Forcepoint
Solution Rider

The terms of this Solution Rider are incorporated by reference into and governed by the terms and conditions of the applicable Forcepoint Subscription Agreement, the Forcepoint Network Security License Agreement, and any other end user agreement with Forcepoint incorporating this Solution Rider, as applicable, (each the "Agreement") when Subscriptions to Products, Solution Bundles, or Packaged Offerings set forth below are purchased pursuant to an Order. "Customer" used in this Solution Rider means the "Subscriber" or "Licensee" as defined in the Agreement. Capitalized terms used but undefined in this Solution Rider have the meanings provided in the Agreement. The current version of this Solution Rider can be found at: Forcepoint Solution Rider and may be modified or updated by Forcepoint from time to time in its sole discretion with or without notice to the Customer.

PRODUCT/SOLUTION SPECIFIC TERMS

Forcepoint ONE – Forcepoint's security access policy enforcement Cloud Services solution:

If in any one calendar month: (i) the total bandwidth used by Customer in the performance of Cloud Services for the security access policy enforcement solution divided by the Permitted Capacity ("Average Bandwidth Use") is greater than 0.02Mbps, then Customer must purchase additional Subscriptions to increase the Permitted Capacity so that the Average Bandwidth Use is no greater than 0.02Mbps; or (ii) the Average Bandwidth Use used exceeds the monthly Average Bandwidth Use used for all customers of the Cloud Services ("Global Average Bandwidth Use") by more than 150%, then Customer will work with Forcepoint on a bandwidth reduction plan. If the bandwidth reduction to no greater than 150% of the Global Average Bandwidth Use is not achieved, then Customer must purchase additional Subscriptions to increase the Permitted Capacity so that the monthly Average Bandwidth Use is no greater than 150% of the Global Average Bandwidth Use. If Customer does not purchase the required additional Subscriptions in (i) and/or (ii), then Forcepoint may terminate the applicable Subscription to Cloud Services upon 30 days' written notice.

Cloud Email – Forcepoint's inbound and outbound email scanning Cloud Services solutions**:**

If in any one calendar month the total number of emails processed in performance of Cloud Services for inbound and outbound scanning of email traffic divided by the Permitted Capacity is greater than either: (i) 10,000 emails per User, then Customer will make reasonable efforts to implement and maintain an accurate list of all valid email addresses belonging to Customer for which Cloud Services scan inbound or outbound email; or (ii) 30,000 emails per User, then Forcepoint may terminate the applicable Cloud Services Subscription upon 30 days' written notice unless Customer purchases Subscriptions to increase the Permitted Capacity.

Cloud Web - Forcepoint's web access filtering Cloud Services solution**:**

If in any one calendar month the total bandwidth used in the performance of Cloud Services for web access filtering divided by the Permitted Capacity is greater than 0.02Mbps, then Forcepoint may terminate the applicable Cloud Services Subscription upon 30 days' written notice unless Customer purchases Subscriptions to increase the Permitted Capacity.

Advanced Malware Detection and Protection for Web - Forcepoint's advanced malware sandbox Cloud Services solution**:**

If in any one calendar month the total number of files sent to the advanced malware sandbox Cloud Services for analysis and/or detonation divided by the Permitted Capacity is greater than 50 files per User, then Forcepoint may terminate the applicable Cloud Services Subscription upon 30 days' written notice unless Customer purchases Subscriptions to increase the Permitted Capacity.

Advanced Malware Detection and Protection for Email - Forcepoint's advanced malware sandbox Cloud Services solution**:**

If in any one calendar month the total number of files sent to the advanced malware sandbox Cloud Services for analysis and/or detonation divided by the Permitted Capacity is greater than 20 files per User, then Forcepoint may terminate the applicable Cloud Services Subscription upon 30 days' written notice unless Customer purchases Subscriptions to increase the Permitted Capacity.

AI Security - Forcepoint's Cloud Services solution for visibility and control over sanctioned and unsanctioned AI tools and agents:

For each 12-month period of the Subscription Term, the total number of Connectors and volume of scanned data may not exceed the maximum quantities and limits set forth below and in the Order. If at any time during the Subscription Term Customer exceeds the applicable quantity or limit, then Forcepoint may terminate the applicable Subscription upon 30 days' written notice unless Customer purchases the necessary additional Connectors and/or volume to increase the Permitted Capacity. "Connector" means a digital repository or system for storing, managing, or retrieving information that is scanned by the Product. Customer may not disconnect a Connector and reconnect it to a different source for purposes of avoiding additional Connector purchases; any such reconnected Connector will count as a unique Connector.

