SOLUTION BRIEF

# FortiSOAR Empowers Security Operations to Accelerate Incident Response

## Executive Summary

**Network attack surfaces continue to expand due to evolving threats and new digital innovations. To keep up, many organizations add point solutions. This increased security complexity contributes to a number of problems: too many vendors to manage, too many alerts to investigate, manual processes that slow response times, and a lack of trained staff to manage the expanding workloads each day. Furthermore, this complexity makes it difficult for security teams to identify optimal solutions for their array of challenges.**

**The addition of security orchestration, automation, and response (SOAR) capabilities to the security architecture can alleviate these pressures. FortiSOAR allows security operations teams to create a custom automated framework that pulls together all of the organization's security tools while eliminating alert fatigue and reducing context switching. This enables security operations teams to not only adapt but also optimize their security processes.**

## Disaggregated Security Creates Alert Fatigue for Staff—and Risk

Security analysts are currently overwhelmed by the number of security alerts they face each day. Increasingly complex and fragmented security infrastructures (too many point products from different vendors) is the main reason for this problem. To keep pace with emerging threats and new risk exposures, the average enterprise now deploys 47 different security solutions and technologies.[1]

While the sheer volume of alerts is a big part of the problem, tracking, investigating, and trying to remediate alerts from many different sources requires a great deal of manual effort on the part of security operations center (SOC) staff. These inefficient processes slow down the incident response process—a current average of 279 days to identify and contain a single breach.[2]

Simultaneously, organizations are struggling with a worldwide cybersecurity skill shortage when it comes to security operations. Nearly two-thirds (65%) of companies currently lack the skilled staff they need to maintain effective security operations.[3] These intersecting factors further increase the chances of a breach going undetected.

Last year, breaches with a life cycle less than 200 days were, on average, $1.22 million less costly than breaches with a life cycle of more than 200 days ($3.34 million vs. $4.56 million, respectively)—a difference of 37%.[6]

The SOAR market is in such a demand for SOC teams it is projected to grow to reach nearly $1.8 billion at a CAGR of 15.6% from 2019 to 2024.[7]

A SOAR solution helps security integrate their countless security tools—allowing separate components to communicate and work together in a defensive coordination. This not only provides greater network visibility but also translates to fewer and more strategic alerts pertaining to cybersecurity.[4] Specifically, SOAR allows security operations teams to automate the tedious and repetitive elements of workflows that do not require human oversight, while maintaining human authority. The best SOAR solutions enrich and contextualize threats to help analysts quickly triage cases according to the severity of the risk, sensitivity, or criticality of the business functions under threat.[5]

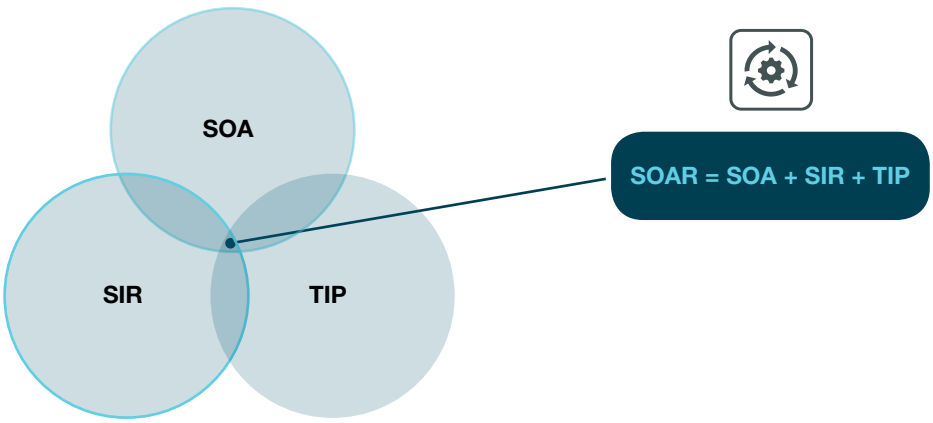


Figure 1: SOAR brings together three key capabilities necessary for timely threat identification and mitigation.

