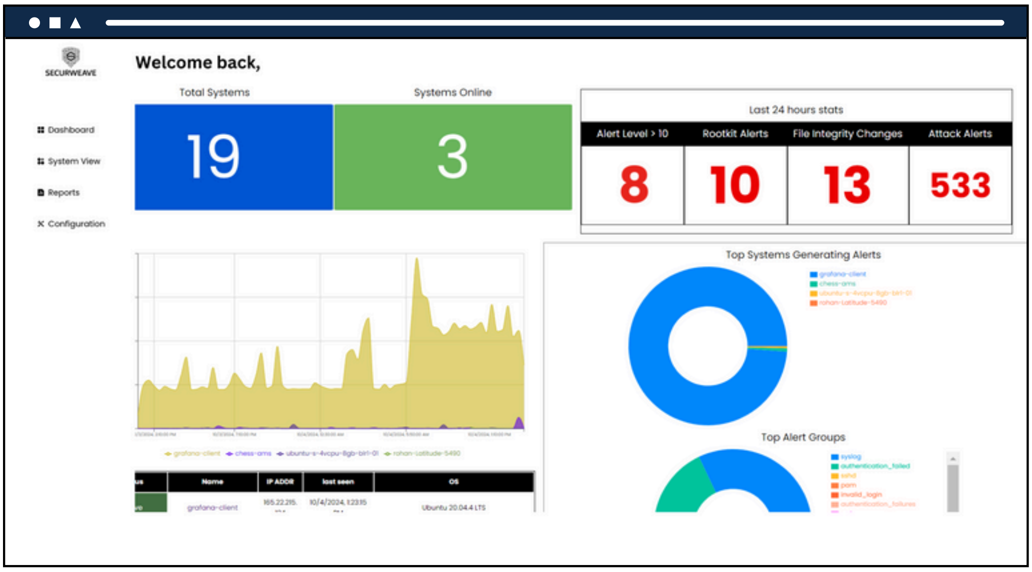
SECURWEAVE

Weaving the fabric of next generation security

SIEM Data Sheet



SECURWEAVE

Welcome back,

- Dashboard
- System View
- Reports
- Configuration

Total Systems: 19

Systems Online: 3

Last 24 hours stats

Alert Level > 10	Rootkit Alerts	File Integrity Changes	Attack Alerts
8	10	13	533

Top Systems Generating Alerts

Top Alert Groups

Name	IP ADDR	last seen	OS
grafana-client	165.22.215.	10/4/2024, 1:23:15	Ubuntu 20.04.4 LTS

Next-Gen SIEM: Advanced Threat Detection and Compliance Solution

Advanced Threat Detection and Incident Response: Protect your systems from ransomware, brute-force attacks, insider threats and more with real-time threat monitoring and rapid incident response.

Cloud-Based Delivery: Simplified SaaS deployment, reducing the complexity and cost of on-premise installations.

OSSEC-Based Technology: Powered by the robust open-source OSSEC, enhanced with proprietary SecurWeave features to ensure enterprise-grade security.

Comprehensive Compliance Monitoring: Ensure your infrastructure meets industry security standards with continuous compliance monitoring and reporting.

Seamless Integration: Easily integrates with SecurWeave’s CHESS, OT, IoT and other security solutions, providing enhanced protection and unified security management.

Today's Challenges

- **Ransomware Attacks:** Every 11 seconds, a ransomware attack occurs, with an average payout of $220,298 (2021 data).
- **Brute-force Attacks:** 30 billion brute-force attempts were recorded globally in 2020.
- **Vulnerability Exploits:** Command and control (C&C) communications continue to be exploited to take over compromised systems.
- **Increasing Complexity:** Leveraging advanced techniques such as polymorphic malware, zero-day exploits and multi-stage attacks.

SIEM

Security Information and Event Management

Why Choose a Cloud-Based SIEM Solution?

1. Real-Time Threat Detection

SecurWeave-SIEM monitors system and network activities in real-time to detect and prevent advanced threats like malware, ransomware, and unauthorized network access. It provides visibility into critical files, sensitive data access, and suspicious activities.

2. Compliance and Reporting

Stay compliant with industry standards and regulations like PCI DSS, HIPAA, GDPR, IEC 62443 and SOX. SecurWeave-SIEM continuously monitors and reports on system and network activities to help meet security requirements.

3. Incident Response & Forensics

In the event of a breach, SecurWeave-SIEM offers forensic data to track the attack source, identify compromised assets and enable swift incident response to mitigate damage.

4. Insider Threat Protection

SecurWeave-SIEM analyzes user behavior and system activities to detect and prevent malicious or suspicious actions by insiders with privileged access.

Key Features of SIEM:

- **File Integrity Monitoring (FIM):** Continuously monitors and verifies changes to critical system files, alerting to unauthorized modifications. This feature is key to meeting PCI DSS requirements and maintaining a robust security posture.
- **Log Monitoring & Analysis:** Aggregates and analyzes logs from various devices and applications, identifying misuse, errors and potential threats by correlating data.
- **Rootkit Detection:** Detects hidden malicious code or rootkits that could compromise system integrity, with alerts for suspicious system changes.
- **Active Response:** Automates real-time responses when specified threats are detected, minimizing risk escalation.
- **Seamless Integration**: Unify security across your network, identity management systems, devices and cloud applications for comprehensive oversight.

SECURWEAVE

securweave.com
info@securweave.com
+91-8790532463

Plot No 13/A, Laxmi Nagar Colony, Manikonda,
Rangareddy Telangana,
India 500089