SafeNova

SafeNova SIEM

Next Generation Security Intelligence Platform

Oneplatform.Completevisibility.Total control.

The Security Challenge

Organizations face a paradox: more security tools, yet less visibility and escalating costs.

01 Tool sprawl

Disconnected solutions create dangerous blind spots and operational complexity

02 Budget Uncertainty

Traditional SIEMs charge by data volume, leading to unpredictable costs and difficult forecasting.

03 Resource Drain

Complex system demand rare, expensive expertise that’s hard to find

04 Compliance Overhead

Manual audit processes waste time and increase risk exposure

SafeNova solves these challenges with unified intelligence

Introducing SafeNova

A Smarter Approach to Enterprise Security

Unified Platform

Simplified management across all security functions.

Agent-Centric Architecture

Predictable, transparent per-asset pricing

Built for Efficiency

Intuitive, low-code configuration reduces deployment time from months to days and lowers training requirements.

Open & Flexible

Standards-based architecture with open APIs prevents vendor lock-in and protects your investment.

The SafeNova Advantage

Intuitive, Low-Code Interface

Empower your team with easy configuration—no specialized expertise required

Unified Agent Architecture

Single agent deployment eliminates complexity and reduces attack surface

Flexible Deployment

Run anywhere your infrastructure lives—no forced cloud migration

Predictable Per-Agent Pricing

No surprises. Budget with confidence using straightforward per-endpoint licensing instead of data volume charges.

Lower Total Cost of Ownership

Reduce infrastructure, licensing, and operational costs by up to 60%

Advanced Threat Detection

AI Behavioral Analytics

Machine learning detects anomalies and unknown threats through intelligent baselining

Real-Time Threat Intel

Integrates VirusTotal, AbuseIPDB for malicious IP, URL, and hash identification with geo-location

Comprehensive Detection

Identifies phishing, DDoS, unauthorized access, malware, ransomware, and insider threats

Advanced Threat Detection

AI Behavioral Analytics

Machine learning detects anomalies and unknown threats through intelligent baselining

Account Compromise Detection

Unusual geolocation, failed logins, odd login times, new devices

Privilege Escalation

New admin rights, group membership changes, SYSTEM-level access

Data Exfiltration

Large outbound traffic, uploads to cloud/personal email, encrypted archives

Anomalous Login Behavior

Unusual time, location, multiple IPs, new device

Advanced Threat Detection

Real-Time Threat Intel

Integrates VirusTotal, AbuseIPDB for malicious IP, URL, and hash identification with geo-location

Malicious IP

Detect and track suspicious IP addresses.

Use threat intelligence feeds for IP reputation checks.

Malicious URL

Scan URLs for phishing, malware, or spam links

Compare URLs with known malicious domain databases.

File Hash Reputation

Calculate MD5/SHA1/SHA256 hashes for detected files.

Cross-check with global threat databases

Reputation Scoring

Map attacker IPs to countries, regions, and ISPs.

Visualize attack origin on a world map for SOC visibility.

Advanced Threat Detection

Comprehensive Detection

Identifies phishing, DDoS, unauthorized access, malware, ransomware, and insider threats

Phishing Attempts

AI-powered email and credential analysis.