AI Security for On-Premises DLP – AI Security SKUs that begin with "DOAI" are designed for Customers with Subscriptions to on-premises, local deployments of Forcepoint Products in the Forcepoint Data Loss Protection Suite Package. For each 12-month period of the Subscription Term, as applicable:

SKU#DOAIAD (Base) – the maximum quantity of Connectors is 5 and the maximum limit for the volume of scanned data is 250TB per year;

SKU#DOAIADAP (Connector Add-On) – the maximum quantity of Connectors is increased by 3 additional Connectors and the maximum limit for the volume of scanned data is increased by an additional 150TB per year; and

SKU#DOAIADDT (Volume of Scanned Data Add-On) – the maximum limit for the volume of scanned data is increased by an additional 50TB per year.

AI Security for Cloud DLP – AI Security SKUs that begin with "DCAI" are designed for Customers with Subscriptions to Forcepoint ONE Data Security Cloud Services or no Subscription to on-premises, local deployments of Forcepoint Products in the Forcepoint Data Loss Protection Suite Package. For each 12-month period of the Subscription Term, as applicable:

SKU#DCAIAD (Base) – the maximum quantity of Connectors is 5 and the maximum limit for the volume of scanned data is 250TB per year;

SKU#DCAIADAP (Connector Add-On) – the maximum quantity of Connectors is increased by 3 additional Connectors and the maximum limit for the volume of scanned data is increased by an additional 150TB per year; and

SKU#DCAIADDT (Volume of Scanned Data Add-On) – the maximum limit for the volume of scanned data is increased by an additional 50TB per year.

The annual TB usage limit is measured by the aggregated volume of all data scanned across all authorized Connectors.

DSPM - Forcepoint's data security posture management solution (DSPM On-Premise and DSPM SaaS)

DSPM On-Prem Structured Data and DSPM SaaS Structured Data – For each 12-month period of the Subscription Term, the maximum number of Connectors may not exceed the total quantity of Connectors set forth in the Order. If at any time during the Subscription Term Customer exceeds the applicable Connector, volume, or scan-frequency limits described below, then Forcepoint may terminate the applicable Subscription upon 30 days' written notice unless Customer purchases the necessary additional Connectors and/or volume to increase the Permitted Capacity. "Connector" means a digital repository or system for storing, managing, or retrieving information that is scanned by the Product. Customer may not disconnect a Connector and reconnect it to a different source for purposes of avoiding additional Connector purchases; any such reconnected Connector will count as a unique Connector.

DSPM SaaS Structured Data – For each 12-month period of the Subscription Term, Customer may not exceed 100 database scans per year, per Connector, and as applicable:

SKU#DSPMSS1 - the total volume of scanned data may not exceed 25TB per year; or

SKU#DSPMSS3 – the total volume of scanned data may not exceed 100TB per year.

The annual TB usage limit is measured by the aggregated volume of all data stored in all authorized Connectors.

DSPM SaaS Unstructured Data (including DDR add-on) – If in any 12-month period of the Subscription Term, the total volume of scanned unstructured data divided by the Permitted Capacity is greater than an average of 30GB per User per year, then Forcepoint may terminate the applicable Subscription upon 30 days' written notice unless Customer purchases Subscriptions to increase the Permitted Capacity.

Advanced Malware Detection and Protection for NGFW - Forcepoint's advanced malware sandbox Cloud Services solution available as a feature pack with Forcepoint's next generation firewall solutions**:**

In each calendar month, the total number of files sent to the advanced malware sandbox Cloud Services for analysis and/or detonation per appliance Unit will not exceed the total File Maximum set forth in the following table:

Product Name	File Maximum

Forcepoint Advanced Malware Detection and Protection – S	3,000
Forcepoint Advanced Malware Detection and Protection – M	9,000
Forcepoint Advanced Malware Detection and Protection – L	15,000
Forcepoint Advanced Malware Detection and Protection – XL	30,000
Forcepoint Advanced Malware Detection and Protection – XXL	60,000

Forcepoint Data Security OCR for Cloud DLP (SKU# ONEDSOCR and DSOCRCLD) - Forcepoint's optical character recognition (OCR) Cloud Services solution**:**

If in any one calendar month the total number of images sent to the optical character recognition Cloud Services for analysis divided by the Permitted Capacity is greater than 420 images per User, then Forcepoint may terminate the applicable Cloud Services Subscription upon 30 days' written notice unless Customer purchases Subscriptions to increase the Permitted Capacity.

