Service Description

ProVision®

Unified Security & Compliance Management

All from a single platform

Revised: August 30th 2024
Version: 24.8.2

FORESITE CYBERSECURITY

As used in this Service Description, "ProVision", "we" or "us" means Foresite Cybersecurity Inc., a Delaware corporation, if the billing address for your order is in the United States, and Foresite MSP Ltd., if the billing address for your order is within the United Kingdom. All terms used but not defined in this Service Description are defined in the Terms of Service or other documents comprising the Agreement between you and us regarding your use of the Service Offering.

Use of Foresite services is subject to the Foresite Master Software License and Services Agreement available at: https://foresite.com/docs/ma/.

The Foresite Cybersecurity Privacy Notices describe how personal information may be collected, used, shared, or otherwise processed by Foresite Cybersecurity as a data controller. The Foresite Cybersecurity Privacy Notices are available at https://foresite.com/about/privacy-policy/.

ProVision Security-Operations & Compliance Platform Overview

The ProVision Security-Operations & Compliance Platform is a cloud-native software solution that enables companies to custom-tailor SOC-as-Service solutions on demand for all their cybersecurity and compliance requirements.

ProVision delivers secure, agile outcomes from a single unified platform. The ProVision platform brings unprecedented observability, reporting, orchestration, automation, and response to all your cybersecurity functions.

ProVision solutions are delivered in a subscription model. Choose a ProVision package or contact sales to build a custom-tailored solution specifically for your business. No onboarding fees. Upgrade anytime.

ProVision packages are user-based licensing. Foresite defines users as any employee, contractor, or person utilizing a computer or application on the company network. Solutions may also be sold as standalone services or as add-ons to ProVision packages.

ProVision packages:

	Essential	Advanced	Complete
24/7 Security Operation Center	✓	✓	✓
Provision Portal, Reporting & Dashboards	✓	✓	✓
SIEM[1,2]	✓	✓	✓
Cloud-Native Data Repository	✓	✓	✓
Security Maturity Assessment	✓	✓	✓
vCISO Concierge	✓	✓	✓
Incident Response SLA	✓	✓	✓
Managed Detection & Response [1,3]	Add-On	✓	✓
Security Validation & Breach Attack Simulation[4]	Add-On	✓	✓
Annual External Penetration Test	Add-On	✓	✓
Firewall Management	Add-On	Add-On	✓
Patch Management [4]	Add-On	Add-On	✓
Compliance Platform	Add-On	Add-On	Add-On
CrowdStrike-as-a-Service	Add-On	Add-On	Add-On
Tenable-as-a-Service	Add-On	Add-On	Add-On
Proofpoint-as-a-Service	Add-On	Add-On	Add-On
Cybersecurity Training & Awareness Platform	Add-On	Add-On	Add-On

[1] Supported Devices/Applications: *https://foresite.com/docs/supported-assets*
[2] Ingestion caps apply.
[3] Requires supported EDR licensing (not included).
[4] Includes endpoint licensing for up to 120% of user count.

Google SecOps Licensure and Platform Management

ProVision is also available utilizing Google SecOps and includes both licensure and platform management to enable greater flexibility for customers who want to manage their own service but rely on Foresite for maintaining the environment.

Definitions

Alert	A log received from the Device/Asset, parsed by VisionLink, and sent to ProVision.
Customer	The company procuring/consuming the service.
Co-Management	Both the Customer and Foresite have full access to the Device/Asset for any changes or updates.
Contract	The contractual agreement between the parties.
Device/Asset	A combination of hardware, software and licensing that is monitored/managed as part of the Service.
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 created as an Event that has been positively identified as a threat or notification and requires follow up with the appropriate resolver group.
Ingestion Cap	The amount of processed log data that can be ingested into the SIEM platform. Ingestion caps are variable based on user size or scope.
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.
N-Day	N-day vulnerabilities are published, known security weaknesses that may or may not have a manufacturer-issued security patch available. The 'n' in n-day acts as a placeholder representing the number of days since the Common Vulnerabilities and Exposure (CVE) Program assigned it an identifier.
Onboarding	The activities and process to bring the Customer into live service.
PoC	Customer point of contact for managed service.
ProVision/Portal	Foresite's next-generation cloud-based managed services platform.
Service Level	Level of service dependent on the type of service.
SIEM	Security information and event management (SIEM) is a security solution that helps organizations detect threats before they disrupt business.
SOAR	Security Orchestration Automation and Response is a security technology solution that helps organizations streamline and automate incident response processes by integrating various security tools and enabling automated workflows. Available with Google SecOps.

SOC	A Security Operations Center (SOC) is a centralized function or team responsible for improving an organization's cybersecurity posture and preventing, detecting, and responding to threats. The SOC team monitors identities, endpoints, servers, databases, network applications, websites, and other systems to uncover potential cyberattacks in real time. It also engages in proactive security work by using the latest threat intelligence to stay current on threat groups and infrastructure and identify and address system or process vulnerabilities before attackers exploit them. Foresite SOCs operate around the clock seven days a week, with global SOCs located in the United States (Overland Park, KS), and in the United Kingdom (Farnborough, Hampshire). 24/7 operations delivered from the US only is an available option. Customers can also elect region specific data locations for certain services. All Foresite employees undergo background checks.
SOS	Scope of Services
Ticket	• ***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 configuration or set of rules). • ***Security Test*** – Used for security testing services such as Penetration Testing, Vulnerability Assessment. • ***Project*** – Used to track project type activity.
User	Foresite defines a User as any employee, contractor, or person utilizing a computer or application on the company network.
VisionLink	Foresite's log-collector responsible for log and security stream aggregation and processing as part of the ProVision Platform.

Service Scope

Hours of Operation	Foresite's managed services are delivered through Foresite's Global Security Operations Centers (SOCs) which 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 only.
Remote Support	All activities are implemented and provided remotely. In the event of issues that require physical or local access, Customer may at times be required for assistance to trouble shoot (e.g., system rebuild, power-cycle, reboot, or console access).
Telephone Support	US: +1 866-478-8324 / UK: +44 800-358-4915

Ticketing	Ticket types include but are not limited to the following: Security Incident, Support Ticket, Change Request, Project and Security Test. The assignee of a Ticket will always be a Foresite SOC representative. If the status of the Ticket is set to 'Waiting for Customer' then the progress of the Ticket is the responsibility of the Customer'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 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 closely with the Customer's designated PoC(s) to progress and resolve the Ticket where appropriate. If Customer does not respond to the Ticket in a timely manner, Foresite reserves the right to resolve or close the Ticket. 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 Customer Tickets or individually depending on the actual Ticket. 'Followers' are confirmed during Onboarding and can be adapted throughout the lifetime of the Contract.

Prerequisites & Customer Responsibilities

The following requirements must be confirmed by the Customer for the operation of the service:

Device/Asset	Suitable infrastructure to be included in the service. A read-only account is required for all EDR monitored services. A full read/write account is required for all managed services.
Software License/Subscriptions	Any Device/Asset in the Service must have the appropriate full manufacturer's product license and subscriptions for the duration of the Service. Device/Assets of Software that are considered end-of-support by the manufacturer can only monitored with best effort and should be upgraded. No managed support is available for Devices/Assets that are considered end-of-support. Customer is responsible for providing all required 3rd party licensing.
Hardware Support	All Devices/Assets must have manufacturer's licensing and maintenance agreements for the duration of the Service.

Software limitations	Only the manufacturer's application(s) and operating system are to be installed and running on the Asset/Device.
Security Configuration	All Devices/Assets that are brought into the Service must contain a valid rule base or configuration to protect the security of the Service. Foresite reserves the right to audit any such configurations and remedial work may be required to address any issues.
Connectivity	Customer will ensure Customer-side access and connectivity to all Device/Assets as appropriate. Foresite is not responsible for resolving Customer's Internet Service Provider (ISP) outages, or issues with Customer's internal network or computing platform infrastructure.
VisionLink / Log Stream	Customer is required to provide VM/s to host Foresite's VisionLink log forwarder.
Customer Point of Contact (PoC)	Customer is responsible for providing Foresite with 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.
Managed Detection & Response (MDR)	Customer is required to provide supported EDR licensing to enable MDR services (not included unless a Foresite CrowdStrike MSSP package is purchased separately). See Managed Detection & Response for full requirements.
Firewall Management	Requires a ProVision package. Foresite will require full read/write access to the Device/Asset under management.

ProVision Portal

The ProVision portal is Foresite's secure software solution to access all ProVision solutions. The ProVision portal enables access to:

- View Dashboards for summary of Service
- Manage Devices/Assets and system inventory
- View and search Alert logs and Events
- Search, update and manage all types of Tickets
- Access the checklist used to manage the Onboarding of a new Customer
- Access the document repository and upload Customer information
- Create and manage users
- View and update user profile and Customer information
- Review and schedule Reports
- Create and manage templates for Assessment services
- View appropriate Knowledge Base articles

Reporting

ProVision 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, graphical, or numerical view in a variety of different formats including bar graphs, line graphs, heat maps, pie charts and more.

Reports can be downloaded as a .csv or .pdf and can also be emailed directly from ProVision using the report scheduler. Reporting includes but is not limited:

- Monthly Management Report (Overview of Service for the period)
- CISO Report (Overview of Service for CISO reporting)
- Estate (Users, Managed Assets/Devices, Compliance)
- Tickets (Management Report, Support Tickets, Security Tickets, Change Requests)
- Service specific reports for areas such as Patch Management, MDR and M365
- Authentication (Management Report, Summary Report, By User, By Device, By Disabled Accounts)
- Accounts (Created, Disabled, Deleted, Enabled, Locked, Password Activity)
- Security Analysis (Management Report, Events, Log Messages, Anti-Virus, Policy Changes)
- Traffic (Management Report, Dropped Traffic, By Source, By Destination, By Destination Port)
- Log Ingestion (Raw log and summarized log information by volume and size)

Additional Reports can be requested during Onboarding and can be adapted throughout the lifetime of the Contract (subject to availability of data). With the aim of continuous improvement, Foresite reserves the right to add/remove/change the reporting within ProVision.

Onboarding

The Foresite Onboarding team will work with Customer to manage ProVision Onboarding. An in-app Onboarding checklist will guide and track the Onboarding progress.

Onboarding times vary based on ProVision solutions, project complexity, and Customer commitment to provide access, resources, and technical requirements timely.

Service Level Agreement (SLA)

Availability of the ProVision Portal
Foresite's ProVision Portal is guaranteed to have an annual availability of 99.99%, excluding any scheduled maintenance windows.

Time-to-Respond
Measured from when the Event or Ticket is created to when it is first touched by a SOC Analyst or Engineer. Auto-generated Tickets are excluded from the SLA measurement as they are typically assigned directly to the Customer.

	Priority	Time to Respond (TTR)
Events	P1 Emergency	15 mins
	P2 Critical	30 mins
	P3 Warning	2 hours
	P4 Informational	n/a

Tickets **Security Incident Support Tickets**	P1 Critical Impact	1 hour
	P2 Significant Impact	4 hours
	P3 Normal/Minor	24 hours
	P4 Low/Information	48 hours
Change Requests	Emergency	1 hour
	Standard	24 hours

SLA Failure Rebate:
At Customer's request, Foresite will pay a rebate each year (following each 12 months of service) in the format of a service credit which can be used to purchase additional services or extend the service period if the SLA has not been met. Customer must log the request for a rebate as a Ticket in the ProVision Portal within 30 days of the proposed missed SLA. Total service credit rebates cannot exceed 10% of the total annual service charge.

Measure	Credit
Availability of the ProVision Portal	Half a day service credit for every hour of availability missed over a 12-month period
Events (Response)	1 hour service credit for every P1 or P2 Event that misses the Response SLA
Tickets (Response)	1 hour service credit for every P1 or P2 Ticket that misses the Response SLA

Maintenance Window
With the unique ProVision infrastructure, it is very rare that maintenance windows are required that incur an interruption to ProVision or the Service. Should there be a requirement for a period to conduct any maintenance, Foresite reserves the right to communicate that maintenance window in advance through the notification system within ProVision.