## FortiSOAR Integrates Security and Automates Responses

FortiSOAR offers the ability for security teams to aggregate and enrich alerts from a wide range of security products. It simplifies orchestration and management by leveraging well-defined playbooks, resulting in the elimination of time-consuming manual workflows.

Figure 2 shows how FortiSOAR helps SOC teams reduce incident response time by as much as 98%. Replacing a series of manual, inefficient, and error-prone steps that may take as long as 15 hours, FortiSOAR automated processes can be completed in a total of 20 minutes, on average.

**Incident Response Time: Manual vs. FortiSOAR**

| Steps | Manual | FortiSOAR |
|---|---|---|
| Enrich artifacts to identify IOCs | 46 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** |

Figure 2: FortiSOAR helps SOC teams reduce incident response time.[8]

As part of the integrated Fortinet Security Fabric architecture, FortiSOAR unifies security tools in a single, federated capacity. This allows FortiSOAR to shift a team's workload by automating the majority of lower-level tier-1 alert processes, allowing SOC analysts to focus on more critical tasks. The following four key use cases demonstrate the immediate value FortiSOAR offers to struggling SOC teams:

### Use Case 1: Unified SOC Workbench

A vendor-agnostic SOAR offering, FortiSOAR simplifies SOC complexity by integrating disparate point security solutions into a centralized orchestration system that can be deployed in virtually any environment. It includes more than 300 out-of-the-box connectors. These enable SOC teams to operate FortiSOAR seamlessly with existing security solutions from other vendors, and to ingest alert information while providing a centralized point of visibility and control across the organization. This integration eliminates ecosystem fragmentation, simplifies security operations processes, and extends the useful life of existing tools to maximize the return on investment (ROI) for those purchases. FortiSOAR enables teams to centralize their entire security process and to respond with all their current tools, which results in faster real-time response.

### Use Case 2: Automated Alert Triage

Due to lengthy incident response processes, it has become increasingly difficult for analysts to keep up with the pace of incoming alerts. FortiSOAR aggregates these alerts in one place while enriching them with added context to accelerate time to resolution. It also helps reduce the number of "false-positive" alerts and provides advanced case management functions that help to define, guide, and speed investigations. FortiSOAR streamlines simple SOC tasks such as alert ingestion, prioritization based on severity levels, assigning tasks, and subroutines. It also automates more complex exchange-to-exchange (E2E) tasks, such as triage, enrichment, investigation, and remediation, cohesively centralizing the security processes by automatically correlating alerts from across a security stack into a single incident.

These sophisticated integration and automation capabilities help to eliminate many of the common burdens associated with alert fatigue. This, in turn, allows SOC analysts to focus on threat hunting, while reducing workloads and the windows of exposure to an active breach threat.

### Use Case 3: Augmenting the SOC to Accelerate Incident Response

The existence of numerous manual workflows impedes alert investigations and increases time to resolution while increasing the risk of human oversights and errors. Organizations in this situation are not merely operationally inefficient; they are at increased risk of a breach. The remedy is to augment the SOC by leveraging FortiSOAR to extend the automation features of the FortiAnalyzer logging and reporting and the FortiSIEM security information and event management (SIEM) solutions. This results in robust orchestration and automation of all SOC processes and an improvement in overall security.

Security teams can increase efficiency by automating every task, change, or update according to the organization's needs. Instead of just automating a single entity, FortiSOAR can augment the entire SOC and improve overall security.

FortiSOAR is uniquely customizable. Security teams can automate any response and subroutine. Where it makes sense, they can set threshold conditions at which FortiSOAR will immediately take an identity offline and leverage its built-in playbooks and connectors to achieve optimal incident response.

**Use Case 4: Unburdening Limited SOC Team Resources**

By streamlining security operations and processes through automated workflows, FortiSOAR reduces the staff time and costs associated with security incident response. As the threat landscape evolves and security devices proliferate, increased SOC efficiency contributes significantly to reducing the total cost of ownership (TCO) for network security.

