DATA SHEET

FortiSOAR™

Available in:

Virtual Machine | Hosted | Cloud

FortiSOAR is a holistic Security Orchestration, Automation and Response workbench, designed for SOC teams to efficiently respond to the ever-increasing influx of alerts, repetitive manual processes, and shortage of resources. This patented and customizable security operations platform provides automated playbooks and incident triaging, and real-time remediation for enterprises to identify, defend, and counter attacks.

FortiSOAR optimizes SOC team productivity by seamlessly integrating with over 350+ security platforms and 3000+ actions. This solution results in faster responses, streamlined containment, and reduced mitigation times, from hours to seconds.

Common SOC Challenges

Too many alerts

Repetitive tasks

Disparate tools

Staff shortages

Highlights

- Manage security alerts, incidents, indicators, assets and tasks through a simplified, easy-to-use GUI
- Increase SOC team productivity by eliminating false positives and focusing only on the alerts that matter
- Track ROI, MTTD, and MTTR through customizable reports and dashboards
- Automate within the Visual Playbook Designer with 350+ security platform integrations and 3000+ actions for automated workflows and connectors
- Minimize human error by employing clear, auditable playbooks and custom modules to handle ever-changing investigation requirements
- Scale your network security solution with a truly multi-tenant distributed architecture from a single, collaborative console
- Identify real threats with automated false positive filtering and predict similar threats and campaigns with FortiSOAR's ML-powered recommendation engine
- Eliminate repetitive tasks through automation, correlation of incidents, threat intelligence, and vulnerability data
- Take advantage of the in-built Incident War Room for streamlining crisis management and collaborative P1 incident investigations
- Reduce security incident discovery times from hours to seconds
- Leverage the FortiSOAR mobile application for taking important decisions and staying informed while on the move
- Build and edit connectors easily within the product user interface using the Connector Builder Wizard
- Flexible Deployment Options - VM, hosted, or cloud. Available on FortiCloud, AWS, Azure, and as management extensions on FAZ/FMG

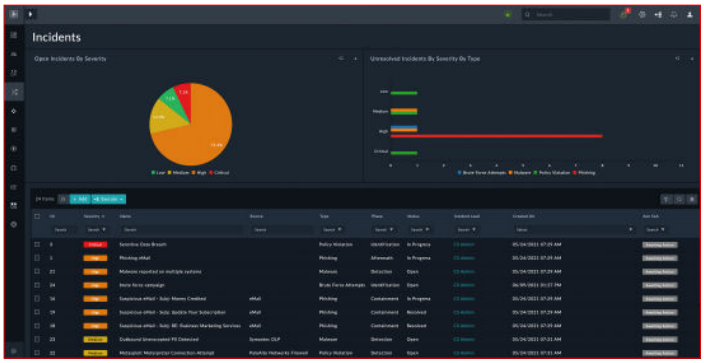
KEY FEATURES

Role-Based, Streamlined Incident Management

FortiSOAR's Enterprise Role-Based Incident Management solution provides organizations with robust field level role-based access control to manage sensitive data in accordance with SOC policies and guidelines.

Easily manage alerts and incidents in a customizable filter grid view with automated filtering, to keep analysts focused on real threats. Execute dynamic actions and playbooks on alerts and incidents and analyze correlated threat data in an intuitive user interface. FortiSOAR's ML-powered Recommendation Engine predicts various fields such as severity, asset, user, based on previously identified cases, aiding the SOC analyst in grouping and linking them together to identify duplicates and campaigns involving similar alerts, common threats, and entities.

The FortiSOAR mobile app adds a new dimension to the incident management and allows users to take actions like monitoring alert queue, triggering important playbooks, and providing critical approvals on the go.

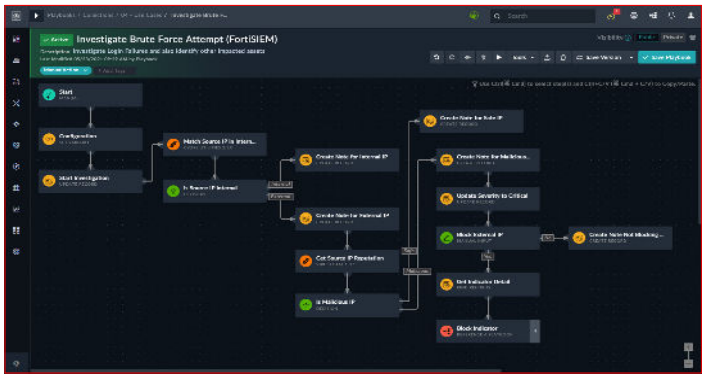


Truly Multi-Tenant

FortiSOAR provides a truly distributed multi-tenant product offering with a scalable, resilient, secure, and distributed architecture, allowing MSSPs to offer MDR-like services, while supporting operations in regional and global SOC environments.