SLA Exceptions
The following exclusions are not included in the SLA calculation:

- Scheduled maintenance work required by Foresite
- Change management requirements affecting managed devices
- Circumstances beyond the reasonable control of Foresite
- Changes Requests not performed by Foresite
- Connectivity disruptions resulting from Customer infrastructure issues

Exclusions

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

Site Visits (on-site Support)	Site visits are not included with the Service.
Services for Device/Assets not	For a full list of vendor products supported, please refer to https://foresite.com/docs/supported-assets

covered within the Service	
Remedial work	Issues caused by Customer initiated changes or failed changes are not covered by the Service.
Installation	Procurement and installation of infrastructure (e.g. Firewall).
Network Re-architecture	Network re-designs or projects to re-architecture the network.

Foresite operates a Fair Use Policy for the number of Tickets and Change Requests used in the Service. There is no limit on the number of Security Incident and Support Tickets used but Foresite reserves the right to review the volume of Change Requests per Customer if it is determined that the Change Requests are being improperly used.

Offboarding / Close Down

The following closed-down activities apply at the end of the Service period:

- Foresite will close the ProVision account and all user accounts for the ProVision Portal
- All copies of VisionLink must be wiped clean and deleted by the Customer. If VisionLink resides within a Customer VM, it is the Customers responsibility to delete it and confirm when it has been completed to Foresite. If VisionLink is supplied as hardware, the Customer retains the hardware. For clarification, it does not need to be shipped back to Foresite.
- Foresite will delete all logs and data stored within ProVision 30 days after the end of the Service period. If the Customer chooses to retain the data, a Ticket must be logged in ProVision prior to the end of service period requesting the data and Foresite will make it available for a limited period. Customer data will be delivered via a read only S3 bucket. Contact the SOC for additional information.

ProVision Solutions

ProVision solutions are available in curated Provision packages and standalone al-la-carte or add-on options. Contact your Foresite reseller or Foresite sales for more information or to add additional modules not covered in your current subscription.

SIEM

ProVision Essential	ProVision Advanced	ProVision Complete
☒	☒	☒

ProVision SIEM is also available a-la-carte in 1TB ingestion packages for Customers where user count vs device count or logging requirement is not a good fit.

Foresite's Monitoring Service delivers real time cybersecurity monitoring providing visibility of cyber threats with actionable intelligence.

ProVision SIEM includes:

Description	Security Monitoring & Analysis
ProVision Platform	✓

Log Storage and Analysis	✓
Security Information Event Management	✓
24/7 Analysis and Alerting	✓
Notification & Escalation	✓
Reporting	✓

Service Scope

Foresite will monitor and analyze the log stream from the Devices/Assets under service. The log source will vary dependent on technology.

Monitored services require VisionLink (Foresite log collector) or api:

- VisionLink is Foresite's software log collector which facilitates the collection of Customer logs across their environment and can be deployed on-premises or in the cloud depending on each individual Customer's need or context.
- Foresite recommends deploying VisionLink on a Customer provided virtual machine. It is the Customers' responsibility to provide the virtual machine infrastructure for VisionLink.
- Customer shall make available log feeds to VisionLink for all monitored devices.
- For services with CrowdStrike, it's the Customer's responsibility to provide an additional virtual machine for the CrowdStrike SIEM Connector if required.

VisionLink Requirements:

- VM specifications depend on the number of Devices/Assets in the Service.
- Typically, Octa core, 1TB HDD and 8GB Memory
- Ubuntu 22.04 LTS (or later approved system)
- Customer is responsible for ensuring the virtual machine is always available for the service.

Alerting & Escalation

Log streams received 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. Events requiring escalation will be brought to the attention of the Customer's designated PoC(s) by the creation of a ticket within ProVision.

Events are classified into 4 severities:

(P1) Emergency	Existence of conditions which indicate a potential security incident has occurred
(P2) Critical	Existence of conditions which indicate the presence of a potential security threat requiring attention
(P3) Warning	Potential Incidents that may have been averted but warrant investigation and confirmation
(P4) Informational	System and vendor information to bring additional context to higher priority Events

All progress of incidents will be tracked within a ProVision Ticket. The SOC may also call the Customer depending on the severity of the Incident. Communication and escalation plan preferences are confirmed during Onboarding and can be tuned throughout the lifetime of the Contract.

Log Retention
Foresite stores ProVision security stream data consisting of processed log information (Alerts) for a minimum period of 1 year unless otherwise specified. 90 days of Alert logs are available and searchable online in the ProVision portal, with the additional 9 months being archived. Additional storage requirements are available.

Additional Checks
Foresite can apply additional checks to a Device/Asset depending on requirement. These checks include ICMP (Ping), HTTP, HTTPS, & SSH. Any additional checks are confirmed during Onboarding and can be adapted throughout the lifetime of the Contract.

Cloud Security Monitoring (AWS / Azure / GCP)
Foresite utilizes Firemon Cloud Defense to provide real-time cloud compliance, inventory, misconfiguration, and threat detection. This service is specific to the cloud security monitoring of AWS, Azure and GCP.

The service natively monitors API activity in your cloud deployments, updates inventory, and runs security and compliance assessments in real-time and provides:

- A searchable cloud asset inventory with a full change history including which IAM entity made the change.
- Highly customizable real-time security assessments to detect misconfigurations based on the classification of the environment.
- Continuous configuration tracking and reporting with environment filtering and compensating controls.
- An intelligent issues feed integrated with inventory.

The Service includes the following:

Cloud Security Monitoring Services	
Asset Inventory	✓
Posture Checks	✓
Assessment Frequency	Real-time
Compliance Reports	✓
Real-Time Threat Detection	✓
Inventory and Configuration History	90 Days
Slack Integration	✓
Knowledge Base	✓

Supported Log Types
Foresite SIEM supports ingestion for the following log sources: https://foresite.com/docs/supported-assets

Recommended Log Sources
Indiscriminate ingestion of logs leads to increased costs and alert fatigue. Understanding the value and ROI on log sources is important in controlling expenses. Foresite recommends Customers include the following log sources as a minimum best practice:

- Firewalls
- Domain Controllers/Active Directory
- EDR/AV
- Servers
- M365/Email

Foresite will work with you to determine the best logging strategy for your business.

Ingestion Caps

ProVision packages include a data ingestion cap, which varies based on package tier (user count):

ProVision Size	Monthly Ingestion Cap
Tier 1: 25-50 Users	85 GB
Tier 2: 51-100 Users	150 GB
Tier 3: 101-150 Users	215 GB
Tier 4: 151-200 Users	280 GB
Tier 5: 201-250 Users	335 GB
Tier 6: 251-300 Users	400 GB
Tier 7: 301-500 Users	580 GB
Tier 8: 501-1,000 Users	1 TB
Tier 9: 1,001-1,500 Users	1.5 TB
Tier 10: 1,501-2,000 Users	2 TB
Tier 11: 2,001-3,000 Users	2.5 TB
Tier 12: 3,001-4,000 Users	3 TB
Tier 13: 4,001-5,000 Users	3.5 TB
Tier 14: 5,001+ Users	Call

The table above entitles the Customer to ingest a limited amount of Customer Data into ProVision during any annual period (the "Ingestion Cap").[1] In the event Customer exceeds the Ingestion Cap during the annual period, Foresite shall bill the Customer for the excess data at the established rate as consumed (the "Overage Fee"). The entire Overage Fee will be invoiced per the terms and conditions of the Sales Order.

[1]Please note that under certain heavily discounted circumstances, there may be variations in Annual Ingestion Cap(s). In such instances, the Ingestion Cap(s) specified in the Sales Order or Scope of Services (SoS) will take precedence.

Incident Response SLA

ProVision Essential	ProVision Advanced	ProVision Complete
✓	✓	✓

Foresite provides an optional Incident Management Retainer available with all ProVision packages.

In the event of a security incident, time is of the essence. Having an incident response retainer means you have a pre-established relationship with a team of experts who can respond quickly. This can minimize the duration of the incident and reduce potential damage.

Service Scope

Submit a ticket within the ProVision platform or contact the SOC at **(US) +1-866-478-8324 (UK) +44 800-358-4915** to initiate incident response services.

The Incident Response SLA service includes:

- Incident Response plan review
- Pre-negotiated rates for services:
  - Incident Response Triage
  - Compromise Assessment
  - Business Email Compromise Investigation

Incident Response Service Level Agreement (SLA):

Incident Response Triage	Foresite will respond via telephone within three (3) hours or less. All service is remote.
Compromise Assessment	Foresite will respond via telephone within three (3) hours or less. All service is remote.
Business Email Compromise Investigation	Foresite will respond via telephone within eight (8) hours or less. All service is remote.

Service Activation
Incident Response SLA requires a Work Authorization and Statement of Work is mutually agreed upon prior to delivery of any incident response service requests.

Scope Considerations

- This service **does not** include any prepaid incident response hours.
  - Customer may elect to purchase prepaid hours to expediate services in the event of an incident or agree to a renegotiated purchasing agreement.
  - Pre-paid incident response hours cannot be rolled over for like services in subsequent years.
  - Incident Response billable hours commence upon Customer service inquiry for Incident Response.
- All Foresite workload is expected to be performed remotely.
  - No expenses for travel and expenses, computer storage media, postage and courier services, and other services pertaining to Incident Response are included in the service.
- Customer is responsible for any approvals required, if necessary, from their cyber insurance carrier.
- Excludes ransomware negotiation and expenses.

Managed Detection & Response (MDR)

ProVision Essential	ProVision Advanced	ProVision Complete
Add-On	✓	✓

Foresite's ProVision Managed Detection and Response provides continuous, expert-driven threat detection, rapid response, and proactive measures to enhance your organization's overall cybersecurity resilience.

Managed Detection and Response service features:

Description	Service
ProVision Platform	✓
24/7 Security Monitoring & Alerting	✓
24/7 Threat Visibility & Investigation	✓
24/7 SOC Human Led Analyst Support	✓
Advanced Threat Hunting	✓

EDR Platform Support & Management	✓
Custom Watchlist Alerting (If supported by EDR platform)	✓
Proactive Response	✓
CrowdStrike-as-a-Service	Add-on

Service Scope

ProVision Platform
Foresite Cybersecurity ProVision Platform is a modern, cloud native SecOPs platform enabling holistic cybersecurity and compliance management to defend against today's threats.

24/7 Security Monitoring & Alerting
Continuous surveillance of an organization's network, endpoints, and other critical assets helps identify potential security incidents in real-time.

24/7 Threat Visibility & Investigation
Foresite's ProVision Managed Detection & Response uses advanced technologies, such as threat intelligence feeds, behavioral analytics, and machine learning, to detect sophisticated and evolving cyber threats. This goes beyond traditional antivirus solutions.

24/7 SOC Human Led Analyst Support
Adversaries never rest. That's why Foresite industry experts are on guard around the clock operating as a valued extension of your team to keep your business safe.

Advanced Threat Hunting
Foresite Analysts will proactively search for indicators of compromise (IoC's) that could be located undetected within the network. Our team will assume an adversary position and initiate investigations to find unusual behavior that could indicate the presence of malicious activity.

EDR Platform Support & Management
At the heart of robust managed detection and response is endpoint security. Foresite is here to aid in the management and fine-tuning of your EDR solution, ensuring you derive optimal value from your investment. Looking for an EDR platform? Foresite offers CrowdStrike-as-a-Service, the market-leading solution in endpoint security.

One of the following EDR platforms is a prerequisite for service. Customer is responsible for providing licensing.

CrowdStrike	*Requirement:* Falcon Prevent and Falcon Insight **Note**: **We offer CrowdStrike-as-a-Service as an optional add-on, wherein Foresite provides all licensing required for the MDR service.**
Microsoft Windows (Defender for Endpoint)	*Requirement: Defender for Endpoint Plan 2*
SentinelOne	*Requirement:* Singularity Complete
VMWare by Broadcom *aka Carbon Black*	*Requirement:* VMWare Carbon Black Endpoint Enterprise
Cisco	*Requirement: Cisco Secure Endpoint Advantage*

Other	*See Sales for other supported technologies*

Proactive Response
Proactive threat hunting activities identify potential threats that may have evaded automated detection. Foresite's rapid and coordinated response takes necessary actions to contain and remediate the threat.

Supported Infrastructure
Windows, macOS, Linux operating systems.
See specific vendor product support for the product deployed**.**

Customer will identify:

Critical Endpoints, Servers, Users, and/or Applications	Foresite Threat Hunting will be greatly improved by the identification of critical assets within the estate. These assets could be anything which are essential to the operation of day-to-day business, including but not limited to, Endpoints, Servers Users, and/or Applications.
Pre-Approved Actions	Customers will advise what pre-approved actions Foresite can undertake. For example, Endpoint isolation should a threat be detected, running full disk scans, first line removal attempts of a potential threat, etc.