DDoS Attacks

Real-time traffic anomaly detection

Unauthorized Access

Behavioral analytics and pattern recognition

Malware & Ransomware

Signature and heuristic-based prevention

Proactive Risk Management

Vulnerability Management

Automated scanning

Continuously discovers software vulnerabilities

Risk prioritization

CVSS scores and asset criticality

Remediation guidance

Actionable steps to patch systems

Configuration Integrity

Continuous auditing

Checks against CIS benchmarks

File Integrity Monitoring

Alerts on unauthorized changes

Auto-remediation

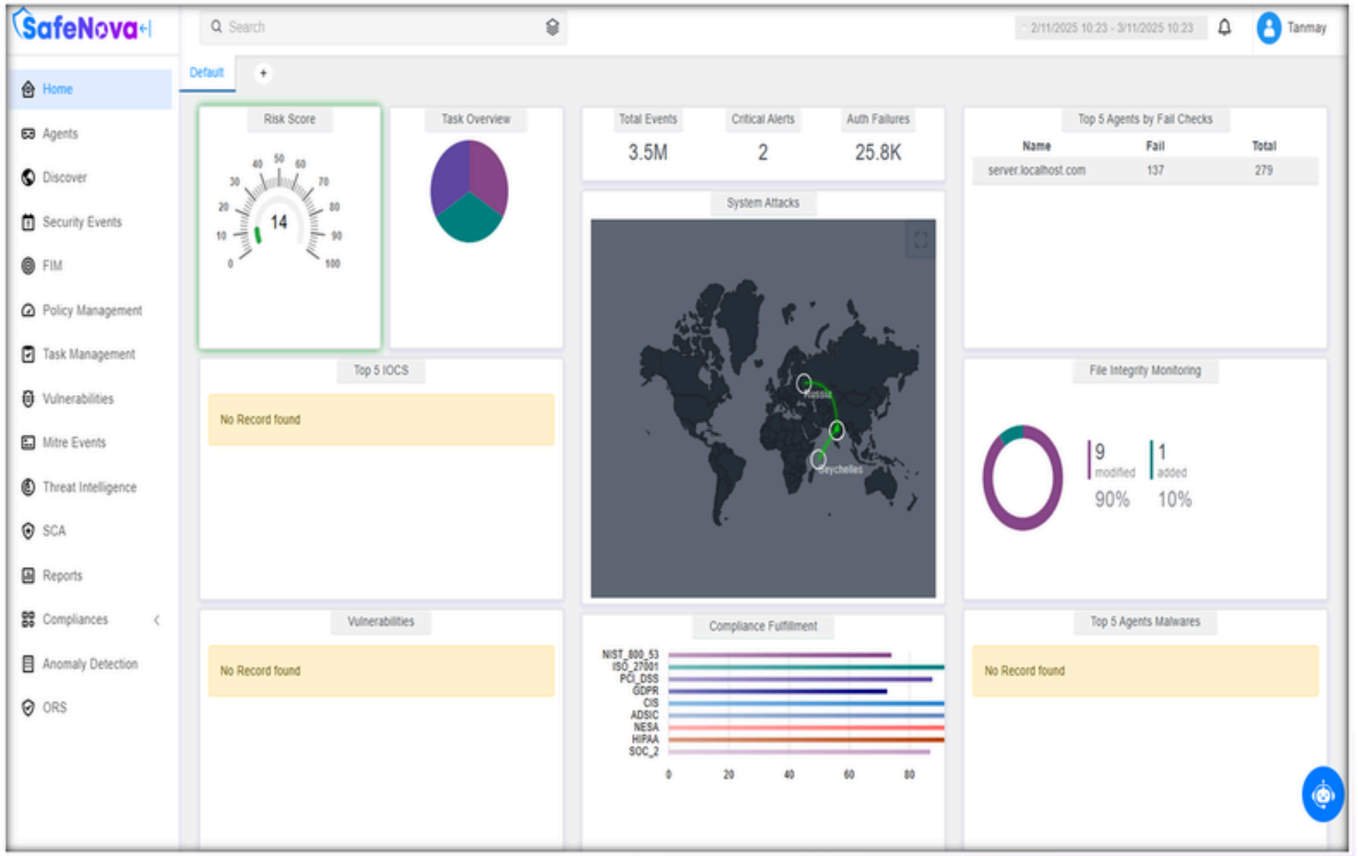
Guided fixes for misconfigurations

Unified Monitoring & Visualization

Transform security data into actionable intelligence with powerful visualization and correlation capabilities.