With the ability to run automation workflows on specific tenants remotely, ability to manage tenant playbooks, modules, views remotely, handling unique customer environments and product diversity becomes streamlined. FortiSOAR also involves tenants in case of approval requirements to control data flow to the master nodes.

Other tenant features include creating tenant-specific alerts, incident views, reports and dashboards, and filter views. Service providers and customers can choose between a dedicated SOAR tenant node for complete isolation and management or a light-weight FortiSOAR agent that can be used to leverage the customer's on-premise integrations. A hybrid model is also possible, providing a lot of flexibility in designing a right fit for various scenarios.



Visual Playbook Builder

FortiSOAR's Visual Playbook Designer allows SOC teams to design, develop, debug, control, and use playbooks in the most efficient manner.

The intuitive design includes a drag and drop interface to string multiple steps together, using 350+ OOB workflow integrations, 3000+ automated actions, a comprehensive expression library for easy development, playbook simulation and referencing, ability to execute code in workflows like python, versioning, privacy control, crash recovery, advanced step controls like looping, error handling, notifications, undo/redo, and more. Advanced features such as playbook prioritization, public/private visibility, and simulation engine provide a greater degree of control in designing a well-orchestrated solution.

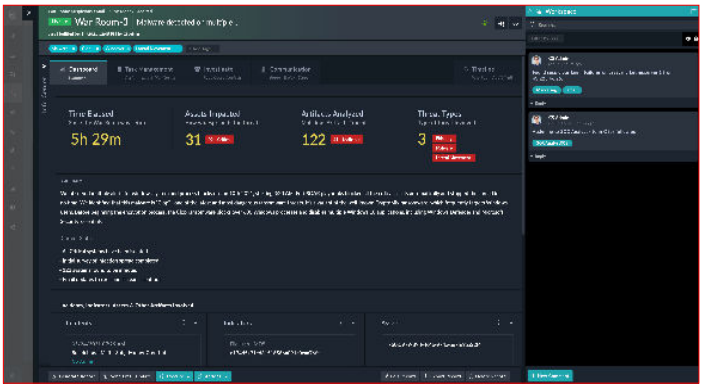
FortiSOAR's extensible platform provides the ability to define new modules with customization of fields, views, and permissions, and creation of smart automated workflows and playbooks on top of them, simplifying the analyst's ability to support solutions for vulnerability and threat management as well as regulation and compliance.

KEY FEATURES

Crisis Management with Incident War Room

FortiSOAR offers a dedicated crisis management framework, the Incident War Room, which can be used for streamlining and collaborative P1 incident investigations. Any critical incident can be a trigger to start a war room around it and quickly gather in team members across the board. It has built-in access control to ensure who gets to see what, task management for assigning, monitoring, and organizing the investigation, dedicated collaboration facility that can work in sync with external collaboration tools like MS teams, Slack, Zoom, and much more.

Purpose-built for crisis management, it takes care of other important elements like Announcements board and a dedicated Reporting section also.

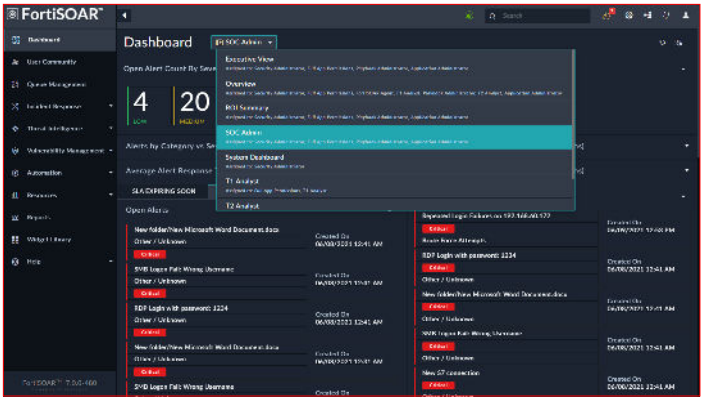


Role-Based Dashboards and Reporting

Role-based dashboards and reporting empower SOC teams to measure, track, and analyze investigations and SOC performance granularly with quantifiable metrics.

