ALERT LOGIC™

SERVICE OVERVIEW

Alert Logic for SOC 2 Compliance

Proect customer data in the cloud and comply with AICPA SOC 2 requirements

SaaS companies and service providers who use the SOC 2 requirements to secure their customer data benefit from an improved overall security posture, better performance and availability of service delivery and a valuable risk assessment tool for prospective business partners. However implementing SOC 2 requirements can be confusing, complex and expensive for many companies, especially those with limited staff and security expertise.

Using Alert Logic solutions, companies can implement a broad range of regulatory and industry security standards (such as SOC 2, PCI DSS, HIPAA, SOX, and GDPR) with less complexity, and at a fraction of the total cost and time of traditional security tools.

Alert Logic integrates cloud-based software, analytics and expert services to **assess**, **detect** and **block** threats to applications and cloud environments to improve your security visibility and compliance programs. We focus on the threats most relevant to cloud-hosted applications by defending each layer of your application and infrastructure stack against hard-to-detect web application attacks. Integrated expert services augment your in-house security team by monitoring your cloud workloads and environment 24/7. Analysts investigate alerts and contact you within 15 minutes if we detect suspicious activity such as: unauthorized access, exposure or modification of accounts, controls or configurations.

- **Reduce your risk** of attacks with continuous vulnerability scanning and configuration inspection of your applications and cloud environments.
- **Quickly respond to attacks** and post-breach activities with distributed IDS sensors that provide full-packet inspection and real-time alerts.
- **Protect customer data** from network and OWASP Top 10 attacks with web application scanning and web application firewall technologies.
- **Prepare for audits, anytime** with the event and log data you need for automated alerts, audit trails and easy access for reporting and audits, stored in our secure SSAE 16 Type 2 audited data centers for as long as you need
- **Free up resources** with ActiveWatch™ experts for daily log reviews and 24/7 event and threat monitoring.

Alert Logic maintains strict compliance with internal and external regulatory requirements for our IT operations and services, including: PCI DSS 3.2 Level 2 Audit, AICPA SOC 1 & 2 Audit, and ISO 27001-2013 certification for UK Operations.

PCI DSS COMPLIANT

AICPA SOC

Egalfire ISO ISO27001 CERTIFIED

Alert Logic AICPA SOC 2 solutions mapping

The integrated services that make up Alert Logic® address a broad range of SOC 2 Trust Services Criteria (TSC) principles to help you prevent incidents that threaten the security, availability, integrity and privacy of customer data.

ALERT LOGIC	AICPA SOC 2 TSC PRINCIPLES
Alert Logic MDR Essentials Vulnerability & Asset Visibility Gain visibility into your environments, and easily identify the remediation steps required to eliminate exposures in cloud and hybrid environments. Quickly understand the state of compliance without hiring new staff. Obtain audit-preparedness reporting that helps IT staff stay one step ahead of requirements, mandates, and auditors. - Asset discovery - Vulnerability scanning - Cloud configuration checks - Endpoint detection - Threat Risk Index - Compliance scanning and reporting	CC 3.2 - Risk Identification CC 6.6 - External Threats CC 6.8 - Unauthorized and Malicious Code Protection CC 7.1 - Configuration and Vulnerability Management
Alert Logic MDR Professional 24/7 Managed Threat Detection and Incident Management Get an intrusion detection system that includes security monitoring and threat analysis from certified security and compliance experts. Reduce network threats without hiring additional security experts. Get help to remediate vulnerabilities and quickly respond to incidents. And leverage compliance-specific reporting to make it easier to evaluate and document your compliance stance. - 24/7 Incident Monitoring & Management - Security Analytics & Threat Intelligence - Log Collection and Monitoring - Intrusion Detection - Security Event Insights and Analysis - Office 365 Log Collection & Search - Cloud Vendor Security Integrations - AWS User Behavior Anomaly Detection - Anti-Virus Integration - File Integrity Monitoring ... plus capabilities in Alert Logic Essentials	CC 3.2 - Risk Identification CC 6.6 - External Threats CC 6.8 - Unauthorized and Malicious Code Protection CC 7.1 - Configuration and Vulnerability Management CC 6.2 - User Registration CC 6.3 - Access Modification and Removal CC 7.2 - Security Event and Anomaly Detection CC 7.3 - Incident Detection and Response
Alert Logic MDR Enterprise Designated Security Expert Receive in-depth individualized evaluation, protection, and customized response services, leveraging the Alert Logic Professional service. - Continuous Threat Hunting - Pro-Active Tuning and Sensor Optimization - Weekly Security Review ... plus capabilities in Alert Logic Essentials & Alert Logic Professional	CC 3.2 - Risk Identification CC 6.6 - External Threats CC 6.8 - Unauthorized and Malicious Code Protection CC 7.1 - Configuration and Vulnerability Management CC 6.2 - User Registration CC 6.3 - Access Modification and Removal CC 7.2 - Security Event and Anomaly Detection CC 7.3 - Incident Detection and Response CC 7.4 - Incident Containment and Remediation