Custom Dashboards

Live visualization, custom views, role-based access

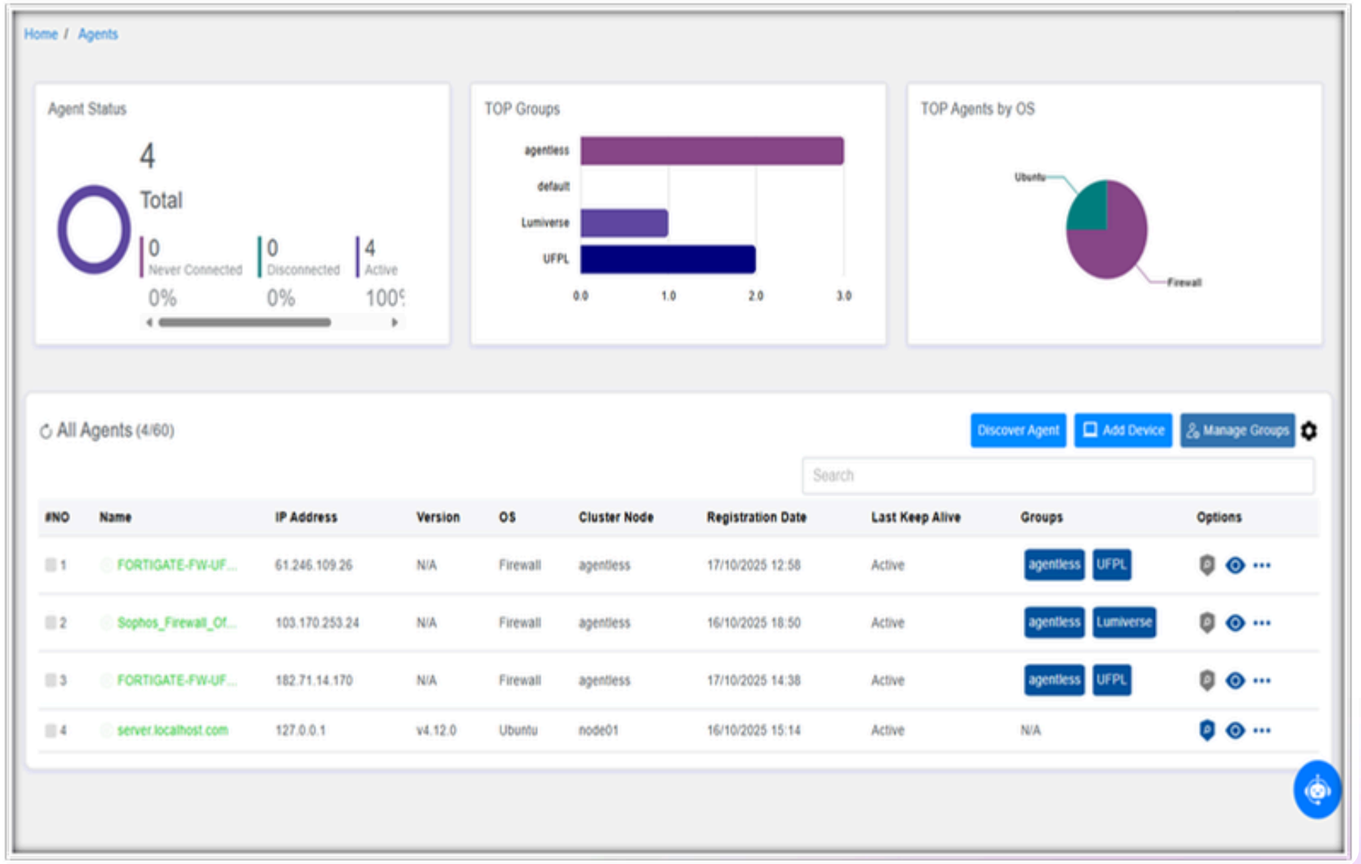


Unified Monitoring & Visualization

Transform security data into actionable intelligence with powerful visualization and correlation capabilities.

