ThreatCure ShieldOpsAI® Platform

Powering Next-Gen Security Operations

Product Datasheet

The ShieldOpsAI is a ML/AI based Security Data Platform provides Comprehensive Threat Hunting capabilities for Security Analyst.

Salient Features

Intelligent Threat Detection & Response

- AI-powered threat detection and response.
- Maps attack patterns for better mitigation.

Proactive Threat Detection & Access Control

- Identifies hidden threats early.
- Zero Trust model ensures secure access.

Adaptive Security Architecture

- Supports on-premises, hybrid, and cloud environments.
- Integrates with SIEM, EDR, and SOAR tools.

ShieldOpsAI®

ThreatCure ShieldOpsAI advance hunting Platform assisting businesses in increasing the visibility of various digital assets, and cloud workloads and aggregating them into a single platform to provide security leadership with a 360-degree view and assist in risk identification. Further assisting the incident response team in defending the fundamental infrastructure and addressing zero-day attacks.

Product Brief

The ShieldOpsAI advance hunting Platform is designed to enhance Next GEN SOC operations with advanced threat detection, automated incident response, and comprehensive analytics. By leveraging industry-leading security posture management, ShieldOps provides organizations with the tools needed to establish a sustainable and future-ready SOC. It seamlessly integrates with existing systems to deliver a holistic view of the threat landscape, empowering organizations to act with precision and confidence.

It reduces manual and time-consuming investigations through automated capability-based interconnectivity, enabling a federated backbone architecture that scales uniformly to on-premises, hybrid and cloud environments. With complete visibility and full control of data flow, ShieldOpsAI white box data ensures transparent security content for effective detection.

THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure ShieldOpsAI® Platform

Powering Next-Gen Security Operations

ShieldOpsAI® Platform

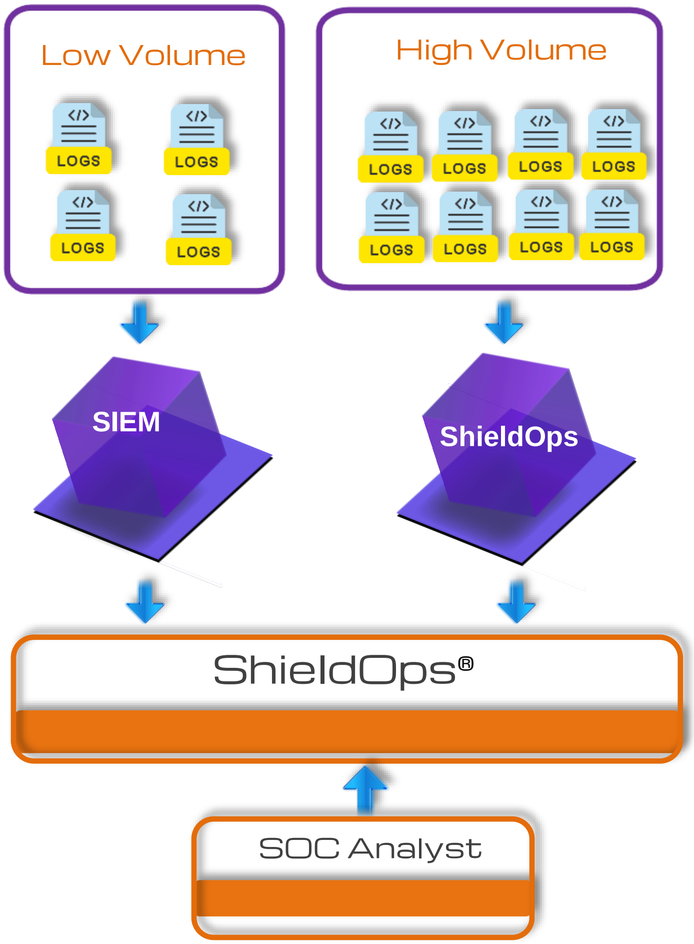
ShieldOps Next-gen Security Platform with Comprehensive Threat Visibility and Proactive Threat hunting.

