FORTRA™

SOLUTION BRIEF (ALERT LOGIC)

Achieving Security Compliance

Security compliance isn't easy nor is it optional. Each regulation related to data protection and privacy an organization must comply with has its own nuances that must be met, tracked, recorded, and ready to withstand an audit. And depending on your industry, it's not just one regulation, or two, but a myriad of regulations to ensure protection for organizations, individuals, and industry groups from breaches and data loss.

Managing security compliance internally can be both cost prohibitive from a technology and people perspective and a struggle for employees who don't have the skills, training, or expertise to make sure compliance is achieved.

Achieving better outcomes and continuous security compliance is within reach with Fortra's Alert Logic Managed Detection and Response (MDR). Without the need to add internal staff, your organization can achieve compliance quickly and with minimal disruption to your business. Our compliance solution is adaptable for your hybrid, cloud, and on-premises environment today and as they change, helping you stay a step ahead of requirements, mandates, and audits.

Why Choose Alert Logic for Security Compliance?

With an Alert Logic MDR solution, you can quickly advance your security compliance strategy without the lag time you would experience if you brought on new team members needing to be fully onboarded and launching technology to internally manage compliance. No longer will you be a step behind in the ever-evolving landscape of laws and standards or weighed down by policy mapping. With the industry's most comprehensive MDR coverage, our expert team works with you 24/7 to quickly ensure you're ready for any compliance audits with audit-ready reports that meet all requirements and mandates as well as satisfy auditors.

With Alert Logic MDR, you'll be assured protection from threats to security, availability, integrity, and customer data privacy, achieving comprehensive compliance with today's mandates and requirements and preparing you for future changes and new regulations.

> "Of the 66% of respondents to the 2022 survey who said they expected the cost of senior compliance staff to increase, nearly half (47%) cited the demand for skilled staff and knowledge as the top reason."
>
> *10 Global Compliance Concerns for 2023*

73% of organizations report compliance as a top cloud challenge.

Flexera 2023 State of the Cloud Report

Benefits of Alert Logic MDR for Your Security Compliance

- Full visibility into the current state of your adherence to compliance regulations and mandates without the burden of hiring new staff to undertake this review
- Expert, informed advice and remediation steps for your unique environment developed by our security compliance experts
- Meet requirements across multiple regulations with our application monitoring and log management
- Audit-ready reporting when you need it for auditors or to prove requirements and mandates are met
- Managed policy mapping that eliminates the risk of compliance gaps and potential audit failure
- Reduce your overall threat risk by increasing visibility to attack surface and potential compromises
- Streamline governance processes, and build compliance controls directly into your IT processes
- Develop trust with your internal stakeholders, customers, and prospects with reliable proof of compliance for those who require it
- Differentiate yourself in today's competitive market with proven security compliance

"Because of the duration of retention that we get with Alert Logic, not only are we able to use that as part of our security apparatus, but it also forms part of our compliance solution because we are able to assert that we can store logs for as long as needed by regulators and auditors."

Cheng Zhou, Director of Site Reliability Engineering, Iodine Software

Alert Logic MDR Solutions — Compliance Mapping

OFFERINGS	PCI DSS 3.2	HIPAA & HITECH	SOC 2 (TSP 100)
Fortra's Alert Logic MDR Essentials **Vulnerability & Asset Visibility** • Asset Discovery • Vulnerability Scanning • Cloud Configuration Checks • Threat Risk Index • Compliance Scanning & Reporting	6.1 — Identify vulnerabilities 11.2 — Perform network vulnerability scans by an ASV (includes 11.2.1, 11.2.2, and 11.2.3)	164.308 (a)(1) — Security Management Process 164.308 (a)(1)(i)(A) – Risk Analysis	CC 3.2 — Risk Identification CC 6.6 — External Threats CC 6.8 — Unauthorized and Malicious Code Protection CC 7.1 — Vulnerability Management

Alert Logic MDR Solutions — Compliance Mapping (continued)

OFFERINGS	PCI DSS 3.2	HIPAA & HITECH	SOC 2 (TSP 100)
Fortra's Alert Logic MDR Professional (includes Essentials) **24/7 Managed Threat Detection & Incident Management** • Incident Monitoring & Threat Management • Security Analytics & Threat Intelligence • Log Collection, Search & Monitoring • Intrusion Detection • Endpoint Detection • Cloud Security Service Integrations • User Behavior Monitoring • Anti-Virus Integration • Real-Time Reporting	10.1 — Implement audit trails 10.2 — Automated audit trails 10.3 — Capture audit trails 10.5 — Secure logs 10.5.5 — Change detection to ensure integrity for log files 10.6 — Review logs 10.7 — Maintain logs online 10.7 — Retain audit trail 10.8.1 — Respond to failures of critical security controls 11.4 — Use intrusion detection and/or intrusion prevention techniques 11.5 — Change detection to ensure integrity for critical system files, configuration files, or content files 12.10.1 — Implement an incident response plan	164.308 (a)(1)(ii)(B) – Risk Management 164.308 (a)(1)(ii)(D) — Information System Activity 164.308 (a)(4)(i) — Information Access Management 164.308 (a)(5)(ii)(B) — Protection from Malicious Software 164.308 (a)(5)(ii)(C) — Login Monitoring 164.308 (a)(6)(ii) — Response & Reporting 164.312 (a) — Access Control 164.312 (b) — Audit Controls 164.312 (c)(1)(2) — Protect from improper alteration or destruction and confirm integrity	CC 6.2 — User Registration CC 6.3 — Access Modification CC 7.2 — Security Event and Anomaly Detection CC 7.3 — Incident Detection and Response
Fortra's Alert Logic MDR Enterprise (includes Professional) **Designated Security Expert** • Continuous Threat Hunting • Proactive Tuning & Sensor Optimization • Weekly Security Review			CC 7.4 — Incident Containment and Remediation

