ORDERING GUIDE

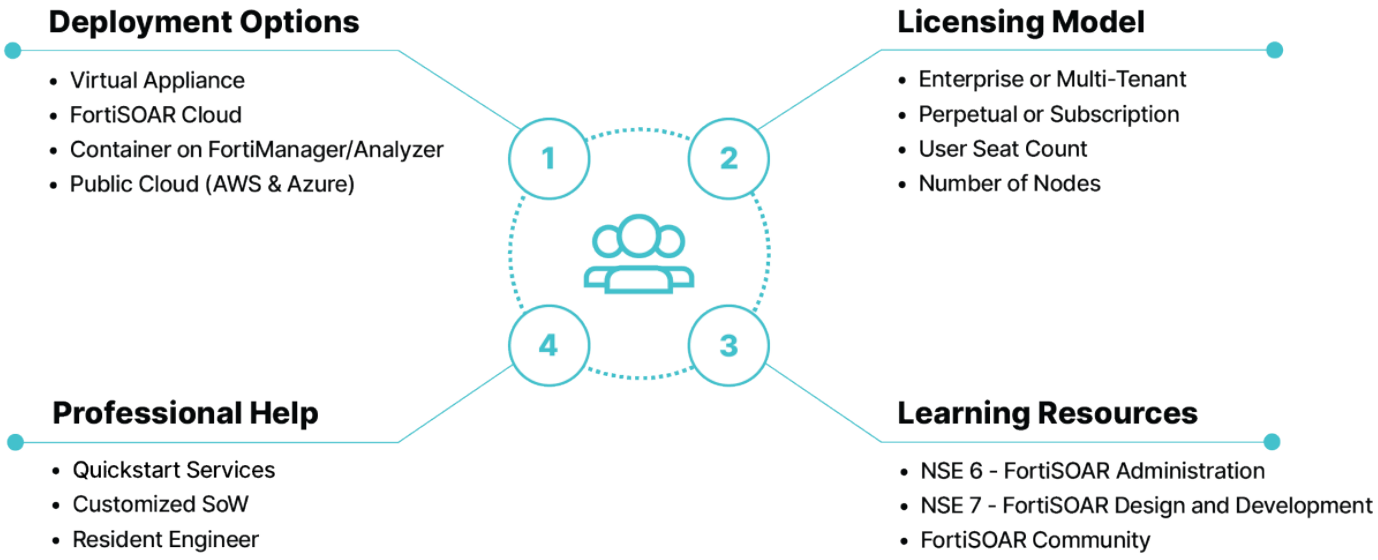
FortiSOAR

Available in

Cloud Virtual

PRODUCT INFORMATION

FortiSOAR is a leading SOAR platform that is used in conjunction with SIEM, UEBA, EDR, or other threat detection platforms. Use this document along with the FortiSOAR Datasheet to plan your purchase and/or deployment. The following is a high-level mind map to enable you to quickly go through all the various aspects that influence your purchase.



DEPLOYMENT OPTIONS

FortiSOAR is available in various form factors ranging from **customer-hosted** on physical or virtual platforms to **Cloud hosting** in platforms such as Amazon AWS, Microsoft Azure, Google GCP, etc. In addition, FortiSOAR is available as a **hosted offering** wherein Fortinet hosts the FortiSOAR instance in FortiCloud for the customer.

LICENSING MODEL

At the heart of it, FortiSOAR licensing is based on two aspects:

1. **User seats**: Can be named or concurrent (count of users that require to simultaneously log in to FortiSOAR at a given point in time).
2. **The number of FortiSOAR nodes**: Start with a single node and expand to more for HA/DR requirements or simply scale out.

FortiSOAR is available in both the **Subscription Licensing** (pay yearly cost including support) and the **Perpetual Licensing** (own the software, and pay support cost every year) models.

FortiSOAR is available in the following editions:

1. **Enterprise**: Designed for accelerating self-managed SOC. Provides all the features except for the ones that are designed for handling tenants or multiple SOCs. For those who need a more tailored capacity, there is an option to purchase a Starter version that offers all the essential functionalities with a daily allowance of 10,000 action executions, ensuring a cost-effective solution for organizations with specific needs.
2. **Multi-Tenant**: Primarily designed for Managed Service Providers offering SOCaaS and/or Managed SOAR offerings. This model is also used by enterprises that have more than one SOC and who require a dedicated SOAR for each of their SOCs as well as require the ability to centrally manage all their SOCs.
3. **HA**: For both Enterprise and Multi-Tenant editions, the HA Edition provides the capability to set up a high-availability cluster, ensuring resilience and continuous operation.