Live Asset Inventory

Integrates VirusTotal, Automatically discover and map all connected devices

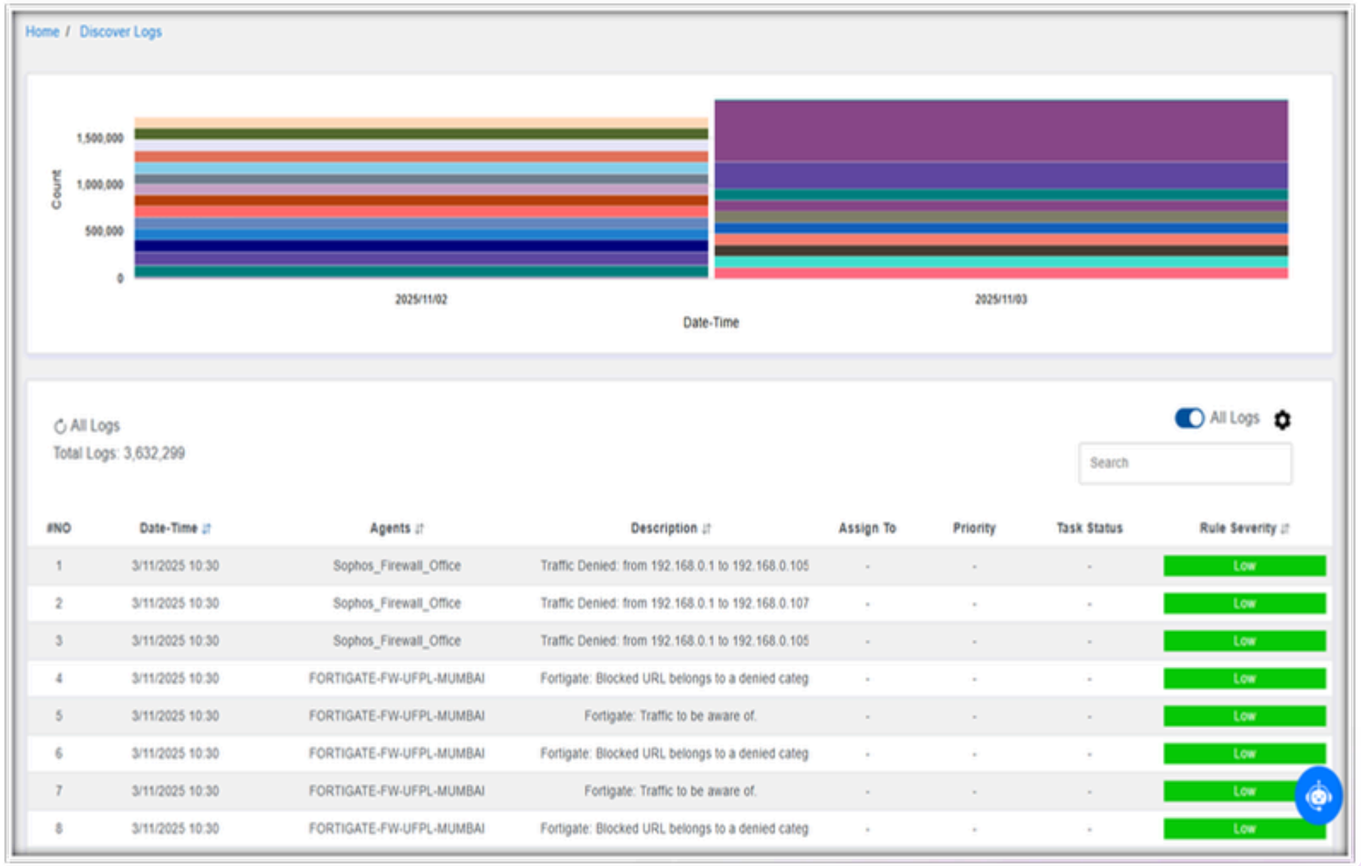


Unified Monitoring & Visualization

Transform security data into actionable intelligence with powerful visualization and correlation capabilities.

