COMPLIANCE & SECURITY MANAGEMENT

Socfortress provides necessary security controls, required by standards such as PCI DSS, HIPAA, GDPR and others. The solution aggregates and analyzes data from multiple systems, mapping security alerts with compliance requirements.

COMPREHENSIVE SIEM SOLUTION

The SOCFortress platform collects, analyzes and correlates data, with the ability to deliver threat detection, compliance management and incident response capabilities.

ENDPOINT DETECTION AND RESPONSE

Socfortress is focused on providing the right visibility, with the insights to help security analysts discover, investigate and respond to threats and attack campaigns across multiple endpoints.

ANTIVIRUS

Ensure your endpoints are protected from malware and ransomware with our proactive AntiVirus solution that blocks malicious files before they are executed on the endpoint.

RICH DASHBOARDS

Quickly drilldown into individual host's processes or view activity on all of your endpoints with our detailed dashboards.

THREAT INTEL

SOCFortress analyzes all relevant metadata in security events, extracts observables and executes threat intel to pinpoint indicators of compromise in real time. Domains, file hashes, IPs, etc. are cross referenced to our threat intelligence platform comprised of nearly 1 million indicators.

CASE MANAGEMENT

Socfortress provides the ability for your analysts to quickly and efficiently collaborate amongst each other when dealing with security alerts with our case management platform.

CUSTOM EVENT ESCALATION

Want to receive your high severity alerts via Slack, PagerDuty, Teams, Email, etc? No problem, SOCFortress works with your IT team to establish a notification system that works best for everyone. Allowing for

even faster response times.

INTEGRATIONS

Integrate with AWS, O365, Google Cloud, and more. SOCfortress enables users to bring other service logs into their platform allowing for quick triage and visuals amongst various log sources.

SOC AS A SERVICE

Let SOCFortress analysts be your dedicated security team. Our certified SOC analysts work around the clock to ensure networks and endpoints are secure. Let SOCFortress handle your security while you focus on growing your business.