One way FortiSOAR reduces staff burdens is by enabling SOC teams to customize the tool's protocols and automated security responses to meet their specific SOC frameworks and requirements. This minimizes the manual effort that is taken during their responses, effectively reducing a team's overall workload.

For ease of onboarding, FortiSOAR offers the option of out-of-the-box, drag-and-drop playbooks for instant configurability and short time to initial value. FortiSOAR also helps SOC teams maintain tribal knowledge. If an employee leaves the organization, their workflow, insight, and experience remain intact, as it is documented within the system.

## A Robust Solution for Mature SOCs

SOCs can be classified into three levels of automation, as shown in Figure 3. Because of their different staffing levels and organizational structures, SOCs at each of these levels have characteristically different challenges. The Fortinet Security Fabric meets the challenges of each automation level with three unique yet integrated offerings: FortiAnalyzer logging and reporting, FortiSIEM security information and event management, and FortiSOAR.

The powerful capabilities of FortiSOAR are most beneficial for SOC automation level 3: experienced security teams, with five or more analysts, well-defined security processes, and sizable security stacks.

**98%**

**Potential reduction in incident response time with FortiSOAR[9]**

Designed for enterprise teams that require full orchestration and automation of security processes, across the Fortinet Security Fabric and in multivendor environments, FortiSOAR builds on the capabilities of FortiAnalyzer and FortiSIEM, adding more comprehensive workflow automation and orchestration, AI-driven alert prioritization, and more built-in connectors for data ingestion and response coordination. FortiSOAR is also highly effective for SOCs that have been using multiple analytical or dedicated products similar to SOAR. These SOCs are likely mature enough for SOAR itself, and FortiSOAR provides an effective and efficient upgrade.

**FortiSOAR: SOC Automation Levels**

- Streamline SOC efficiencies and accelerate incident response

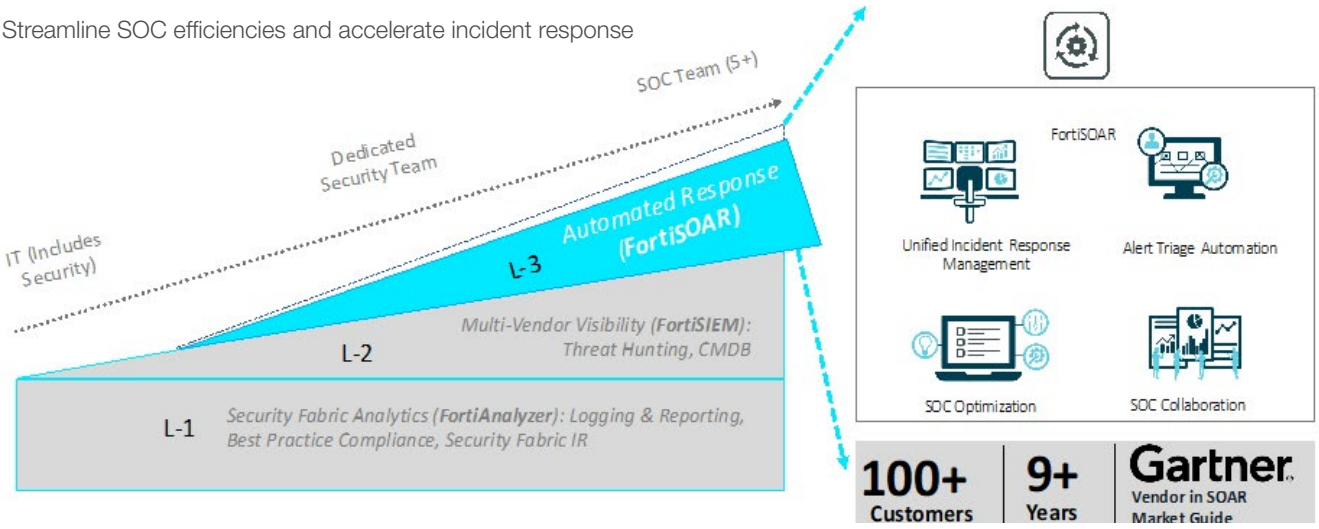


Figure 3: FortiSOAR designed for the highest level of SOC automation.