A Federated Backbone for Security Operations

90 %
Cost Savings
Compared to SIEM

5 X
Fast Time to Value
By Fast Customer
Onboarding

10 X
Productivity
Through Automation



Decoupling: Make data acquisition and parsing part of the backbone, enable all tools unfederated access to the data.

Process Overview:

Low Volume Data: Logs with lower data volume are routed to the SIEM, where they undergo detailed analysis.

High Volume Data: ShieldOpsAI efficiently processes high-volume logs and integrates them into the ShieldOps SOAR platform for advanced analysis SOC Insights.

SOC Analyst: All insights and incidents are presented in an intuitive format through ShieldOpsAI, empowering SOC analysts to manage threats efficiently.

ThreatCure ShieldOpsAI® Platform

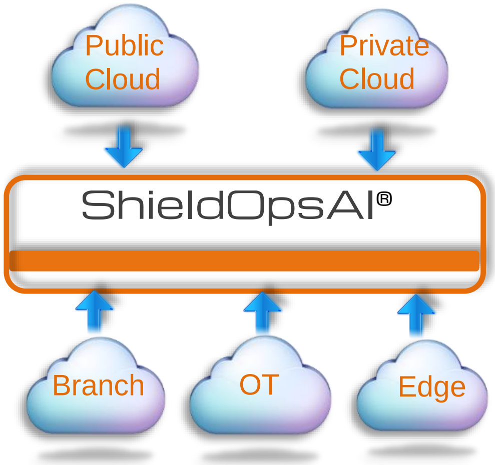
Powering Next-Gen Security Operations

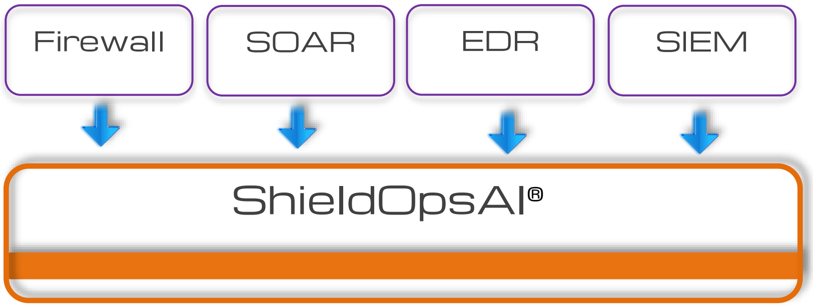
ShieldOps® Platform

ShieldOpsAI Next-gen Security Platform with Comprehensive Threat Visibility and Proactive Threat hunting.

ShieldOps Platform Key Features

- AI-Driven Threat Detection
- Comprehensive Threat Hunting
- Centralized Monitoring
- Seamless Integration
- Zero Trust Security Model
- Incident Response Optimization
- Scalability and Flexibility
- Advanced Security Analytics
- Cost-Effective Operations
- Cloud-Ready Architecture





Unified & Centralized Security Operations

- Single-pane-of-glass visibility for SOC analysts.
- Unified threat data for faster decision-making.
- Streamlined incident response with centralized management.

Comprehensive Cloud & Edge Security

- Seamlessly integrates with ShieldOpsAI Threat Hunting Engine to collect data from Public and Private Clouds, Branch Offices, OT, and Edge Devices.
- Ensures a consistent security posture across hybrid environments.

Seamless Integration with Security Tools

- Seamlessly integrates with Firewalls, SOAR, EDR, SIEM, TIP and more for enhanced efficiency.