Onboarding Stages:

CrowdStrike (if applicable)	For Customers utilizing CrowdStrike Customer-provided licenses only. An MSP authorization form will be required. (Not applicable for Foresite provided MSSP licensing). *May also require the Customer to provide a VM to host a CrowdStrike SIEM Connector. https://www.crowdstrike.com/blog/tech-center/integrate-with-your-siem/*
Sensor Rollout	Customer is responsible for deployment of EDR agents on their endpoints (if applicable).
Policy Implementation	Foresite recommended policies are put in place that include individual profiles for Standard Endpoints, High-value Endpoints, Standard Servers, Mission Critical Servers.
Tuning	Data and Alerts will be reviewed, and tuning recommended based on Threat Hunting results, false positive alerts, Customer requirements.

Google SecOps Platform Management

Google SecOps Platform Management offers a comprehensive suite of services to streamline and enhance your security operations. Foresite's expertise covers platform management for Google SecOps, handling day-to-day tasks and freeing your team to focus on strategic threats.

This service also includes implementation and integration services, parsing support, rule authoring, continuous log ingestion health monitoring, and ongoing reporting to ensure a seamless setup and maximizing the value of

Google Security Operations.

Service Deliverables (Google SecOps Platform Management)

- Foresite will monitor and report on infrastructure availability and uptime of the Google SecOps platform.
- Foresite will support Customer on and develop configurations in Google SecOps for monitoring of anomalies in IAM or authentication data, local workstation/EDR data, and network telemetry.
- Foresite will assist or directly integrate security devices (firewalls, routers, load balancers, proxy services, DNS) with Google SecOps.
- Foresite will provide ongoing operations and reporting for the following:
    - Ingest volume
    - Ingest log sources
    - Number of service Tickets opened with Google SecOps SIEM or Google SecOps SOAR.
- Google Security Operations licensing is based on the volume of raw logs ingested, measured in terabytes. Customer is responsible for purchasing sufficient licenses to meet their requirements. Google Security Operations licensing is subject to Google's Terms and Conditions: https://cloud.google.com/terms

Activity	Description	Deliverable
Reference Architecture Review	Review customer requirements and architecture to develop the best methodology for Managed Services Onboarding.	• Kick Off Call • Project Schedule • Schedule Meeting Cadence
Use Case Development	Guided customer development of data ingestion methodology, SIEM, and SOAR use cases.	• SOAR Use Cases • SIEM Use Cases • Data Ingestion Methodology
Google SecOps Onboarding	Foresite will guide customer through SecOps tenant and necessary SSO and RBAC configurations for identity provider.	• Customer and Foresite access to Google SecOps tenant • Integrated Identity Provider • RBAC Configuration
Platform Management Onboarding	Foresite will create an account in the ProVision Portal for customer access to Foresite investigated Tickets surfaced from Google SecOps, and access to ancillary managed service resources. Configure Client SOAR instance with integrations and apply orchestration and automation playbooks.	• Customer access to ProVision ticketing • Customer access to ProVision Onboarding Checklist • Customer escalation procedures documented • Google SecOps SIEM to SOAR integration • Third Party SOAR Marketplace Integrations • Foresite Playbooks applied for enrichment and automation • End to end testing • 24x7x365 security triage
Data Source Access Validation	Confirm in-scope log sources. Establish and validate access of named log sources for ingestion into Google SecOps.	• Log Source Configuration • Scoping Document
Data Source Onboarding	Define and implement log methodology to include product details, log format,	• Visual confirmation of Data Sources ingested and

	ingestion details. Stack rank and ingest by priority of log source.	normalized in Google SecOps
Data Source Optimization and Tuning	Optimize and validate the efficacy of ingestion and UDM normalization in Google SecOps.	• Parser deployment utilizing SecOps default parsers • Defined scope and prioritized parser development opportunities • Custom parser development pricing optional
Rules and Detection Logic Development	Develop and implement rules aligned to specified log sources or log source categories to identify potential threats.	• Deployment of Foresite rules content library • Ongoing updates to Foresite detection content • Defined scope and prioritized rule development opportunities • Custom rule development pricing optional
Dashboard and Reporting Creation	Once data is normalized in Google SecOps, Foresite can begin uploading of the Foresite dashboard content library.	• Default Dashboard Configuration • Foresite dashboard content library • Defined scope and prioritized dashboard development opportunities
TAM (Technical Account Manager)	Foresite will review/monitor active Tickets, escalations, customer emails, and milestones. Foresite will identify gaps between purchased deliverables and customer goals. If applicable, highlight opportunities where other services can support customer goals.	• Services oversight • Services gap analysis • Services and roadmap management • Cadence and Health Checks • Ongoing Support for Google SecOps

Exclusions (Google SecOps Platform Management)

Any services not explicitly listed above shall be considered out of scope. Additionally, the areas that are out of scope for this project include, but are not limited to, the following list. If any of these items are required for your organization, they can be scoped separately.

- Foresite will not provide any operational activity to monitor or action Alerts and Detections. All 24x7 operational activities are the responsibility of the customer.
- Foresite will not act as the first line of support for Google SecOps related outages or system events.
- Foresite will not provide managed security services or active monitoring of the Google SecOps environment; customers will be expected to notify Foresite of any data health and performance monitoring issues.
- Foresite will not provide pipeline surveillance between Google SecOps SIEM and Google SecOps SOAR; any misconfigurations between the Google SecOps SIEM and Google SecOps SOAR environment will require the customer to open support cases with Google directly.
- Incident Response
- Device logging remediation (Foresite is not responsible for remediating any issues with the source device)

- Certificate management or monitoring
- Forwarder management or OS upgrades
- Raising or configuring network changes to allow data sources to flow into SecOps

Cybersecurity Maturity Assessment

ProVision Essential	ProVision Advanced *	ProVision Complete *
✓	✓	✓

Security Maturity Assessment (CMA) is a questionnaire-based self-assessment available within the ProVision portal. Based on the NIST Cybersecurity Framework (CSF), CMA provides Customers with a quick, easy, and cost-effective method to evaluate cybersecurity maturity and risks against a national standard created at the U.S. Department of Commerce.

The NIST Cybersecurity Framework helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data. The Framework is voluntary. It gives your business an outline of best practices to help you decide where to focus your time and money for cybersecurity protection. The Framework gives your business an outline of best practices to help you decide where to focus your time and money. The informative references included help tie the responses to other frameworks such as NIST 800-53, ISO, or CIS for deeper investigation.

The NIST CSF focuses on six key areas:

1. **Govern:** The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.
2. **Identify:** What processes and assets need protection?
3. **Protect:** Implement appropriate safeguards to ensure protection of the enterprise's assets.
4. **Detect:** Implement appropriate mechanisms to identify the occurrence of cybersecurity incidents.
5. **Respond:** Develop techniques to contain the impacts of cybersecurity events.
6. **Recover:** Implement the appropriate processes to restore capabilities and services impaired due to cybersecurity events.

Through a series of multiple-choice questions focused on these categories, Foresite will evaluate and score your overall cybersecurity maturity against best practices so you can make better and more informed business decisions about your cybersecurity strategy. It also provides a risk matrix that assists in determining the priority of decisions based on risk.

Use Cases:

Baseline Cybersecurity Maturity	Gain a quick, easy, and cost-effective evaluation of how well your business is prepared to defend against today's cyber threats.
Prioritize Cyber Initiatives	Arm yourself with information to make better business decisions. Visualize how investments in focus areas can significantly improve your security maturity and reduce risks.
Ability to Demonstrate Maturity	Whether it is for a Board of Directors, investor, or key stakeholders, the ability to demonstrate where you are in your cybersecurity journey is critical to ensure alignment, and appropriate focus and investment in line with your company goals and objectives.
Track Progress	See how your efforts and focus contribute to your company's security

	maturity over time.

Frequently Asked Questions

1. **Does the Cybersecurity Maturity Assessment suffice for a NIST gap assessment?**
   Unfortunately, no. The MA addresses high-level summarized questions based on the premise of each category. The results provide a very effective preliminary indicator regarding your business's cyber-maturity; however, it should not be considered a replacement for a full assessment by a skilled auditor that evaluates each category and many subcategories for compliance.

Security Validation & Breach Attack Simulation

ProVision Essential	ProVision Advanced *	ProVision Complete *
Add-On	✓	✓

**Eligible ProVision packages IP/Asset Cap includes 1.2x the total licensed user count. Additional IP/Assets available to purchase if necessary. Also available as a standalone solution.*

Powered by Horizon3.ai's NodeZero platform, Foresite's continuous, managed autonomous testing service enables Customers to continuously find, fix, and verify their exploitable attack surface to continuously improve the security effectiveness with ongoing, unlimited, and orchestrated penetration tests.

Implement a Continuous Find, Fix, and Verify Loop
The platform empowers your organization to reduce your security risk by autonomously finding exploitable weaknesses in your network, giving you detailed guidance about how to prioritize and fix them, and helping you immediately verify that your fixes are effective.

Find Your Most Critical Risks, Fix What Matters Most
Uncover blind spots in your security posture that go beyond known and patchable vulnerabilities, such as easily compromised credentials, exposed data, misconfigurations, poor security controls, and weak policies.

NodeZero pivots through your network, chaining together weaknesses just as an attacker would and then safely exploits them. You have full visibility into your penetration test's progress, and the exploits being executed in a real-time view.

When the test is complete, the results are prioritized for your immediate action. The dashboard reveals your critical weaknesses, their impact on your organization, and provides detailed remediation guidance for addressing them both systemically, and individually.

Understand the Path, Proof, and Impact
You have clear visibility into proven attack paths, step-by-step summaries of each path, and a clear understanding of their impact on your organization. NodeZero provides proof of the exploitation, its impact on your organization, and mitigation recommendations.

Features
Autonomously reveals proven attack paths in your network
Prioritizes and details the fixes that should be implemented
Shows you how these weaknesses impact your organization

Enables quick and ongoing verification that your fixes are effective

Customer is required to provide the following to enable the service:

Internal Pen Testing Prerequisites	Internal pen testing requires a virtual machine where a NodeZero Runner agent will be deployed. *C*onfiguration varies for on-premises vs. cloud-based deployments: • **On-premises:** Deploy an .iso, permitting outbound firewall rules. • **Cloud-based:** A Kali image where software can be deployed (documentation will be provided).
System Requirements	The installation is required for the entirety of the service. Instructions for installation will be provided during Onboarding. • 2 CPU cores • 16GB RAM • 60GB HDD.

Service Scope
Foresite's Security Validation & Breach Attack Simulation Services are accessible through the ProVision Portal. Foresite will make commercially reasonable efforts to ensure Services are accessible and functional on a continuous basis, excluding scheduled maintenance periods.

What is included?
- Foresite will assist with product implementation and provide technical support for the platform.
- Customer will have full access to purchased packages via their ProVision account.
- The platform is designed to be a self-service portal to underpin your cybersecurity testing capabilities.

Onboarding
1. Foresite will provide a kickoff call to discuss/determine the following:
    a. Validate prerequisites (NodeZero Runner).
        i. Important consideration for N-Day assessments speed…especially in large, segmented networks.
    b. Management access:
        i. Co-managed options (Customer access level to the NodeZero platform):
            1. **"Full access":** Customer can run their own tests. Foresite will also have full access.
    c. Overview of platform architecture, components and user interface.
    d. Discuss a typical deployment, time taken, knowledge transfer etc.
    e. Review available test types:
        i. Black-box
        ii. AD password audit
        iii. Pre-packaged specific tests
    f. Review options within test setup
        i. Scheduling
        ii. Scope
        iii. IP targets
        iv. Approvals
    g. Review runtime views & options within, show attack chain views & exploit & remediation wiki
    h. Review interface output & discuss findings
    i. Review report types

2. Customer must complete Test Request and Rules of Engagement (ROE) templates in ProVision for each test, which includes:
    a. IP addresses/ranges
    b. Select NodeZero Runner
    c. Select attack scenario:
        i. MiTM (Man in The Middle)
        ii. Bute Force options
        iii. Exploitation options
        iv. Password recovery
        v. Post-exploitation options
    d. Select run-time length
        i. The longer man-in-the-middle attacks run, the higher chance of capturing a hash and identifying additional weaknesses.
3. Customer will create and configure the assessments and Foresite can assist when requested.

Assessment Cadence
Default recurring testing occurs monthly. Customers can perform unlimited ad hoc assessments or adjust assessment frequency if desired.