Security Management Center Service (SMCaaS) - Forcepoint's security management center Cloud Services solution available for managing Forcepoint's NGFW Hardware**:**

The total number of Forcepoint NGFW Units that may be managed by each SMCaaS set forth in the Order will not exceed the total NGFW Unit Maximum set forth in the following table:

Product Name	NGFW Unit Maximum
Forcepoint Security Management Center Service – XS	10 Units
Forcepoint Security Management Center Service – S	20 Units

If at any time during the Subscription Term the total number of Units managed by the SMCaaS exceeds the applicable NGFW Unit Maximum, then Forcepoint may terminate the applicable Cloud Services Subscription upon 30 days prior written notice unless Customer purchases Subscriptions to increase the Permitted Capacity.

Cloud Access Security Broker (CASB) – Forcepoint's security access policy enforcement Cloud Services solution**:**

If in any one calendar month the total bandwidth used in the performance of Cloud Services for security access policy enforcement solution divided by the Permitted Capacity is greater than 0.02Mbps, then Forcepoint may terminate the applicable Cloud Services Subscription upon 30 days' written notice unless Customer purchases Subscriptions to increase the Permitted Capacity.

Remote Browser Interface (RBI) – Forcepoint's internet and internal application access policy enforcement Cloud Services solution**:**

If in any one calendar month the total throughput including data sent and received through Cloud Services for internet and internal application access policy enforcement divided by the Permitted Capacity is greater than 3 Gigabytes per User, then Forcepoint may terminate the applicable Cloud Services Subscription upon 30 days prior written notice unless Customer purchases additional Permitted Capacity.

Forcepoint Dedicated IP (Dedicated IP) – Forcepoint's offering that enables Customers to configure a set of domains or IPs to receive traffic from the Cloud Services solution using a dedicated IP address that is assigned to the Customer**:**

Each Subscription to Dedicated IP is made available only with the Cloud Service to which it is associated and may be used with only one activation key for such Cloud Service. A Customer who has more than one Cloud Service activation key and wishes to use Dedicated IP for the additional activation key(s) will be required to purchase an additional Dedicated IP subscription for each additional Cloud Service activation key.

Professional Services Residency –

The Professional Services Residency Services Offering is provided pursuant to the applicable Forcepoint Services Offering descriptions and is performed remotely (not at Customer's site) by Services Personnel for up to the number of months associated with the SKU over consecutive months and up to 40 hours per week. Work must begin within 90 days from the Order date. Such Services are provided during Forcepoint's normal local business hours, Monday – Friday, subject to Forcepoint's recognized holidays. Forcepoint will assign a primary contact for the Services but reserves the right in its discretion to substitute other resources to perform the Services.

Designated Support Engineer – 12-Month Increment –

The Forcepoint Designated Support Engineer (DSE) Technical Support Services Offering is provided pursuant to the applicable Forcepoint Services Offering descriptions and is performed remotely (not at Customer's site) by Services Personnel for up to the selected quantity of Services Hours. Work must begin within 90 days from the Order date. Such Services are provided during Forcepoint's normal local business hours, Monday – Friday, subject to Forcepoint's recognized holidays, unless previously agreed by Forcepoint. The Customer must use the Services Hours before the expiration of the applicable Subscription to Forcepoint Technical Support or the conclusion of the Services Offering duration specified on the Order, whichever occurs first.

U.S. Federal Government Preferred Support (SKU# FEDSR) – Forcepoint's premium support add-on providing priority routing to U.S.-based Forcepoint Technical Support personnel:

U.S. Federal Government Preferred Support is available as an add-on to Customer's Subscription to Forcepoint Technical Support and is only provided after Customer has paid the associated additional fees. Customers with the U.S. Federal Government Preferred Support add-on will have Technical Support requests submitted during Forcepoint's U.S. regional business hours routed to U.S.-based Support personnel; for support requests submitted outside of U.S. regional business hours, Customers may elect to have the case handled by a non-U.S.-based Support personnel or to queue the case for handling by U.S.-based Support personnel during available U.S. regional business hours. Routing of Support requests to U.S.-based personnel is subject to availability and applicable Product-specific expertise within the U.S. Support team. The Forcepoint Technical Support Description, including any response times and service level targets, are based on Forcepoint's global support resources, and may be limited by Customer's restriction of Support to U.S.-based Support personnel under this add-on.

Light User Subscriptions –

All "Light User" subscriptions may only be used for students, temporary/seasonal workers, guest wifi users, retail workers, and manufacturing line workers for whom having access to the Internet and/or email is not: (1) in any way a component of their work function, or (2) to exceed

5% of any 8-hour day.