FortiSOAR's ready-made library of industry standard, persona-focused dashboard templates, intuitive drag and drop visual layout builders, ensures SOC teams have the best tools to optimize their time and resources. Comprehensive charts, listings, counters, and performance metrics help create rich views and informative data models. FortiSOAR also provides industry-standard reports for Incident Closure, Incident Summary, Weekly Alert and Incident Progress, IOC Summary, and many others.

It enables SOC teams to track metrics such as MTTR and MTTD over various NIST approved incident phases, analyst loads, escalation ratios, Automation ROIs, and other SOC performance metrics.



Threat Intel Management

FortiSOAR delivers Enhanced Threat Intelligence Management Support leveraging its deep integration with FortiGuard offering unrestricted lookup of indicator reputations, threat categories, and Threat Encyclopedia access. Ingestion of structured and unstructured feeds is supported with the ability to import indicators from CSV/STIX files and exporting indicators in STIX format.

Analysts can also manage indicators more easily with TLP (Traffic Light Protocol) for indicator sharing, indicator expiry, and exclusion lists. FortiSOAR also includes multiple out-of-box playbooks for sharing indicators with standard SIEM and UEBA products.

FortiSOAR Mobile Application

FortiSOAR mobile application is an extension of FortiSOAR's Web interface, which facilitates important and urgent actions such as immediate approvals, notifications, and threat monitoring allowing SOC teams and executives to act swiftly and provide critical inputs on the go.

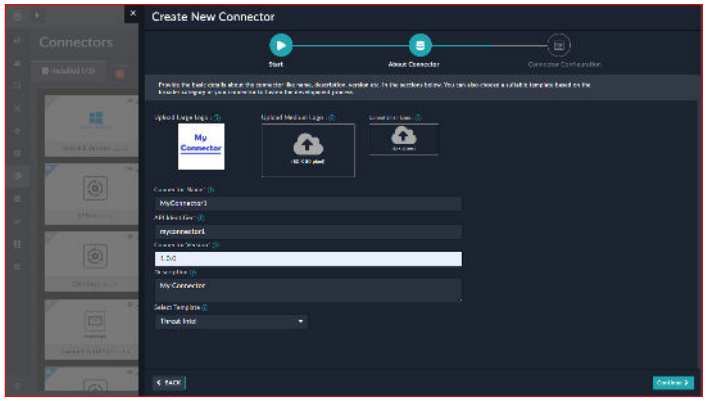
Analysts can easily navigate FortiSOAR through the application's rich user experience and execute actions like viewing and reassigning records, providing approvals, triggering important playbooks, and monitoring alert queues.

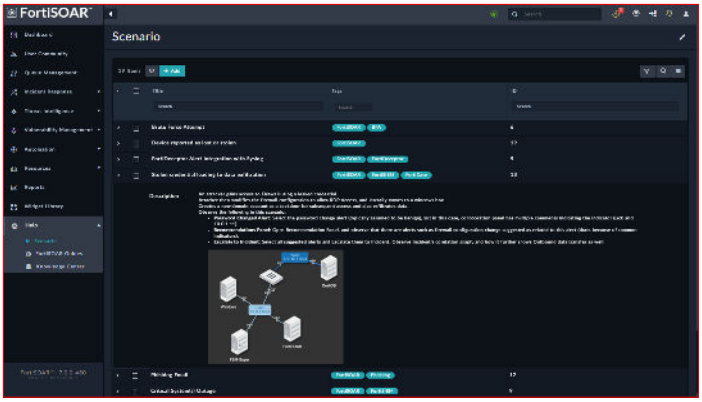
KEY FEATURES

Connector and Widget Creation Studio

With the built-in Connector Wizard, analysts can easily create custom connectors for sending and retrieving data from various third-party products as well as edit existing connectors. The easy-to-use interface offers a built-in testing framework and facilitates building connectors directly in the product UI using a guided wizard framework. Analysts can select from multiple pre-made templates to help develop their connectors, ensuring best practices.

In a similar manner, the Widget Creation Wizard allows for building custom new widgets within the UI, ensuring that users are never limited in ways to represent their data as required.





Incident Response Content Pack

The FortiSOAR Incident Response Content Pack enables Analysts and Users to experience the power of FortiSOAR's incident response. Built with a modular architecture, the Incident Response Content Pack is the implementation of best practices to configure and implement an efficient Security Orchestration, Automation, and Response solution in an optimal manner.