Assessment Types

1. **Internal Penetration Testing**
   In an internal penetration test, the assessment takes the perspective of an attacker or malicious insider who has already gained access to your internal network.

   NodeZero will assess the following and more:
   - On-premises infrastructure
   - Cloud infrastructure
   - Identity and access management infrastructure
   - Data infrastructure
   - Virtual infrastructure

   The platform autonomously discovers and exploits weaknesses in your network just as an attacker would. It moves laterally in your environment by:
   - Compromising credentials through credential attacks
   - Mining exposed data
   - Bypassing security controls
   - Exploiting key vulnerabilities and misconfigurations

   The platform orchestrates hundreds of offensive security tools and chains weaknesses together to demonstrate the types of impacts attackers seek:
   - Domain compromise
   - Business email compromise
   - Access to sensitive data exposure
   - Ransomware
   - Ability to pivot to the cloud
   - And more!

2. **External Penetration Testing**
   External penetration testing finds an organization's footprint on the internet, using tools and methods an

attacker would.

- Verify if public facing assets open doors are vulnerable to ransomware exposure
  - Understand what attack paths ransomware actors can exploit to breach the perimeter, move laterally within the network, and gain access to “crown jewel” data.
- Visualize the risk and impact
  - See the risk and impact of misconfigured third-party applications and weak or default credentials as an attacker would use them to breach your perimeter.
- Improve asset management
  - Continuously discover public-facing assets, hybrid cloud assets, and internal assets.
- Understand third-party and supply chain risks
  - NodeZero can be run continuously, both internally and externally, providing an immediate understanding of third-party and supply chain risks.
- Save time and resources
  - Penetration tests can be set up within minutes and executed as often as needed. No extensive tuning, training, or certifications are required, and results are prioritized with proof, so time and resources can be spent fixing only what matters.
- Continuous security assessments
  - Run autonomous penetration tests as often as needed so blue and red teams can complement each other’s efforts.

3. N-Day Testing

When a significant N-day vulnerability is disclosed, time is of the essence, and you must quickly verify that your organization is not exploitable. When vulnerabilities become public, attackers weaponize them within days and even hours.

Foresite’s Security Validation & Breach Attack Simulation allows you to shorten the critical timeframe for testing within 24 hours even for the largest networks with appropriate preconfigured runners.

For identified vulnerabilities that are likely to be exploited, the platform provides proof of concept exploit to understand the impact of the vulnerability. Foresite provides contextual understanding of your environment to help you prioritize your remediations and understand when you should patch outside of your regular cycle for a particular threat.

4. AD Password Audit

Attackers don’t hack in, they log in. Compromised credentials underpin a high percentage of cyber-attacks. To make sure you’re not leaving a welcome mat out for bad actors, you should continually verify the effectiveness of your credential policies. Foresite offers you a fast and effective method for uncovering any gaps in your password policy and streamlining your remediation.

- Reveals user passwords in your Active Directory (AD) environment that are likely targets for credential stuffing, password spray, credential reuse, and password cracking attacks
- Cracks passwords based on public breach data, open-source intelligence (OSINT) tied to your company, and any weak password terms that you can provide
- Provides a prioritized list of risky accounts along with detailed remediation guidance
- Enables you to regularly audit passwords as employees join or leave your organization

When the audit is complete, Foresite gives you a detailed and actionable summary and ranks your users by their credential risk. You can drill into specifics, and Foresite provides proof that the password was cracked, as well as mitigation steps and guidance for improving your overall password policy.

The audit ranks all users audited by their risk level, which is a function of guess ability, how the password was cracked, and password similarity.

Foresite's Security Validation & Breach Attack Simulation can easily and regularly audit your organization and receive prioritized guidance for your riskiest accounts. We rate accounts with easily guessable passwords as critical. These accounts are the ones most at risk of being compromised by online attacks such as password spray and credential stuffing.

5. Phishing Impact Test

Phishing is the most common type of cyberattack. There are over 1.35 million unique phishing sites detected worldwide. In response to this pervasive threat, it's likely your ITOps and SecOps teams conduct security training and in-house phishing tests to raise security awareness and see who is susceptible. It's time to go a step further:

- Ensure that everyone in the organization understands the proven impact – not just the theoretical possibilities – of falling victim to a phishing scam
- Understand what assets are most vulnerable so that you can better protect them
- Efficiently evaluate systemic changes you can take to minimize your risks

Foresite provides a consolidated summary of your Phishing Impact test, showing you the number of compromised credentials and the key weaknesses and impacts with detailed guidance about how to remediate them most effectively and efficiently.

- Integrate with Your Phishing Campaign App
    - Foresite supplements your simulated phishing tools, such as KnowBe4, Proofpoint, InfosecIQ, and in-house efforts.
    - Simply copy a script into your phishing landing page. Then the credentials of the users who responded to the lure will appear in the supporting Foresite internal penetration test you've created to run for the duration of the campaign
- Reveal Critical Impacts from Phished Credentials
    - Automatically captures the credentials of the simulated phishing attack victims and uses them to penetration test your internal network. You can use the report from this test to assess the business risk of a successful phishing attack and identify security controls that can be put in place to mitigate this risk
- Capturing the Phished Credentials
    - Phished user's credentials are entered into our secure platform. By default, the phishing script will tell the user their login is incorrect to gain additional credentials.
    - Tests are conducted with secure methods that ensure cleartext credentials are not maintained outside of the test's ephemeral infrastructure.

Easily understand how a phished credential impacts your environment and what an attacker can access:

- What type of data can the phisher access? Is it protected data? Crown jewels?
- Can the phisher gain admin access to hosts in your network?
- Can the phisher move laterally to cloud environments?
- Can the phisher elevate privileges and compromise other credentials?

What Could an Attacker Do with This Phished Credential?

- Understand how each phished credential can impact your environment, including the data and domain privileges it can obtain
- Report on proofs of weaknesses exploited and their associated impacts
- Shows how we were able to achieve domain compromise with a phished credential beyond

simulation, to demonstrate proof

Test Your Access Policies, Test Your Responses:

- Helps users understand the potential gravity of being phished
- Helps security teams assess their defenses.

Prioritize and Identify Systemic Issues:

- Easily understand which weaknesses need to be addressed to better protect your organization.
- Prioritize your organization's weaknesses and groups systemic issues so that you can address them holistically

Reporting
The full suite of reports is available within the NodeZero console with the following report types made available in ProVision portal under Security Tests:

1. **Executive Summary**: Provides an assessment overview including the time the test started and finished, and number of hosts identified, Impact (critical findings and a brief overview of attacks), and Weaknesses & Mitigations
2. **Pen Test**: Provides a detailed dive into hosts and ports/service enumerated, and findings with detailed remediation steps
3. **Hosts**: Provides a breakdown of discovered hosts and ports/services enumerated only

Reviews
Foresite's Offensive Security team will provide a quarterly review meeting to discuss findings, discuss risk mitigation, provide recommendations to improve security posture, and answer Customer questions.

Penetration Testing

ProVision Essential	ProVision Advanced *	ProVision Complete *
Add-On	✓ Includes Annual External Pen Test Only	✓ Includes Annual External Pen Test Only

**Eligible ProVision packages IP/Asset Cap includes 1.2x the total licensed user count. Additional IP/Assets available to purchase if necessary. Also available as a standalone solution.*

Foresite's Consultant-led penetration test simulates a hacker attempting to gain access into network infrastructures or information systems through manual (hands on) exploitation of vulnerabilities. Foresite follows 'NIST SP 800-115 Technical Guide to Information Security Testing and Assessment' as our testing framework.

Penetration testing is a manual approach performed by Foresite consultants looking to evade or overthrow the security features of system components. It is designed to exploit discovered weaknesses and determine risk exposure, giving full visibility into how malicious entities may be attacking your systems and to what extent they are at risk.

Any exploit that would result in a Denial of Service, disrupt services or system access, or result in the actual penetration of the system and risk damaging the system will not be performed. These vulnerabilities will be listed as potential vulnerabilities and will require further investigation.

Internal Network Assessment activities require network access by one of the following methods:

1. Virtual installation of Foresite .ISO within Customer environment
2. Onsite at the request of the Customer (Additional Cost)
3. Preconfigured physical appliance shipped and installed (Additional Cost).

Customer will choose a testing method:

White-box:	Customer provides detailed information about the network, often including IP addresses/ranges, sensitive device IPs, network diagrams, and other pertinent documents.
Gray-box:	Customer provides limited information such as number of active devices, number of subnets, and IP addresses/ranges.
Black-box:	Customer provides network access to resources/equipment. No network information is provided, except static IPs.

Project Phases:

Discovery and Enumeration	a) **Fingerprinting:** Fingerprinting is the systematic discovery of a target in order to build an attack profile. With no inside knowledge of your infrastructure, Foresite will identify its access points and address ranges, determine associated domain names, attempt to gain insight into user id/password makeup, identify potential social engineering avenues, and gather information about your infrastructure. These determinations will be accomplished using publicly available information. Note that no social engineering will be attempted during this phase. Once this phase is complete, Foresite will contact your point of contact and confirm finding regarding discovered IP-address ranges. Fingerprinting is only necessary if a Black-box approach is used. b) **Host, Service, and Application Identification:** This activity includes identifying all accessible hosts and their associated services and applications within the identified IP-address ranges in their entirety. Where possible, identification will include system type, O/S type, services type, and service version.
Vulnerability Identification	This activity involves identifying vulnerabilities for each identified host and associated services using both public and proprietary techniques. Foresite will correlate the vulnerabilities to determine if a combination of vulnerabilities will allow for a larger exploit. We will provide a risk rating based upon technical, legal and regulatory, and business issues.
Validation and Assessment	Foresite will conduct a false positive analysis to confirm that the vulnerabilities identified via scanning are indeed actual confirmed or potential vulnerabilities. This activity will be conducted by a Foresite consultant using manual testing methods. Any exploit that would result in a Denial of Service, disrupt services or system access, or result in the actual penetration of the system and risk damaging the system will not be performed. These vulnerabilities will be listed as potential vulnerabilities and will

	require further investigation.
Exploitation and Penetration Testing	Penetration Testing activities may be performed on specific network segments, VLANs, or whole networks and are based on a case-by-case basis with the Customer. Penetration Testing includes exploitation and attempts to gain access via identified vulnerabilities to gather additional data or to devices. Upon gaining access to a device, Foresite will gather additional information to move laterally (if needed/required) within the environment. This may include installing tools on devices, adding user accounts, or utilization of installed software/applications for "malicious" actions. All tools and accounts to be removed upon completion of testing.

Important Considerations

1. Penetration testing activities have inherent risks and could cause unforeseen adverse effects in Customer environment including crashing servers, exposing sensitive data, corrupting production data, disruptions or other effects. The Customer understands and accepts these risks.
2. Foresite does not engage in Denial of Service (DOS) testing unless explicitly requested and will not engage in any test which would result in a DOS.
3. Testing will be scheduled during times most conducive to your organization, and no tests which would be potentially disruptive to normal business will be conducted during business hours.
4. Unless separately defined for testing, if a web application is found within the range of tested IP(s), Foresite performs only basic unauthenticated application testing.

A Scope of Services (SoS) will be provided to define the specifics for this type of engagement. The Customer must complete an in-app Rules of Engagement (ROE) for this engagement.

vCISO Concierge

ProVision Essential	ProVision Advanced	ProVision Complete
✓	✓	✓

Foresite vCISO Concierge is your gateway to experienced cybersecurity and compliance expertise at your fingertips. Certified Foresite experts, averaging 20+ years of experience leading cyber initiatives are at your service to provide expert advice, direction, and feedback for your cyber initiatives. Our team's goal is to help strengthen your security posture while ensuring you check all the boxes for data privacy and regulatory requirements.

The vCISO Concierge will oversee your Foresite cybersecurity program providing experienced leadership.

What is Included?

- Annual cybersecurity and compliance posture and planning review (upon request)
- Security Maturity Assessment
- Compliance questions or recommendations
- Unbiassed technology recommendations
- Prioritization advice
- Planning assistance and recommendations

What is not included? (Contact Sales for a quote if additional vCISO services are needed)

- Policy review or creation.

- Gap assessments
- Audits
- Tabletop exercises
- Incident Response Management
- Board Presentations
- Employment candidate interviews

Service Scope
To engage your vCISO concierge, please submit a ticket request in the ProVision portal. Typically, vCISO requests will be answered within 8 hours during regular business hours.