$5.7 million is the average cost of a breach of organizations with high levels of compliance failures.

Cost of a Breach Report 2022

Alert Logic MDR Solutions — Compliance Mapping (continued)

OFFERINGS	GDPR	SOX 404
Fortra's Alert Logic MDR Essentials **Vulnerability & Asset Visibility** • Asset Discovery • Vulnerability Scanning • Cloud Configuration Checks • Threat Risk Index • Compliance Scanning & Reporting	Article 24 — Responsibility of the controller Article 25 — Data protection by design and by default Article 32 — Security of processing Article 35 — Data protection impact assessment	DS 5.9 — Malicious Software Prevention, Detection and Correction
Fortra's Alert Logic MDR Professional (includes Essentials) **24/7 Managed Threat Detection & Incident Management** • Incident Monitoring & Threat Management • Security Analytics & Threat Intelligence • Log Collection, Search & Monitoring • Intrusion Detection • Endpoint Detection • Cloud Security Service Integrations • User Behavior Monitoring • Anti-Virus Integration • Real-Time Reporting	Article 34 — Communication of a personal data breach	DS 5.5 — Security Testing, Surveillance and Monitoring DS 5.6 — Security Incident Definition DS 13.3 — IT Infrastructure Monitoring
Fortra's Alert Logic MDR Enterprise (includes Professional) **Designated Security Expert** • Continuous Threat Hunting • Proactive Tuning & Sensor Optimization • Weekly Security Review		BAI03.03 — Develop solution components

Alert Logic MDR Solutions — Compliance Mapping (continued)

OFFERINGS	ISO 27001/27002	NIST 800-171	NIST 800-53
Fortra's Alert Logic MDR Essentials **Vulnerability & Asset Visibility** • Asset Discovery • Vulnerability Scanning • Cloud Configuration Checks • Threat Risk Index • Compliance Scanning & Reporting	8.1 — Responsibility for assets 12.6 — Technical vulnerability management	3.1 — Access Control 3.3 — Audit and Accountability 3.4 — Configuration Management 3.11 — Risk Assessment 3.12 — Security Assessment 3.13 — System and Communications Protection 3.14 — System and Information Integrity	RA-3 Risk Assessment RA-5 Vulnerability Scanning
Fortra's Alert Logic MDR Professional (includes Essentials) **24/7 Managed Threat Detection & Incident Management** • Incident Monitoring & Threat Management • Security Analytics & Threat Intelligence • Log Collection, Search & Monitoring • Intrusion Detection • Endpoint Detection • Cloud Security Service Integrations • User Behavior Monitoring • Anti-Virus Integration • Real-Time Reporting	12.2 — Protection from malware 12.4 — Logging and Monitoring 16.1 — Management of information security incidents and improvements	3.5 - Identification and Authentication 3.6 — Incident Response	CA-2 Security Assessments CA-3 Information System Connections CA-7 Continuous Monitoring IR-5 Incident Monitoring IR-6 Incident Reporting IR-7 Incident Response Assistance SC-7 Boundary Protection SI-3 Intrusion Detection Tools and Techniques SI-4 The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system SI-5 Security Alerts and Advisories SI-7 Software and Information Integrity

Alert Logic MDR Solutions — Compliance Mapping (continued)

OFFERINGS	ISO 27001/27002	NIST 800-171	NIST 800-53
Fortra's Alert Logic MDR Enterprise (includes Professional) **Designated Security Expert** • Continuous Threat Hunting • Proactive Tuning & Sensor Optimization • Weekly Security Review	14.1 — Security requirements of information systems		

bcs The Chartered Institute for IT

"Deploying Alert Logic assisted the improvement of BCS statements of compliance to ourselves and prospective customers, including any GDPR questionnaires we receive."

Dale Titcombe, Head of IT, BCS

Alert Logic is a PCI Security Standards Council Approved Scanning Vendor (ASV) and 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 2, Type 2 Audit, ISO 27001-2013, and ISO/IEC 27701:2019 certification for UK operations.

For more information, please visit **AlertLogic.com**

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.