Modules –

Modules include a 36-month limited warranty from the date of purchase covering defects in workmanship and materials. All other warranties, express, implied, or otherwise, are expressly disclaimed.

Mini Modules and Transceivers –

Mini Modules and Transceivers include a 12-month limited warranty from the date of purchase covering defects in workmanship and materials. All other warranties, express, implied, or otherwise, are expressly disclaimed.

Network Security Accessories –

Network Security Accessories include a 90-day warranty from the date of purchase covering defects in workmanship and materials. All other warranties, express, implied, or otherwise, are expressly disclaimed.

AI AGENT AND AUTOMATED ACCESS TERMS — ALL FORCEPOINT PRODUCTS

These terms apply to all Products and APIs made available under the Agreement, and the obligations herein survive the expiration or termination of the Agreement. In the event of a conflict between these terms and other provisions of this Solution Rider or the Agreement, these terms control with respect to Automated Access and Agent use.

1. Definitions

"Agent" means software (including LLM-based systems and robotic process automation tools) that autonomously initiates actions (including API calls and data retrieval) to interact with the Products without contemporaneous human initiation of each request.

"API" means an application programming interface made available by Forcepoint for use by Customers in relation to Products.

"Automated Access" means access to the Products, APIs, or Documentation, including their outputs, through any automated means, including scripts, bots, Agents, MCP clients or servers, or other software capable of initiating requests without contemporaneous human initiation of each request.

"Credentials" means API keys, tokens, OAuth credentials, service accounts, client secrets, certificates, or other mechanisms used to authenticate requests to the Products.

"Sensitive Data" means sensitive or special categories of personal data of Customer, which includes protected health information, payment card data, government-issued identification numbers, biometric data, or other personal data, that potentially subjects Customer to its own heightened obligations under separate laws and regulations.

2. Permitted Access; No Circumvention

Customer will access the Products and APIs only in accordance with the applicable Documentation and Agreement and will not misrepresent or mask the identity of any calling client or the source of automated requests. Customer will not circumvent any rate limits, access controls, or usage restrictions, including through Credential rotation, token pooling, or use of multiple accounts to exceed applicable limits. Forcepoint may impose and enforce reasonable rate limits, quotas, and concurrency limits on the Products and APIs, including Automated Access, as reasonably determined by Forcepoint, including to protect security and service integrity. Forcepoint may throttle or reject requests in excess of applicable limits without liability. Product-specific consumption caps in this Solution Rider apply in addition to these rights. Subject to Applicable Laws, Forcepoint may monitor usage of the Products and APIs to verify compliance, maintain security, and detect abuse, including scraping, compromised Credentials, or anomalous Automated Access. Forcepoint may suspend or restrict access without prior notice if Forcepoint reasonably believes Customer's use poses a security or operational risk; Forcepoint will notify Customer promptly and work in good faith to resolve the issue.

3. Customer Responsibilities for Automated Access and Sensitive Data

Customer is solely responsible for maintaining the security of all Credentials and for all related activities, including those involving Automated Access, the creation, modification, deletion, export, transmission, and retrieval of Customer data in bulk, and use and access by authorized users, Agents, or any third party with access to Customer's Credentials. Actions initiated through Credentials (including by Agents or through Automated Access) are deemed actions of Customer and its authorized users for all purposes under the Agreement. Customer is solely responsible for configuring and managing Automated Access and Agents to operate within authorized permissions in the Agreement and in accordance with Documentation. Customer is solely responsible for consequences arising from

Customer's use of Agents or Automated Access, including malfunction, misconfiguration, runaway use, emergent behavior, or use of Sensitive Data. Customer is solely responsible for configuring and managing Automated Access and Agents to prevent unauthorized Sensitive Data transmission to and through the Products and APIs and acknowledges that Agents may lack the judgment to exclude Sensitive Data without such controls. Customer is solely responsible for any third-party tools, Agents, MCP servers, plugins, or connectors used in connection with the Products and APIs, including their selection, security, configuration, and compliance with the Agreement. FORCEPOINT DOES NOT CONTROL AND IS NOT RESPONSIBLE FOR ANY SUCH THIRD-PARTY TOOLS. FORCEPOINT MAKES NO WARRANTY OR REPRESENTATION REGARDING THEIR COMPATIBILITY, INTEROPERABILITY, SECURITY, OR CONTINUED AVAILABILITY WITH THE PRODUCTS OR APIS.