Firewall Management

ProVision Essential	ProVision Advanced	ProVision Complete *
Add-On	Add-On	✓

Also available as a standalone solution (requires an ingestion purchase if not included in a ProVision package).

Reliable cybersecurity infrastructure management for firewalls. Get the most out of your security investment with:

- 24x7x365 access to skilled security professionals.
- Discover and remediate security gaps before they are a problem.
- We will help you with full incident analysis, remediation, change control, and system updates/upgrades.
- Completely managed or co-managed solutions.

PREREQUISITE
Firewall management requires a ProVision subscription or SIEM data package.

Firewall Management includes:

Description	Security Monitoring & Analysis (MA2)
ProVision Platform	▯
Log Storage and Analysis	▯
Security Information Event Monitoring	▯
24x7x365 Analysis and Alerting	▯
Notification & Escalation	▯
Reporting	▯
Incident Remediation	▯
Change Requests	▯
System Upgrades*	▯
System Configuration Backup**	Option

**System Upgrades are included for minor upgrades that can be performed remotely. If onsite work is recommended and required, this will be covered by an additional Scope of Services (SOS).*

***Backups of the Device/Asset are the responsibility of the Customer. At Customer request, Foresite will perform a manual configuration backup prior to implementing any Change Requests, subject to the technology allowing it.*

Service Scope
Customer will choose a management program:

Co-Management	Customer has full read/write access to their infrastructure. 1. Customer is required to document all changes they make via a change request Ticket in ProVision. 2. Customer can use a combination of Customer implemented and Foresite implemented changes throughout the lifetime of the Service.
Full-Management	Customer has read-only access to their infrastructure

Foresite will provide management services for the Device/Asset that includes policy updates, rule base changes and configuration changes as required for the operation of the service.

Managed Exposure Management Platform

ProVision Essential	ProVision Advanced	ProVision Complete
Add-On	Add-On	Add-On

Foresite delivers Managed Exposure Management services as a managed SaaS solution. The offering is powered by the Tenable One Exposure Management Platform. Provided as a service, Foresite owns and includes all licensing requirements included in the service delivery.

The service helps organizations gain visibility across the modern attack surface, focus efforts to prevent likely attacks, and accurately communicate cyber risk to support optimal business performance.

The platform combines the broadest vulnerability coverage spanning IT assets, cloud resources, containers, web apps and identity systems, builds on the speed and breadth of vulnerability coverage from Tenable Research, and adds comprehensive analytics to prioritize actions and communicate cyber risk.

Managed Exposure Management Platform allows organizations to:

- Gain comprehensive visibility across the modern attack surface
- Anticipate threats and prioritize efforts to prevent successful attacks
- Communicate cyber risk to make better decisions

Available Service Packages:

	Threat Vulnerability Management	T1 Standard	T1 Enterprise	Identity
Vulnerability Management[1]	✓	✓	✓	-
Web APP Scanning[2]	✓	✓	✓	-
CNAPP Cloud Security	-	✓	✓	-
Active Directory Identity Security	-	✓	✓	✓
OT and ISC Cyber Risk Management	-	✓	✓	-
External Attack Surface Management	-		✓	-
Calculate, Communicate and Compare your Cyber Risk	-	✓	✓	-

Lumin Exposure View	-	✓	✓	-
Asset Inventory	-	✓	✓	-
Attack Path Analysis	-	-	✓	-

[1]PCI ASV scans are not included in standard service offering. Contact sales for more information.
[2]Also available as a stand-alone service.

Features:

Vulnerability Management[1]	Powered by tenable.io (vulnerability management). The service provides the industry's most comprehensive vulnerability coverage with real-time continuous assessment of your organization. Built-in prioritization, threat intelligence and real-time insight help you understand your exposures and proactively prioritize remediations. Discover, assess, and prioritize vulnerabilities. **See Everything.** Find hidden vulnerabilities with continuous, always-on asset discovery and assessment of known and unknown assets in your environment, even highly dynamic cloud or remote workforce assets. **Find and Fix Vulnerabilities Before Attacks Happen.** With the industry's most extensive CVE and configuration coverage you can quickly see scan results and determine exposures. Intuitive dashboard visualizations and easy to understand risk scores ensure you get immediate insight to reduce risk. **Prioritize Vulnerabilities.** Identify which vulnerabilities to fix first with automated prioritization that combines vulnerability data, threat intelligence and data science. Built-in prioritization capabilities ensure high risk vulnerabilities are quickly patched. **Respond Faster to Disrupt Attacks.** Use easy-to-understand risk scores to quickly begin remediation before a breach happens. Take advantage of more than 200 integrations to automate workflows and take decisive action.
Web APP Scanning[2]	Powered by tenable.io (web app scanning). Simple, scalable and automated vulnerability scanning for web applications. Take advantage of web application security built by the largest vulnerability research team in the industry. From OWASP Top 10 risks to vulnerable web app components and APIs, Tenable Web App Scanning provides comprehensive and accurate vulnerability assessment. Gain unified visibility of IT and web application vulnerabilities for operational efficiency. **Simple.** Set up new web app scans in seconds by using the same workflows you are already familiar with. No need to spend hours or days manually tuning scans. **Unified.** View vulnerable web app components and custom code vulnerabilities alongside your IT and cloud assets. Eliminate complexity from managing multiple, siloed solutions. **Accurate.** Comprehensive web app assessments built by experts give you

	confidence that your development teams aren't wasting time on false positives or missing high-risk vulnerabilities.
CNAPP Cloud Security	Powered by tenable.cs (Unified Cloud Native Application Protection Platform (CNAPP). With Tenable Cloud Security you can easily ramp up security across all your AWS, Azure and GCP environments. From full asset discovery and deep risk analysis to runtime threat detection and compliance, you can reduce complexity, minimize your cloud exposure and enforce least privilege at scale. Tenable's comprehensive approach accurately visualizes and prioritizes security gaps and gives you the built-in expertise and tools you need to remediate risks that matter most. Comprehensive CNAPP: Secure Your Cloud and Cloud Identities. As a full CNAPP solution, Tenable Cloud Security enables you to secure your cloud infrastructure from development to runtime. It continuously analyzes all your cloud resources — across infrastructure, workloads, data, identities and applications — to single out the most important risks, spot unknown threats and deliver actionable insights within hours. The solution also addresses a key risk to your cloud infrastructure — identities — by detecting, prioritizing and remediating risky entitlements and misconfigurations at scale. Cloud Security Posture Management (CSPM) and Compliance. Monitor risk by continuously reviewing and assessing cloud environment settings and configurations. By mapping discovered risks against security standards and policies, you can attain and maintain compliance and regulation management across multi-cloud environments. **Cloud Infrastructure Entitlement Management (CIEM).** Gain actionable visibility into all identities and entitlements, and full risk context that reveals and prioritizes hidden dangers like toxic combinations and privilege escalation. Control your access entitlements with auto-remediation of excessive permissions and unused entitlements. Tenable CIEM is the most comprehensive and accurate solution for managing human and service identities in cloud infrastructure environments and achieving least privilege at scale. **Cloud Workload Protection (CWPP).** Continuously scan, detect and visualize your most critical workload risks, including vulnerabilities, sensitive data, malware and misconfigurations, across virtual machines, containers and serverless functions. **Kubernetes Security Posture Management (KSPM).** Reveal, prioritize, and remediate security gaps and automate compliance for Kubernetes clusters across your cloud infrastructure. Using Tenable Cloud Security, you can unify visibility into Kubernetes container configurations and empower stakeholders with steps to mitigate misconfigurations. **Infrastructure as Code Security (IaC).** Shift left on security by enabling developers to scan, detect and fix misconfigurations and other risks in IaC to harden your cloud infrastructure as part of the CI/CD pipeline. Tenable's CNAPP solution enables teams to embed security into workflows in DevOps tooling including Hashi Terraform and

	AWS CloudFormation, and automatically remediate prioritized findings in their native IaC environments. **Just-In-Time (JIT) Access**. Grant developers' speedy approval for as-needed, time-limited access and avoid long-standing privileges, while reducing your cloud attack surface. Tenable's CNAPP solution offers temporarily elevated access that enforces fine-grained least privilege policies — minimizing risk while addressing business needs. **Cloud Detection and Response.** Improve your cloud security posture by automating threat detection with continuous behavioral analysis and anomaly detection against built-in and custom policies. Tenable Cloud Security examines enriched cloud provider logs to provide context around each risk, enabling your SecOps teams to rapidly investigate and remediate. You can also query data using intuitive tools and easily integrate with SIEMs (Splunk, IBM QRadar, etc.) and ITSMs (ServiceNow, Jira, etc.) to help you further accelerate response times.
Active Directory Identity Security	Powered by tenable.ad (active directory). Take control of your Active Directory (AD) and Azure AD security to find and fix flaws before they become business-impacting issues. Tenable Identity Exposure is a fast, agentless Active Directory security solution that allows you to see everything in your complex Active Directory environment, predict what matters to reduce risk and eliminate attack paths before attackers exploit them. **Find and Fix Active Directory Weaknesses Before Attacks Happen**. Discover and prioritize exposures within Active Directory using Tenable's Identity Risk Score. Reduce your identity risk with step-by-step remediation guidance. **Detect and Respond to Active Directory Attacks in Real Time.** Detect Active Directory attacks like DCShadow, Brute Force, Password Spraying, DCSync and more. Tenable Identity Exposure enriches your SIEM, SOC or SOAR with attack insights so you can quickly respond and stop attacks.
OT and ISC Cyber Risk Management	Powered by tenable.ot (operational technology). Get in-depth operational technology (OT) asset visibility to better understand, manage and reduce your cyber risk. Tenable OT Security is an industrial security solution for your modern industrial enterprise. It can help you identify assets in your OT environment, communicate risk, prioritize action and enable your IT and OT security teams to work better together. With a comprehensive set of security tools and reports, Tenable OT Security provides unmatched visibility across IT and OT security operations and delivers deep situational awareness across all global sites and their respective assets — from Windows servers to PLC backplanes — in a single interface. **In-depth Asset Visibility.** Immediately discover all devices on your network whether they are active or dormant and get visibility into make, model and firmware version. **Exposure Management.** Track risk scores and identify vulnerable assets, giving you a simple method to mitigate threats and make the best use of your security team's

	time. **Streamlined Audits.** Validate configuration, change logs and access controls to ensure systems are compliant against corporate policies.
External Attack Surface Management	Powered by tenable.asm (attack surface management). Gain Visibility into Your External Attack Surface. Get comprehensive visibility into all your internet-connected assets, services and applications to better understand your organization's full digital footprint and better assess and manage risk. Tenable Attack Surface Management continuously maps the entire internet and discovers connections to your internet-facing assets so you can discover and assess the security posture of your entire external attack surface. **Discover What you Own.** Discovery is key. Find more with Tenable Attack Surface Management to access an attack surface map of more than 5 billion assets to discover domains related to assets in your inventory. Get more done with notifications on changes in your attack surface for continuous monitoring. **Understand Business Context.** Get full business context by leveraging more than 200 fields of metadata to help you make more informed decisions about previously unknown internet-connected assets. Streamline asset management by leveraging filters, tags and datatypes to understand your full external footprint.
Calculate, Communicate and Compare your Cyber Risk	Powered by Tenable Lumin. Visualize and explore your cyber risk, track risk reduction over time, measure the effectiveness of your security operations and benchmark against your peers. Use Tenable Lumin, an advanced visualization, decision support, analytics and measurement solution, to understand and reduce your cyber risk. Lumin transforms vulnerability data into meaningful insights to help you prioritize decision-making across your entire organization. **Calculate**. Advanced analysis and risk-based exposure scoring weighs asset value and criticality, vulnerabilities, threat context and security program effectiveness – providing clear guidance about what to focus on. **Communicate.** Visualizations of the entire attack surface allow anyone – from analyst to executive – to quickly understand and communicate your organization's Cyber Exposure. **Compare.** Exposure quantification and benchmarking allow you to compare your effectiveness for internal operations and against peers. Identify areas of focus and optimize security investments.
Lumin Exposure View	Allows you to quickly view your global Cyber Exposure Score (CES), see its changes and trends over time, view important benchmark comparisons, and assess your overall risk. The Lumin Exposure View includes several tools that help you understand:

	• Your overall security posture as it relates to your business context. • The criticality of your assets • The effectiveness of your efforts to remediate vulnerabilities across your workspace. An exposure card represents the incoming data from your configured tags and data sources. It aggregates and normalizes the data to provide a visualization of your CES and other metrics. Users can create custom cards or use Tenable-provided cards to gain insight and guidance on what areas need the most attention.
Asset Inventory	Allows you to easily view and manage all of your assets in one location, regardless of their source. You can quickly see which assets are new or updated in the last week, as well as analyze which percentage of assets comes from each individual source. You can also view, manage, and apply tags to assets.
Attack Path Analysis	Helps organizations gain visibility across the modern attack surface, focus efforts to prevent likely attacks, and accurately communicate cyber risk to optimize business performance. The platform combines the broadest vulnerability coverage spanning IT assets, cloud resources, containers, web apps, and identity systems, and builds on the speed and breadth of vulnerability coverage from Tenable Research and adds comprehensive analytics to prioritize actions and communicate cyber risk. The Tenable One platform enables you to: • Get comprehensive visibility of all assets and vulnerabilities, whether on-premises or in the cloud, and understand where they are exposed to risk. • Anticipate threats and prioritize efforts to prevent attacks by using generative AI and the industry's largest data set of vulnerability and exposure context. • Communicate exposure risk to business leaders and stakeholders with clear KPIs, benchmarks, and actionable insights. • Leverage the broadest vulnerability coverage spanning IT assets, cloud resources, containers, web apps, and identity systems. • Integrate with third-party data sources and tools for enhanced exposure analysis and remediation.