Real-Time Correlation

Connect the dots across millions of events to identify true threats instantly



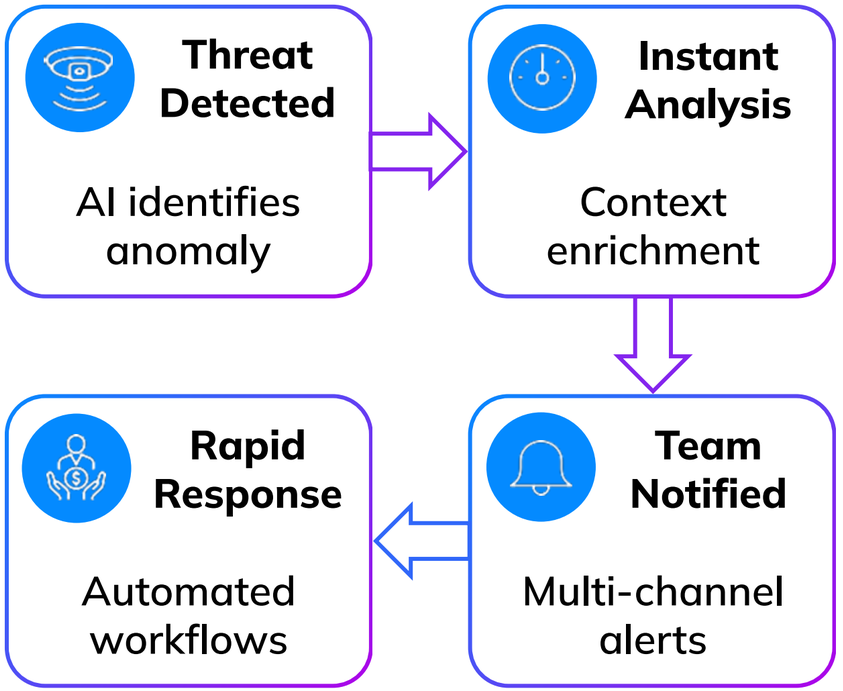
Unified Monitoring & Visualization

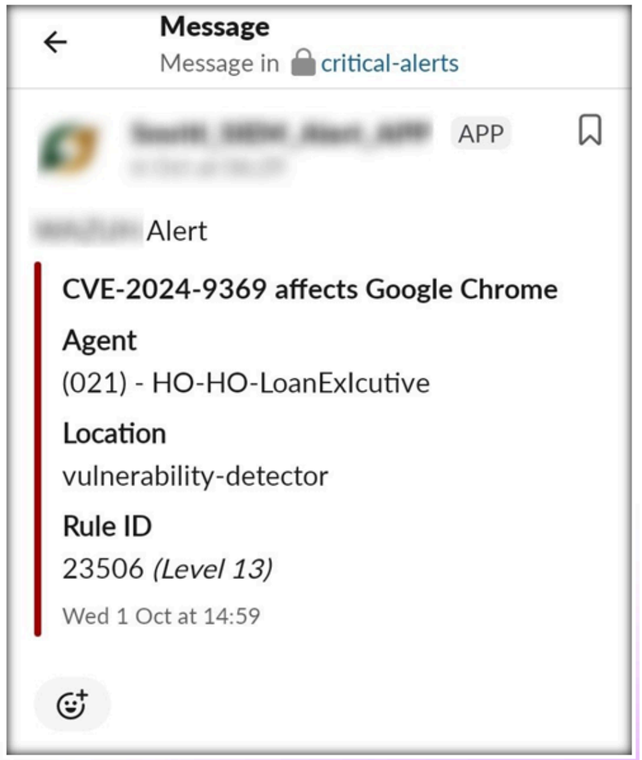
Transform security data into actionable intelligence with powerful visualization and correlation capabilities.

Mobile Alerts

Slack, Telegram, Email, SMS respond anywhere

Real-TimeAlertingThatWorks





Automated Compliance & Reporting

Simplify audits and maintain continuous compliance with automated evidence collection and comprehensive reporting.

04

Automated Evidence Collection

Continuous gathering and timestamping of compliance evidence reduces manual work by up to 80%.

03

Flexible Reporting

Generate compliance reports instantly or schedule them automatically

02

Multi-Framework Support

Pre-configured compliance modules for PCI DSS, NIST 800-53, GDPR, HIPAA, ISO 27001, SOC 2, NESA, CIS, ADSIC

01

Pre-Built Templates

Leverage hundreds of out-of-the-box rules and report templates that map directly to compliance requirements.

Reduce audit preparation time by up to 70% and streamline regulatory readiness

Integration Ecosystem

Threat Intelligence

- VirusTotal
- AbuseIPDB
- Osquery
- Docker Listener

Cloud Platforms

- Amazon AWS
- Office 365
- Google Cloud Platform
- GitHub

Smart Alerting

- Slack
- Telegram
- Email
- SMS notifications

Architecture Overview

SafeNova SIEM Workflow Overview

1. Log Sources (Endpoint Devices)
Operating System Devices: Windows, macOS, Linux (computers, laptops, servers, VMs)
Network Devices: Firewalls, routers, switches (Syslog – Port 514)
Applications: SAP, ERP, Antivirus, other software (API Integration)

