ALERT LOGIC®

SERVICE OVERVIEW:

ALERT LOGIC® FOR SOC-2 COMPLIANCE

PROTECT 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 Security-as-a-Service 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 24x365. Analyst 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 24x365 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 · Goalfire ISO 27001 CERTIFIED

ALERT LOGIC AICPA SOC 2 SOLUTIONS MAPPING

The integrated services that make up Alert Logic® Cloud Defender® 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 SERVICE	AICPA SOC 2 TSC PRINCIPLES
Threat Manager™ with ActiveWatch™ Get expert protection against web application and server threats with managed intrusion detection and unlimited internal and external vulnerability scanning with 24x365 monitoring & threat analysis. - Quarterly assessments of network security configurations - Intrusion Detection to detect threats against protected data - Threat and Vulnerability database of 97,000+ signatures and updated regularly	**CC 3.1** – Threat Identification **CC 3.3** – Environmental, Regulatory, and Technological Changes **CC 5.1** – Logical Access **CC 5.6** – Unauthorized External Access **CC 5.8** – Viruses and Malicious Code Protection **CC 6.1** – System Vulnerabilities **CC 6.2** – Incident Management **CC 7.3** – Change Management
Cloud Insight™ and Cloud Insight™ Essentials for AWS Get agentless, API-automated controls for automated and continuous AWS environment discovery, configuration assessment, security incident containment and remediation response support for threats identified by Amazon GuardDuty™, and software vulnerability scanning so you can: - Discover what assets you have, where they are and how they fit together - See where and how to fix potential configuration mistakes that leave you open to compromise - Understand why, where and how to react to Amazon GuardDuty findings - Reduce your attack surface with visibility into vulnerabilities hidden at all layers of your application stack	CC 3.1 – Threat Identification CC 3.3 – Environmental, Regulatory, and Technological Changes CC 5.1 – Logical Access CC 5.6 – Unauthorized External Access CC 6.1 – System Vulnerabilities CC 7.3 – Change Management
Web Security Manager™ Premier with ActiveWatch™ Detect and block web application attacks in real-time with an expert-managed Web Application Firewall (WAF) - Identify and stop OWASP Top 10 attacks that can enable data breaches - Inspect HTTP traffic on day 1 with out-of-the-box rules and signatures covering more than 10,000 vulnerabilities - Fully managed by Alert Logic web application security experts	CC 6.2 – Incident Management
Log Manager™ with ActiveWatch™ and Log Review Easily capture, process and analyze event and log data required to identify security issues across your entire environment. Log data with audit trails stored in secure SSAE 16 Type 2 audited data centers for as long as you need. - Deploys in minutes to capture and identify suspicious activity related to your operating systems, applications, networks and services - Count on security experts who review all your log events every day to identify any issue that might affect the security of your customer data - Access and search through all your log data stored securely in our SSAE 16 Type 2 data centers for incident response or quarterly audits with	**CC 5.2** – User Registration **CC 5.4** – Access Modification / Removal **CC 6.1** – System Vulnerabilities **CC 6.2** – Incident Management
ActiveWatch™ Alert Logic security experts are part of an integrated solution, providing continuous threat research, monitoring, and analysis to deliver valuable outcomes such as actionable incident reports and accurate blocking of malicious web requests. - 24x365 monitoring & threat analysis with 15-minute incident response - Expert tuning of WAF signatures and rules to block new threats - Quarterly vulnerability and configuration assessments for audits - Daily review of log events to identify suspicious changes and events - Threat research with regular updates to keep up with latest threats	**CC 3.1** – Threat Identification **CC 3.3** – Environmental, Regulatory, and Technological Changes **CC 5.6** – Unauthorized External Access **CC 6.1** – System Vulnerabilities **CC 6.2** – Incident Management **CC 7.3** – Change Management

ALERT LOGIC®