4. Data Minimization; Restrictions Regarding AI and Machine Learning

Customer will not and will not permit Agents to: (a) engage in background collection or scraping unrelated to an authorized user request; (b) create persistent copies, archives, or databases of Product or API-obtained data except as expressly permitted; or (c) perform bulk export except through Forcepoint-authorized mechanisms. Customer will delete data obtained through the Products or APIs within 30 days after the authorized purpose is fulfilled or upon Forcepoint's written request and will certify such deletion in writing within 10 days of request. Where Customer is subject to a documented legal retention obligation, Customer will segregate and restrict access to the retained data and certify deletion promptly upon expiry of the retention period. Customer will not use any data accessed through the Products (including Customer data, Forcepoint proprietary data, usage data, metadata, outputs, or any derivative thereof) to train, fine-tune, improve, evaluate, or benchmark any: (a) AI model or machine learning algorithms intended for use by or for the benefit of any third party; (b) foundation model, large language model, or general-purpose AI model, whether proprietary or open source; or (c) AI model or machine learning algorithms that competes with or is intended to provide functionality of or substitute for the Products or any Forcepoint offering. Customer will not use data attributable to or derived from another Forcepoint customer or tenant to benefit Customer or any third party.

5. Security Incident Notification

Customer will promptly notify Forcepoint upon discovery of: (a) an actual or suspected compromise of Credentials; (b) unauthorized access to the Products or APIs through Customer's systems or Credentials; or (c) anomalous Automated Access that may materially affect the security, integrity, or availability of the Products or APIs. Customer will reasonably cooperate with Forcepoint to investigate and remediate, including rotating or revoking affected Credentials and suspending relevant Automated Access, as needed. These obligations are in addition to any notification requirements under the Agreement, the Forcepoint Data Processing and Protection Measures, and Applicable Law.

SOLUTION BUNDLES AND PACKAGED OFFERINGS SPECIFIC TERMS

These tables list the Products that are included in a bundle of Products that may appear as a single item in an Order.

Forcepoint CASB API Add-On for DLP On-Premise (SKU# DLPCAIPCOP)

Product Name	Unit Metric
Forcepoint ONE – CASB API App Scanning – 3 App Pack • Deployment option: Cloud	User
Forcepoint DLP SSE Applications • Deployment option: Cloud	User

Forcepoint CASB API with Cloud DLP (SKU# DLPCAIPCLD)

Product Name	Unit Metric
Forcepoint ONE – CASB API App Scanning – 3 App Pack • Deployment option: Cloud	User
Forcepoint ONE – Data Security for Cloud Apps and Web • Deployment option: Cloud	User

Forcepoint ONE - Web Security Edition (SKU# ONESWG)

Product Name	Unit Metric
Forcepoint ONE – Web Security • Deployment option: Cloud	Users
Forcepoint ONE – CASB Cloud App Security (inline) • Deployment option: Cloud	Users
Forcepoint ONE – RBI Essential • Deployment option: Cloud	User
Essential Support	N/A

The Forcepoint ONE – Web Security Edition includes Essential Support unless the Quotation separately includes Enhanced Support or Enterprise Support for Forcepoint ONE – Web Security Edition in which case such higher level of support will be provided for those Products in lieu of Essential Support.

Forcepoint ONE – Web Security Edition (SKU#ONEWEB)

Product Name	Unit Metric
Forcepoint ONE – Endpoint Web Protection • Deployment option: Cloud	Users
Forcepoint ONE – CASB Cloud App Security (inline) • Deployment option: Cloud	Users
Forcepoint ONE – ZTNA protection for 1 app • Deployment option: Cloud	Users
Essential Support	N/A

The Forcepoint ONE – Web Security Edition includes Essential Support unless the Quotation separately includes Enhanced Support or Enterprise Support for Forcepoint ONE – Web Security Edition in which case such higher level of support will be provided for those Products in lieu of Essential Support.

Forcepoint ONE – CASB Cloud App Security

Product Name	Unit Metric
Forcepoint ONE – CASB Cloud App Security (inline) • Deployment option: Cloud	Users
Forcepoint ONE – CASB API App scanning – 3 App Pack • Deployment option: Cloud	Users
Essential Support	N/A

The Forcepoint ONE – CASB Cloud App Security includes Essential Support unless the Quotation separately includes Enhanced Support or Enterprise Support for Forcepoint ONE – CASB Cloud App Security in which case such higher level of support will be provided for those Products in lieu of Essential Support.

