DATA SHEET

FortiSOAR™

Adaptive Security for SOC Teams and Enterprises

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 300+ security platforms and 3000+ actions. This 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

FortiSOAR enables SOC teams to quickly and securely:

- 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, MTTR through customizable reports and dashboards
- Automate within the Visual Playbook Designer, with 300+ security platform integrations & 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 recommendation engine
- Eliminate Repetitive Tasks through automation, correlation of incidents, threat intelligence & vulnerability data
- Improve efficiency & effectiveness of SOC processes by customizing and employing FortiSOAR's automation templates to save time and resources
- Reduce security incident discovery times from hours to seconds

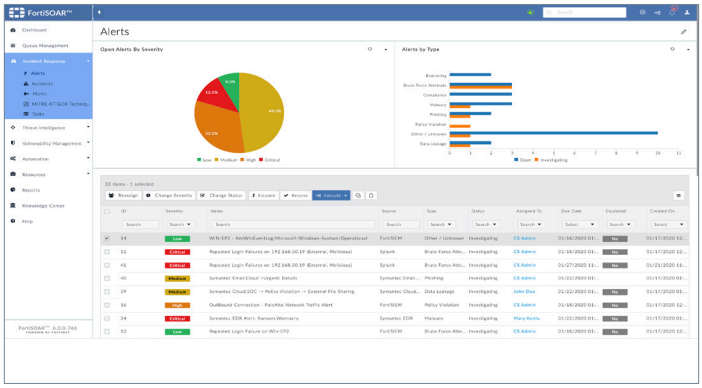
Key Features

Role-Based 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 Recommendations 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.



Role-Based Dashboards & Reporting

Role-based dashboards and reporting, empowers 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. Track metrics such as MTTR, MTTD over various NIST approved incident phases, analyst loads, escalation ratios, Automation ROI's and other SOC performance metrics.

Multi-Tenancy

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.

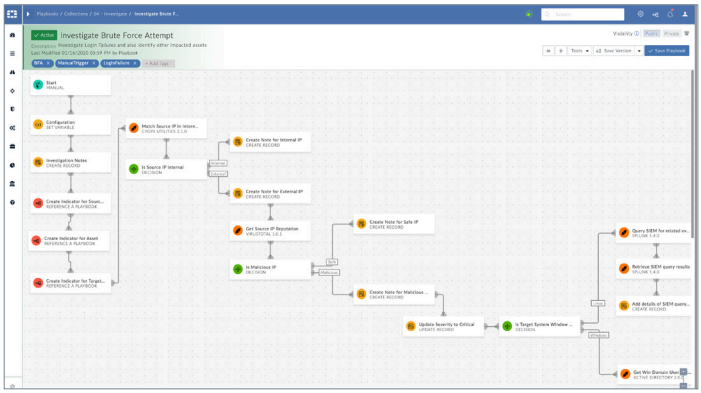
With the ability to run automation workflows on specific tenants remotely, handling unique customer environments & product diversity becomes streamlined. FortiSOAR also involves tenants in case of approval requirements to control data flow to the master nodes. Other tenant features include creating tenant-specific alerts, incident views, reports and dashboards, and filter views.

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 300+ 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 and more.

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.



Maximize your ROI with FortiSOAR

Steps	Manual	FortiSOAR
Enrich Artifacts To Identify IOCs	45 - 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 & Annotate an Incident	60 minutes	5 minutes
Block IOCs on a Firewall (e.g. FortiGate)	45 minutes to 2 hours	2 minutes
Remediation & 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 & Integrations

FortiSOAR 3rd Party Connectors & Integrations provide unlimited access to hundreds of products including desktop security software, directories, network infrastructure, and other third-party security systems maximizing your ROI and providing unparalleled visibility and control across your network through Security Orchestration, Automation and Response (SOAR). FortiSOAR seamlessly integrates with other vendors and technologies. The following are a sample of the connectors that FortiSOAR integrates with:

Network & Firewall	FortiOS, Cisco Meraki MX VPN Firewall, Infoblox DDI, CISCO Umbrella Enforcement, Empire, CISCO Firepower, ForeScout, Zscaler,Imperva Incapsula, NetSkope, RSA Netwitness Logs And Packets, PaloAlto Firewall, CISCO ASA, SOPHOS UTM-9, Fortigate Firewall, Arbor APS, F5 Big-IP, Proofpoint TAP, Check Point Firewall, CISCO Catalyst, Citrix NetScaler WAF, Sophos XG, Cisco Stealthwatch, Pfsense, Symantec Messaging Gateway
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
DevOps	AWS Athena, AWS S3, Twilio, IBM BigFix, AWS EC2
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
Analytics	Fortinet FortiSIEM, 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
Fortinet Connectors	FortiMail, FortiEDR, FortiAnalyzer, FortiGate, FortiSandbox, FortiGuard Webfilter lookup, FortiOS

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

www.fortinet.com