Client will ensure client-side access and connectivity to all Device/Assets as appropriate. Foresite is not responsible for resolving Client's Internet Service Provider (ISP) outages, or issues with Client's internal network or computing platform infrastructure
- ***Client Point of Contact (POC)*** – The Client is responsible for providing Foresite a primary point of contact (POC). The POC will provide access to knowledgeable technical staff, and/or third party resources, to assist Foresite with any hands-on support or working with third-party vendors

9.0 Exclusions

The following (without limitation) are not included in the Service;

- ***Site Visits (on-site Support)*** - Any site visits by Foresite are not included with the Service. Any required visits can be negotiated under a Foresite professional services agreement
- ***Services for Device/Assets not covered within the Service***
- ***Remedial work*** – Any issues caused by Client initiated Changes or failed Changes are not covered by the Service.

Foresite operate a Fair Use Policy for the number of Change Requests used in the Service (see table in section 2). Foresite reserve the right to review the volume of Change Requests per Client if it is determined that the Change Requests are being improperly used.

10.0 End of Agreement (close-down)

The following (without limitation) closed-down activities apply at the end of the Service period;

- Foresite will close the ProVision Client account and all User accounts for the ProVision Portal
- Foresite will remove the Device/Asset from SMP
- Foresite will delete all logs and data stored within ProVision 30 days after the end of the Service period. If the Client choses to retain the data, Client must provide suitable storage for the logs to be shipped to.

----- End -----