Service Scope

Tenable Licensing	Foresite owns and provides all the required licensing necessary to deliver managed offering as a turnkey solution. (Optional) Foresite can also deliver managed services for Customer owned licensing.	
Tenable One Portal	Customer has optional full co-management access to the Tenable One platform.	
Onboarding	**Account Creation**	Foresite will build out the Tenable account and add it to ProVision. (Ensuring that the number of licenses are accurate along with the correct

		service type).
	Kickoff Meeting	Walk the Customer through the prospective services and discuss the Onboarding process. Foresite will also collect important information to ensure smooth Onboarding.
	Tenable User Creation	Foresite will create all the Customer users within their Tenable account and designate the correct privileges (Admin/Basic User etc.)
	ProVision Account Creation	Foresite will create a ProVision Account and all the Customer contacts as users within the Provision portal. An initial implementation Ticket will be opened that includes links to installation instructions, as well as contract information (number of licenses etc.). This will be used to track Onboarding progress
	Client Reviews Implementation Material	Customer will review the implementation instructions (FW Rules, Required Ports for Operation etc.) and reach out via the ProVision Ticket with any initial questions that arise. Foresite will respond accordingly.
	Host Initial Implementation Meeting	Foresite to conduct meetings with Customer to walk through the implementation documentation and overall technical process in more detail. We will begin talks about the Customers' architecture to understand what ranges need to be scanned and how best to accommodate it.
	Continued Implementation Meetings	Subsequent implementation sessions will be held on an ad-hoc basis between Foresite/Customer until the Customer is in a 'ready' state.
	Complete Scan Configuration and Kickoff Discovery Scans	Foresite will finalize scan configurations and run an initial discovery scan at the agreed upon date. Discovery & vulnerability scan reports can be auto emailed to Customer POC's.
Reports	All reports and deliverables will be available in the Provision portal.	
Support & Maintenance	Foresite will deliver all required support, maintenance, and management of Attack Surface Management solutions.	

Patch Management

ProVision Essential	ProVision Advanced	ProVision Complete *
Add-On	Add-On	✓

**Eligible ProVision packages Asset Cap includes 1.2x the total licensed user count. Additional Assets available to purchase if*

necessary.

Also available as a standalone solution.

Mitigate the root cause of 60% of data breaches by proactively addressing known vulnerabilities. Foresite's automated patch management solution offers a comprehensive view of your security landscape, pinpointing non-compliant systems. By minimizing time-to-patch, we effectively lower your cybersecurity risk.

Foresite's Patch Management Service is available for Windows and Linux Servers, Windows and MacOS workstations and hundreds of third-party applications. The Service is provided using Ivanti End Point Manager (EPM) and ProVision.

ProVision Patch Management includes:

Description	
ProVision Platform	✓
Reporting	✓
Ivanti EPM Software	✓
Patch related vulnerability scan (not all vulnerabilities)	✓
Automated patching based on severity and device type (e.g., workstations or servers)	✓
Auto reboots (where allowed)	✓
Patch Monitoring	✓
Patch anywhere (on prem or at home - requires internet access)	✓

Service Scope

Foresite will monitor the identified Assets in Service to keep up to date with software patches across the estate. Foresite will work with the Customer to identify the Assets in scope and provide the Ivanti EPM agent for the Customer to install.

Patch Management reports are available within ProVision and additional reports can be made available upon request.

All Foresite activities will be implemented remotely. In the event of issues that require physical or local access to the Device/Asset, Customer may at times be required for assistance to troubleshoot.

Automation

Foresite's patching process Is highly automated, allowing for faster patching in accordance with Customer approved guidelines. This includes a regular patch maintenance window, ideally weekly or monthly, that can be agreed on during Onboarding.

Patches are deployed automatically in a staged approach to a smaller test group then after a week to the rest of the estate. This is an extra safety measure approach to capture any potential compatibility issues before full deployment.

Patch Releases

Microsoft releases their monthly patches on the second Tuesday of each month. With various standards in mind that look for patches to be installed between 14 days to 30 days after release, we start each patch cycle for the Microsoft operating systems following patch Tuesday. Many other third-party software providers will release ad hoc.

Supported Infrastructure
Windows, macOS, Linux operating systems plus most major applications such as MS Office, browsers, Adobe, and Java (see full supported applications list).

Onboarding
Foresite will work with the Customer to identify and bring all Devices/Assets into the Patch Management Service during the Onboarding process as follows:

Pilot	One or 2 devices of each type (e.g., Server, Workstation) to prove the model and ensure there are no compatibility issues. This will involve installing the Patch Management Agent, ensuring it's reporting into the service and can deploy patches. It will test the full patch process to identify any potential issues such as firewall or app blocking. The agent is usually manually installed on these devices at this stage.
Test Group	Foresite will work with the Customer to identify a group of devices (typically up to 10) that will receive patches first for each patching period. This tests mass deployment in the Customer environment using software deployment tools or group policy to install the agent remotely.
Estate Roll Out	Installation of the Patch Management agent to all infrastructure in the Service. All Assets/Devices in this group will receive patches a week after the test group.

Continuous Compliance Automation Platform

ProVision Essential	ProVision Advanced	ProVision Complete
Add-On	Add-On	Add-On

Powered by Apptega, Foresite's Compliance Platform enables Customers to dramatically improve and reduce the cost burden of managing cybersecurity and compliance audits.

Automatically and continuously track cybersecurity compliance to 30+ industry-standard frameworks like ISO 27001, SOC2, CMMC, PCI and more, to quickly identify security gaps, giving you the roadmap to remediation.

Get ahead of cybersecurity threats before they arise with out-of-the box risk, vendor risk and audit management.

Features:

Empowered Compliance	Empower continuous compliance programs at scale.
Build Great Cybersecurity	Go beyond one-time compliance. Assess and remediate within a living program and confidently report with one click.
Pass Audits with Ease	Quickly achieve compliance for auditors, Customers, stakeholders, and

	your BOD faster than any approach.
Boost Efficiency by 50%	Crosswalk all your compliance frameworks in seconds. Streamline management, audits, and reporting forever.
Risk Manager	Score, rank, and report on risks and how you are squashing them. *(Available as an add-on to base package.)*
Vendor Assessment	Assess and manage 3rd parties, providing confidence in compliance. *(Available as an add-on to base package.)*
Audit Manager	Speed prep, share evidence, and validate controls when it matters most. *(Available as an add-on to base package.)*

Capabilities:

Assess	Quickly complete questionnaire-based assessments and use autoscoring to pinpoint gaps.
Build, Manage and Report	End-to-end management of cybersecurity and compliance all on one easy-to-use platform.
Collaborate	Enjoy enterprise-class capabilities paired with consumer app simplicity.
Connect	Quickly connect your entire ecosystem with pre-built connectors and open API.

All the Compliance Frameworks you Need:

Foresite's Compliance Platform supports 30+ different frameworks including ISO 27001, NIST 800-171, NIST 800-53, CMMS 2.0, SOC2, PCI DSS, CIS, NIST CSF, HIPPA, GDPR, ISO 42001 and more.

Available packages:

	Starter	Advanced	Premium
Build & Assess			
Number of Frameworks	1	4	Unlimited
Standard Assessments	1	4	Unlimited
Harmony Framework Crosswalk	1	4	Unlimited
Assess Risk	✓	✓	✓
Custom Assessments	-	Unlimited	Unlimited
Program Management			
Vendors	✓	✓	✓
Vendor Risk Questionnaire	Add-on	Add-on	✓
Task Packs	1	✓	✓
Policy and Plan Templates	✓	✓	✓
Documents	50 GB limit	100 GB limit	300 GB limit
Manage Risks	✓	✓	✓
Reporting and Dashboards			
Standard, Assessment & Risk Reports	✓	✓	✓
Scheduled Reports	✓	✓	✓
Audit Reports	Add-on	Add-on	✓

Vendor Reports	-	Add-on	✓
Audit Manager			
Active Audits	Add-on	Add-on	✓
Inactive/Completed Audits	Add-on	Add-on	✓
External Audit Users	Add-on	Add-on	✓

Service Scope
The Compliance Platform is a SaaS solution:

What is included?

- Foresite will assist with product implementation and provide technical support for the platform.
- Customer will have full access to purchased packages via their ProVision account.

What is not included?

- The Compliance platform is designed to be a self-service portal to underpin your cybersecurity and compliance management program.
- The platform does not include vCISO support to conduct gap assessments, audits, policy review or creation, uploading of Customer evidence, etc.
- Many Customers prefer a white glove approach to cybersecurity and compliance management, in which case we recommend pairing Compliance Platform with Foresite vCISO services to receive a tailored comprehensive solution for your needs led by Foresite's industry experts.

Strategic Solution Management

ProVision Essential	ProVision Advanced	ProVision Complete
Add-On	Add-On	Add-On

Managing security shouldn't be a complicated problem for your business. Millions of open cyber-security requisitions globally, staffing shortages, and product skills/expertise deficits add to the challenge of bringing on new or managing existing strategic technology solutions important to your business's overall security posture.

Foresite strategic solution management services allow you to operationalize strategic investments and gain efficiencies while complementing your existing security team's efforts. Led by highly experienced and credentialed security engineers, Foresite delivers comprehensive co- or full management around many leading security solutions.

Featured Solutions include

- Managed Crowdstrike
- Managed Tanium
- Managed Tenable
- Managed Endpoint Security (variety of vendors)
- Managed Proofpoint

CrowdStrike

As an authorized CrowdStrike MSSP, Foresite provides co- and fully managed services for the CrowdStrike Falcon Platform. Bring your own license or purchase Foresite's CrowdStrike-as-a-Service that includes all licensing and services needed to operationalize the industry's most complete AI-native defense.

Why CrowdStrike? CrowdStrike protects the people, processes and technologies that drive modern enterprise with a single agent solution to stop breaches, ransomware, and cyber-attacks.

- **Cloud native.** Eliminates complexity and simplifies deployment to drive down operational costs.
- **AI powered.** Harnesses the power of big data and artificial intelligence to empower your team with instant visibility.
- **Single agent.** Delivers everything you need to stop breaches — providing maximum effectiveness on day one.

With CrowdStrike, Customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native CrowdStrike Falcon® platform.

- **Better protection.** Get protection across the entire threat lifecycle by combining machine learning, artificial intelligence, behavioral analytics and proactive threat hunting in a single solution - all powered by Threat Graph, the security industry's largest cloud analytics platform.
- **Better performance.** A single lightweight agent works everywhere, including virtual machines and data centers - providing protection even when endpoints are offline.
- **Better value.** Get better protection while eliminating on-premises infrastructure and consolidating your endpoint agents with an extensible platform that grows and adapts to your needs without adding complexity.

Powered by the CrowdStrike® Security Cloud and AI, the Falcon platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting, and prioritized observability of vulnerabilities.

Single, universal agent for security consolidation. CrowdStrike Falcon gives you an intelligent, lightweight agent that consolidates point products and stops advanced attacks — both malware and malware-free — while capturing rich endpoint activity for industry-leading detection and response.