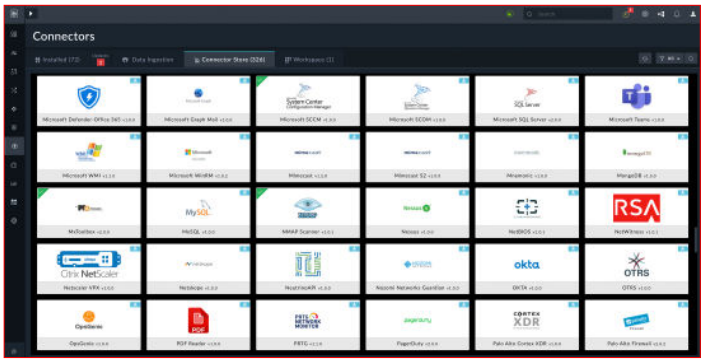
The content pack consists of various default modules, comprehensive collection of utility and use case Playbooks, industry-standard Dashboards and Roles, as well as many samples, simulations, and training data that enable SOC teams to experience the power of FortiSOAR and get a quick head start.

Maximize Your ROI with FortiSOAR

Steps	Manual	FortiSOAR
Enrich Artifacts to Identify IOCs	45 to 60 minutes	3 minutes
Perform Triaging on Events from SIEM	20 minutes	1 minute
Submit a Zip to the Detonation Engine	1 hour to 6 hours	1 minute
Isolate Affected Devices	10 minutes	1 minute
Analyze, Create, and Annotate an Incident	60 minutes	5 minutes
Block IOCs on a Firewall (e.g. FortiGate)	45 minutes to 2 hours	2 minutes
Remediation and Incident Response	60 minutes to 6 hours	5 minutes
Prepare and send an Incident Summary Report	2 to 3 hours	2 minutes
TOTAL	**4.5 TO 15 hours**	**20 minutes**

CONNECTORS AND INTEGRATIONS

FortiSOAR third party connectors and integrations provide unlimited access to hundreds of products including desktop security software, directories, network infrastructure, and other third-party security systems maximizing your ROI in addition, providing unparalleled visibility and control across your network through Security Orchestration, Automation, and Response (SOAR). FortiSOAR seamlessly integrates with other vendors and technologies and offers a built-in connector builder wizard to build new connectors easily or edit the ones already there.



The following are a few notable integrations that FortiSOAR offers today:

Fortinet Connectors	FortiGate, FortiAnalyzer, FortiSIEM, FortiEDR, FortiNAC, FortiDeceptor, FortiSandbox, FortiMail, FortiGuard, FortiAI, FortiManager, FortiMonitor, FortiEMS
Network and Firewall	FortiGate, Cisco Meraki MX VPN Firewall, Infoblox DDI, CISCO Umbrella Enforcement, Cisco Meraki MX L7 Firewall, Empire, CISCO Firepower, ForeScout, Zscaler, Imperva Incapsula, NetSkope, RSA Netwitness Logs And Packets, PaloAlto Firewall, CISCO ASA, SOPHOS UTM-9, Arbor APS, F5 Big-IP, Proofpoint TAP, Check Point Firewall, CISCO Catalyst, Citrix NetScaler WAF, Sophos XG, Cisco Stealthwatch, Pfsense, Symantec Messaging Gateway, PRTG, Centreon
Analytics and SIEM	FortiSIEM, FortiAnalyzer, RSA Netwitness SIEM, Sophos Central, Rapid7 InsightIDR, LogPoint, Micro Focus ArcSight Logger, Alienvault USM Anywhere, xMatters, Sumo Logic, LogRhythm, Syslog, Elasticsearch, McAfee ESM, IBM QRadar, ArcSight, Splunk, ReversingLabs A1000
Vulnerability Management	Rapid7 Nexpose, Kenna, Qualys, Tripwire IP360, Symantec CCSVM, Tenable IO, ThreadFix, Tenable Security Center
Ticket Management	ConnectWise Manage, Foresight, Zendesk, ServiceAide, Manage Engine Service Desk Plus, Salesforce, BMC Remedy AR System, OTRS, Request Tracker, JIRA, Pagerduty, RSA Archer, Cherwell, ServiceNow
Endpoint Security	Endgame, Trend Micro Control Manager, CrowdStrike Falcon, FireEye HX, Carbon Black Defense, Malwarebytes, McAfee EPO, Symantec EDR Cloud, Microsoft WMI, TrendMicro Deep Security, Symantec EPM, Symantec DLP, WINRM, NetBIOS, Microsoft SCCM, Microsoft SCOM, CISCO AMP, Carbon Black Protection Bit9, CYLANCE Protect, SentinelOne, Carbon Black Response, TANIUM
Threat Intel	EmailRep, AlienVault USM Central, Trend Micro SMS, Malware Domain List, Infocyte, Attivo BOTsink, FireEye ISIGHT, Vectra, Phishing Initiative, Threatcrowd, ThreatConnect, CRITS, McAfee Threat Intelligence Exchange, Facebook ThreatExchange, Intel 471, Soltra Edge, Anomali STAXX, Recorded Future, AlienVault OTX, MISP, DARKTRACE, IBM X-Force, ANOMALI THREATSTREAM, BluVector, ThreatQuotient
DevOps	AWS Athena, AWS S3, Twilio, IBM BigFix, AWS EC2
Sandbox	FortiSandbox, GitLab, ThreatSTOP, Intezer Analyze, FireEye AX, CISCO Threat Grid, URLSCAN.Io, Joe Sandbox Cloud, Koodous, Trend Micro DDAN, Symantec CAS, HYBRID-ANALYSIS, VMRAY, PaloAlto WildFire, Malwr, Lastline, SecondWrite, Cuckoo
Email and Email Security	GSuite For GMail, Microsoft Exchange, SMTP, IMAP, Mimecast, Symantec Email Security Cloud, FireEye EX, CISCO ESA
Investigation	FortiAnalyzer, FortiSIEM, FortiMail, Securonix SNYPR, Symantec ICDx, Symantec Security Analytics, NMAP Scanner, Protectwise, PhishTank, CloudPassage Halo, TruSTAR, Have I Been Pwned, Farsight Security DNSDB, Cofense PhishMe, RSA Netwitness