Forcepoint ONE – Cloud Security Edition (SKU#ONESSE)

Product Name	Unit Metric
Forcepoint ONE – Web Security • Deployment option: Cloud	Users
Forcepoint ONE – CASB Cloud App Security (inline) • Deployment option: Cloud	Users
Forcepoint ONE - CASB API App scanning – 3 App Pack • Deployment option: Cloud	Users
Forcepoint ONE – RBI Essential • Deployment option: Cloud	Users
Essential Support	N/A

The Forcepoint ONE – Cloud Security Edition includes Essential Support unless the Quotation separately includes Enhanced Support or Enterprise Support for Forcepoint ONE – Cloud Security Edition in which case such higher level of support will be provided for those Products in lieu of Essential Support.

Forcepoint ONE - Cloud Security Edition (SKU# ONECLOUD)

Product Name	Unit Metric
Forcepoint ONE - Endpoint Web Protection • Deployment option: Cloud	Users
Forcepoint ONE – Full ZTNA Private App Security • Deployment option: Cloud	Users
Forcepoint ONE - CASB Cloud App Security (inline) • Deployment option: Cloud	Users
Forcepoint ONE - CASB API App scanning – 3 App Pack • Deployment option: Cloud	Users
Essential Support	N/A

The Forcepoint ONE – Cloud Security Edition includes Essential Support unless the Quotation separately includes Enhanced Support or Enterprise Support for Forcepoint ONE – Cloud Security Edition in which case such higher level of support will be provided for those Products in lieu of Essential Support.

Forcepoint Data Loss Protection Suite (IP Protection) –

Product Name	Unit Metric
Forcepoint DLP Endpoint (IP Protection) • Deployment option: On-premise	Device
Forcepoint DLP Discover (IP Protection) • Deployment option: On-premise	User
Forcepoint DLP Network (IP Protection) • Deployment option: On-premise	User

For those Products included in the Forcepoint Data Loss Protection Suite Package that are normally licensed by Device, a Subscription for 1 User translates to a Subscription for 1 Device.

Forcepoint FlexEdge Secure SD-WAN Bundles – The following applies to each of the Forcepoint FlexEdge Secure SD-WAN bundles in this Solution Rider:

The Forcepoint FlexEdge Secure bundle includes: (1) Essential Support unless the Quotation separately includes Enhanced Support or Enterprise Support for Forcepoint FlexEdge Secure bundle, in which case such higher level of support will be provided for those Products in lieu of Essential Support; (2) the limited warranty provided via Advanced Return Material Authorization Support as defined in Forcepoint's Technical Support Description during the Subscription Term; and (3) either (i) the Connectivity and Access Software Package (CS), or (ii) the Connectivity and Access & Threat Inspection Software Package (CTS), which will be separately listed in the Quotation.

Forcepoint FlexEdge Secure SD-WAN S60L –

Product Name	Unit Metric
Forcepoint Secure SD-WAN 60L Appliance	1 Unit
Forcepoint FlexEdge Secure SD-WAN Manager	1 Node
Essential Support	12 Months

Forcepoint FlexEdge Secure SD-WAN S120 –

Product Name	Unit Metric
Forcepoint Secure SD-WAN 120 Appliance	1 Unit
Forcepoint FlexEdge Secure SD-WAN Manager	1 Node
Essential Support	12 Months

Forcepoint FlexEdge Secure SD-WAN S120L –

Product Name	Unit Metric
Forcepoint Secure SD-WAN 120L Appliance	1 Unit
Forcepoint FlexEdge Secure SD-WAN Manager	1 Node
Essential Support	12 Months

Forcepoint FlexEdge Secure SD-WAN S120W –

Product Name	Unit Metric
Forcepoint Secure SD-WAN 120W Appliance	1 Unit
Forcepoint FlexEdge Secure SD-WAN Manager	1 Node
Essential Support	12 Months

Forcepoint FlexEdge Secure SD-WAN S120WL –

Product Name	Unit Metric
Forcepoint Secure SD-WAN 120WL Appliance	1 Unit
Forcepoint FlexEdge Secure SD-WAN Manager	1 Node
Essential Support	12 Months

Forcepoint FlexEdge Secure SD-WAN S352 –

Product Name	Unit Metric
Forcepoint Secure SD-WAN 352 Appliance	1 Unit
Forcepoint FlexEdge Secure SD-WAN Manager	1 Node
Essential Support	12 Months

Forcepoint FlexEdge Secure SD-WAN S355 –

Product Name	Unit Metric
Forcepoint Secure SD-WAN 355 Appliance	1 Unit
Forcepoint FlexEdge Secure SD-WAN Manager	1 Node
Essential Support	12 Months