- All platform capabilities are delivered via one agent that is easy to deploy and manage.
- Easy deployment with a cloud-native architecture for instant operation, with no reboots required after installation.
- Single agent extends across on-premises, remote deployments, and cloud workloads for consistent visibility and protection across endpoint, clouds, and identities.
- Lightweight agent with minimal impact on endpoint performance and end-user productivity.
- Simplified management from one unified console.

Modularity. The CrowdStrike Falcon platform is designed as a highly modular and extensible offering that helps Customers solve new security challenges with a single click and without the need to re-architect or re-engineer the architecture, removing friction associated with security deployments.

CrowdStrike modules:

Falcon Prevent	Falcon Prevent offers the ideal AV replacement solution by combining the most effective prevention technologies with full attack visibility and simplicity — you'll be up and ready immediately.
Falcon Insight XDR	Falcon Insight XDR delivers detection, investigation, and response to ensure nothing is missed and breaches are stopped.
ThreatGraph	The industry's leading cloud-scale AI brains behind CrowdStrike® Security

(7/15/30)	Cloud predicts and prevents modern threats in real time.
Falcon Overwatch	Partners you with a team of elite cybersecurity experts to hunt continuously within the Falcon platform for faint signs of sophisticated intrusions leaving attacker nowhere to hide.
Device Control	Falcon Device Control provides the needed visibility and granular control to limit risks associated with USB devices.
Spotlight	Modern vulnerability management with no infrastructure to manage, no scanning impact to hosts, and no waiting weeks or months for stale results.
Discover	Identifies unauthorized accounts, devices, IoT/OT systems and applications anywhere in your environment in real time, enabling faster remediation to improve your overall security posture.
Falcon Firewall Management	Enables creation, management, enforcement of firewall rules and polices across Windows and MacOS environments. Host firewall management allows users to have visibility control over firewall rules present in their environment.
Falcon Identity Threat Protection	Detects and stops identity-based breaches in real time. Classifies identities, gain gradual and continuous insights into every account to highlight and identity security gaps across hybrid identity stores. Evaluates identities and risk with continuous multi-directory visibility, auto classification and AD overview.

Licensing Options:

1. CrowdStrike-as-a-Service includes all licensing (Foresite owned), support and management delivered as a packaged SaaS solution.

   CrowdStrike-as-a-Service packages:

	MSSP Defend	MSSP Advanced Defend
Falcon Prevent	✓	✓
Falcon Insight XDR	✓	✓
ThreatGraph (7/15/30)	✓	✓
Falcon Overwatch	-	✓
Device Control	Add-On	Add-On
Spotlight	Add-On	Add-On
Discover	Add-On	Add-On
Falcon Firewall Management	Add-On	Add-On
Falcon Identity Threat Protection	Add-On	Add-On

2. Customer may elect to provide their own licensing for Foresite management.

Scope of Service
Foresite will assist with remote product implementation; however, Customer is responsible for deployment of agents to endpoints. Foresite will provide product support and management.

See Managed Detection and Response above. -Typically, CrowdStrike is deployed as part of Foresite's MDR offering.

Tanium

With Tanium, an organization has the power to review, manage, control, and secure their endpoints in seconds. Tanium's capabilities are available on Windows, Mac, and Linux operating systems and allow for easy reporting and management of the systems. By combining endpoint operations, such as application management and patching, and cybersecurity operations (i.e. threat response alerting and administrator access rights review), a team can quickly assess where they are and where they need to go to manage their computing systems.

Service Scope
Customer is responsible for providing all required Tanium licensing.

Product implementation (Available for an additional one-time charge).

Foresite strategic platform management ensures your Tanium investment will be effectively operationalized and supported bringing peace of mind to stakeholders.

Service includes remote management only. Customer may be required to provide onsite assistance under certain troubleshooting circumstances or where physical access is required to support an asset requirement.

Foresite delivers comprehensive management of the Tanium platform including:

- Full or co-management of Tanium, operating as an extension of your team.
- Health monitoring
- Establishing and defining the best approach to user permissions for your organization
- Individual configuration, monitoring, and support of all the Tanium modules
- Reporting
- Quarterly business reviews

Managed services are licensed per modules as follows:

Modules	Description
Core, Asset, Discover	**Core** • **Interact** - Perform basic functions such as asking questions, consuming data, and deploying actions across your enterprise. • **Connect** - Capture accurate and complete endpoint data from Tanium and send it to 3rd party locations and systems. • **Trends** - Visualize, understand, and communicate trends and correlations of endpoint security and operational health data. • **Impact** - Understand the administrative realm of your enterprise by visualizing and contextualizing access rights to reduce the attack surface. Foresite to support setup and tuning of Impact and overview of the lateral movement findings. **Asset** • Get a complete view of your enterprise inventory by aggregating live asset data with recent data from offline assets. **Discover** • Find, report on, and take action against unmanaged endpoints.
Patch, Deploy	**Patch** • Minimize critical security vulnerabilities by automating patch delivery. • Foresite will support setup and tuning of Patch, patch scans, patch lists, maintenance windows, and patch deployments.

	Deploy • Install, update, or remove software on a flexible set of targets. • Foresite management includes setup and tuning of Deploy, software packages and bundles, maintenance windows, and deployments. Management is a fixed cost for both and/or either module.
Provision	Enables bare-metal provisioning of Microsoft Windows or Linux to on-premises and internet-connected devices. It also enables re-imaging outdated or broken devices. Foresite management supports setup and tuning of Provision, OS Deployments, and module configuration. Customer is responsible for providing OS images, OS volume licensing, credentials, and needed endpoint configurations such as domain join, and provisioning endpoints.
Performance	Monitor, investigate, and remediate endpoint performance issues. Foresite supports setup and tuning of the module, including Profiles, analyzing Events, monitoring applications, and helping to use the module to resolve system issues.
Threat Response	Detect, react, and recover quickly from attacks and the resulting business disruptions. Foresite supports setup and tuning of Threat Response and profile deployment, support management of Index and Recorder, assists with exclusions and response activity, and helps with intel management and deployments. Customers is required to review and respond to Threat Response alerts with assistance from Foresite.
Enforce	Simplify and centralize management and policies of all end user computing devices to eliminate and mitigate vulnerabilities and business risk. Foresite supports setup and tuning of Enforce and assist with Enforce policies. Customers is responsible for BitLocker management and policy design
Software Bill of Materials	Identify vulnerabilities found inside of application dependencies and modules such as Log4j. Foresite will set up and start tracking SBOM vulnerabilities and report on them when found. Requires Tanium Asset.
Certificate Manager	Gain visibility into the digital certificates across your endpoints. Foresite will deploy certificate audits and provide regular reports of certificate issues.
Reveal	Identify sensitive data and embedded libraries on endpoints to assist in regulatory compliance, information security, and data privacy. Foresite supports setup and tuning of Reveal and will assist with profile and pattern

	management. We will also notify when suspect data is found. Customer is responsible for investigating rule matches and remediating data violations.
Benchmark	Understand the state of your security program, compared to other Tanium Cloud Customers. You can use the reports to communicate key trends, improvements, and industry benchmarks for executive and board-level reporting. Foresite supports setup and tuning of Benchmark will use the reported concerns to find ways to increase your security profile.
Comply	Evaluate endpoints daily for security configuration exposures and software vulnerabilities using industry security standards, vulnerability definitions, and custom compliance checks. Foresite supports setup and tuning of Comply, offers best practice support for setting up vulnerability and compliance assessments, and assists with reports and findings analyses.
Integrity Monitor	Plan, install, and monitor file and registry integrity. Track and alert changes to critical file systems. Foresite supports setup and tuning of Integrity Monitor watchlists, monitors, rules, and alerts. Customer is responsible for management and tuning watchlists, monitors, rules, labels, and investigating unapproved file activity.
Engage	With Engage, you can create surveys to collect qualitative feedback from endpoint users and deploy remediations to correct problems on the endpoints. Foresite will assist with configuring the module, creating surveys based on Customer needs and supporting the built-in remediation tasks
Investigate	Correlate performance events and activities that came from one or multiple hosts. Add activities that have forensic value to investigations to triage issues more quickly and add notes and comments about these data points and the conditions in which they occur for team collaboration. Foresite will manage the configuration and health of the module(s) and provide investigative assistance as needed. Dependencies are based on the modules licensed

Tenable

As an authorized Tenable MSSP, Foresite provides full and co-comanaged services for the Tenable One Platform. Bring your own license or purchase Foresite's managed SaaS package that includes all licensing and services needed to operationalize your attack surface management initiatives.

See Attack Surface Management above.

Endpoint Security

Foresite provides full and co- AV and EDR platform management services. Foresite is an authorized CrowdStrike and Carbon Black partner. Management support is also available for Microsoft, Cisco, and SentinelOne.

Management options include platform management only or fully managed detection and response. Bring your own license or purchase Foresite's MSSP CrowdStrike package.

See Managed Detection and Response above.

Proofpoint

Foresite provides management and monitoring services for the Proofpoint Email Security platform. Bring your own licensing and Foresite will provide the services to operationalize Proofpoint's email security platform.

Proofpoint management services are designed to enhance and optimize the capabilities of your Proofpoint implementation to ensure your cybersecurity infrastructure is maintained and continuously improved.

We take a proactive approach to the management of your Proofpoint integration, encompassing configuration, comprehensive policy reviews and compliance checks. This dynamic methodology ensures that your Proofpoint environment is always at its peak performance, fully harnessing its potential to safeguard your digital communications against evolving threats.

Service Scope
Foresite management services for Proofpoint are available a la carte from the list of supported modules below.

Modules	Description	Management (MA4)
Proofpoint Protection Server/Proofpoint on Demand (POD)	The primary management console for Proofpoint email Protection. Foresite will manage the POD configuration, making recommendations to ensure adherence to best practices and help with any necessary configuration changes for your specific environment, i.e. troubleshooting any mail flow issues and making the necessary changes to ensure legitimate mail flows properly.	✓
Admin Portal	The Admin Portal is the new look management console. Foresite will manage the Admin Portal in conjunction with the original management console to ensure adherence to security best practices.	✓
Targeted Attack Protection (TAP) URL Defense/ Attachment Defense	Targeted Attack Protection identifies various threats in emails such as Malware, Phishing, Impostor, or Telephone Orientated Attacks (TOAD) threats. TAP also creates alerts when these threats are delivered, as well as when a malicious URL is clicked. Foresite will manage the URL Defense and Attachment Defense configurations making recommendations to ensure adherence to best practices. Foresite will also monitor (MA2) TAP alerts via a log stream,	✓

	providing analysis and recommended actions when threats are delivered.	
Threat Response Auto Pull (TRAP)	Threat Response Auto Pull removes emails from user inboxes when it is determined that threats were delivered. Foresite will manage TRAP configuration and make recommendations to help ensure adherence to security best practices.	✓
Isolation	Isolation is used to redirect URL clicks in emails to the Proofpoint Isolation browser. Foresite will manage the Isolation configuration, making recommendations to ensure adherence to security best practices.	✓
CLEAR Phish Alarm	Phish Alarm is the Phish Report button end users can use to report suspicious emails to Proofpoint. Foresite will manage the configuration for Phish Alarm making recommendations to ensure adherence to security best practices.	✓
CLEAR PSAT	PSAT is the Security Awareness Training and Phishing Simulation module.	-
Email Fraud Defense	EFD helps with the entire DMARC implementation/monitoring process.	-
Email Archive	Email Archive is Proofpoint's email archiving solution.	-

Please contact Sales for further information about supportability of the above modules or any Proofpoint products/modules that are not listed.

Onboarding
Foresite will work with the Customer to onboard the Service. The client is responsible for ensuring Foresite has access to each Proofpoint console that is included in the Service.

- This requires a licensed mailbox in the client environment.
  - Example: soc.foresite@*clientdomain*.com
  - This email address should be configured to auto forward mail to soc@foresite.com
- This new email address should then be added as an administrator in each applicable Proofpoint console.

Contact Sales for other strategic solution management inquiries.
Foresite will provide a Scope of Services (SoS)describing specific service details for each strategic technology management solution.

Security Testing

ProVision Essential	ProVision Advanced	ProVision Complete
Add-On	Add-On	Add-On

Also available as a standalone solution.

Vulnerability Scanning

Vulnerability scans assess computers, systems, and networks for security weaknesses, also known as vulnerabilities. Scans can be conducted as a one-time service or as a recurring service with a Tenable subscription (**see Attack Surface Management**).