TRAINING SERVICES

Fortinet training services offers FortiSOAR specific training in the design and administration of FortiSOAR. The following courses are available:

FortiSOAR Administrator Training and Certification

2 full days or 3 half days Instructor-led Training, or self-led on demand

Learn about FortiSOAR architecture, and how to deploy, configure, manage, operate, and monitor FortiSOAR in a SOC environment. You will also learn about system customization, HA deployment, role-based access control (RBAC), and system monitoring tools.

https://training.fortinet.com/local/staticpage/view.php?page=library_fortisoar-administrator

FortiSOAR Design and Development

3 full days instructor-led training, or self-led on demand

Learn how to use FortiSOAR to design simple to complex playbooks, examine the role of FortiSOAR in mitigating malicious indicators, and learn how to create interactive dashboards to display relevant information about alerts and incidents. You will also learn how to integrate FortiSOAR with FortiGate, FortiSIEM, and FortiMail.

https://training.fortinet.com/local/staticpage/view.php?page=library_fortisoar-design-and-development

PROFESSIONAL SERVICES

Automation is a journey, and we recognize that you would need different levels of support during different phases of personalizing FortiSOAR for your organization:

1. **QuickStart Service**: This helps you set up FortiSOAR using standardized best practices and getting you started with FortiSOAR, enabling you to immediately realize the value of FortiSOAR. This service also includes knowledge transfer to help you manage the new environment.
2. **Scoped Engagements**: This is a customized SoW-based engagement for your tactical needs ranging from ad-hoc assistance hours to specific needs such as building modules, playbooks, integrations, etc.
3. **Resident Engineer Program**: This is a more strategic engagement to hire a dedicated SOAR engineer for a 6 to 12 months duration.

Refer to FortiSOAR Services Catalogue for additional information.

OTHER RESOURCES

FortiSOAR Platform Documentation: https://docs.fortinet.com/product/fortisoar

FortiSOAR Content Hub: https://fortisoar.contenthub.fortinet.com

FortiSOAR Connectors List: https://docs.fortinet.com/fortisoar/connectors

FortiSOAR Public Github: https://github.com/fortinet-fortisoar

FortiSOAR Community: https://community.fortinet.com/t5/FortiSOAR/gh-p/fortisoar

ORDER INFORMATION

DEPLOYMENT OPTIONS AND LICENSING MODEL			
FortiSOAR Edition	**Customer Hosted Subscription**	**Customer Hosted Perpetual**	**Fortinet Hosted Cloud Subscription**
FortiSOAR Enterprise Edition	FC-10-SRVMS-389-02-DD	LIC-FSRENT-2	FC-10-SRCLD-385-02-DD *
FortiSOAR Enterprise Edition (Renewal)	FC-10-SRVMS-385-02-DD		
FortiSOAR Multi Tenant Edition - Manager	FC-10-SRVMS-390-02-DD	LIC-FSRMTT-2	FC-10-SRCLD-386-02-DD *
FortiSOAR Multi Tenant Edition – Manager (Renewal)	FC-10-SRVMS-386-02-DD		
Add User Seat	FC-10-SRVMS-384-02-DD	LIC-FSRAUL-1	FC-10-SRCLD-384-02-DD
Add Tenants on ManagerNode	Included	Included	Included
Add Tenant as Dedicate SOAR Node (Single User Locked) - aka Dedicated Tenant Node	FC-10-SRVMS-387-02-DD	LIC-FSRMTD-1	FC-10-SRCLD-387-02-DD
Add Tenant as Dedicated SOAR Node (Multiple User Capable) - aka Regional SOC Instance	FC-10-SRVMS-388-02-DD	LIC-FSRMTR-2	FC-10-SRCLD-388-02-DD
FortiSOAR Starter Edition (10,000 actions/day allowed)	FC-10-SRVMS-1023-02-DD		
FortiSOAR HA Edition	FC-10-SRVMS-1121-02-DD	LIC-FSRHA-2	
Add Cloud Storage (1000GB with 8GB RAM and 4vCPU)			FC1-10-SRCLD-584-01-DD
FortiMonitor subscription for Advanced Health Monitoring Requirements		FC2-10-MNCLD-437-01-DD **	
SECURITY SERVICES			
Subscription Service for FortiSOAR Threat Intel Management Service including FortiGuard Premium Threat Feed	FC-10-SRVMS-592-02-DD	FC-10-SRVMP-592-02-DD	FC-10-SRCLD-592-02-DD
Support Services			
FortiCare Premium Contract	Included	See Below	Included
FortiCare BPS	Included	See Below	Included
Support SKU for Perpetual Licensing Model			
FortiCare Premium Contract for FortiSOAR Enterprise Edition	-	FC1-10-SRVMP-248-02-DD	-
FortiCare Premium Contract for FortiSOAR Multi Tenant Manager Edition	-	FC2-10-SRVMP-248-02-DD	-
FortiCare Premium Contract for FortiSOAR Multi Tenant - Dedicated Tenant	-	FC3-10-SRVMP-248-02-DD	-
FortiCare Premium Contract for FortiSOAR Multi Tenant - Regional SOC Instance	-	FC4-10-SRVMP-248-02-DD	-
FortiCare Premium Contract for FortiSOAR HA Edition		FC5-10-SRVMP-248-02-DD	
Support SKU with BPS for Perpetual Licensing Model			
FortiCare Premium Contract for FortiSOAR Enterprise plus FortiCare BPS	-	FC1-10-SRVMP-338-02-DD	-
FortiCare Premium Contract for FortiSOAR Multi Tenant plus FortiCare BPS	-	FC2-10-SRVMP-338-02-DD	-
FortiCare Premium Contract for FortiSOAR Multi Tenant - Dedicated Tenant plus FortiCare BPS	-	FC3-10-SRVMP-338-02-DD	-
FortiCare Premium Contract for FortiSOAR Multi Tenant - Regional SOC Instance plus FortiCare BPS	-	FC4-10-SRVMP-338-02-DD	-
Professional Services			
Per Day Charge for Resource Service (SOW)		FP-10-00000-M08-00-00	
Per Hour Charge for Service Delivered After-Hours/Weekend. Must order a minimum of 4 hours, and must use a minimum of 4 hours at a time		FP-PS001-HR	
Custom Travel & Expenses for On Site Professional Services		FP-MISC-TE	
FortiSOAR Deployment QuickStart Service		FP-10-QSSOAR-DP1-00-00	
Training Services			
FortiSOAR Administrator Training (Instructor-led) - 2 full days or 3 half days		FT-FSR-ADM	
FortiSOAR Administrator Training self-paced on-demand labs		FT-FSR-ADM-LAB	
FortiSOAR Administrator Certification Exam		NSE-EX-FTE2	
FortiSOAR Design and Development Course (Instructor-led) * **		FT-FSR-DEV	
FortiSOAR Design and Development self-paced on-demand labs * **		FT-FSR-DEV-LAB	