Forcepoint FlexEdge Secure SD-WAN S1202 –

Product Name	Unit Metric
Forcepoint Secure SD-WAN 1202 Appliance	1 Unit
Forcepoint FlexEdge Secure SD-WAN Manager	1 Node
Essential Support	12 Months

Forcepoint FlexEdge Secure SD-WAN S2201 –

Product Name	Unit Metric
Forcepoint Secure SD-WAN 2201 Appliance	1 Unit
Forcepoint FlexEdge Secure SD-WAN Manager	1 Node
Essential Support	12 Months

Forcepoint FlexEdge Secure SD-WAN S2205 –

Product Name	Unit Metric
Forcepoint Secure SD-WAN 2205 Appliance	1 Unit
Forcepoint FlexEdge Secure SD-WAN Manager	1 Node
Essential Support	12 Months

Forcepoint FlexEdge Secure SD-WAN S2210 –

Product Name	Unit Metric
Forcepoint Secure SD-WAN 2210 Appliance	1 Unit
Forcepoint FlexEdge Secure SD-WAN Manager	1 Node
Essential Support	12 Months

Forcepoint FlexEdge Secure SD-WAN S3401 –

Product Name	Unit Metric
Forcepoint Secure SD-WAN 3401 Appliance	1 Unit
Forcepoint FlexEdge Secure SD-WAN Manager	1 Node
Essential Support	12 Months

Forcepoint FlexEdge Secure SD-WAN S3405 –

Product Name	Unit Metric
Forcepoint Secure SD-WAN 3405 Appliance	1 Unit
Forcepoint FlexEdge Secure SD-WAN Manager	1 Node
Essential Support	12 Months

Forcepoint FlexEdge Secure SD-WAN S3410 –

Product Name	Unit Metric
Forcepoint Secure SD-WAN 3410 Appliance	1 Unit
Forcepoint FlexEdge Secure SD-WAN Manager	1 Node
Essential Support	12 Months

Connectivity and Access Software Package (CS) –

Product Name	Unit Metric
SD-WAN functionality	1 Node/12 Months
Base Layer-7 firewall functionality	1 Node/12 Months

Connectivity and Access & Threat Inspection Software Package (CTS) –

Product Name	Unit Metric
SD-WAN functionality	1 Node/12 Months
Base Layer-7 firewall functionality	1 Node/12 Months
Intrusion Prevention System functionality	1 Node/12 Months
TLS Encryption functionality	1 Node/12 Months
QUIC Inspection functionality	1 Node/12 Months
AV functionality	1 Node/12 Months
Threat Seeker Cloud URL filtering	1 Node/12 Months

RETIRED SOLUTION BUNDLES AND PACKAGED OFFERINGS

The solution bundles and packaged offerings in this section have been retired from the list of available Forcepoint offerings and/or have reached their end of life.

Forcepoint Advanced Threat Protection - Web Security Edition

Product Name	Unit Metric
Forcepoint Web Security • Deployment option: Cloud, Hybrid, On-Premise	Users
Forcepoint Advanced Malware Detection • Deployment option: Cloud	Users
Forcepoint Remote Browser Isolation - Selective • Deployment option: Cloud	Users (limited to 25)

Forcepoint Advanced Threat Protection – Web Security Edition includes a Subscription for 25 Users for Forcepoint Remote Browser Isolation – Selective. Additional subscriptions for Forcepoint Remote Browser Isolation – Selective may be purchased separately. Technical Support must be purchased separately.

Forcepoint Advanced Threat Protection - Email Security Edition

Product Name	Unit Metric
Forcepoint Email Security • Deployment option: Cloud, Hybrid, On-Premise	Users
Forcepoint Advanced Malware Detection • Deployment option: Cloud	Users
Forcepoint Remote Browser Isolation - Selective • Deployment option: Cloud	Users (limited to 25)

Forcepoint Advanced Threat Protection – Email Security Edition includes a Subscription for 25 Users for Forcepoint Remote Browser Isolation – Selective. Additional subscriptions for Forcepoint Remote Browser Isolation – Selective may be purchased separately. Technical Support must be purchased separately.

Forcepoint Data Security Suite - Workforce Edition

Product Name	Unit Metric
Forcepoint DLP Endpoint (IP Protection) • Deployment option: On-premise	Device
Forcepoint DLP Discover (IP Protection) • Deployment option: On-premise	User
Forcepoint DLP Network (IP Protection) • Deployment option: On-premise	User
Essential Support for Forcepoint Data Security Suite - Workforce Edition	N/A

The Forcepoint Data Security Suite Package includes Essential Support unless this Quotation separately includes Enhanced Support or Enterprise Support for such Package in which case such higher level of support will be provided for those Products in lieu of Essential Support. For those Products included in the Forcepoint Data Security Suite Package that are normally licensed by Device, a Subscription for 1 User translates to a Subscription for 1 Device.