A vulnerability scan is the first step performed in the process of conducting a vulnerability assessment. Vulnerability scans create auto-generated reports which generally detect only surface level vulnerabilities. The scans should not be used in lieu of a full assessment.

Vulnerability scans are a passive approach to vulnerability management, as they don't go beyond reporting on detected vulnerabilities. Foresite follows 'NIST SP 800-115 Technical Guide to Information Security Testing and Assessment' as our testing framework.

Vulnerability Assessment Testing

A vulnerability assessment is less thorough than a penetration test, as it doesn't involve social engineering attacks or exploits designed to breach your security infrastructure.

Foresite consultants will review the results of an automated vulnerability scan, which involves a nominal amount of manual evaluation. The use of additional tools (manual testing methods) may be necessary to determine actual vulnerabilities from potential or non-existent vulnerabilities (false positives).

Any exploit that would result in a Denial of Service, disrupt services or system access, or result in the actual penetration of the system and risk damaging the system will not be performed. These vulnerabilities will be listed as potential vulnerabilities and will require further investigation. Foresite follows 'NIST SP 800-115 Technical Guide to Information Security Testing and Assessment' as our testing framework.

Approved Scanning Vendor (ASV) Scanning

Approved Scanning Vendor (ASV) scans begin with an automated enumeration process to identify all the hosts and services running in your environment. Once enumeration is complete, the manual assessment phase tests for the presence of known vulnerabilities in web-applications, system applications, networking devices, and operating systems that correlate to the enumeration results. The scan engine is regularly updated with the latest vulnerabilities.

In accordance with PCI DSS Requirement 11.2.2, merchants and service providers specifically require quarterly external vulnerability scans which must be performed by an ASV. The scan is performed from a point external to the target network so that internet-facing ports and services are assessed.

Once a passing scan is performed, an Attestation of Scan Compliance is provided for documentation.

Application Testing

Application testing will be performed in one of the following manners:

White-box:	Customer provides static application code and any necessary credentials to execute on testing.
Gray-box:	Customer provides application information and any necessary information.
Black-box:	Customer provides limited information with no credentials being provided.

Application Testing includes attempts at exploiting identifiable vulnerabilities within applications or APIs. Application Testing can be performed with the following options:

- Unauthenticated. Unauthenticated testing involves assessing a web application's security without logging in, focusing on vulnerabilities accessible to anonymous users.
- Authenticated. Authenticated testing examines a web application using valid credentials to evaluate security from both the unauthenticated perspective, as well as the perspective of a logged-in user, ensuring proper enforcement of permissions and access controls.

Foresite follows the Open Web Application Security Project® (OWASP) guidelines to assess applications for common vulnerabilities.

OWASP is a nonprofit foundation that works to improve the security of software. Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

Deliverables include a full analysis of findings and recommendations.

A Scope of Services (SoS) will be provided to define the specifics for this type of engagement. Customer must complete an in-app Rules of Engagement (ROE) for this engagement.

Mobile Application Testing

Mobile Application Testing includes attempts at exploiting identifiable vulnerabilities within mobile applications.

Foresite follows the Open Web Application Security Project® (OWASP) guidelines to assess applications for common vulnerabilities.

OWASP is a nonprofit foundation that works to improve the security of software. Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

OWASP Top 10 Categories are available at: https://owasp.org/www-project-mobile-top-10/

Deliverables include a full analysis of findings and recommendations.

A Scope of Services (SOS) will be provided to define the specifics for this type of engagement. Customer must complete an in-app Rules of Engagement (ROE) for this engagement.

Wireless Testing

Wireless testing can be performed:

Onsite	Allows consultants to map the signal strength (heat map) of wireless signal propagation. Otherwise, testing activities will be performed remotely.

Remote	Testing will be performed using an appliance / device shipped to the identified location(s).

Testing Includes:

Identifying Wireless Networks	Perform passive and active scanning to identify available "seen" and “hidden” wireless networks and determine ownership so as not to test out-of-scope networks.
Vulnerability Research	Identified and in-scope wireless networks are then tested to identify and verify vulnerabilities in preparation for exploitation.
Exploitation	Leverage identified weaknesses (vulnerabilities) in attempts to gain access to wireless assets and seek to pivot to the internal network.
Reporting	Reporting captures executed methods and findings into a comprehensive document. This includes detailed technical risks, vulnerabilities and how they were found, notation of successful exploits and recommendations for remediation and implementation of appropriate security controls.

A Scope of Services (SoS) will be provided to define the specifics for this type of engagement. Customer must complete an in-app Rules of Engagement (ROE) for this engagement.

Email-Based Social Engineering (Phishing)

Phishing is when attackers send malicious emails designed to trick people into falling for a scam. The intent is often to get users to reveal financial information, system credentials or other sensitive data.

An email phishing campaign will test employees' knowledge and compliance with security procedures and their response to social engineering exploits.

Foresite will utilize common ruses delivered via email to in-scope users attempting to gain access to sensitive information. Our host will attempt to request information such as usernames, passwords, and other sensitive information in a secure and controlled method that mimics the same types of attacks an actual hacker would use.

A Scope of Services (SoS) will be provided to define the specifics for this type of engagement. Customer must complete an in-app Rules of Engagement (ROE) for this engagement.

Phone-Based Social Engineering (Vishing)

Foresite social engineers will perform typical telephone attacks against in-scope personnel designed to gain the target's confidence and convince them to perform an action or provide sensitive data to test their response to social engineering exploits.

A Scope of Services (SoS) will be provided to define the specifics for this type of engagement. Customer must complete an in-app Rules of Engagement (ROE) for this engagement.

Short Message Service (SMS) (Text-Based) (Smishing)

Smishing (SMS text phishing) is a type of phishing that takes place via short message service (SMS) messages — otherwise known as the text messages that you receive on your phone through your cellular carrier. The goal of smishing here is to scam or otherwise manipulate consumers or an organization's employees to test their

cybersecurity awareness.

Foresite will utilize common ruses delivered via SMS to in-scope users. These types of messages generally involve some type of content that will prompt them to click on a link. Successful execution can take the user to a website that prompts them to provide their login details or other information. The goal here is to get them to provide information that attackers can use to access personal or work-related accounts, commit identity fraud, or engage in some other type of malicious activities.

A Scope of Services (SoS) will be provided to define the specifics for this type of engagement. Customer must complete an in-app Rules of Engagement (ROE) for this engagement.

Physical Security Testing

Foresite engineers will provide onsite physical site testing including:

Physical Security Testing:	This includes general observation of physical security measures, attempts to enter the building and secure areas inside of the building without authorization using methods such as “piggybacking” (following authorized users), “jimmying” or “carding” door latches, or similar methods.
Physical Security Review:	This includes general observation of physical security measures.

Foresite personnel will not use destructive entry methods, damage property, or impersonate public safety or government officials. Foresite personnel may impersonate employees, Customers or vendors in attempts to gain access to sensitive information.

A Scope of Services (SoS) will be provided to define the specifics for this type of engagement. Customer must complete an in-app Rules of Engagement (ROE) for this engagement.

USB Drops (Optional)

To determine employees’ knowledge and compliance with security procedures, our social engineering USB Drop campaign service provides a simulated test of your organization's security measures. By strategically placing USB devices in targeted areas (by client or Foresite personnel), Foresite will attempt exploiting human curiosity and trust, enticing individuals to plug in these seemingly harmless USB devices. By doing so, we can assess the effectiveness of your organization's security protocols and identify potential vulnerabilities that could be exploited by malicious actors.

Red Team Engagement

Red Team Assessments are performed to mimic actions of an actual attacker. Foresite performs activities as required from all security services to reach an end-goal (typically domain control or sensitive data access) as defined during the initiation of the engagement. Activities that may be performed to accomplish the service include Email (phishing), Phone (vishing) and SMS (smishing) Social Engineering campaigns, External and Internal Penetration Testing, External and Internal Application Penetration Testing, Physical Location Penetration Testing, and Wireless Penetration Testing.

Open-Source Intelligence (OSINT)

OSINT refers to the process of gathering and analyzing publicly available information to enhance security

posture and gain a deeper understanding of potential threats and vulnerabilities.

Foresite will perform internet reconnaissance to discover information about the Customer's business, networks, employees, partners and anything that could be used to assist in an attack against organizational information systems or employees. This will include searches for sensitive information disclosures made by Customer employees or business partners. Reconnaissance utilizes Google searches, technical support forums, email crawlers, and social media searches as an example.

Insider Threat

Insider Threat assessments are performed to mimic actions of a malicious insider or compromised user account. Foresite will perform activities as required from internal testing services to reach an end goal of domain control, sensitive data access, or otherwise defined during initiation of the engagement. Activities will be modeled after real world TTP's (Tactics, Techniques, and Procedures) to provide a better understanding of Customer's strengths and weaknesses.

Testing with Account Credentials: Foresite will perform testing using a Foresite appliance and Customer provided user credentials. Testing will be performed to identify what an adversary would be able to achieve if access to the network is obtained and if the adversary has a set of credentials.

Testing with Customer Device and Account Credentials: Utilizing a customer provided device and user credentials, Foresite will attempt to subvert device security controls and pivot off the device to gain access to information and other devices.

GRC Consulting Services (Governance, Risk and Compliance)

No matter your industry, no matter the size of your business, Foresite is here to help your organization thrive. We provide expert advice from vCISO, gap assessment, to full attestations on many frameworks to navigate increasingly complex and rapidly changing cybersecurity compliance regulations. Our team will help ensure your business meets all the regulatory data security requirements that pertain to your industry's cyber compliance.

Small business or large enterprise, from reporting processes to understanding risks, we can help you find the cyber security compliance services that work for your specific needs.

Our expert consultants will custom-tailor a Scope-of-Services specifically for your GRC engagement.

Service Scope

Foresite offers fixed cost engagements for the following:

NIST CSF Assessment
NIST 800-53 Assessment
ISO 27001 Readiness
SOC2 Readiness
CMMC/171 Assessment
CIS Top Controls
GLBA/FTC Safeguard Rule
HIPAA Risk Assessment
PCI Gap Assessment

PCI Audit
Active Directory Review
Office 365 Review

vCISO hourly retainers are also available for the following:

Policy Review and Creation
Incident Response Management
Strategy and Planning Support
And more

Cybersecurity Training & Awareness Platform

Foresite delivers comprehensive solutions to mitigate end-user risks. Cybersecurity Awareness Training, Phishing, Dark Web, Security Policies, & an Interactive Portal - we cover it all.

Cybersecurity Awareness Training

Meet cyber-compliance training mandates and keep your staff informed of the latest cyber threats with continuous annual training and ongoing videos. Weekly 2-minute micro-training video & short quiz combined with a monthly security newsletter keep cybersecurity short, engaging, and interactive.

An interactive leaderboard can ignite friendly competition with just their screen name's honor at stake. For managers, employee names are featured, with a report for performance evaluations, they can track just who needs more time bulking up!

Tracking and reporting available for HR & auditors.

Dark Web Monitoring

Foresite brings the dark web to light, continuously monitoring the dark web for hidden cybercrime activities where criminals often buy and sell stolen data such as credit card numbers, passwords, and social security numbers that can damage your brand and reputation. We automatically detect and alert imminent threats attributed to your domain so action can be taken to protect your business.

The sooner end-users are notified of a breach, the sooner they can change their passwords. End-users also can scan the dark web for their personal, friends, and family accounts with no limit.

Employee Vulnerability Assessment

Identify human vulnerabilities and their related risks. Based on NIST standards, our Security Risk Assessment assesses your client's administrative, physical, and technical vulnerabilities; identifies the associated risks, and provides recommendations for improvement.

Policies & Procedure Templates

Security policies are key to establishing expectations and explaining repercussions to protect your client organizations. Our document management portal contains a variety of customizable security policies from BYOD to Security Incident Response.

Business Operations

Terms of Use

Access and use of Foresite products described in this Service Description are governed by the Foresite Order Form and Foresite Software Master Agreement available at https://foresite.com/docs/ma/.

Purchasing the Service Offering

The Service Offering is offered on a subscription basis for either a one-year or three-year term unless specifically noted as one-time on the Sales Oder Form. Subscription Services automatically renew for successive twelve (12) months each, unless a party gives the other party written notice of non- renewal at least thirty (30) days prior to the expiration of the then-current term, or the Contract is terminated sooner as provided in the Terms and Conditions. Foresite reserves the right to increase fees by up to five (5%) upon renewal.