* A FortiCloud Premium Account License (FC-15-CLDPS-219-02-DD) is required to use the FortiSOAR Cloud service.
** Recommended FortiMonitor's 25-pack Device/Server Subscription Solution Bundle. For more information, see the FortiMonitor Data Sheet.
*** No certification exam for the Design and Development course.

Sample BOQ

Customer 1: An enterprise customer wants to host FortiSOAR within their premises. They need a perpetual license for 10 analysts along with 2 years of support and want to add Threat Intelligence Service including FortiGuard feeds. They also need training for developers along with a development instance for ongoing playbook and connector creation:

- LIC-FSRENT-2 (FortiSOAR Enterprise Edition with 2 seats included - Perpetual)
- LIC-FSRAUL-8 (8 Additional User Seats)
- FC1-10-SRVMP-248-02-24 (FortiCare Premium Contract for FortiSOAR Enterprise Edition for 24 months)
- FC-10-SRVMP-592-02-24 (2 year Subscription Service for FortiSOAR Threat Intel Management Service including FortiGuard Premium Threat Feed)
- FortiSOAR Free Trial OR FC-10-SRVMS-1023-02-24 (FortiSOAR Starter Edition for 2 years) as a development instance
- FT-FSR-DEV (NSE 7 FortiSOAR Design & Development Training)

If PS is needed, a quote from PS team can be requested.

Customer 2: An MSSP customer wants to leverage Fortinet's Hosted Option and needs a license for 10 analysts. They also need training for their developers:

- FC-10-SRCLD-386-02-DD (FortiSOAR Hosted Cloud Subscription - Enterprise Edition with 2 seats and support included)
- FC-15-CLDPS-219-02-DD (FortiCloud Premium Account License)
- FT-FSR-DEV (NSE 7 FortiSOAR Design & Development Training)

If PS is needed, a quote from PS team can be requested.

FREQUENTLY ASKED QUESTIONS

I need more than one node for creating a highly available environment. What all parts do I need to order?

Assuming that you need an enterprise edition in the Subscription mode with 10 user seats, you would order:

1. 1 Qty of FortiSOAR Enterprise node – this includes 2 user seats per node (additional node for HA)
2. 1 Qty of FortiSOAR HA Edition node
3. 8 Qty of User Seats
4. Support

I need more information about Fortinet's hosted deployment option.