## Managing Risk, Resources, and Results

Security operations will continue to face the dual pressures of an expanding attack surface and a lack of resources and thus struggle to keep pace with growing risk exposure. An effective, fully featured SOAR solution can help mature SOC teams address these difficulties while also enhancing, optimizing, and fortifying their organization's security processes.

FortiSOAR offers a nimble and customizable solution that helps security operations to quickly adapt their response to an ever-evolving threat landscape. Teams can leverage the automation and orchestration capabilities in FortiSOAR to advance their entire incident response process. The outcome for organizations is a simplified security ecosystem, elimination of alert fatigue, accelerated response times, and a reduced burden on limited SOC team resources, while maximizing team collaboration.

In addition, FortiSOAR offers simplified licensing via a user-based, predictable licensing model. This allows teams to leverage the efficiencies of FortiSOAR while staying within budget, regardless of the volume of incidents they handle. With an inherently scalable architecture, FortiSOAR delivers high availability for growing enterprise organizations, enabling the solution to expand across growing and/or distributed organizations without seriously impacting the resources needed for deployment and management at scale.

## FortiSOAR Is a Standalone SOAR Offering

- Collects data from multiple sources for organizations, helps them understand the information, and optimizes security processes, while providing an automated response

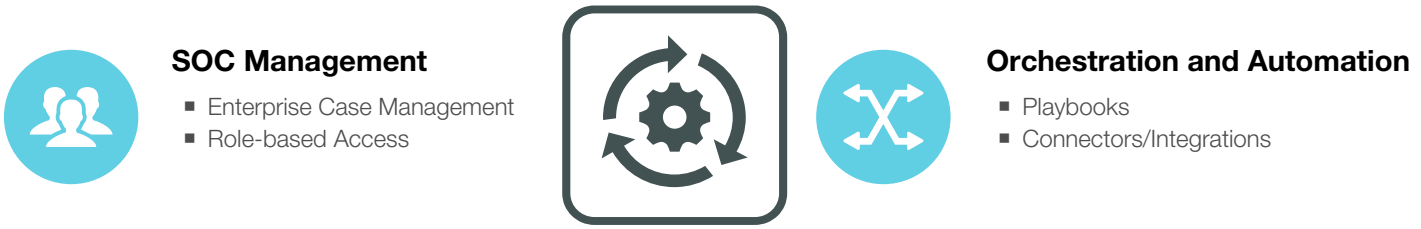


Figure 4: FortiSOAR brings together a crucial offering with the key capabilities necessary for an enterprise security architecture.

[1] "53% of enterprises have no idea if their security tools are working," Help Net Security, July 31, 2019.

[2] "2019 Cost of a Data Breach Report," Ponemon Institute and IBM Security, 2019.

[3] "Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)² Cybersecurity Workforce Study, 2019," (ISC)², 2019.

[4] Muhammad Omar Khan, "Why SOAR is a Good Bet For Fighting Mega Cyber Security Breaches," Entrepreneur, May 23, 2019.

[5] Cian Walker, "SOAR: The Second Arm of Security Operations," Security Intelligence, April 9, 2019.

[6] "2019 Cost of a Data Breach Report," Ponemon Institute and IBM Security, 2019.

[7] "Security Orchestration Automation & Response (SOAR) World Markets, Outlook to 2024: The High Number of False Security Alerts Presents Lucrative Market Opportunities," Research and Markets, November 15, 2019.

[8] Internal Fortinet calculations.

[9] Ibid.

FORTINET

www.fortinet.com



May 12, 2020 3:49 AM

587297-0-0-EN

D:\Fortinet\Solution Briefs\teal solution briefs\FortiSOAR\sb-FA-fortisoar-empowers-security-operations-to-accelerate-incident-response-NEW-552020