AI-Driven Automation & Threat Mitigation

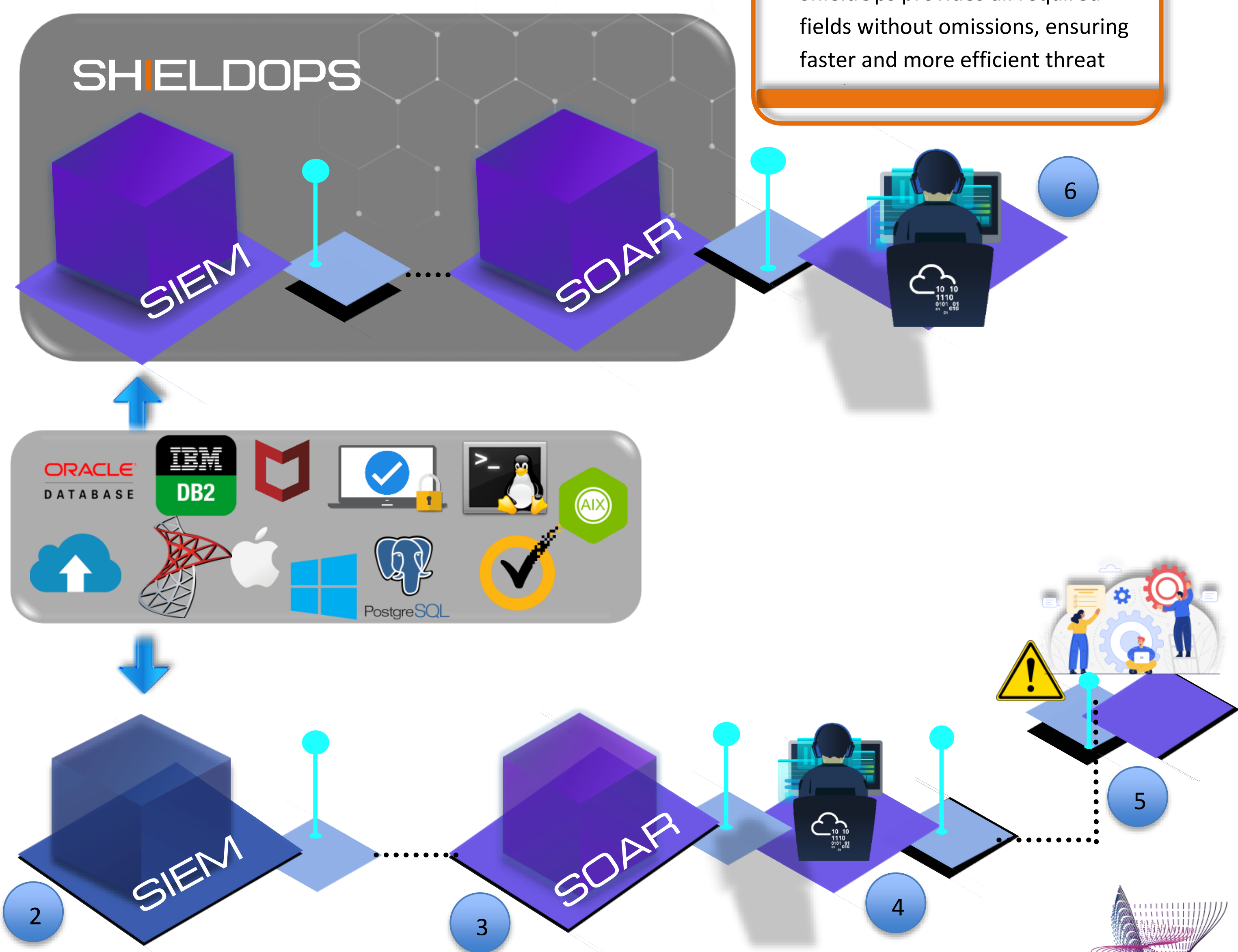
- Automates security workflows and policy enforcement.
- Accelerates incident containment with intelligent automation.

THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure ShieldOpsAI® Platform

Powering Next-Gen Security Operations

ThreatCure Shield OpsAI



ShieldOps provides all required fields without omissions, ensuring faster and more efficient threat

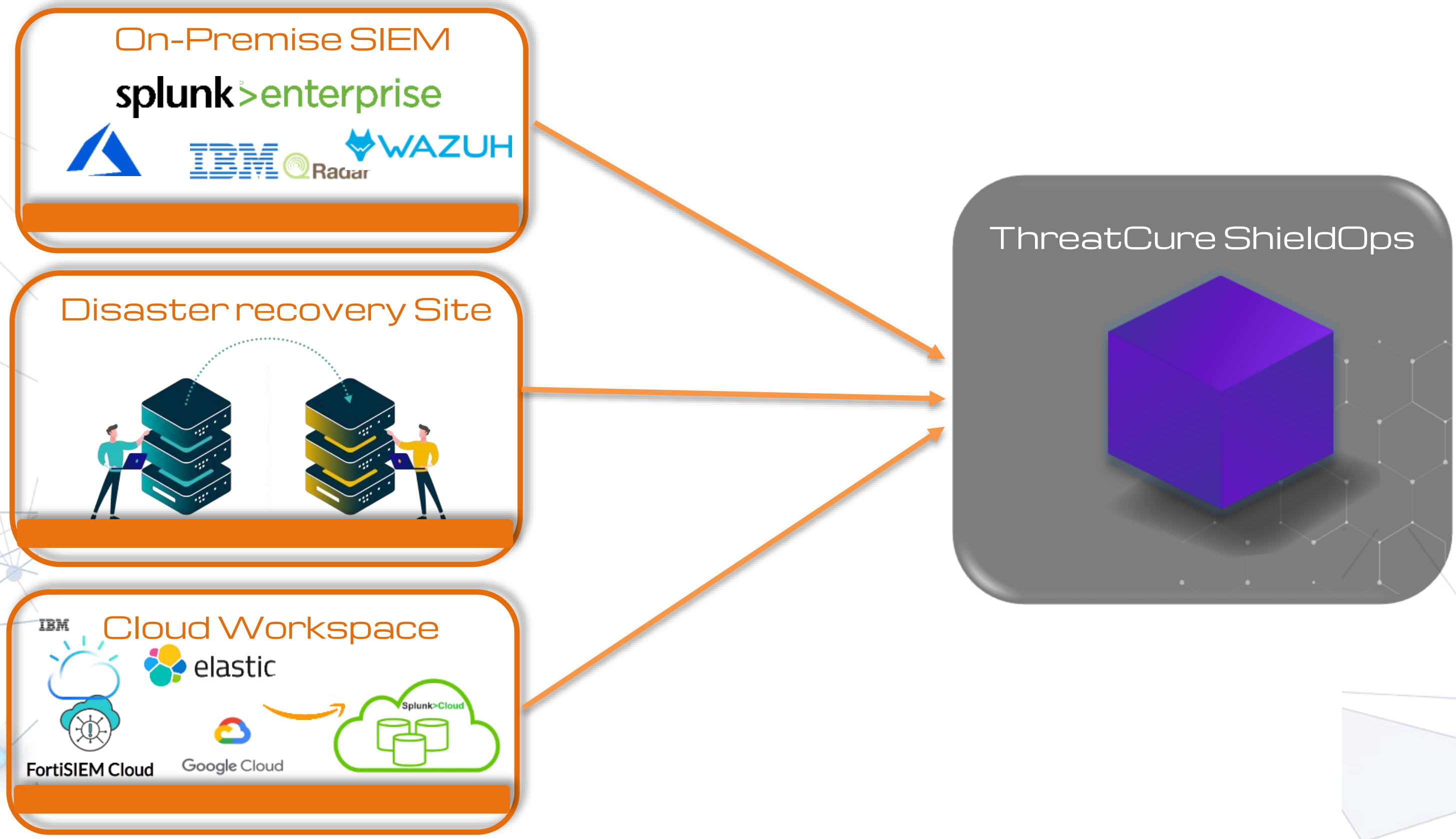
ShieldOpsAI Unified Monitoring

1. Log Sources Integration
   - Logs are collected and sent to SIEM for analysis.
2. SIEM Detects Offenses
   - SIEM generates offenses and forwards them to the SOAR platform.
3. SOAR Processes Offenses
   - SOAR allows analysts to review and conduct deeper investigations into offenses.
4. Analyst Reviews Offenses
   - Analysts identify missing fields in logs and escalate unresolved issues to the engineering team.
5. Traditional Delays
   - The engineering team takes up to a week to analyze and resolve issues.
6. ShieldOps Advantage
   - ShieldOps ensures all fields are complete, enabling faster and more efficient threat resolution.

THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure ShieldOpsAI® Platform

Powering Next-Gen Security Operations



ThreatCure Shield OpsAI

Centralized Monitoring

ShieldOpsAI provides a single window to monitor and manage security events across various environments, ensuring seamless integration.

Key Advantage

ShieldOpsAI eliminates the need for siloed monitoring systems by consolidating all critical data into a unified, user-friendly platform, empowering security teams to respond efficiently and effectively.

Integration with On-Premise SIEM

Seamlessly integrates with leading SIEM solutions to enable centralized log management and comprehensive threat analysis.

Disaster Recovery Visibility

ShieldOpsAI provides a single-pane-of-glass view for monitoring disaster recovery sites, ensuring resilience and uninterrupted operations.

ThreatCure ShieldOpsAI® Platform

Powering Next-Gen Security Operations

Challenges in Modern SOC Operations

Vendor Lock-In Restricts Flexibility

- Limits flexibility and restricts adoption of best-in-class security solutions

High Monitoring Costs

- Expenses rise quickly with increased data volumes.

Scalability Issues

- Lack of unified architecture hinders scalability and slows threat response.

Integration and Efficiency Constraints

- Requires extensive administrative effort for integrations, reducing SOC efficiency.

Distinct Features

- **Sustainable SOC Growth**:
  - Build a resilient and scalable SOC leveraging best-of-breed security platforms that adapt to evolving threats and business needs.
- **Enhanced Security Posture:**
  - Proactive threat detection reduces risk exposure and ensures rapid threat identification.
- **Reduced Response Time:**
  - Automated workflows lead to faster incident handling, reducing Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).
- **Cost Efficiency:**
  - Optimizes security operations with automation, reducing the need for extensive in-house security teams.
- **Improved Decision-Making:**
  - Data-driven insights support informed decision-making and strategic planning.
- **Architecture:**
  - Cloud-native, microservices-based with containerized deployments to optimize scalability and flexibility.
- **Automation Framework:**
  - Playbook-based with support for custom scripts.
- **Analytics Engine:**
  - AI/ML algorithms for advanced threat recognition.

ThreatCure ShieldOpsAI® Platform

Powering Next-Gen Security Operations

ShieldOpsAI® Platform Benefits

Automated capability-based interconnectivity: ShieldOps Platform intelligently links various security tools and capabilities to create a cohesive defense system. This automated integration allows different components to work together seamlessly, improving response times and reducing manual effort.

Federated architecture that scales uniformly to on-premises and cloud: With its federated architecture, ShieldOps can easily adapt to both on-premises and cloud environments. This uniform scalability ensures that your security framework remains consistent and effective, regardless of where your systems and data are located.

Complete visibility and full control of data flow: The platform provides comprehensive monitoring of data movement across your network. This visibility enables you to detect, track, and manage data flows, ensuring that sensitive information is secure and potential threats are identified quickly.

Transparent security content for effective threat detection: ShieldOps offers clear and accessible security mechanisms that enhance threat detection. The transparency of these security protocols helps your team understand how threats are identified and addressed, leading to more accurate and reliable protection.

Get Started Today

For more information about the ThreatCure ShieldOps® Platform and to schedule a demo, please contact:

- Website: www.threatcure.net
- Email: info@threatcure.net
- Phone: +123-456-7890