* FortiSOAR can be integrated with many other vendors and technologies in addition to those listed here.

FORTISOAR CLOUD

Fortinet also offers cloud-based FortiSOAR service to enable customers who want to leverage Fortinet managed FortiSOAR platform. Customers and partners can easily access their FortiSOAR Cloud from their FortiCloud Single-Sign-On Portal.

ORDER INFORMATION

PRODUCT	SKU	DESCRIPTION
FortiSOAR Subscription License	FC-10-SRVMS-385-02-DD	One year subscription for FortiSOAR Enterprise Edition - 2 User Logins included plus 24×7 FortiCare support
	FC-10-SRVMS-386-02-DD	One year subscription for FortiSOAR Multi Tenant Edition - 2 User Logins Included plus 24×7 FortiCare support
	FC-10-SRVMS-387-02-DD	One year subscription for FortiSOAR Multi Tenant Edition - Dedicated Tenant - Restricted to 1 User Login (Included) plus 24×7 FortiCare support
	FC-10-SRVMS-388-02-DD	One year subscription for FortiSOAR Multi Tenant Edition - Regional SOC Instance - 2 User Login Included plus 24×7 FortiCare support
	FC-10-SRVMS-384-02-DD	One year subscription for FortiSOAR User Seat License - One Additional User Logins plus 24×7 FortiCare support
FortiSOAR Perpetual License	LIC-FSRENT-2	FortiSOAR Enterprise Edition - 2 User Logins Included (Perpetual License)
	LIC-FSRMTT-2	FortiSOAR Multi Tenant Edition - 2 User Logins Included (Perpetual License)
	LIC-FSRMTD-1	FortiSOAR Multi Tenant Edition - Dedicated Tenant - Restricted to 1 User Login (Included)
	LIC-FSRMTR-2	FortiSOAR Multi Tenant Edition - Regional SOC Instance - 2 Users Login Included (Perpetual License)
	LIC-FSRAUL-1	FortiSOAR User Seat License - Additional User Logins (Perpetual License) - add-on by 1
	FC1-10-SRVMP-248-02-DD	FortiCare 24×7 support for FortiSOAR Enterprise Edition
	FC2-10-SRVMP-248-02-DD	FortiCare 24×7 support for FortiSOAR Multi Tenant Edition
	FC3-10-SRVMP-248-02-DD	FortiCare 24×7 support for FortiSOAR Multi Tenant - Dedicated Tenant
	FC4-10-SRVMP-248-02-DD	FortiCare 24×7 support for FortiSOAR Multi Tenant - Regional SOC Instance
FortiSOAR Cloud	FC-10-SRCLD-385-02-DD	One year subscription for FSR CLOUD Enterprise Edition - 2 User Logins included plus 24×7 FortiCare support
	FC-10-SRCLD-386-02-DD	One year subscription for FSR CLOUD Multi Tenant Edition - 2 User Logins Included plus 24×7 FortiCare support
	FC-10-SRCLD-384-02-DD	One year subscription for FSR CLOUD User Seat License -One Additional User Logins plus 24×7 FortiCare support