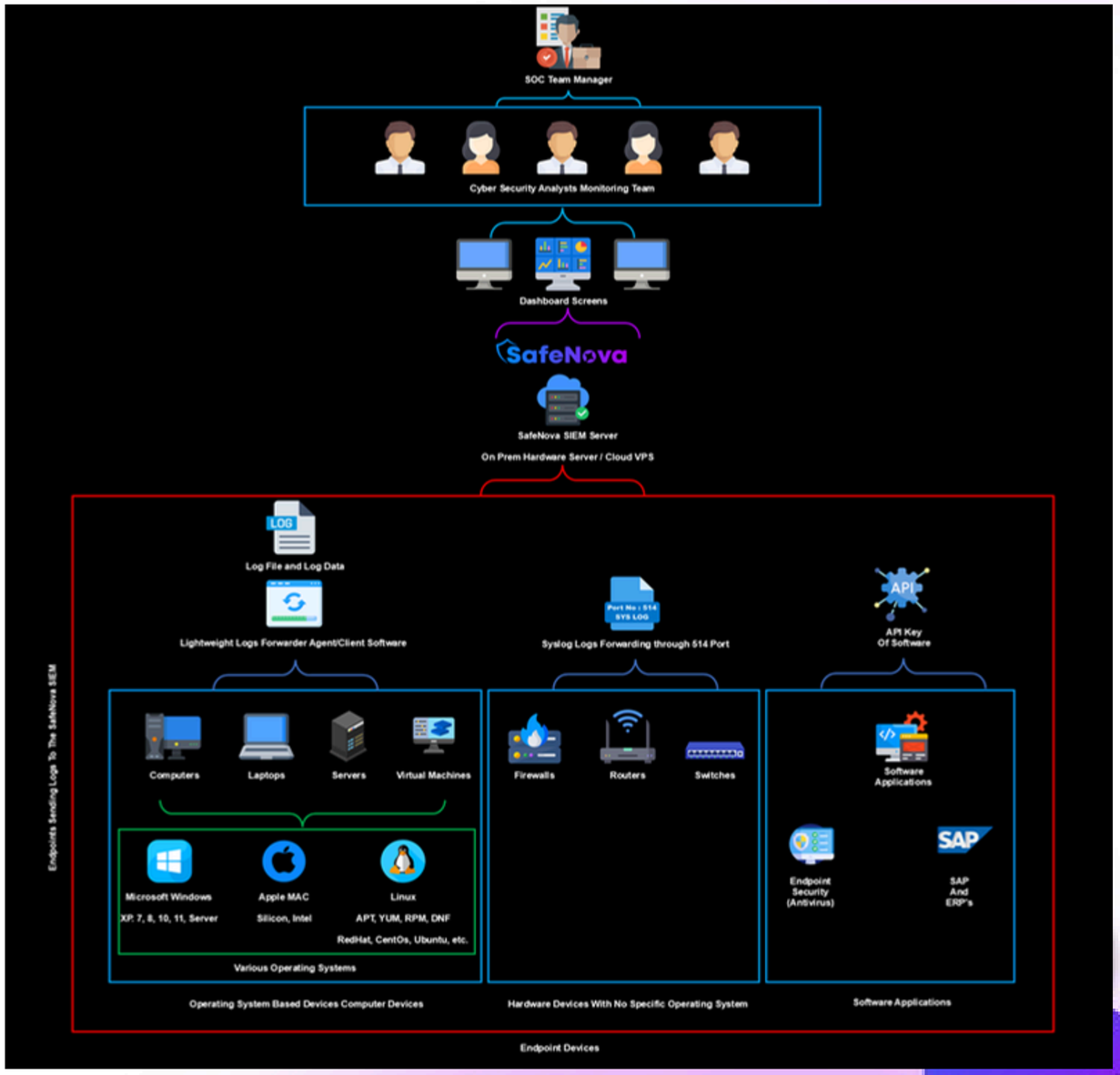
2. Log Collection Layer
Agent/Client Software: Forwards OS-based logs
Syslog Forwarding: For network hardware logs
API Key Integration: For application logs

3. SafeNova SIEM Server
Hosted on On-Prem / Cloud VPS Functions:
Log parsing and normalization
Event correlation and detection
Alert generation and reporting

4. Monitoring & Visualization
Dashboard Screens for real-time alerts, trends, and incidents

5. SOC Operations
Cyber Security Analysts: Continuous monitoring and investigation
SOC Manager: Oversees operations, escalation, and compliance

End-to-End Flow:
Devices & Apps → Log Forwarding → SafeNova SIEM → Dashboards → SOC Analysts → SOC Manager



Deploy With Confidence

01

Day 1-2: SIEM Server Installation & Deployment
- Install SIEM (on-prem or cloud)
- Configure core components and connectivity

02

Day 3-5 : Integration & Threat Feeds
- Connect firewalls, servers, and tools
- Integrate external threat intelligence

03

Day 6-8 : Custom Rules & Compliance Setup
- Create correlation and alert rules
- Apply compliance dashboards (ISO, PCI-DSS)

04

Day 9-10 : Dashboard & Reporting
- Build monitoring dashboards
- Configure automated reports

05

Day 11+ : Production Monitoring & Optimization
- Start live monitoring and response
- Continuous tuning and team training

SafeNova

Your Trusted Security Partner

Stay Secure. Stay Ahead.

Technical Deep-Dive

60-minute live demo tailored to your environment

Proof of Concept

30-day fully-supported trial with your own data

Custom Proposal

Detailed licensing, services, and ROI analysis

SafeNova empowers organizations with smarter, faster, more reliable threat detection.