Forcepoint Data Advantage (ML1, ML2 & EL1) –

Product Name	Unit Metric
Forcepoint DLP Suite (IP Protection)	User
Forcepoint DLP Cloud Applications (IP Protection)	User
Forcepoint CASB – Security Suite	User
CASB core licenses embed a limit on the number of supported cloud applications - Forcepoint CASB - Security Suite - supports a total of 15 applications regardless of the mix of Governance and Cloud protection	
Forcepoint CASB Implementation – Intermediate	N/A
Forcepoint Dynamic Data Protection – Add On	User
Enhanced Support for Forcepoint Data Advantage	N/A

For 5-year Terms, a Virtual Resident Engineer (VRE) is available during the 3 months. A VRE is a remote, flexible Full-time Equivalent (FTE) and does not include travel & expenses

Forcepoint Edge Advantage (ML1, ML2 & EL1) –

Product Name	Unit Metric
Forcepoint Web Security	User
Forcepoint Web Security Cloud App Control	User
Forcepoint Web Security – DLP Module (On-premise and Hybrid deployment types only)	User
Forcepoint Email Security	User
Forcepoint Security Management Center - High Availability	Node
Forcepoint Security Management Center	Node
Forcepoint SMC Domains	Node
Forcepoint SMC Additional Log Server	Node
Forcepoint NGFW Software Subscription	Node
Forcepoint NGFW URL Filtering	Node
Forcepoint CASB – Security Suite	User
CASB core licenses embed a limit on the number of supported cloud applications - Forcepoint CASB - Security Suite - supports a total of 15 applications regardless of the mix of Governance and Cloud protection	
Forcepoint CASB Implementation – Intermediate	N/A
Enhanced Support for Forcepoint Edge Advantage	N/A

For 5-year Terms, a Virtual Resident Engineer (VRE) is available during the first 3 months. A VRE is a remote, flexible Full-time Equivalent (FTE) and does not include travel & expenses

Forcepoint Data Advantage (EL2, EL3, EL4, and EL5) –

Product Name	Unit Metric
Forcepoint DLP Suite (IP Protection)	User
Forcepoint DLP Cloud Applications (IP Protection)	User
Forcepoint CASB – Security Suite	User
CASB core licenses embed a limit on the number of supported cloud applications - Forcepoint CASB - Security Suite - supports a total of 15 applications regardless of the mix of Governance and Cloud protection	
Forcepoint CASB Implementation – Intermediate	N/A
Forcepoint Dynamic Data Protection – Add On	User
Enterprise Support for Forcepoint Data Advantage	N/A

For 5-year Terms, a Virtual Resident Engineer (VRE) is available during the first year. A VRE is a remote, flexible Full-time Equivalent (FTE) and does not include travel & expenses

Forcepoint Data Advantage and Edge Advantage Bundles –

Forcepoint Advantage– Organic Growth: During the Subscription Term, Forcepoint will make available upon request additional Units at no additional charge for the Forcepoint Advantage package to allow for an increase to the Permitted Capacity resulting from Customer's natural business growth during the Subscription Term ("Organic Growth"). Organic Growth does not include: (i) third party use of or access to Customer's network, including use or access by Customer's contractors or customers, or (ii) inorganic corporate growth activity, including mergers, acquisitions, joint ventures, or take-overs. Forcepoint may charge for usage that it determines does not result from Organic Growth. Any such additional Permitted Capacity will co-terminate with the applicable Subscription Term. No credit or refund will be provided if there is a decrease in usage. Customer may not transfer any of Customer's rights to use the Products or assign the Organic Growth rights in this Quotation to another person or entity without first obtaining prior written approval from Forcepoint. For those Products included in the Forcepoint Advantage Package that are normally licensed by Device, a Subscription for 1 User translates to a Subscription for 2 Devices.

When multiple Forcepoint Advantage packages are purchased, the same Product Name may appear in multiple Forcepoint Advantage packages. If a Product Name appears in multiple Forcepoint Advantage packages, then Forcepoint will provision one instance of that Product, but such Product may be used in the context of each Advantage Package where its name is listed.

Forcepoint FlexEdge Secure SD-WAN S60 –

Product Name	Unit Metric
Forcepoint Secure SD-WAN 60 Appliance	1 Unit
Forcepoint FlexEdge Secure SD-WAN Manager	1 Node
Essential Support	12 Months