Refer to FortiCloud Datasheet: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiCloud.pdf

What is included in the FortiSOAR Starter Edition? Any limitations?

FortiSOAR Starter Edition carries all the features of the FortiSOAR Enterprise Edition, only limited in allowing 10,000 automation actions/day. It comes with 2 default users, allows to add more user seats and can be setup in an HA cluster. An automation action is roughly defined as a step in a playbook, except that it does not account certain utility actions like Decision, Trigger etc.

What does concurrent user mean? How does it benefit the customer?

FortiSOAR does not impose any restrictions on creating a user. Technically, your entire organization can log in to FortiSOAR. The only restriction is how many of them can log in at the same time (aka concurrently).

This model comes in handy for optimizing the number of user licenses you need. For example, let's assume you have 2 admins and 30 analysts across 3 shifts. In this case, you could reduce the number of seats to 12 (2 reserved for admins and 10 floating amongst the analysts).

Do I need to buy a node for playbook/connector development work?

You can leverage the FortiSOAR Free Trial license or Starter Edition for such dev/test work based on the capacity required. The FortiSOAR Trial license is perpetually valid, allowing 2 user accounts as well as 1000 playbook actions/day whereas the Starter Edition allows 10,000 actions/day without posing any user limitations as such.

Can I host FortiSOAR on Hypervisor or Cloud platform that is not listed above?

FortiSOAR has ready-made images available for VMware Hypervisor and Amazon AWS AMI. For any other physical, virtual, or cloud hosting you can install FortiSOAR on top of Rocky Linux 9.x or RHEL 9.x.

Is there any charge for using a connector?

FortiSOAR does not impose any charge on installing/using a connector. However please note that the target application (for example VirusTotal) might need you to procure their service/API, etc. for being consumed by the connector.

What are my options to build a new connector, or enhance an existing connector?

Option 1 – FortiSOAR provides full IDE to build, test, and publish connectors. Leverage that to build a new or enhance an existing connector. You can also submit the one that you built to the FortiSOAR Community.

See the instructions here: https://github.com/fortinet-fortisoar/how-tos

Option 2 – Request your Account Manager to create a task for FortiSOAR R&D to build the connector. The success of this option is dependent on various aspects, some of which are:

- Access/Availability of target application to Test
- Access/Availability of target application's API
- Demand for the desired integration

Several such criteria would be applied by the FortiSOAR PM to decide the timeline of delivery for the requested integration

Option 3 – Leverage FortiSOAR Professional Services (PS) to quickly build the integration scoped to your needs. This option requires you to purchase PS and it is likely to have the fastest turnaround time. It is suitable if you urgently need an integration that is not on the store.

What does the new Threat Intel Management SKU, FC-10-SRXXX-592-02-DD, entitle me to and what is still available without this SKU?

This SKU allows you to leverage the uncapped (limited to 100 feeds/day without this SKU) daily FortiGuard daily threat Intel feeds in FortiSOAR. The feed is an extensive dataset, comprising of IPs, URLs, Domain and malicious hashes carefully curated by our team of experts. The entire feeds database is labelled with the relevant threat types, and associated LockHeed Martin Kill Chain Phases, that enables user with contextual information to understand the nature of threat. In addition to these feeds, the new SKU option also enables the following features in the FortiSOAR Threat Intel Management experience:

- Provide 'Contextual Sighting' Information: For every indicator that is created, FortiSOAR automatically looks up a match in its feeds database and links these matched indicators automatically to the extracted indicator. The advantage of this is two-fold:
- Getting good contextual information even when information about these suspicious targets is not yet available with the standard enrichment sources.
- Providing users with a dashboard displaying the relevance of various intelligence sources based on the number of actual sightings in their environment.
- No limit on the feed volume that can be ingested per day in the 'Threat Intel Management' module using the FortiSOAR Feeds API.

If the Threat Intel Management Service Subscription is 'Disabled', then the 'Ingest Feed' step can insert only 1000 records per day in the 'Threat Intel Management' module. Once this limit is exceeded, further feed ingestion playbooks start failing with the: 'Daily Feed Ingestion Limit reached' error till the counter is reset at midnight (UTC).

An example of how this works: If you have 100 records left from the 1000 records per day limit, and you send 200 records as part of the ingestion feed, only 100 records are saved, and the remaining 100 are ignored.

- No limit on the number of feeds that be exported using the FortiSOAR 'TAXII API' for sharing processed threat intelligence to SIEMs, Firewalls etc. If this SKU is not enabled, the TAXII-compatible API provides only 100 records as part of the API response.

For more information on TIM, see the Threat Intel Management Solution Pack documentation in the FortiSOAR Content Hub.

Visit www.fortinet.com for more details